

hexagon:2610.00198v1

# Infinitely Many Elliptic Curves of Exact Ranks Five, Six, and Seven

P. M. Aronow

Patrick Lopatto

#### AUTHORS' NOTE

With the exception of this note, the entire document is machine-written. We have carefully supervised its preparation to ensure that the proofs are readable and that previous literature is appropriately cited. We are releasing this manuscript on Hexagon to disseminate the result as quickly as possible because it may be of interest to the mathematical community. We welcome suggestions concerning mathematical corrections, omitted citations, and attribution of ideas.

P. L. was partially supported by NSF grant DMS-2450004.

#### ABSTRACT

We prove that for each  $r \in \{5, 6, 7\}$ , there exist infinitely many elliptic curves over  $\mathbb{Q}$ , pairwise nonisomorphic over  $\overline{\mathbb{Q}}$ , whose Mordell–Weil rank over  $\mathbb{Q}$  is exactly  $r$ . Zywinia recently proved the analogous statement for  $0 \leq r \leq 4$  over every number field, and our proof follows his strategy. For each  $r$ , we give an explicit pair of 2-isogenous elliptic curves whose discriminants are, up to constants, products of powers of twelve binary linear forms in two integer parameters. The families are obtained from Zywinia’s curves of rank four, or from a related pair of curves, by base change along a conic. Explicit rational points give lower bounds for the images of the two descent maps. We specialize at parameters in a fixed congruence class at which the twelve linear forms, divided by fixed constants, take prime values. There, necessary local conditions in the descent become linear equations over  $\mathbb{F}_2$ , and their solution spaces have the same dimensions as the lower bounds. The coefficients of these equations are determined by the congruence class up to a single sign, and both values of this sign give the same bound. The Green–Tao–Ziegler theorem on linear equations in primes then gives infinitely many such specializations, with infinitely many  $j$ -invariants.

# Contents

|        |                                                  |    |
|--------|--------------------------------------------------|----|
| 1      | Introduction                                     | 1  |
| 1.1    | Main result . . . . .                            | 1  |
| 1.2    | Background . . . . .                             | 2  |
| 1.3    | Exact ranks . . . . .                            | 3  |
| 1.4    | The method and its sources . . . . .             | 4  |
| 1.5    | Computer verification . . . . .                  | 8  |
| 1.6    | Organization and notation . . . . .              | 9  |
| 2      | Overview of the proof                            | 10 |
| 2.1    | The shape of the families . . . . .              | 10 |
| 2.2    | Descent and the lower bound . . . . .            | 11 |
| 2.3    | Upper bounds from local conditions . . . . .     | 12 |
| 2.4    | Reciprocity and the free sign . . . . .          | 14 |
| 2.5    | An example: the rank-six family . . . . .        | 15 |
| 2.6    | Infinitely many prime specializations . . . . .  | 18 |
| 2.7    | Where the families come from . . . . .           | 19 |
| PART I | Descent and prime values                         | 20 |
| 3      | Descent by a rational 2-isogeny                  | 21 |
| 3.1    | Valuations and squareclasses . . . . .           | 21 |
| 3.2    | Descent maps and the rank . . . . .              | 23 |
| 3.3    | Support and local images . . . . .               | 27 |
| 3.4    | Local conditions as linear equations . . . . .   | 29 |
| 4      | Families with twelve linear factors              | 32 |
| 4.1    | Twelve-form data . . . . .                       | 32 |
| 4.2    | Prime specializations . . . . .                  | 36 |
| 4.3    | Rows at the moving primes . . . . .              | 38 |
| 4.4    | Reciprocity and the sign $\epsilon$ . . . . .    | 39 |
| 4.5    | The rank criterion . . . . .                     | 42 |
| 5      | Linear equations in primes                       | 45 |
| 5.1    | The theorem of Green, Tao, and Ziegler . . . . . | 46 |
| 5.2    | Distinct prime values . . . . .                  | 49 |

|         |                                                        |     |
|---------|--------------------------------------------------------|-----|
| 5.3     | Local factors in a congruence class . . . . .          | 50  |
| 5.4     | Prime specializations of a twelve-form datum . . . . . | 51  |
| PART II | The three families                                     | 54  |
| 6       | The rank-five family                                   | 55  |
| 6.1     | The datum . . . . .                                    | 55  |
| 6.2     | Rational points and the lower bound . . . . .          | 58  |
| 6.3     | The congruence class and the real cone . . . . .       | 61  |
| 6.4     | Local conditions at the fixed places . . . . .         | 63  |
| 6.5     | Characters at the moving primes . . . . .              | 68  |
| 6.6     | The matrices and the upper bound . . . . .             | 71  |
| 6.7     | Exact rank and infinitude . . . . .                    | 74  |
| 6.8     | Five independent points on $E$ . . . . .               | 76  |
| 7       | The rank-six family                                    | 78  |
| 7.1     | The datum . . . . .                                    | 78  |
| 7.2     | Rational points and the lower bound . . . . .          | 81  |
| 7.3     | The congruence class and the real cone . . . . .       | 83  |
| 7.4     | Local conditions at the fixed places . . . . .         | 85  |
| 7.5     | Characters at the moving primes . . . . .              | 89  |
| 7.6     | The matrices and the upper bound . . . . .             | 93  |
| 7.7     | Exact rank and infinitude . . . . .                    | 96  |
| 8       | The rank-seven family                                  | 98  |
| 8.1     | The datum . . . . .                                    | 99  |
| 8.2     | Rational points and the lower bound . . . . .          | 101 |
| 8.3     | The congruence class and the real cone . . . . .       | 105 |
| 8.4     | Local conditions at the fixed places . . . . .         | 108 |
| 8.5     | Characters at the moving primes . . . . .              | 112 |
| 8.6     | The matrices and the upper bound . . . . .             | 116 |
| 8.7     | Exact rank and infinitude . . . . .                    | 120 |
| 9       | Proof of the main theorem                              | 122 |
| A       | Computer verification                                  | 124 |
| A.1     | Running the programs . . . . .                         | 124 |
| A.2     | Conventions . . . . .                                  | 125 |
| A.3     | What the programs check . . . . .                      | 126 |
| A.4     | What the programs do not check . . . . .               | 129 |
| A.5     | The row codes . . . . .                                | 130 |
| B       | Origin of the three families                           | 133 |
| B.1     | The rank-five family . . . . .                         | 133 |

|     |                                 |     |
|-----|---------------------------------|-----|
| B.2 | The rank-six family . . . . .   | 136 |
| B.3 | The rank-seven family . . . . . | 138 |
|     | References                      | 142 |

# Introduction

## 1.1 Main result

Let  $E$  be an elliptic curve over  $\mathbb{Q}$ . The Mordell–Weil theorem states that the group  $E(\mathbb{Q})$  of rational points of  $E$  is finitely generated [31, 50]; see also [43, Theorem VIII.6.7]. The rank of this group is called the rank of  $E$ , and we denote it by  $\text{rank } E(\mathbb{Q})$ . The rank is a basic invariant of  $E$ , but it remains poorly understood. In particular, little is known about which integers occur as the rank of infinitely many elliptic curves over  $\mathbb{Q}$ . Here we count curves up to isomorphism over  $\overline{\mathbb{Q}}$ , so that the twists of a single curve are counted only once.

In this article, we establish that the integers five, six, and seven occur in this way.

**Theorem 1.1.** *For each  $r \in \{5, 6, 7\}$ , there exist infinitely many elliptic curves  $E$  over  $\mathbb{Q}$ , pairwise nonisomorphic over  $\overline{\mathbb{Q}}$ , such that  $\text{rank } E(\mathbb{Q}) = r$ .*

Two elliptic curves over  $\mathbb{Q}$  are isomorphic over  $\overline{\mathbb{Q}}$  if and only if they have the same  $j$ -invariant [43, Proposition III.1.4(b)]. Thus Theorem 1.1 states that for each  $r \in \{5, 6, 7\}$ , infinitely many distinct  $j$ -invariants occur among the elliptic curves over  $\mathbb{Q}$  of rank  $r$ . In particular, these curves are not all twists of finitely many curves.

Each case of Theorem 1.1 comes from an explicit family. For each  $r$ , we fix twelve binary linear forms  $L_i = a_iM + b_iN$  ( $0 \leq i \leq 11$ ) with integer coefficients, we set

$$F = L_0L_1L_2L_3, \quad H = L_4L_5L_6L_7, \quad J = L_8L_9L_{10}L_{11},$$

and we fix nonzero integers  $A, B$ , and  $C$  such that  $A^2F + 4BH = CJ$  identically in  $M$  and  $N$ . For integers  $M$  and  $N$  with  $F(M, N)H(M, N)J(M, N) \neq 0$ , we consider the elliptic curves

$$E_{M,N}: y^2 = x^3 + AFx^2 - BFHx, \quad E'_{M,N}: y^2 = x^3 - 2AFx^2 + CFJx, \quad (1.1)$$

which are related by an isogeny of degree two whose kernel is generated by the point  $(0, 0)$ . The identity  $A^2F + 4BH = CJ$  states that the discriminant of the quadratic polynomial  $x^2 + AFx - BFH$  equals  $CFJ$ . The discriminant of  $E_{M,N}$  is then  $16B^2CF^3H^2J$  (Lemma 4.2), which is a constant times a product of powers of the twelve linear forms.

The family also comes with positive integers  $c_0, \dots, c_{11}$ , a modulus  $W$ , a residue class  $(M_0, N_0)$  modulo  $W$ , and an open cone  $\mathcal{K}_r \subset \mathbb{R}^2$ . We prove that if  $(M, N) \equiv (M_0, N_0)$

(mod  $W$ ),  $(M, N) \in \mathcal{K}_r$ , and the twelve numbers  $p_i = L_i(M, N)/c_i$  are distinct primes outside a fixed finite set, then  $\text{rank } E_{M,N}(\mathbb{Q}) = r$ ; see Theorems 6.7, 7.8, and 8.9. Using the Green–Tao–Ziegler theorem on linear equations in primes [16–18], we find infinitely many such pairs  $(M, N)$ , with infinitely many values of  $M/N$ . Since the  $j$ -invariant of  $E_{M,N}$  takes each value for at most twelve values of  $M/N$  (Lemma 4.3), these curves have infinitely many  $j$ -invariants. The main data of the three families are listed in Table 1.1.

| $r$ | $A$   | $B$   | $C$   | $(d_E, d_{E'})$ | $W$          | Section |
|-----|-------|-------|-------|-----------------|--------------|---------|
| 5   | 1500  | 2700  | 57600 | (3, 4)          | 19984345920  | 6       |
| 6   | 70    | 784   | 1764  | (4, 4)          | 780373440    | 7       |
| 7   | 91205 | 33124 | 9     | (5, 4)          | 308403583488 | 8       |

Table 1.1. The three families. The integers  $A$ ,  $B$ , and  $C$  satisfy  $A^2F + 4BH = CJ$ . The numbers  $d_E$  and  $d_{E'}$  are the dimensions of the images of the two descent maps at every specialization that we use, so that  $\text{rank } E_{M,N}(\mathbb{Q}) = d_E + d_{E'} - 2 = r$ , and  $W$  is the modulus of the congruence class.

## 1.2 Background

It is not known whether the ranks of elliptic curves over  $\mathbb{Q}$  are bounded; see [33, §3] for the history of this question. Earlier, it was often expected that they are unbounded. In [33], Park, Poonen, Voight, and Wood proposed a heuristic which predicts the opposite: for each  $0 \leq r \leq 20$ , infinitely many elliptic curves over  $\mathbb{Q}$  have rank  $r$ , and only finitely many have rank greater than 21. The ranks in Theorem 1.1 lie in the range where this heuristic predicts infinitely many curves.

Curves of large rank are usually found among the specializations of an elliptic curve over  $\mathbb{Q}(t)$  with many independent sections. Mestre constructed elliptic curves over  $\mathbb{Q}(t)$  of rank at least 12 [30]. Elkies announced constructions of higher rank in his 2007 lectures [13] and gave explicit formulas and proofs in [14, Theorems 1–3]: an elliptic K3 surface over  $\mathbb{Q}(t)$  of rank 17, quadratic base changes of this surface with rank at least 18, and a base change over a curve of genus one with rank at least 19, which has infinitely many rational fibers of rank at least 19. A specialization of the rank-17 surface is a curve over  $\mathbb{Q}$  with at least 28 independent rational points [14, Theorem 2].

For a nonisotrivial elliptic curve over  $\mathbb{Q}(t)$ , Silverman’s specialization theorem [42, Theorem C, p. 208], also stated in [43, Theorem C.20.3], implies that the specialization map on sections is injective at all but finitely many rational values of  $t$ . Hence all but finitely many rational fibers have rank at least the rank over  $\mathbb{Q}(t)$ . Specialization yields only lower bounds. For example, Dujella and Peral proved in [10, §3] that infinitely many curves over  $\mathbb{Q}$  induced by rational Diophantine triples have rank at least seven, and in [11, §4] they constructed an elliptic curve over  $\mathbb{Q}(u)$  with torsion subgroup  $\mathbb{Z}/4\mathbb{Z}$  and

rank exactly six. The rank of a fiber may exceed the generic rank, and to determine it exactly one needs an upper bound as well, which in practice comes from descent. As Zywinia remarks in [55, §1], even with an elliptic curve of rank 18 over  $\mathbb{Q}(t)$ , it is unclear how to find a fixed  $r \geq 18$  such that infinitely many of its fibers have rank exactly  $r$ .

### 1.3 Exact ranks

For ranks zero and one, infinitely many curves over  $\mathbb{Q}$  of exactly that rank, pairwise nonisomorphic over  $\overline{\mathbb{Q}}$ , have been known for some time. Mazur and Rubin proved the rank-zero case over every number field [29, Corollary 1.11 and proof of Lemma 5.4]. Over  $\mathbb{Q}$ , the rank-one case follows, for example, from the theorem of Bhargava and Skinner that a positive proportion of elliptic curves over  $\mathbb{Q}$  have rank one [2].

An earlier use of prime values and 2-descent to preserve a generic rank is Zywinia's nonisotrivial rank-zero surface with infinitely many rank-zero fibers [53, Theorem 1.2].

In [52], Zywinia proved the corresponding statement for rank two.<sup>1</sup> His curves are  $y^2 = x^3 - 5(m + 16n^2)x^2 + 4(m + 16n^2)(m + 25n^2)x$ , where  $m$ ,  $m + 16n^2$ , and  $m + 25n^2$  are primes congruent to 11 modulo 24. He bounds the rank from above by descent through the rational 2-isogeny, with local computations at 2 and at the three primes, and he obtains infinitely many such triples of primes from the theorem of Tao and Ziegler on polynomial progressions in the primes [47, Theorem 1.3] (see also [48]). The rank-one case over every number field was proved independently by Koymans and Pagano [26] and by Zywinia [54]. Savoie constructed infinitely many curves of rank two over  $\mathbb{Q}(i)$ , all with  $j$ -invariant 1728 [37].

In [55, Theorem 1.1], Zywinia proved that for every number field  $K$  and every  $0 \leq r \leq 4$ , there exist infinitely many elliptic curves over  $K$  of rank  $r$ , pairwise nonisomorphic over  $\overline{K}$ . For each  $r$ , he uses an explicit nonisotrivial elliptic curve of rank  $r$  over  $K(T)$  with a point of order two, and he shows that infinitely many of its specializations have rank  $r$ ; we describe his method in Section 1.4. Our proof of Theorem 1.1 follows his strategy. Over  $\mathbb{Q}$ , Theorem 1.1 extends the range  $0 \leq r \leq 4$  of [55, Theorem 1.1] to  $r \in \{5, 6, 7\}$ . We do not consider other number fields.

Two recent results are close to Theorem 1.1. In [38, Theorem 1.1], Savoie proved that for each  $r \in \{4, 6\}$ , there exist infinitely many elliptic curves over  $\mathbb{Q}(i)$  of rank exactly  $r$ , pairwise nonisomorphic over  $\mathbb{Q}(i)$ , not obtained by base change from  $\mathbb{Q}$ , and all with  $j$ -invariant 1728. His curves are quartic twists  $y^2 = x^3 + bx$ . Their points come from factorizations  $b = ef$  with  $e + f$  a square, the upper bounds come from descent through the endomorphism  $1 + i$ , and Kai's theorem [23] on prime values of linear forms over

---

<sup>1</sup>Under the parity conjecture, earlier constructions of infinitely many curves over  $\mathbb{Q}$  of rank exactly two were given by Byeon and Jeong [4, Theorem 1.1] and by Jeong [22, Theorem 1.1]. These are twist families with constant  $j$ -invariant 0 or 1728.

number fields supplies the specializations. Since the  $j$ -invariant is constant, all of these curves are isomorphic over  $\overline{\mathbb{Q}}$ . Compared with Theorem 1.1, the ground field and the notion of infinitude differ: our curves are defined over  $\mathbb{Q}$  and have infinitely many  $j$ -invariants. Both works use explicit points whose classes have prescribed prime supports, and both express the local conditions in the descent through quadratic residue symbols. Savoie uses the graph and matrix descriptions of Kling and Savoie [25, Theorem 5.2 of the cited preprint]. In his rank-six family, he reduces the pairwise symbols to one undetermined sign and proves that both resulting Laplacians have the same kernel [38, Lemmas 4.1–4.2]. In [28, Proposition 6.1], Lu constructed five independent sections over the function field of a curve of genus one with infinitely many rational points, and obtained infinitely many elliptic curves over  $\mathbb{Q}$ , pairwise nonisomorphic over  $\overline{\mathbb{Q}}$ , of rank at least five. As Lu notes, these results give lower bounds and do not determine the ranks.

## 1.4 The method and its sources

We now describe the ingredients of the proof of Theorem 1.1 and their origins. Section 2 gives a more detailed overview.

**Descent by a rational 2-isogeny.** For a pair  $(M, N)$  with  $FHJ \neq 0$ , let  $\phi: E_{M,N} \rightarrow E'_{M,N}$  be the isogeny between the curves in (1.1), and let  $\hat{\phi}$  be its dual. The descent map  $\delta_E$  sends the identity of  $E_{M,N}(\mathbb{Q})$  to the trivial class in  $\mathbb{Q}^\times / \mathbb{Q}^{\times 2}$ , the point  $(0, 0)$  to the class of  $-BFH$ , and every other point  $(x, y)$  to the class of  $x$ . It is a homomorphism with kernel  $\hat{\phi}(E'_{M,N}(\mathbb{Q}))$ . The map  $\delta_{E'}$  on  $E'_{M,N}(\mathbb{Q})$  is defined in the same way and has kernel  $\phi(E_{M,N}(\mathbb{Q}))$ . If  $d_E$  and  $d_{E'}$  denote the dimensions over  $\mathbb{F}_2$  of the images of  $\delta_E$  and  $\delta_{E'}$ , then  $\text{rank } E_{M,N}(\mathbb{Q}) = d_E + d_{E'} - 2$ . Descent is the method by which Mordell and Weil proved finite generation [31, 50]. The form of it that we use, for a rational 2-isogeny, is classical. We follow Tate’s 1961 Haverford lectures as expanded in [44, §§3.4–3.6], together with [43, Example X.4.8 and Proposition X.4.9] and [5, §14]. The rank formula in the form above is [55, Lemma 3.1]; see also [44, §3.6].

We bound  $d_E$  and  $d_{E'}$  from below by the classes of explicit rational points. For the upper bounds, we use that for every place  $v$  of  $\mathbb{Q}$ , the image of  $\delta_E(E_{M,N}(\mathbb{Q}))$  in  $\mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2}$  lies in the image of the local descent map on  $E_{M,N}(\mathbb{Q}_v)$ , and similarly for  $E'_{M,N}$ . These are the local conditions that define the Selmer groups of  $\phi$  and  $\hat{\phi}$  [43, §X.4]. We impose only the conditions that we need, at finitely many places, and show that the resulting upper bounds agree with the lower bounds.

**Local conditions as linear equations.** At the specializations we use, every class in the image of  $\delta_E$  is represented by a product of  $-1$ , a few fixed primes, and some of the primes  $p_i$  that divide  $BFH$  (Lemma 3.6). Once we fix these generators, we may regard

a class as a vector over  $\mathbb{F}_2$ , and the local condition at a prime  $p_i$  is a linear equation in this vector whose coefficients are Legendre symbols modulo  $p_i$ . The local conditions at the fixed places are linear equations as well. Such matrices occur in Rédei's arithmetic treatment [34, §5 and p. 59, footnote 11] of the Rédei–Reichardt formula for the 4-rank of the narrow class group of a quadratic field [35]. For elliptic curves, Monsky gave a binary-matrix description of full 2-descent for the congruent-number curves in his appendix to [20, pp. 365–369, especially p. 366]. Feng used quadratic-residue graphs and their binary Laplacians in descent by a 2-isogeny [15, §§2–3]. Xiong and Zaharescu treated the Selmer groups of a 2-isogeny of these curves and of its dual in a similar way [51, §3.1, Theorem 3], and Kane and Klagsbrun constructed the corresponding matrices for a rational 2-isogeny and its dual in families of quadratic twists [24, §4]. In these congruent-number and quadratic-twist treatments, the primes are the prime factors of a twisting parameter, and the Legendre symbols among them vary with the parameter. In our families, a congruence condition on  $(M, N)$  determines every entry of the matrices as a function of a single undetermined sign, which we discuss below.

**Prime values and descent.** To control the primes of bad reduction of  $E_{M,N}$ , we specialize at pairs  $(M, N)$  where the twelve linear forms take prime values, up to the fixed factors  $c_i$ . Prime values of polynomials have long been used for this purpose in the fibration method. Colliot-Thélène and Sansuc used Schinzel's Hypothesis H [39], which is a conjecture, to study the Hasse principle and weak approximation on fibrations [7]; see also [8]. Swinnerton-Dyer [46] introduced this approach for certain genus-one pencils over  $\mathbb{Q}$  whose Jacobians have full rational 2-torsion. Colliot-Thélène, Skorobogatov, and Swinnerton-Dyer [9, Introduction] developed it further for suitable pencils over number fields, choosing primes so as to control the 2-Selmer groups. These results assume Hypothesis H and the finiteness of the relevant Tate–Shafarevich groups. Bender and Swinnerton-Dyer [1, Theorems 1–2] extended this method to certain pencils of 2-coverings whose generic Jacobians have exactly one nonzero rational 2-torsion point. Colliot-Thélène [6, Theorems A–B and §1.4] recast their solubility criteria in terms of the vertical Brauer–Manin obstruction, using the Selmer groups of a 2-isogeny and its dual; these results retain the same conjectural assumptions. Skorobogatov and Swinnerton-Dyer [45] developed a version of this descent for certain Kummer surfaces which still assumes the finiteness of the relevant Tate–Shafarevich groups but does not require Hypothesis H. When the polynomials are linear forms in two variables, as they are for a fibration over the projective line whose degenerate fibers lie over rational points, the Green–Tao–Ziegler theorem can take the place of Hypothesis H. Browning, Matthiesen, and Skorobogatov used additive combinatorics together with descent over  $\mathbb{Q}$  to treat pencils of conics and quadrics with rational degenerate fibers [3, Theorems 1.1–1.2]. Harpaz, Skorobogatov, and Wittenberg adapted the fibration method over  $\mathbb{Q}$  using simultaneous linear prime values in [19], for suitable fibrations of this kind. Kai [23] extended the Green–Tao–

Ziegler theorem to prime elements of number fields. Koymans and Pagano combine four prime-valued linear forms, prescribed quadratic characters at fixed auxiliary primes, and Hilbert reciprocity to control a twist's Selmer group [26, §3, Theorems 3.3 and 3.5].

**Linear equations in primes.** Green and Tao [18] proved an asymptotic formula for the number of integer points in a convex region at which a system of affine-linear forms of finite complexity takes prime values, assuming two conjectures: the Möbius–nilsequences conjecture and the inverse conjecture for the Gowers norms. The first was proved by Green and Tao [16, Theorem 1.1], and the cases of the second that were not previously known were proved by Green, Tao, and Ziegler [17, Theorem 1.3], whose later corrections are recorded in the bibliography. We use this theorem for twelve affine-linear forms in two variables with pairwise nonproportional linear parts. Such a system has complexity at most ten by [18, Lemma 1.6], and Section 5 states the form of the theorem that we need. It produces prime values at points of a prescribed congruence class and cone, provided that there is no local obstruction, but it gives no control of the Legendre symbols among the resulting primes.

**Zywina's strategy.** In [55], Zywina starts from a nonisotrivial elliptic curve  $y^2 = x^3 + ax^2 + bx$  over  $K(T)$  whose discriminant is a product of linear factors over  $K$ , so that its bad fibers lie over finitely many points  $e \in K$ . Sections of this curve and of the 2-isogenous curve over  $K(T)$  bound the images of the descent maps from below at all but finitely many specializations. He chooses a finite set  $S$  of primes of  $K$  containing the denominators of the bad parameters, together with two auxiliary primes  $q_1, q_2$  outside  $S$ . Kai's theorem [23, Proposition 13.2] then provides  $S$ -integers  $m$  and  $n$  such that the elements  $m - en$  are pairwise nonassociate prime elements of the ring of  $S'$ -integers, where  $S' = S \cup \{q_1, q_2\}$ , and  $(m, n)$  satisfies prescribed local conditions; he specializes at  $t = m/n$  [55, Proposition 5.9]. Using local computations at these primes, auxiliary primes, global reciprocity, and the Selmer ratio of the isogeny, Zywina shows that the Selmer groups of the specialized isogenies are spanned by the classes of the sections. The rank of the specialization then equals the rank over  $K(T)$ .

The axiomatic form of this argument is [55, Theorem 4.1]. We write  $\mathcal{A}$  for the set of additive fibers, and  $\mathcal{M}$  (respectively  $\mathcal{M}'$ ) for the set of multiplicative fibers of type  $I_{2n}$  on the first curve and  $I_n$  on the second (respectively the reverse). Besides conditions on the bad fibers, Theorem 4.1 of [55] requires that the images of the two descent maps over  $K(T)$  have dimensions at least  $|\mathcal{A}| + |\mathcal{M}| - 1$  and  $|\mathcal{A}| + |\mathcal{M}'| - 1$ . These conditions force the rank over  $K(T)$  to equal  $2|\mathcal{A}| + |\mathcal{M}| + |\mathcal{M}'| - 4$ , which is the upper bound  $\deg \mathcal{N} - 4$  of Shioda [41, Corollary 2], where  $\mathcal{N}$  is the conductor of the elliptic surface. In characteristic zero, Shioda's stronger bound  $\text{rank } E(\bar{K}(T)) \leq \deg \mathcal{N} - 4 - 2p_g$  [41, Corollary 3, equation (1.13')] shows that equality in  $\deg \mathcal{N} - 4$  forces the geometric genus  $p_g$  to be zero; see also [55, §2]. Zywina's surfaces are rational elliptic surfaces with a

point of order two, whose rank is at most four by [32, Corollary 2.1]. For  $r = 4$ , he uses the pair

$$\begin{aligned} E_Z: y^2 &= x^3 - 70(T^2 - 25^2)x^2 + 2^4 7^2 (T^2 - 11^2)(T^2 - 25^2)x, \\ E'_Z: y^2 &= x^3 + 140(T^2 - 25^2)x^2 + 2^2 3^2 7^2 (T^2 - 25^2)(T^2 - 39^2)x \end{aligned} \quad (1.2)$$

of [55, §6.5], whose six bad fibers lie over  $T = \pm 11, \pm 25, \pm 39$ .

**Conic base change.** Our families arise by base change of degree two. For the rank-five family, we start from the curve  $E'_Z$  in (1.2), and for the rank-six family from  $E_Z$ . For the rank-seven family, we start from a related 2-isogenous pair of the same form, with bad fibers over  $T = \pm 1, \pm v, \pm w$  for certain rational numbers  $v$  and  $w$ . In each case, the base change is along a conic over which an additional point becomes rational; Section 2.7 explains how it produces the twelve forms  $L_i$  and the identity  $A^2 F + 4BH = CJ$ , and Appendix B gives the details. Making a quadratic section rational by a base change of degree two is a classical way to raise the rank of an elliptic surface; see Mestre's conic construction [30, §2.2] and Elkies's discussion [13, Lecture III, p. 2003]. Dujella, Kazalicki, and Peral describe the corresponding divisor and square conditions for models  $y^2 = x^3 + ax^2 + bx$  in [12, §1.1]. Salgado gives general results on new independent sections from moving multisections [36, Corollary 4.3], and Loughran and Salgado develop this method using conic bundles [27, §1.2 and Theorem 2.4]. In [11, §4], Dujella and Peral raise the rank of an elliptic curve over  $\mathbb{Q}(u)$  from four to six by imposing two conditions, each of which defines a conic. Such a base change need not raise the rank. For the rank-seven family, the point supplied directly by the conic has a square  $x$ -coordinate, so its class under  $\delta_E$  is trivial, and the additional class comes from another point (Appendix B). For this reason, the proofs do not use the construction. We verify the new classes directly at every specialization, and Appendix B only explains where the families come from.

**What is new.** The proof of Theorem 1.1 differs from the maximal-rank argument of [55] in the following ways.

- *Three families.* These are the families of Table 1.1, with their points, congruence classes, and cones.
- *Explicit matrices instead of the criterion of maximal rank.* After the base change, each family has twelve bad fibers: four additive fibers at the zeros of  $F$ , and eight multiplicative fibers at the zeros of  $H$  and  $J$ , which form the sets  $\mathcal{M}$  and  $\mathcal{M}'$  respectively. The number  $2|\mathcal{A}| + |\mathcal{M}| + |\mathcal{M}'| - 4$  is then 12, while the ranks we prove are 5, 6, and 7. Since infinitely many fibers of each family have rank  $r \leq 7$ , Silverman's theorem [42, Theorem C, p. 208] implies that the rank of the family over  $\mathbb{Q}(M/N)$  is at most  $r$ . Thus the families do not have maximal rank, and [55, Theorem 4.1] does not apply. (The fiber types and K3 classification of these elliptic surfaces are proved in Remark 4.5, using [40, 49].) Instead, for a fixed congruence class and cone, we write the local conditions at 2, at 3, at one or two further fixed primes, at the real place, and

at the twelve primes  $p_i$  as the rows of explicit matrices over  $\mathbb{F}_2$  with twelve or thirteen columns. Their ranks show that the images of  $\delta_E$  and  $\delta_{E'}$  are spanned by the classes of explicit points. We display the matrices with labeled rows and columns, explain each entry through tables of residues, and give rank certificates that can be checked by hand.

- *One free sign.* The congruence class determines every entry of the matrices as a function of the sign  $\varepsilon = (N/p_0)$ , which it does not determine. When  $\varepsilon$  changes sign, every row coming from one of the primes  $p_i$  changes by the same vector, and both values of  $\varepsilon$  give the same upper bound (Lemma 4.17). The analytic input is therefore used only to produce prime values in a congruence class and a cone, and we need no condition on quadratic residue symbols among the growing primes. The related one-sign reduction and common-kernel mechanism over  $\mathbb{Q}(i)$  in [38, Lemmas 4.1–4.2] is a precedent for this step.
- *The ground field.* The proof takes place over  $\mathbb{Q}$  and uses the Green–Tao–Ziegler theorem directly, instead of Kai’s extension to number fields.

The proof of Theorem 1.1 is unconditional. It does not use the finiteness of Tate–Shafarevich groups, the parity conjecture, analytic ranks, or a specialization theorem: both the upper and the lower bounds are proved directly at each prime specialization.

## 1.5 Computer verification

In Part II, we use finite arithmetic of the following kinds:

- the identity  $A^2F + 4BH = CJ$ , and the identities stating that the listed points lie on the curves, which are homogeneous polynomial identities of degree at most twelve in  $(M, N)$ ;
- the values of  $W$ ,  $M_0$ , and  $N_0$  given by the Chinese remainder theorem;
- the factorizations of the coefficients  $b_i$  and of the determinants  $a_i b_j - a_j b_i$ ;
- the residues of the primes  $p_i$  modulo small primes, and the Legendre symbols that they determine;
- the ranks of matrices over  $\mathbb{F}_2$  with twelve or thirteen columns.

We state each of these claims precisely, so that a reader can check it by hand or with any computer algebra system. For instance, a homogeneous identity of degree at most twelve in  $(M, N)$  holds if it holds at  $N = 1$  for thirteen distinct values of  $M$ . For the ranks, we display the matrices and give certificates in the form of triangular minors. Appendix A describes the supplied scripts, which use exact arithmetic, and lists the claims that they check. The uniform arguments, which apply to every pair  $(M, N)$  in an infinite progression, and the analytic input are proved in the text and are not checked by computer.

## 1.6 Organization and notation

Section 2 gives an overview of the proof, including a dimension count for one of the families. Part I develops the general tools. Section 3 recalls descent by a rational 2-isogeny over  $\mathbb{Q}$  and over its completions, proves the rank formula (Lemma 3.5) and the local lemmas that we need, and shows how local conditions become rows of a matrix over  $\mathbb{F}_2$  (Lemma 3.10). Section 4 introduces twelve-form data (Definition 4.1) and their prime specializations, computes the local images at the twelve primes  $p_i$  and the Legendre symbols among them, and proves the rank criterion of Proposition 4.18. Section 5 states the Green–Tao–Ziegler theorem in the form that we use and proves Proposition 5.5, which gives infinitely many prime specializations in a congruence class and a cone. Part II treats the three families. Sections 6 to 8 prove Theorems 6.7, 7.8, and 8.9 by checking the hypotheses of Propositions 4.18 and 5.5, and Section 9 deduces Theorem 1.1. Appendix A describes the computer verification, and Appendix B explains how the three families were found.

Throughout, for a field  $K$  of characteristic zero, we write  $K^\times / K^{\times 2}$  for the group of squareclasses of  $K$ , which we regard as a vector space over  $\mathbb{F}_2$ , and  $[u]$  for the class of  $u \in K^\times$ . For a prime  $p$ , we write  $v_p$  for the  $p$ -adic valuation on  $\mathbb{Q}$  and on  $\mathbb{Q}_p$ , and we set  $\mathbb{Q}_\infty = \mathbb{R}$ . For an odd prime  $p$  and an integer  $z$  prime to  $p$ , we write  $(z/p)$  for the Legendre symbol. At a prime specialization, for  $0 \leq i \leq 11$  and an integer  $z$  prime to  $p_i$ , we define  $\lambda_i(z) \in \mathbb{F}_2$  by  $(z/p_i) = (-1)^{\lambda_i(z)}$ , so that  $\lambda_i(zz') = \lambda_i(z) + \lambda_i(z')$ . We write the free sign as  $\varepsilon = (N/p_0) = (-1)^\eta$  with  $\eta \in \mathbb{F}_2$ . The remaining notation, including the curves  $E_{\alpha,\beta}$ , the isogeny  $\phi$  and its dual  $\hat{\phi}$ , and the descent maps, is introduced in Sections 3 and 4.

## Overview of the proof

In this section, we explain how the proof of Theorem 1.1 works. We describe the steps for a general family of the form (1.1), in the order in which Part I carries them out, and in Section 2.5 we follow them through the rank-six family. Precise statements and complete proofs are given in Sections 3 to 8, and we point to them as we go. Nothing in this section is used later.

The proof has three parts. Fix one of the three families. First, we bound the dimensions  $d_E$  and  $d_{E'}$  of the images of the two descent maps from below by the classes of explicit rational points, at every pair  $(M, N)$  at which the twelve forms take prime values up to fixed factors. Second, we bound them from above by local conditions at finitely many places, provided that  $(M, N)$  also lies in a fixed congruence class and a fixed open cone. Most of the work lies in this step. Third, we use the Green–Tao–Ziegler theorem to produce infinitely many such pairs  $(M, N)$ , and we show that the resulting curves have infinitely many  $j$ -invariants.

### 2.1 The shape of the families

Recall the curves  $E_{M,N}$  and  $E'_{M,N}$  of (1.1). When  $(M, N)$  is fixed, we write  $E = E_{M,N}$  and  $E' = E'_{M,N}$ , and

$$\alpha = AF, \quad \beta = -BFH, \quad \alpha' = -2AF, \quad \beta' = CFJ$$

for their coefficients. Since  $\alpha^2 - 4\beta = F(A^2F + 4BH)$ , the identity  $A^2F + 4BH = CJ$  says exactly that  $\beta' = \alpha^2 - 4\beta$ , that is, that  $E'$  is the curve  $y^2 = x^3 - 2\alpha x^2 + (\alpha^2 - 4\beta)x$ , which is 2-isogenous to  $E$  (Lemma 4.2). Note that all four coefficients are constants times products of the forms  $L_i$ , and so is the discriminant  $16B^2CF^3H^2J$  of  $E$ . Every prime of bad reduction of  $E$  therefore divides  $2BC$  or one of the twelve values  $L_i(M, N)$ .

The twelve linear factors are what make the descent computable at infinitely many pairs  $(M, N)$ . Suppose that  $L_i(M, N) = c_i p_i$  for  $0 \leq i \leq 11$ , where the  $c_i$  are fixed positive integers and  $p_0, \dots, p_{11}$  are distinct primes outside a fixed finite set  $S$ . Such a pair is a prime specialization (Definition 4.6), and the  $p_i$  are its moving primes. At a prime specialization, each  $p_i$  divides exactly one of the twelve values, and only to the first power (Lemma 4.8). The moving primes grow with  $(M, N)$ , but their number and the way in which they divide the coefficients of the curves do not change. In the three families,  $c_i$  is

the largest divisor of  $L_i(M, N)$  composed of the primes 2 and 3, which is the same for all  $(M, N)$  in the congruence class that we choose below. In the rank-five and rank-six families, some cofactors must be larger than one. Indeed, the zero lines of the twelve forms modulo 2 are all three lines of  $\mathbb{F}_2^2$ , and modulo 3 they are all four lines of  $\mathbb{F}_3^2$ . It follows that for every pair  $(M, N)$ , at least one of the values  $L_i(M, N)$  is even, and at least one is divisible by 3.

The forms come in three groups of four, according to whether  $L_i$  divides  $F$ ,  $H$  or  $J$ . We write  $I_F = \{0, 1, 2, 3\}$ ,  $I_H = \{4, 5, 6, 7\}$  and  $I_J = \{8, 9, 10, 11\}$  for the corresponding sets of indices. At a prime specialization, a moving prime  $p_i$  with  $i \in I_F$  divides  $\alpha$ ,  $\beta$  and  $\beta'$ ; a moving prime with  $i \in I_H$  divides  $\beta$  but not  $\alpha$  or  $\beta'$ ; and a moving prime with  $i \in I_J$  divides  $\beta'$  but not  $\alpha$  or  $\beta$ . The eight moving primes that divide  $\beta$  have indices in  $G_E = I_F \cup I_H$ , and the eight that divide  $\beta'$  have indices in  $G_{E'} = I_F \cup I_J$ . As we explain in Section 2.3, the group of a moving prime decides the local condition that it imposes.

## 2.2 Descent and the lower bound

We use descent by the rational 2-isogeny  $\phi: E \rightarrow E'$  and its dual  $\hat{\phi}$ . Recall from the introduction that the descent map  $\delta_E$  sends a point  $(x, y)$  with  $x \neq 0$  to the class  $[x]$  in  $\mathbb{Q}^\times / \mathbb{Q}^{\times 2}$ , the point  $T = (0, 0)$  to  $[\beta]$ , and the identity to  $[1]$ . It is a homomorphism with kernel  $\hat{\phi}(E'(\mathbb{Q}))$ , and the map  $\delta_{E'}$  on  $E'(\mathbb{Q})$ , defined in the same way, has kernel  $\phi(E(\mathbb{Q}))$  (Proposition 3.4). Writing  $d_E$  and  $d_{E'}$  for the dimensions over  $\mathbb{F}_2$  of the images, we have

$$\text{rank } E_{M,N}(\mathbb{Q}) = d_E + d_{E'} - 2$$

by Lemma 3.5. The proof of Theorem 1.1 reduces to computing  $d_E$  and  $d_{E'}$  exactly, at every prime specialization in a suitable infinite set. For the rank-six family, for example, we must show that  $d_E = d_{E'} = 4$ .

We obtain the lower bounds from explicit points. Each family has a few points on  $E$  and on  $E'$  whose coordinates are polynomials in  $M$  and  $N$  with rational coefficients (Tables 6.3, 7.2, and 8.3). The  $x$ -coordinate of each point is a constant times a product of four of the forms  $L_i$ , and the condition that the point lies on the curve is an identity between binary quartic forms, which a reader can check by comparing five coefficients (for example, Lemma 7.1). At a prime specialization, the class of such a point is  $[g \prod_{j \in \mathcal{J}} p_j]$ , where  $g$  is a product of  $-1$  and primes of  $S$ , and  $\mathcal{J}$  is a set of four indices, which we call its moving support. The class  $[\beta]$  of  $T$  has the moving support  $G_E$ . Note that the exponent of  $p_j$  in a class is its  $p_j$ -adic valuation modulo 2, since the  $p_j$  are distinct primes outside  $S$ . To prove that the classes are independent, it suffices to order them so that each has a moving prime that occurs in none of the later ones (Lemma 3.12); then no nontrivial product of them is a square. Counting  $T$  and  $T'$ , we find  $k_E$  independent classes in the

image of  $\delta_E$  and  $k_{E'}$  in the image of  $\delta_{E'}$ , where

$$(k_E, k_{E'}) = (3, 4), \quad (4, 4), \quad (5, 4)$$

in the rank-five, rank-six and rank-seven families (Lemmas 6.2, 7.2, and 8.3). This implies that  $d_E \geq k_E$  and  $d_{E'} \geq k_{E'}$ .

### 2.3 Upper bounds from local conditions

For the upper bound, we must exclude every class that does not come from the points. Every class in  $\delta_E(E(\mathbb{Q}))$  is the class of a rational point. By Proposition 3.4, its image in  $\mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2}$  therefore lies in the image  $\delta_{E,v}(E(\mathbb{Q}_v))$  of the local descent map, for every place  $v$ . We use only finitely many of these conditions, and in order to make them the same for all  $(M, N)$  in an infinite set, we replace the local images at the fixed places by subgroups that contain them (see Remark 3.11 for how this compares with the Selmer group). It is not clear in advance that these weaker conditions suffice. In the three families they do, and they cut out exactly the span of the classes of the points.

To write the conditions as linear equations, we first fix finitely many classes that span the image. By Lemma 3.6, every class in  $\delta_E(E(\mathbb{Q}))$  is represented by a squarefree divisor of  $\beta$ , with a sign. At a prime specialization, the primes dividing  $\beta$  are the eight moving primes  $p_j$  with  $j \in G_E$  and some primes of  $S$ . We fix an ordered list  $\Gamma_E$  consisting of  $-1$  and of distinct primes of  $S$ , which contains every prime of  $S$  that divides  $\beta$ ; the list  $\Gamma_{E'}$  is chosen in the same way. Let  $\mathcal{B}_E = (\Gamma_E; p_j \ (j \in G_E))$ . By Lemma 4.8, the classes of the  $n_E = |\Gamma_E| + 8$  entries of  $\mathcal{B}_E$  are independent and span a subgroup that contains  $\delta_E(E(\mathbb{Q}))$ . We may then regard every class in  $\delta_E(E(\mathbb{Q}))$  as a vector  $\mathbf{w} \in \mathbb{F}_2^{n_E}$  of exponents, and each local condition becomes a linear equation in  $\mathbf{w}$ . Indeed, let  $U_v$  be a subgroup of  $\mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2}$  that contains the local image, and let  $f: \mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2} \rightarrow \mathbb{F}_2$  be a linear map that vanishes on  $U_v$ . Evaluating  $f$  at the entries of  $\mathcal{B}_E$  gives a row vector  $r$  with  $r \cdot \mathbf{w} = 0$  for every class  $\mathbf{w}$  in  $\delta_E(E(\mathbb{Q}))$  (Lemma 3.10). If  $\mathbf{M}_E$  is a matrix of such rows, we conclude that

$$d_E \leq n_E - \text{rank } \mathbf{M}_E.$$

When  $\text{rank } \mathbf{M}_E = n_E - k_E$ , this upper bound matches the lower bound of Section 2.2, and  $\delta_E(E(\mathbb{Q}))$  is the span of the classes of the points (Corollary 3.13). The same construction applies to  $E'$ , with  $\beta'$ ,  $G_{E'}$ , a list  $\Gamma_{E'}$  and the basis  $\mathcal{B}_{E'}$ .

We take rows at two kinds of places. At the moving primes, we determine the local images from the valuations of the coefficients alone (Lemmas 3.8 and 4.9). Writing  $p = p_i$ , we have the following.

| $i \in$ | $v_p(\alpha)$ | $v_p(\beta)$ | $v_p(\beta')$ | $\delta_{E,p}(E(\mathbb{Q}_p))$ | $\delta_{E',p}(E'(\mathbb{Q}_p))$ |
|---------|---------------|--------------|---------------|---------------------------------|-----------------------------------|
| $I_F$   | 1             | 1            | 1             | $\{[1], [\beta]\}$              | $\{[1], [\beta']\}$               |
| $I_H$   | 0             | 1            | 0             | not used                        | $\{[1]\}$                         |
| $I_J$   | 0             | 0            | 1             | $\{[1]\}$                       | not used                          |

At a prime  $p_i$  with  $i \in I_J$ , the condition on  $E$  says that every class in  $\delta_E(E(\mathbb{Q}))$  is a square in  $\mathbb{Q}_{p_i}$ . The entries of  $\mathcal{B}_E$  are units at  $p_i$ . The valuations are therefore even automatically, and the condition says that the Legendre symbol modulo  $p_i$  of the class is 1. In other words, the row has the entry  $\lambda_i(g)$  at each constant  $g \in \Gamma_E$  and the entry  $\lambda_i(p_j)$  at each moving prime  $p_j$ , where  $(z/p_i) = (-1)^{\lambda_i(z)}$ .

At a prime  $p_i$  with  $i \in I_F$ , a class lies in  $\{[1], [\beta]\}$  if and only if its Legendre symbol modulo  $p_i$ , after the factor  $p_i$  is removed, equals that of  $\beta/p_i$  when the class has odd valuation at  $p_i$ , and equals 1 otherwise. The row has the same entries as before, except at the column of  $p_i$  itself, where the entry is the character  $\lambda_i(\beta/p_i)$ . With  $\beta = \kappa_E \prod_{j \in G_E} p_j$ , where  $\kappa_E$  is a constant, we have  $\lambda_i(\beta/p_i) = \lambda_i(\kappa_E) + \sum_{j \in G_E \setminus \{i\}} \lambda_i(p_j)$ . For the curve  $E'$ , the roles of  $H$  and  $J$  are exchanged, since  $\alpha'^2 - 4\beta' = 16\beta$ . Altogether, each curve has eight moving rows: four at the primes  $p_i$  with  $i \in I_F$ , and four at the primes  $p_i$  with  $i \in I_J$  for  $E$ , or  $i \in I_H$  for  $E'$  (Definition 4.10 and Lemma 4.11).

We obtain the other rows at the fixed places: 2, 3, one or two further primes of  $\Gamma_E$  or  $\Gamma_{E'}$ , and the real place. Here we bound the local images by going through the points of  $E(\mathbb{Q}_v)$ : the identity, the point  $T$ , the other points of order two (Lemma 3.7), and the points with  $y \neq 0$ , sorted by the valuation of  $x$ . For most valuations of  $x$ , one term of the cubic  $x^3 + \alpha x^2 + \beta x$  has strictly smallest valuation and determines the valuation and the leading digits of the cubic (Lemma 3.1); in the remaining cases, the residues of the coefficients decide. The condition that the cubic is the square  $y^2$  (Lemma 3.2) then restricts the class of  $x$ . These arguments use only the relation  $\beta' = \alpha^2 - 4\beta$  and the valuations and residues of the coefficients at the fixed prime, modulo a small power of it. The congruence class of  $(M, N)$  fixes these residues, and the fixed-place lemmas (Lemmas 6.5, 7.5, and 8.6) state the resulting subgroups  $U_v$  at the finite fixed places, which are the same for every pair in the class.

At the real place, we use that all twelve forms are positive on the cone. We then have  $\alpha' < 0 < \beta'$ , and the cubic  $x^3 + \alpha'x^2 + \beta'x$  is negative for  $x < 0$ . Every point of  $E'(\mathbb{R})$  other than the identity has  $x > 0$  or is the point  $T'$ , whose class  $[\beta']$  is trivial. The local image is trivial, which gives the row that records the sign. On  $E$ , the point  $T$  has the negative class  $[\beta]$ , and the real place gives no condition. At the finite fixed places, the entry of a fixed row at the column of a moving prime  $p_j$  depends only on the residue of  $p_j$  modulo 8 or modulo the fixed prime, which the congruence class also fixes. In the real row, every moving prime is positive and therefore has entry 0.

## 2.4 Reciprocity and the free sign

We have seen that the fixed rows are the same at all prime specializations in the chosen congruence class and cone. However, the moving rows consist of Legendre symbols modulo the moving primes, and a priori these depend on  $(M, N)$ . There are two kinds of entries.

We first consider the entries  $\lambda_i(g)$  and  $\lambda_i(\kappa_\star)$ , for  $\star \in \{E, E'\}$ , which are characters of fixed integers. By quadratic reciprocity and its supplementary laws, such a character depends only on the residues of  $p_i$  modulo 8 and modulo the odd primes dividing the integer (Lemma 4.13). The modulus  $W$  of the congruence class is divisible by a power of 2 and by these odd primes, and the class fixes the residues of all the  $p_i$  modulo them (Tables 6.7, 7.6, and 8.8).

We now turn to the cross symbols  $\lambda_i(p_j)$ , with  $i \neq j$ , which are characters of one moving prime modulo another. The residue computations above do not evaluate them. The observation that makes them computable is that the moving primes are values of linear forms in the same two variables. Any three of these forms are linearly dependent, and reducing such a relation modulo one of the primes relates the other two. We have  $M = c_0 p_0$ , since  $L_0 = M$ . Reducing  $c_j p_j = a_j M + b_j N$  modulo  $p_0$ , we find  $c_j p_j \equiv b_j N \pmod{p_0}$ , which implies that

$$\left(\frac{p_j}{p_0}\right) = \left(\frac{b_j c_j}{p_0}\right) \varepsilon, \quad \varepsilon = \left(\frac{N}{p_0}\right).$$

Quadratic reciprocity then determines  $(p_0/p_j)$ . For  $i, j \geq 1$ , eliminating  $N$  between  $L_i \equiv 0$  and  $L_j$  modulo  $p_i$ , we find  $b_i L_j \equiv \Delta_{ji} M \pmod{p_i}$ , where  $\Delta_{ji} = a_j b_i - a_i b_j$ . This expresses  $(p_j/p_i)$  as  $(p_0/p_i)$  times the character of a fixed integer (Lemma 4.12). Writing  $\varepsilon = (-1)^\eta$  with  $\eta \in \mathbb{F}_2$ , we find

$$\lambda_i(p_j) = \gamma_{ij} + \eta,$$

where  $\gamma_{ij} \in \mathbb{F}_2$  is computed from characters of fixed integers at  $p_0$  and  $p_i$ , which the congruence class determines (Corollary 4.14). Only the pairs  $(i, j)$  that occur in the rows need to be controlled. A pair with both indices in  $I_H$ , or both in  $I_J$ , never occurs (Remark 4.15), and the determinants  $\Delta_{ij}$  of these pairs need no condition. This is why some primes of  $S$ , such as 131, 257, 409 and 2089 in the rank-five family, need not divide  $W$ .

We conclude that at the prime specializations in the congruence class, the matrix  $\mathbf{M}_\star$  depends on  $(M, N)$  only through  $\eta$ . We write it as  $\mathbf{M}_\star(\eta)$ . However, we have no means of prescribing the sign  $\varepsilon$ . It is a Legendre symbol modulo the growing prime  $p_0$ , and the Green–Tao–Ziegler theorem produces prime values in a congruence class and a cone, but it gives no control of the Legendre symbols among these primes. We must prove the upper bound for both values of  $\varepsilon$ .

The way out is to observe how the matrix changes with  $\eta$ . The fixed rows and the entries of the moving rows in the constant columns do not involve  $\eta$ . Each entry of a moving row in a moving column  $j \neq i$  changes by  $\eta$ . The entry in the column of  $p_i$  is  $\lambda_i(\kappa_*)$  plus a sum of seven cross symbols, and it changes by  $7\eta = \eta$  as well. In other words, every moving row satisfies

$$r_i^*(\eta) = r_i^*(0) + \eta u_*,$$

where  $u_*$  is the vector with entry 1 at the eight moving columns and 0 elsewhere.

Now suppose that there exists a set of rows of  $\mathbf{M}_*(0)$ , containing an even number of moving rows, such that  $u_*$  is their sum. The same set of rows of  $\mathbf{M}_*(1)$  then also sums to  $u_*$ , because the extra copies of  $u_*$  cancel in pairs. Then  $u_*$  lies in both row spaces, and since every row of one matrix is the corresponding row of the other, or that row plus  $u_*$ , the two matrices have the same row space (Lemma 4.17). In particular, they have the same rank and the same kernel, and one rank computation covers both values of  $\varepsilon$ . The parity condition cannot be dropped: if a moving row of  $\mathbf{M}_*(0)$  were equal to  $u_*$ , the corresponding row of  $\mathbf{M}_*(1)$  would be zero. In five of the six cases (three families, two curves),  $u_*$  is the sum of some fixed rows and exactly two moving rows; for the curve  $E'$  of the rank-five family, it is the sum of four moving rows (Lemmas 6.6, 7.7, and 8.8).

Proposition 4.18 collects these steps. Let  $\mathcal{P}$  be a set of prime specializations on which the fixed rows and the numbers  $\lambda_i(g)$ ,  $\lambda_i(\kappa_*)$  and  $\gamma_{ij}$  are constant. The proposition states that if, for both curves, the image of  $\delta_*$  contains  $k_*$  independent classes,  $\text{rank } \mathbf{M}_*(0) = n_* - k_*$ , and  $u_*$  has a representation as above, then  $d_* = k_*$  and  $\text{rank } E_{M,N}(\mathbb{Q}) = k_E + k_{E'} - 2$  at every  $(M, N) \in \mathcal{P}$ .

## 2.5 An example: the rank-six family

We now follow these steps through the family of Section 7. Here  $A = 70$ ,  $B = 784$  and  $C = 1764$ , and the identity  $A^2F + 4BH = CJ$  is 196 times  $25F + 16H = 9J$ . The forms  $L_0 = M$  and  $L_1 = N$  have  $c_0 = c_1 = 1$ , so that  $p_0 = M$ ,  $p_1 = N$  and  $\varepsilon = (p_1/p_0)$ . The lists of constants are  $\Gamma_E = \Gamma_{E'} = (-1, 2, 3, 7)$ , and the bases

$$\mathcal{B}_E = (-1, 2, 3, 7; p_0, \dots, p_7), \quad \mathcal{B}_{E'} = (-1, 2, 3, 7; p_0, \dots, p_3, p_8, \dots, p_{11})$$

have  $n_E = n_{E'} = 12$  entries.

**The points.** Besides  $T$ , we use three points on each curve (Table 7.2). For example,  $P_1 = (14H, 588D_0H)$  with  $D_0 = M^2 + 30N^2$  lies on  $E$ , because  $F + H = 126D_0^2$  (see (7.2)). At a prime specialization, we have  $H = 2p_4p_5p_6p_7$ , and the class of  $P_1$  is  $[28p_4p_5p_6p_7] = [7p_4p_5p_6p_7]$ . The four classes on  $E$  are

$$\begin{aligned} \delta_E(T) &= [-p_0p_1 \cdots p_7], & \delta_E(P_1) &= [7p_4p_5p_6p_7], \\ \delta_E(P_2) &= [-p_1p_2p_4p_5], & \delta_E(P_3) &= [-7p_1p_3p_4p_6]. \end{aligned}$$

The prime  $p_0$  occurs in the first class and in none of the others,  $p_7$  occurs in the second class and in neither of the last two,  $p_2$  occurs in the third class and not in the fourth, and  $p_3$  occurs in the fourth. This triangular pattern shows that the four classes are independent, and  $d_E \geq 4$ . The same argument on  $E'$  gives  $d_{E'} \geq 4$  (Lemma 7.2).

**The congruence class and the fixed rows.** The congruence class  $\mathcal{P}_6$  consists of the pairs  $(M, N) \equiv (M_0, N_0)$  modulo

$$W = 2^6 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 23 = 780373440,$$

and the cone  $\mathcal{K}_6$  is  $\{29N < M < 31N, N > 0\}$  (Section 7.3). By Lemma 7.5, every  $(M, N) \in \mathcal{P}_6$  has the following properties: the image of  $\delta_{E,2}$  lies in the subgroup generated by  $[-1]$  and  $[5]$ , whose classes have even valuation at 2; the image of  $\delta_{E,3}$  is trivial; and the image of  $\delta_{E,7}$  lies in  $\{[1], [7]\}$ . These bounds give four fixed rows of  $\mathbf{M}_E(\eta)$ : one at 2, two at 3 (one for the valuation and one for the unit part), and one at 7. On  $E'$ , we obtain two rows at 2, one at 7 and one at the real place. Each matrix has  $4 + 8 = 12$  rows.

**A moving row.** We compute the row of  $\mathbf{M}_E(\eta)$  at the prime  $p_{10}$ . Since  $10 \in I_J$ , the local image of  $E$  at  $p_{10}$  is trivial, and the row consists of the characters  $\lambda_{10}$  of the entries of  $\mathcal{B}_E$ . By Table 7.6, every  $(M, N) \in \mathcal{P}_6$  has

$$p_{10} \equiv 7 \pmod{8}, \quad p_{10} \equiv 2 \pmod{3}, \quad p_{10} \equiv 6 \pmod{7}.$$

By the supplementary laws, we have  $(-1/p_{10}) = -1$  and  $(2/p_{10}) = 1$ . Since 3, 7 and  $p_{10}$  are congruent to 3 modulo 4, and 2 and 6 are not squares modulo 3 and 7, quadratic reciprocity yields  $(3/p_{10}) = -(p_{10}/3) = 1$  and  $(7/p_{10}) = -(p_{10}/7) = 1$ . The entries in the constant columns  $-1, 2, 3, 7$  are 1, 0, 0, 0.

For the cross symbols, we use the linear relations among the forms. Since  $L_3 = 25M - 169N$ ,  $L_{10} = M - 2N$ ,  $c_3 = 8$  and  $c_{10} = 3$ , we have

$$8p_3 = 25p_0 - 169p_1, \quad 3p_{10} = p_0 - 2p_1.$$

Reducing the second relation modulo  $p_0$ , we find  $3p_{10} \equiv -2p_1 \pmod{p_0}$ , which implies that  $(p_{10}/p_0) = (-6/p_0)\varepsilon$ . On  $\mathcal{P}_6$ , we have  $p_0 \equiv 3 \pmod{8}$  and  $p_0 \equiv 1 \pmod{3}$ . Then  $(-1/p_0) = (2/p_0) = -1$  and  $(3/p_0) = -(p_0/3) = -1$ , which gives  $(-6/p_0) = -1$  and  $(p_{10}/p_0) = -\varepsilon$ . As  $p_0$  and  $p_{10}$  are both congruent to 3 modulo 4, quadratic reciprocity implies that  $(p_0/p_{10}) = \varepsilon$ , that is,  $\lambda_{10}(p_0) = \eta$ .

Next, we reduce both relations modulo  $p_{10}$ . The second becomes  $p_0 \equiv 2p_1 \pmod{p_{10}}$ , and since  $(2/p_{10}) = 1$ , we have  $(p_1/p_{10}) = (p_0/p_{10}) = \varepsilon$ , that is,  $\lambda_{10}(p_1) = \eta$ . Inserting  $2p_1 \equiv p_0$  into the first relation, multiplied by 2, we find  $16p_3 \equiv -119p_0 \pmod{p_{10}}$ , where  $119 = 7 \cdot 17$ . We computed  $(7/p_{10}) = 1$  above, and  $(17/p_{10}) = (p_{10}/17) = (16/17) = 1$ , since  $p_{10} \equiv 16 \pmod{17}$  by Table 7.6. Hence  $(p_3/p_{10}) = (-1/p_{10})\varepsilon = -\varepsilon$ , that is,

$\lambda_{10}(p_3) = 1 + \eta$ . The other cross symbols are computed in the same way, from the integers listed in Table 7.11 and the characters in Table 7.9, and Table 7.12 collects the results. The row is

|                  | -1 | 2 | 3 | 7 | $p_0$  | $p_1$  | $p_2$  | $p_3$      | $p_4$      | $p_5$  | $p_6$      | $p_7$  |
|------------------|----|---|---|---|--------|--------|--------|------------|------------|--------|------------|--------|
| $r_{10}^E(\eta)$ | 1  | 0 | 0 | 0 | $\eta$ | $\eta$ | $\eta$ | $1 + \eta$ | $1 + \eta$ | $\eta$ | $1 + \eta$ | $\eta$ |

For  $\eta = 0$ , it is the row at  $p_{10}$  of Table 7.13. Note that the row is orthogonal to the classes of the points, for both values of  $\eta$ . For instance, its entries at 7 and at  $p_4, \dots, p_7$  sum to  $0 + (1 + \eta) + \eta + (1 + \eta) + \eta = 0$  in  $\mathbb{F}_2$ . This says that  $7p_4p_5p_6p_7$  is a square modulo  $p_{10}$ , which must be so, since  $[7p_4p_5p_6p_7]$  is the class of the rational point  $P_1$ .

**The count.** The matrix  $\mathbf{M}_E(0)$  of Table 7.13 has twelve rows and twelve columns. By Lemma 7.7, it has an  $8 \times 8$  submatrix that becomes lower triangular with ones on the diagonal after its rows and columns are reordered; the row at  $p_{10}$  supplies the diagonal entry in the column of  $p_3$ . This implies that  $\text{rank } \mathbf{M}_E(0) \geq 8$ . The four classes of the points lie in the kernel. Hence the rank is exactly 8, and the kernel is spanned by these classes. The vector  $u_E$  is the sum of the fixed row at 2 and the two moving rows at  $p_1$  and  $p_8$ , and by Lemma 4.17, the matrix  $\mathbf{M}_E(1)$  has the same kernel. We conclude that  $d_E = 4$  and that  $\delta_E(E(\mathbb{Q}))$  is spanned by the four classes above. The same count on  $E'$  yields  $d_{E'} = 4$ , with  $u_{E'}$  the sum of the fixed row at 7 and the moving rows at  $p_1$  and  $p_4$ . By Lemma 3.5, we have

$$\text{rank } E_{M,N}(\mathbb{Q}) = d_E + d_{E'} - 2 = 4 + 4 - 2 = 6$$

at every prime specialization in  $\mathcal{P}_6 \cap \mathcal{K}_6$ , which is the rank statement of Theorem 7.8.

**The three families.** Table 2.1 summarizes the same count for all three families. In each case, the rank of  $\mathbf{M}_\star(0)$  is the largest value that the points allow, namely  $n - k_\star$ , since every row vanishes on the  $k_\star$  classes of the points.

Table 2.1. The dimension count in the three families of Sections 6 to 8. Here  $n = n_E = n_{E'}$  is the number of columns, “rows” is the number of fixed rows plus the eight moving rows, “rank” is  $\text{rank } \mathbf{M}_\star(0)$ , and  $d_\star = n - \text{rank } \mathbf{M}_\star(0)$ .

| $r$ | $\Gamma_E = \Gamma_{E'}$ | $n$ | curve $E$    |         |      |       | curve $E'$         |         |      |          |
|-----|--------------------------|-----|--------------|---------|------|-------|--------------------|---------|------|----------|
|     |                          |     | fixed places | rows    | rank | $d_E$ | fixed places       | rows    | rank | $d_{E'}$ |
| 5   | $(-1, 2, 3, 5)$          | 12  | 2, 3, 5      | $5 + 8$ | 9    | 3     | 2, 5, $\infty$     | $3 + 8$ | 8    | 4        |
| 6   | $(-1, 2, 3, 7)$          | 12  | 2, 3, 7      | $4 + 8$ | 8    | 4     | 2, 7, $\infty$     | $4 + 8$ | 8    | 4        |
| 7   | $(-1, 2, 3, 7, 13)$      | 13  | 2, 3         | $4 + 8$ | 8    | 5     | 2, 7, 13, $\infty$ | $6 + 8$ | 9    | 4        |

## 2.6 Infinitely many prime specializations

We have explained why the rank statement holds at every prime specialization in  $\mathcal{P}_r \cap \mathcal{K}_r$ , and it remains to show that there are infinitely many of them. We write  $M = M_0 + WX$  and  $N = N_0 + WY$  with  $(X, Y) \in \mathbb{Z}^2$ . The twelve numbers  $p_i = L_i(M, N)/c_i$  are the values at  $(X, Y)$  of the affine-linear forms

$$\ell_i(X, Y) = \frac{L_i(M_0, N_0)}{c_i} + \frac{W}{c_i}(a_i X + b_i Y), \quad 0 \leq i \leq 11,$$

whose linear parts are pairwise linearly independent, since  $\Delta_{ij} \neq 0$ . The theorem of Green and Tao on linear equations in primes [18], which is unconditional by [16, 17], is an asymptotic formula for the sum of  $\prod_i \Lambda(\ell_i(X, Y))$  over the points  $(X, Y)$  of a dilated convex region, where  $\Lambda$  is the von Mangoldt function (Theorem 5.1). Apart from the weights and from the contribution of prime powers, which is negligible, this sum counts the points at which all twelve forms take prime values. The main term is the area of the region times a product of local factors, and it is positive if all the forms are positive on the region and no prime  $q$  is a local obstruction.

We choose the congruence class in such a way that no prime is a local obstruction (Lemma 5.4). For a prime  $q$  dividing  $W$ , each form  $\ell_i$  is constant modulo  $q$ , and this constant is prime to  $q$  by the choice of  $(M_0, N_0)$  and of the cofactors. For a prime  $q$  not dividing  $W$ , there is an obstruction only if the zero lines of the twelve forms  $L_i$  modulo  $q$  cover all  $q + 1$  lines through the origin of  $\mathbb{F}_q^2$ . This cannot happen for  $q \geq 13$ , since there are only twelve forms. In the three families, every prime  $q \leq 11$  divides  $W$ , except  $q = 5$  in the rank-seven family, which is checked directly. The points at which two values coincide, or at which a value is a prime of  $S$  or a power of a prime with exponent at least two, lie on comparatively few lines, and they contribute only to the error term (Lemma 5.3). Finally, every form  $L_i$  is positive on the cone  $\mathcal{K}_r$  (Lemmas 6.4, 7.4, and 8.5). Combining these facts, we obtain infinitely many prime specializations in  $\mathcal{P}_r \cap \mathcal{K}_r$  (Proposition 5.5).

It remains to show that these curves represent infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes. At a prime specialization,  $M$  and  $N$  are coprime. Each ratio  $M/N$  therefore comes from at most two prime specializations, and there are infinitely many ratios. The  $j$ -invariant of  $E$  is

$$j(E_{M,N}) = \frac{256(A^2F + 3BH)^3}{B^2CH^2J}.$$

By Lemma 4.3, the numerator and the denominator are binary forms of degree 12 in  $(M, N)$  without a common zero, so that each value of  $j$  is taken for at most twelve ratios  $M/N$ . The curves have infinitely many  $j$ -invariants, and they represent infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes, because curves with distinct  $j$ -invariants are not isomorphic over  $\overline{\mathbb{Q}}$ . This proves the infinitude statements of Theorems 6.7, 7.8, and 8.9, and Section 9 deduces Theorem 1.1 from these three theorems.

## 2.7 Where the families come from

Each family is a base change of a 2-isogenous pair over  $\mathbb{Q}(t)$ , along a conic  $z^2 = q(t)$  that has rational points above each of the six bad parameters  $t = \pm e$  of the pair. The starting pairs and earlier uses of this device are described in Section 1.4, and Appendix B gives the details. When we parametrize the conic by  $M/N$ , the parameter  $t$  becomes a quotient of two binary quadratic forms. Each of the six factors  $t \mp e$  then pulls back to a constant times a product of two of the forms  $L_i$ , divided by the denominator. The three factors  $t^2 - e^2$  pull back to constant multiples of  $F$ ,  $H$  and  $J$ , divided by the square of the denominator, and the linear relation among these three quadratic polynomials in  $t$  becomes the identity  $A^2F + 4BH = CJ$ , up to a constant factor. Appendix B also relates some of the points of each family to points of the starting pair or to points over the conic.

PART I

Descent and prime values

## Descent by a rational 2-isogeny

This section collects the facts about descent by a rational 2-isogeny that we use. For an elliptic curve  $E_{\alpha,\beta}: y^2 = x^3 + \alpha x^2 + \beta x$ , we define the descent maps (Definition 3.3) and recall that they are homomorphisms whose kernels are the images of the two isogenies (Proposition 3.4). The rank of  $E_{\alpha,\beta}(\mathbb{Q})$  is determined by the dimensions of the images of the two descent maps (Lemma 3.5). We bound these images from above in two ways: globally, by the prime divisors of  $\beta$  (Lemma 3.6), and locally, at an odd prime where the coefficients have one of two valuation patterns (Lemma 3.8). In Section 3.4, we write local conditions as linear equations over  $\mathbb{F}_2$  (Lemma 3.10) and record how explicit points give matching lower bounds (Lemma 3.12 and Corollary 3.13).

Descent by a 2-isogeny is classical. We follow [43, Example X.4.8 and Proposition X.4.9] and [44, Sections 3.4–3.6]. Zywinia’s work [55, Section 3], whose strategy we follow, starts from the same formalism. We include short proofs of the facts we use, so that every upper bound in this paper can be checked line by line. The results of this section are used in Section 4, where Lemma 3.8 gives the linear conditions at the twelve moving primes, and in Sections 6 to 8, where the local conditions at the fixed places are proved with Lemmas 3.1, 3.2, and 3.7.

### 3.1 Valuations and squareclasses

A place of  $\mathbb{Q}$  is a prime  $p$  or  $\infty$ , and  $\mathbb{Q}_\infty = \mathbb{R}$ . Primes are positive. For a prime  $p$ , we write  $v_p$  for the  $p$ -adic valuation on  $\mathbb{Q}_p$ , normalized by  $v_p(p) = 1$ , with  $v_p(0) = +\infty$ , and  $\mathbb{Z}_p^\times$  for the group of units of  $\mathbb{Z}_p$ . For a field  $K$ , the group  $K^\times / K^{\times 2}$  of squareclasses is a vector space over  $\mathbb{F}_2$ . We write its group law multiplicatively, call its elements classes, and write  $[u]$  for the class of  $u \in K^\times$ ; linear independence and spans refer to this vector space. For a place  $v$ , we let  $\text{loc}_v: \mathbb{Q}^\times / \mathbb{Q}^{\times 2} \rightarrow \mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2}$  be the homomorphism induced by the inclusion  $\mathbb{Q} \subset \mathbb{Q}_v$ .

For an odd prime  $p$  and  $z \in \mathbb{Z}_p^\times$ , we write  $(z/p)$  for the Legendre symbol of the reduction of  $z$  modulo  $p$ , and we define  $\chi_p(z) \in \mathbb{F}_2$  by

$$\left(\frac{z}{p}\right) = (-1)^{\chi_p(z)}. \quad (3.1)$$

Then  $\chi_p(zw) = \chi_p(z) + \chi_p(w)$ , and  $\chi_p(z)$  depends only on  $z$  modulo  $p$ . We use  $\chi_p(z)$  mostly for integers  $z$  prime to  $p$ . After Lemma 3.2, we extend  $\chi_p$  to  $\mathbb{Q}_p^\times$ .

**Lemma 3.1** (Dominant terms). *Let  $p$  be a prime, and let  $z_1, \dots, z_m \in \mathbb{Q}_p$  with  $z_1 \neq 0$ .*

- (a) *If  $v_p(z_1) < v_p(z_k)$  for  $2 \leq k \leq m$ , then  $v_p(z_1 + \dots + z_m) = v_p(z_1)$ .*
- (b) *If  $h \geq 1$  is an integer and  $v_p(z_k) \geq v_p(z_1) + h$  for  $2 \leq k \leq m$ , then there exists  $t \in \mathbb{Z}_p$  such that  $z_1 + \dots + z_m = z_1(1 + p^h t)$ .*

*Proof.* Under the hypothesis of (b), each quotient  $z_k/z_1$  with  $k \geq 2$  has valuation at least  $h$ . Then  $t = p^{-h} \sum_{k \geq 2} z_k/z_1$  lies in  $\mathbb{Z}_p$ , and  $z_1 + \dots + z_m = z_1(1 + p^h t)$ . The hypothesis of (a) is the case  $h = 1$  of (b), because valuations are integers. As  $1 + pt$  is a unit, we obtain  $v_p(z_1 + \dots + z_m) = v_p(z_1)$ .  $\square$

In the local computations of this paper,  $z_1, \dots, z_m$  are the terms of the right side of a Weierstrass equation. We then call  $z_1$  the *dominant term*.

**Lemma 3.2** (Squareclasses of  $\mathbb{Q}_p$ ). *Let  $p$  be a prime, and write  $u \in \mathbb{Q}_p^\times$  as  $u = p^k u_0$  with  $k = v_p(u)$  and  $u_0 \in \mathbb{Z}_p^\times$ .*

- (a) *Let  $p$  be odd. Then  $u$  is a square if and only if  $k$  is even and  $\chi_p(u_0) = 0$ . The map  $[u] \mapsto (k \bmod 2, \chi_p(u_0))$  is a well-defined isomorphism  $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \rightarrow \mathbb{F}_2^2$ .*
- (b) *Let  $p = 2$ . Then  $u$  is a square if and only if  $k$  is even and  $u_0 \equiv 1 \pmod{8}$ . Every class in  $\mathbb{Q}_2^\times / \mathbb{Q}_2^{\times 2}$  is equal to  $[(-1)^{e_1} 2^{e_2} 5^{e_3}]$  for exactly one  $(e_1, e_2, e_3) \in \mathbb{F}_2^3$ . For the class of  $u$ , we have  $e_2 = k \bmod 2$ , and*

$$(e_1, e_3) = (0, 0), (1, 1), (0, 1), (1, 0) \quad \text{according as} \quad u_0 \equiv 1, 3, 5, 7 \pmod{8}. \quad (3.2)$$

- (c) *If  $p$  is odd and  $h \geq 1$ , or if  $p = 2$  and  $h \geq 3$ , then every element of  $1 + p^h \mathbb{Z}_p$  is a square in  $\mathbb{Q}_p$ .*

The isomorphisms in (a) and (b) are the coordinates on  $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$  that we use to write local conditions, and we name them as follows. At  $p = 2$ , the coordinates of the class of  $z \in \mathbb{Q}_2^\times$  are the bits  $e_1(z), e_2(z), e_3(z)$  of (b). At an odd prime  $p$ , we write  $z \in \mathbb{Q}_p^\times$  as  $z = p^k z_0$  with  $z_0 \in \mathbb{Z}_p^\times$ , and we set

$$v_p(z) = k \bmod 2, \quad \chi_p(z) = \chi_p(z_0), \quad (3.3)$$

so that  $(z_0/p) = (-1)^{\chi_p(z)}$ . By (a), the map  $[z] \mapsto (v_p(z), \chi_p(z))$  is an isomorphism  $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \rightarrow \mathbb{F}_2^2$ . At the real place,  $\mathbb{R}^\times / \mathbb{R}^{\times 2} = \{[1], [-1]\}$ , and the coordinate of the class of  $z \in \mathbb{R}^\times$  is  $\text{sgn}(z) \in \mathbb{F}_2$ , which is 1 if  $z < 0$  and 0 if  $z > 0$ . All these coordinates are linear maps from the groups of squareclasses to  $\mathbb{F}_2$ . We use the indexed symbols  $\lambda_i$  for the characters at the moving primes  $p_i$  of Section 4:  $\lambda_i(z) = \chi_{p_i}(z)$  for integers  $z$  prime to  $p_i$ .

*Proof of Lemma 3.2.* We begin with (a). The two conditions are necessary: a square  $w^2$  has even valuation  $2v_p(w)$ , and its unit part is the square of the unit part of  $w$ . Conversely,

it suffices to show that a unit  $u_0$  with  $\chi_p(u_0) = 0$  is a square. This is Hensel's lemma; we recall the argument. Since  $\chi_p(u_0) = 0$ , there exists  $z_1 \in \mathbb{Z}$  with  $z_1^2 \equiv u_0 \pmod{p}$ . Suppose that  $z_n \in \mathbb{Z}_p$  satisfies  $z_n^2 \equiv u_0 \pmod{p^n}$ . There exists  $t \in \mathbb{Z}$  with  $2z_n t \equiv (u_0 - z_n^2)/p^n \pmod{p}$ , because  $2z_n$  is a unit, and we set  $z_{n+1} = z_n + tp^n$ . Then

$$z_{n+1}^2 = z_n^2 + 2z_n tp^n + t^2 p^{2n} \equiv u_0 \pmod{p^{n+1}}. \quad (3.4)$$

The sequence  $(z_n)$  converges in  $\mathbb{Z}_p$  because  $z_{n+1} - z_n \in p^n \mathbb{Z}_p$ , and its limit is a square root of  $u_0$ . The map in (a) is a homomorphism, because valuations add and  $\chi_p$  is additive. It vanishes on squares, and its kernel consists of squares by the criterion just proved. It is surjective, because the classes of  $p$  and of a unit  $u_0$  with  $\chi_p(u_0) = 1$  map to  $(1, 0)$  and  $(0, 1)$ .

For (b), the two conditions are necessary because the square of an odd integer is 1 modulo 8. Conversely, let  $u_0 \equiv 1 \pmod{8}$ , and let  $z_3 = 1$ . If  $z_n$  is odd and  $z_n^2 \equiv u_0 \pmod{2^n}$  with  $n \geq 3$ , we set  $z_{n+1} = z_n + e2^{n-1}$  with  $e \in \{0, 1\}$ . Since  $2n - 2 \geq n + 1$ , we have

$$z_{n+1}^2 \equiv z_n^2 + e2^n z_n \pmod{2^{n+1}}, \quad (3.5)$$

and exactly one choice of  $e$  gives  $z_{n+1}^2 \equiv u_0 \pmod{2^{n+1}}$ , because  $z_n$  is odd and  $u_0 - z_n^2 \equiv 0 \pmod{2^n}$ . The limit of  $(z_n)$  is a square root of  $u_0$ . The numbers  $(-1)^{e_1 5^{e_3}}$  with  $(e_1, e_3) = (0, 0), (1, 1), (0, 1), (1, 0)$  are 1,  $-5, 5, -1$ , which are congruent to 1, 3, 5, 7 modulo 8. Given  $u = 2^k u_0$ , we choose  $e_2 = k \pmod{2}$  and  $(e_1, e_3)$  by (3.2). Then  $u / ((-1)^{e_1} 2^{e_2} 5^{e_3})$  has even valuation and unit part congruent to 1 modulo 8, and it is a square by the criterion just proved. If two triples give the same class, then the quotient  $(-1)^{d_1} 2^{d_2} 5^{d_3}$  is a square. Its valuation shows that  $d_2 = 0$ , and the list of residues above then shows that  $d_1 = d_3 = 0$ .

Finally, (c) follows from (a) and (b), since an element of  $1 + p^h \mathbb{Z}_p$  is a unit congruent to 1 modulo  $p$  (if  $p$  is odd and  $h \geq 1$ ) or modulo 8 (if  $p = 2$  and  $h \geq 3$ ).  $\square$

### 3.2 Descent maps and the rank

Let  $K$  be a field of characteristic 0, and let  $\alpha, \beta \in K$  with  $\beta(\alpha^2 - 4\beta) \neq 0$ . We write

$$E_{\alpha, \beta}: y^2 = x^3 + \alpha x^2 + \beta x, \quad T = (0, 0). \quad (3.6)$$

Since  $\beta \neq 0$  and  $\alpha^2 - 4\beta \neq 0$ , the cubic  $x(x^2 + \alpha x + \beta)$  has three distinct roots. Then  $E_{\alpha, \beta}$  is an elliptic curve, with origin  $O$  at infinity, and  $T$  is a point of order two; it is the only point of  $E_{\alpha, \beta}$  with  $x = 0$ . We set

$$\alpha' = -2\alpha, \quad \beta' = \alpha^2 - 4\beta. \quad (3.7)$$

Note that  $\alpha'^2 - 4\beta' = 16\beta$ . Then  $\beta'(\alpha'^2 - 4\beta') \neq 0$ , and  $E_{\alpha', \beta'}$  is again an elliptic curve. We write  $E = E_{\alpha, \beta}$  and  $E' = E_{\alpha', \beta'}$ , and  $T' = (0, 0)$  and  $O'$  for the corresponding points of  $E'$ ;

points of  $E'$  are written  $(x', y')$ . We define  $\phi: E \rightarrow E'$  and  $\hat{\phi}: E' \rightarrow E$  by  $\phi(O) = \phi(T) = O'$ ,  $\hat{\phi}(O') = \hat{\phi}(T') = O$ , and

$$\phi(x, y) = \left( \frac{x^2 + \alpha x + \beta}{x}, \frac{y(x^2 - \beta)}{x^2} \right), \quad \hat{\phi}(x', y') = \left( \frac{y'^2}{4x'^2}, \frac{y'(x'^2 - \beta')}{8x'^2} \right) \quad (3.8)$$

for  $x \neq 0$  and  $x' \neq 0$ . Note that on  $E$ , the first coordinate  $x'$  of  $\phi(x, y)$  is equal to  $y^2/x^2$ . The identity

$$\left( \frac{x^2 + \alpha x + \beta}{x} \right)^2 - 2\alpha \frac{x^2 + \alpha x + \beta}{x} + \alpha^2 - 4\beta = \frac{(x^2 - \beta)^2}{x^2} \quad (3.9)$$

implies that  $x'(x'^2 - 2\alpha x' + \beta')$  is the square of the second coordinate  $y(x^2 - \beta)/x^2$ , so  $\phi$  maps  $E$  into  $E'$ . A parallel identity shows that  $\hat{\phi}$  maps  $E'$  into  $E$ .

**Definition 3.3** (Descent maps). Let  $K, \alpha, \beta$  be as above. The *descent map*  $\delta_{\alpha, \beta}^K: E_{\alpha, \beta}(K) \rightarrow K^\times / K^{\times 2}$  is defined by

$$\delta_{\alpha, \beta}^K(O) = [1], \quad \delta_{\alpha, \beta}^K(T) = [\beta], \quad \delta_{\alpha, \beta}^K((x, y)) = [x] \quad \text{for } x \neq 0. \quad (3.10)$$

For  $\alpha, \beta \in \mathbb{Q}$ , we write  $\delta = \delta_{\alpha, \beta}^{\mathbb{Q}}$  and, for a place  $v$ ,  $\delta_v = \delta_{\alpha, \beta}^{\mathbb{Q}_v}$ . For the curve  $E' = E_{\alpha', \beta'}$ , we write  $\delta' = \delta_{\alpha', \beta'}^{\mathbb{Q}}$  and  $\delta'_v$ ; in particular  $\delta'(T') = [\alpha'^2 - 4\beta']$ . When a curve has a name, such as  $E$ , we also write  $\delta_E$  and  $\delta_{E, v}$ .

**Proposition 3.4** (Descent via a 2-isogeny). *Let  $K$  be a field of characteristic 0, let  $\alpha, \beta \in K$  with  $\beta(\alpha^2 - 4\beta) \neq 0$ , and let  $E = E_{\alpha, \beta}$  and  $E' = E_{\alpha', \beta'}$ .*

- (a) *The maps  $\phi: E(K) \rightarrow E'(K)$  and  $\hat{\phi}: E'(K) \rightarrow E(K)$  are homomorphisms with kernels  $\{O, T\}$  and  $\{O', T'\}$ , and  $\hat{\phi} \circ \phi = [2]$  on  $E(K)$  and  $\phi \circ \hat{\phi} = [2]$  on  $E'(K)$ .*
- (b) *The map  $\delta_{\alpha, \beta}^K$  is a homomorphism with kernel  $\hat{\phi}(E'(K))$ , and  $\delta_{\alpha', \beta'}^K$  is a homomorphism with kernel  $\phi(E(K))$ .*
- (c) *Let  $K = \mathbb{Q}$ . For every  $P \in E(\mathbb{Q})$  and every place  $v$ , we have  $\delta_v(P) = \text{loc}_v(\delta(P))$ .*

Part (a) is classical; see [44, Section 3.4] and [43, Example III.4.5 and Theorem III.4.8]. Part (b) is [44, Proposition 3.8] for  $K = \mathbb{Q}$ ; for general  $K$ , see [43, Example X.4.8 and Proposition X.4.9] and [55, Section 3.1]. Since the upper bounds of this paper rest on (b) and (c), we give their elementary proof.

*Proof of Proposition 3.4(b) and (c).* Throughout the proof, we write  $\delta = \delta_{\alpha, \beta}^K$  and  $\delta' = \delta_{\alpha', \beta'}^K$ . We first show that  $\delta$  and  $\delta'$  are homomorphisms, using the chord-and-tangent construction of the group law [43, Section III.2, especially Proposition III.2.2]. We then determine the two kernels: we check that the images of the isogenies lie in them, and we write down a preimage of every element of each kernel. Part (c) follows directly from the definitions.

**The homomorphism property.** Since  $-(x, y) = (x, -y)$ ,  $-T = T$  and  $-O = O$ , we have  $\delta(-P) = \delta(P)$  for every  $P$ . It therefore suffices to show that  $\delta(P)\delta(Q)\delta(R) = [1]$  whenever  $P + Q + R = O$ . If one of the three points is  $O$ , the other two are negatives of each other, and  $\delta(P)\delta(-P) = \delta(P)^2 = [1]$ . Otherwise, the line through  $P$  and  $Q$  (the tangent line if  $P = Q$ ) meets  $E$  at  $P, Q, R$ , counted with multiplicity. This line is not vertical, since a vertical line through  $P$  meets  $E$  at  $-P$  and at  $O$ . We write it as  $y = mx + n$ . The  $x$ -coordinates of  $P, Q, R$  are then the three roots, counted with multiplicity, of

$$x^3 + \alpha x^2 + \beta x - (mx + n)^2 = x^3 + (\alpha - m^2)x^2 + (\beta - 2mn)x - n^2, \quad (3.11)$$

whose product is  $n^2$ . If  $n \neq 0$ , no root is 0. Then none of  $P, Q, R$  is  $T$ , and the product of their classes is  $[n^2] = [1]$ . If  $n = 0$ , the polynomial (3.11) is  $x(x^2 + (\alpha - m^2)x + \beta)$ . Since  $\beta \neq 0$ , the root 0 is simple, which implies that exactly one of  $P, Q, R$  is  $T$ . The  $x$ -coordinates of the other two are the roots of  $x^2 + (\alpha - m^2)x + \beta$ , whose product is  $\beta$ . The product of the three classes is  $[\beta] \cdot [\beta] = [1]$ . The same argument applies to  $\delta'$ , and both maps are homomorphisms.

**The kernel of  $\delta$ .** We first show that  $\hat{\phi}(E'(K)) \subseteq \ker \delta$ . We have  $\hat{\phi}(O') = \hat{\phi}(T') = O$ . If  $x' \neq 0$  and  $y' \neq 0$ , then  $\hat{\phi}(x', y')$  has  $x$ -coordinate  $(y'/2x')^2 \neq 0$ , whose class is trivial. If  $x' \neq 0$  and  $y' = 0$ , then  $\hat{\phi}(x', 0) = T$ , and  $x'$  is a root of  $x'^2 - 2\alpha x' + \beta'$ , whose discriminant is  $16\beta$ . Then  $16\beta = (2x' - 2\alpha)^2$ , and  $\delta(T) = [\beta] = [1]$ .

Conversely, let  $P \in \ker \delta$ . If  $P = O$ , then  $P = \hat{\phi}(O')$ . If  $P = T$ , then  $\beta = s^2$  with  $s \in K^\times$ , and the points  $(\alpha \pm 2s, 0)$  lie on  $E'$ , since  $(\alpha \pm 2s)^2 - 2\alpha(\alpha \pm 2s) + \alpha^2 - 4s^2 = 0$ ; their  $x$ -coordinates are nonzero because their product is  $\beta' \neq 0$ , and  $\hat{\phi}(\alpha \pm 2s, 0) = T$ . Finally, let  $P = (x, y)$  with  $x = s^2$  and  $s \in K^\times$ ; here  $y$  may be 0. We set

$$x' = \alpha + 2s^2 + \frac{2y}{s}, \quad y' = 2sx'. \quad (3.12)$$

Using  $y^2 = s^6 + \alpha s^4 + \beta s^2$ , we find

$$\left(\alpha + 2s^2 + \frac{2y}{s}\right)\left(\alpha + 2s^2 - \frac{2y}{s}\right) = (\alpha + 2s^2)^2 - \frac{4y^2}{s^2} = \alpha^2 - 4\beta = \beta'. \quad (3.13)$$

This implies that  $x' \neq 0$  and that  $x' + \beta'/x' = 2\alpha + 4s^2$ . Then

$$x'^3 - 2\alpha x'^2 + \beta' x' = x'^2 \left(x' - 2\alpha + \frac{\beta'}{x'}\right) = 4s^2 x'^2 = y'^2, \quad (3.14)$$

and  $(x', y') \in E'(K)$ . By (3.8), the  $x$ -coordinate of  $\hat{\phi}(x', y')$  is  $s^2 = x$ , and its  $y$ -coordinate is

$$\frac{2sx'(x'^2 - \beta')}{8x'^2} = \frac{s}{4} \left(x' - \frac{\beta'}{x'}\right) = \frac{s}{4} \cdot \frac{4y}{s} = y, \quad (3.15)$$

where we used (3.13) to write  $x' - \beta'/x'$  as the difference of the two factors on its left side. We conclude that  $P = \hat{\phi}(x', y')$ , and that  $\ker \delta = \hat{\phi}(E'(K))$ .

**The kernel of  $\delta'$ .** The argument is the same with the roles of the two curves exchanged. We have  $\phi(O) = \phi(T) = O'$ . For  $x \neq 0$  and  $y \neq 0$ , the  $x'$ -coordinate of  $\phi(x, y)$  is  $(y/x)^2$ . For  $x \neq 0$  and  $y = 0$ , we have  $\phi(x, 0) = T'$ ; since  $x$  is a root of  $x^2 + \alpha x + \beta$ , we have  $\beta' = \alpha^2 - 4\beta = (2x + \alpha)^2$ , which is a square. This proves that  $\phi(E(K)) \subseteq \ker \delta'$ .

Conversely, if  $\delta'(T') = [1]$ , then  $\beta' = s^2$  with  $s \in K^\times$ . The points  $((-\alpha \pm s)/2, 0)$  lie on  $E$ , their  $x$ -coordinates are nonzero because their product is  $\beta$ , and both map to  $T'$ . Finally, let  $(x', y') \in E'(K)$  with  $x' = s^2$  and  $s \in K^\times$ . We set

$$x = \frac{1}{2} \left( s^2 - \alpha + \frac{y'}{s} \right), \quad y = sx. \quad (3.16)$$

Using  $y'^2 = s^6 - 2\alpha s^4 + \beta' s^2$ , we find

$$\left( s^2 - \alpha + \frac{y'}{s} \right) \left( s^2 - \alpha - \frac{y'}{s} \right) = (s^2 - \alpha)^2 - \frac{y'^2}{s^2} = \alpha^2 - \beta' = 4\beta. \quad (3.17)$$

Then  $x \neq 0$  and  $\beta/x = (s^2 - \alpha - y'/s)/2$ , which implies that  $x + \beta/x = s^2 - \alpha$  and  $x - \beta/x = y'/s$ . Using the first of these identities, we find  $x^3 + \alpha x^2 + \beta x = x^2(x + \alpha + \beta/x) = s^2 x^2 = y'^2$ , and  $(x, y) \in E(K)$ . By (3.8) and the second identity, we have

$$\phi(x, y) = \left( \frac{y^2}{x^2}, s \left( x - \frac{\beta}{x} \right) \right) = (s^2, y') = (x', y'). \quad (3.18)$$

Hence  $\ker \delta' = \phi(E(K))$ .

**Compatibility with localization.** Let  $K = \mathbb{Q}$ ,  $P \in E(\mathbb{Q})$  and  $v$  a place. The point  $P$  is also a point of  $E(\mathbb{Q}_v)$ , and the formulas (3.10) for  $\delta$  and  $\delta_v$  are the same. The map  $\text{loc}_v$  sends  $[x]$  to the class of  $x$  in  $\mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2}$ , which gives  $\delta_v(P) = \text{loc}_v(\delta(P))$ .  $\square$

**Lemma 3.5** (Rank from the images of the two descent maps). *Let  $\alpha, \beta \in \mathbb{Q}$  with  $\beta(\alpha^2 - 4\beta) \neq 0$ , let  $E = E_{\alpha, \beta}$  and  $E' = E_{\alpha', \beta'}$ , and let*

$$d = \dim_{\mathbb{F}_2} \delta(E(\mathbb{Q})), \quad d' = \dim_{\mathbb{F}_2} \delta'(E'(\mathbb{Q})). \quad (3.19)$$

*Then  $\text{rank } E(\mathbb{Q}) = d + d' - 2$ .*

The formula is [44, Section 3.6], where it is written as  $2^{\text{rank } E(\mathbb{Q})} = \#\delta(E(\mathbb{Q})) \cdot \#\delta'(E'(\mathbb{Q}))/4$ , and [55, Lemma 3.1]. It holds whether or not  $\alpha^2 - 4\beta$  is a square in  $\mathbb{Q}$ . In the families of Section 4,  $\alpha^2 - 4\beta$  is not a square (Lemma 4.8), but the proof below does not need this.

*Proof.* Let  $\Gamma = E(\mathbb{Q})$ ,  $\Gamma' = E'(\mathbb{Q})$ ,  $r = \text{rank } E(\mathbb{Q})$ , and let  $2^t$  be the order of  $\Gamma[2]$ . Then  $t \in \{1, 2\}$ , since  $T \in \Gamma[2]$  and  $\Gamma[2]$  has at most four elements. By Proposition 3.4(b), the map  $\delta$  induces an isomorphism  $\Gamma/\hat{\phi}(\Gamma') \rightarrow \delta(\Gamma)$ , and  $\delta'$  induces an isomorphism  $\Gamma'/\phi(\Gamma) \rightarrow \delta'(\Gamma')$ . Comparing orders, we find

$$[\Gamma : \hat{\phi}(\Gamma')] = 2^d, \quad [\Gamma' : \phi(\Gamma)] = 2^{d'}. \quad (3.20)$$

Since  $\hat{\phi} \circ \phi = [2]$ , we have  $2\Gamma \subseteq \hat{\phi}(\Gamma') \subseteq \Gamma$ , and  $[\Gamma : 2\Gamma] = 2^d [\hat{\phi}(\Gamma') : 2\Gamma]$ .

We compute the second index. The homomorphism  $\Gamma' \rightarrow \hat{\phi}(\Gamma')/2\Gamma$  that sends  $Q$  to the coset of  $\hat{\phi}(Q)$  is surjective. Its kernel consists of the points  $Q$  with  $\hat{\phi}(Q) = 2P = \hat{\phi}(\phi(P))$  for some  $P \in \Gamma$ , that is, of the points of  $\phi(\Gamma) + \{O', T'\}$ , by Proposition 3.4(a). We obtain

$$[\hat{\phi}(\Gamma') : 2\Gamma] = [\Gamma' : \phi(\Gamma) + \{O', T'\}] = 2^{d'} / [\phi(\Gamma) + \{O', T'\} : \phi(\Gamma)]. \quad (3.21)$$

The last index is 1 if  $T' \in \phi(\Gamma)$  and 2 otherwise. If  $\phi(P) = T'$ , then  $2P = \hat{\phi}(T') = O$ , and  $P \in \Gamma[2]$ . Conversely,  $\phi$  maps  $\Gamma[2]$  into  $\ker \hat{\phi} = \{O', T'\}$ , since  $\hat{\phi}(\phi(P)) = 2P$ , and its kernel is  $\{O, T\}$ ; the image  $\phi(\Gamma[2])$  has  $2^{t-1}$  elements. It follows that  $T' \in \phi(\Gamma)$  if and only if  $t = 2$ , and in both cases

$$[\hat{\phi}(\Gamma') : 2\Gamma] = 2^{d'+t-2}. \quad (3.22)$$

By the Mordell–Weil theorem [43, Theorem VIII.6.7],  $\Gamma \cong \mathbb{Z}^r \oplus \Gamma_{\text{tors}}$  with  $\Gamma_{\text{tors}}$  finite. For a finite abelian group  $U$ , the quotient  $U/2U$  and the subgroup  $U[2]$  have the same order, which implies that  $[\Gamma : 2\Gamma] = 2^r \cdot 2^t$ . Combining the three displays, we obtain  $2^{r+t} = 2^d \cdot 2^{d'+t-2}$ , which gives  $r = d + d' - 2$ .  $\square$

### 3.3 Support and local images

**Lemma 3.6** (Support of the global image). *Let  $\alpha, \beta \in \mathbb{Z}$  with  $\beta(\alpha^2 - 4\beta) \neq 0$ . Then every class in  $\delta(E_{\alpha, \beta}(\mathbb{Q}))$  is represented by a signed squarefree divisor of  $\beta$ . Equivalently,  $\delta(E_{\alpha, \beta}(\mathbb{Q}))$  lies in the subgroup of  $\mathbb{Q}^\times / \mathbb{Q}^{\times 2}$  spanned by  $[-1]$  and the classes of the primes dividing  $\beta$ .*

This is [44, Proposition 3.8(c)].

*Proof.* The classes  $\delta(O) = [1]$  and  $\delta(T) = [\beta]$  have the required form. Let  $P = (x, y)$  with  $x \neq 0$ , and let  $p$  be a prime not dividing  $\beta$ . It suffices to show that  $r = v_p(x)$  is even, since then removing square factors from  $x$  leaves a signed product of distinct primes dividing  $\beta$ .

Suppose first that  $y = 0$ . Then  $x$  is a root of  $x^2 + \alpha x + \beta$ . If  $r < 0$ , the term  $x^2$  has valuation  $2r$ , smaller than  $v_p(\alpha x) \geq r$  and  $v_p(\beta) \geq 0$ , and Lemma 3.1(a) implies that the sum  $x^2 + \alpha x + \beta$  has valuation  $2r$ , so that it is not 0. If  $r > 0$ , the term  $\beta$  has valuation 0, smaller than those of  $x^2$  and  $\alpha x$ , and again the sum is not 0. We conclude that  $r = 0$ .

Suppose now that  $y \neq 0$ . If  $r < 0$ , the term  $x^3$  of  $x^3 + \alpha x^2 + \beta x$  has valuation  $3r$ , smaller than  $v_p(\alpha x^2) \geq 2r$  and  $v_p(\beta x) \geq r$ . By Lemma 3.1(a), we have  $2v_p(y) = 3r$ , and  $r$  is even. If  $r > 0$ , the term  $\beta x$  has valuation  $r$ , smaller than  $v_p(\alpha x^2) \geq 2r$  and  $v_p(x^3) = 3r$ , and we find  $2v_p(y) = r$ . In all cases  $r$  is even.  $\square$

**Lemma 3.7** (Points of order two). *Let  $K$  be a field of characteristic 0, and let  $\alpha, \beta \in K$  with  $\beta(\alpha^2 - 4\beta) \neq 0$ . The points of order two of  $E_{\alpha, \beta}(K)$  are  $T$  and the points  $(x_0, 0)$  with  $x_0 \in K$  a*

root of  $x^2 + \alpha x + \beta$ . Points  $(x_0, 0)$  with  $x_0 \neq 0$  exist if and only if  $\alpha^2 - 4\beta$  is a square in  $K$ . In that case there are exactly two of them,  $(x_0, 0)$  and  $(x_1, 0)$ , with  $x_0 \neq x_1$  and  $x_0 x_1 = \beta$ , and their classes are  $\delta_{\alpha, \beta}^K((x_k, 0)) = [x_k]$ ; in particular  $[x_0][x_1] = [\beta]$ .

*Proof.* Recall that  $-(x, y) = (x, -y)$  on the model (3.6). A point  $P \neq O$  therefore satisfies  $2P = O$  if and only if  $y = 0$ , that is, if and only if  $x(x^2 + \alpha x + \beta) = 0$ . The root  $x = 0$  gives  $T$ . The quadratic  $x^2 + \alpha x + \beta$  has a root in  $K$  if and only if its discriminant  $\alpha^2 - 4\beta$  is a square in  $K$ . Its two roots are then distinct because  $\alpha^2 - 4\beta \neq 0$ , and both are nonzero because their product is  $\beta \neq 0$ . Their classes are given by (3.10).  $\square$

The next lemma gives the local conditions at the moving primes of Section 4. Its first part applies when  $p$  divides the coefficient  $\alpha$  and divides  $\beta$  exactly once, and its second part when  $\alpha$  and  $\beta$  are units but  $p$  divides  $\alpha^2 - 4\beta$  exactly once. The second part is the case  $n = 1$  of [55, Lemma 3.3(i)], applied after exchanging the two isogenous curves. We give elementary valuation proofs of both parts.

**Lemma 3.8** (Local images at odd primes). *Let  $p$  be an odd prime, and let  $\alpha, \beta \in \mathbb{Z}_p$ .*

- (a) *If  $v_p(\alpha) \geq 1$  and  $v_p(\beta) = 1$ , then  $\beta(\alpha^2 - 4\beta) \neq 0$  and  $\delta_p(E_{\alpha, \beta}(\mathbb{Q}_p)) = \{[1], [\beta]\}$ .*
- (b) *If  $\alpha, \beta \in \mathbb{Z}_p^\times$  and  $v_p(\alpha^2 - 4\beta) = 1$ , then  $\delta_p(E_{\alpha, \beta}(\mathbb{Q}_p)) = \{[1]\}$ .*

Here  $\delta_p = \delta_{\alpha, \beta}^{\mathbb{Q}_p}$ .

*Proof.* In both parts, we first show that  $v_p(\alpha^2 - 4\beta) = 1$ . We deduce that  $E(\mathbb{Q}_p)[2] = \{O, T\}$ , so that  $T$  is the only affine point of  $E = E_{\alpha, \beta}$  over  $\mathbb{Q}_p$  with  $y = 0$ . We then treat the points  $(x, y)$  with  $x \neq 0$  and  $y \neq 0$  according to the sign of  $r = v_p(x)$ . For such a point, we have  $[y^2] = [1]$  and  $y^2 = x^3 + \alpha x^2 + \beta x$ .

**Part (a).** Since  $v_p(\alpha^2) \geq 2$  and  $v_p(4\beta) = 1$ , Lemma 3.1(a) implies that  $v_p(\alpha^2 - 4\beta) = 1$ . Then  $\alpha^2 - 4\beta \neq 0$ , and  $\beta \neq 0$ . As  $v_p(\alpha^2 - 4\beta)$  is odd,  $\alpha^2 - 4\beta$  is not a square in  $\mathbb{Q}_p$  by Lemma 3.2(a), and Lemma 3.7 shows that  $T$  is the only point of order two in  $E(\mathbb{Q}_p)$ . The points  $O$  and  $T$  have classes  $[1]$  and  $[\beta]$ .

Let  $(x, y) \in E(\mathbb{Q}_p)$  with  $x \neq 0$ , so that  $y \neq 0$ . If  $r \leq 0$ , then

$$v_p(\alpha x^2) \geq 1 + 2r \geq 3r + 1, \quad v_p(\beta x) = 1 + r \geq 3r + 1, \quad (3.23)$$

and the term  $x^3$  is dominant. By Lemma 3.1(b) with  $h = 1$ , we have  $y^2 = x^3(1 + pt)$  with  $t \in \mathbb{Z}_p$ . The factor  $1 + pt$  is a square by Lemma 3.2(c), and we find  $[x] = [x^3] = [y^2] = [1]$ . If  $r \geq 1$ , then

$$v_p(\beta x) = 1 + r, \quad v_p(\alpha x^2) \geq 1 + 2r \geq (1 + r) + 1, \quad v_p(x^3) = 3r \geq (1 + r) + 1, \quad (3.24)$$

and  $\beta x$  is the dominant term. By Lemma 3.1(b) and Lemma 3.2(c), we obtain  $y^2 = \beta x(1 + pt)$  with  $t \in \mathbb{Z}_p$  and  $1 + pt$  a square. This implies that  $[\beta x] = [1]$ , that is,  $[x] = [\beta]$ . Every point therefore has class  $[1]$  or  $[\beta]$ , and both classes occur.

**Part (b).** Here  $v_p(\alpha^2 - 4\beta) = 1$  by hypothesis, and as in part (a),  $T$  is the only affine point of  $E(\mathbb{Q}_p)$  with  $y = 0$ . We first show that  $\beta$  is a square in  $\mathbb{Q}_p$ . Indeed, we have  $\chi_p(\beta) = \chi_p(4\beta) = \chi_p(\alpha^2) = 0$ , since  $4\beta \equiv \alpha^2 \pmod{p}$  and  $\alpha$  is a unit. As  $\beta$  is a unit, Lemma 3.2(a) shows that  $\beta$  is a square, and  $\delta_p(O) = \delta_p(T) = [1]$ .

Let  $(x, y) \in E(\mathbb{Q}_p)$  with  $x \neq 0$ , so that  $y \neq 0$ . If  $r \leq -1$ , then  $v_p(\alpha x^2) = 2r \geq 3r + 1$  and  $v_p(\beta x) = r \geq 3r + 1$ . As in part (a), Lemma 3.1(b) and Lemma 3.2(c) give  $y^2 = x^3(1 + pt)$  and  $[x] = [1]$ . If  $r \geq 1$ , then  $v_p(\beta x) = r$ , while  $v_p(\alpha x^2) = 2r$  and  $v_p(x^3) = 3r$  are at least  $r + 1$ . The same argument gives  $y^2 = \beta x(1 + pt)$  and  $[x] = [\beta] = [1]$ .

It remains to treat  $r = 0$ . Let  $D = \alpha^2 - 4\beta$  and  $z = x + \alpha/2 \in \mathbb{Z}_p$ , so that

$$y^2 = x(x^2 + \alpha x + \beta) = x\left(z^2 - \frac{D}{4}\right). \quad (3.25)$$

If  $z$  is a unit, then  $v_p(z^2) = 0 < 1 = v_p(D/4)$ , and by Lemma 3.1(b), we have  $z^2 - D/4 = z^2(1 + pt)$  with  $t \in \mathbb{Z}_p$ . This is a square by Lemma 3.2(c), and (3.25) implies that  $[x] = [1]$ . If  $z \in p\mathbb{Z}_p$ , then  $v_p(z^2) \geq 2 > 1 = v_p(D/4)$ , and we have  $v_p(z^2 - D/4) = 1$  by Lemma 3.1(a). Since  $x$  is a unit, the right side of (3.25) then has valuation 1, which is impossible for the square  $y^2$ . Every point therefore has class  $[1]$ .  $\square$

### 3.4 Local conditions as linear equations

We now write the local conditions as linear equations over  $\mathbb{F}_2$ . We also record the two elementary facts that turn explicit points into lower bounds. Linear equations over  $\mathbb{F}_2$  whose coefficients are Legendre symbols are a standard tool in 2-descent: examples include Monsky's appendix to [20, pp. 365–369, especially p. 366] for full 2-descent on the congruent-number curves, and for descent by a 2-isogeny they appear in [15, Sections 2–3], [51, Section 3.1, Theorem 3] and [24, Section 4].

**Definition 3.9** (Ambient bases and rows). Let  $\alpha, \beta \in \mathbb{Q}$  with  $\beta(\alpha^2 - 4\beta) \neq 0$ , and let  $E = E_{\alpha, \beta}$ . Let  $\mathcal{B} = (g_1, \dots, g_n)$  be a list of nonzero rational numbers. For  $\mathbf{w} \in \mathbb{F}_2^n$  we write

$$[\mathbf{w}]_{\mathcal{B}} = [g_1^{w_1} \cdots g_n^{w_n}] \in \mathbb{Q}^\times / \mathbb{Q}^{\times 2}, \quad (3.26)$$

and we call  $\mathbf{w}$  a coordinate vector of this class. We say that  $\mathcal{B}$  is an *ambient basis* for  $E$  if the map  $\mathbf{w} \mapsto [\mathbf{w}]_{\mathcal{B}}$  is injective and its image contains  $\delta(E(\mathbb{Q}))$ . Let  $v$  be a place of  $\mathbb{Q}$ , let  $U_v \subseteq \mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2}$  be a subgroup containing  $\delta_v(E(\mathbb{Q}_v))$ , and let  $f: \mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2} \rightarrow \mathbb{F}_2$  be a linear map that vanishes on  $U_v$ . The *row* defined by  $(v, U_v, f)$  is the vector  $r \in \mathbb{F}_2^n$  with entries

$$r_j = f(\text{loc}_v([g_j])), \quad 1 \leq j \leq n. \quad (3.27)$$

For  $r, \mathbf{w} \in \mathbb{F}_2^n$ , we write  $r \cdot \mathbf{w} = \sum_j r_j w_j$ .

**Lemma 3.10** (Local conditions give upper bounds). *In the setting of Definition 3.9, let  $r$  be the row defined by  $(v, U_v, f)$ . Then  $r \cdot \mathbf{w} = 0$  for every  $\mathbf{w} \in \mathbb{F}_2^n$  such that  $[\mathbf{w}]_{\mathcal{B}} \in \delta(E(\mathbb{Q}))$ . If, moreover,  $\mathcal{B}$  is an ambient basis for  $E$  and  $\mathbf{M}$  is a matrix over  $\mathbb{F}_2$  with  $n$  columns whose rows are rows in the sense of Definition 3.9, possibly at different places, then the coordinate vectors of the classes in  $\delta(E(\mathbb{Q}))$  form a subspace of  $\ker \mathbf{M}$ , and*

$$\dim_{\mathbb{F}_2} \delta(E(\mathbb{Q})) \leq n - \text{rank } \mathbf{M}. \quad (3.28)$$

*Proof.* The map  $\mathbf{w} \mapsto f(\text{loc}_v([\mathbf{w}]_{\mathcal{B}}))$  is linear, because  $\text{loc}_v$  and  $f$  are homomorphisms, and by (3.27) it is equal to  $\mathbf{w} \mapsto r \cdot \mathbf{w}$ . If  $[\mathbf{w}]_{\mathcal{B}} = \delta(P)$  with  $P \in E(\mathbb{Q})$ , then Proposition 3.4(c) implies that  $\text{loc}_v([\mathbf{w}]_{\mathcal{B}}) = \delta_v(P) \in U_v$ , and we obtain  $r \cdot \mathbf{w} = f(\delta_v(P)) = 0$ . If  $\mathcal{B}$  is an ambient basis, the map  $\mathbf{w} \mapsto [\mathbf{w}]_{\mathcal{B}}$  identifies  $\delta(E(\mathbb{Q}))$  with a subspace of  $\mathbb{F}_2^n$ , which lies in  $\ker \mathbf{M}$  by the first part. This proves (3.28), since  $\dim \ker \mathbf{M} = n - \text{rank } \mathbf{M}$ .  $\square$

In practice,  $f$  is written in the coordinates named after Lemma 3.2. At an odd prime  $p$ , a linear map on  $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \cong \mathbb{F}_2^2$  is a combination of the valuation coordinate  $v_p$  and the character coordinate  $\chi_p$  of (3.3). If  $U_p = \{[1]\}$ , both coordinates vanish on  $U_p$ . If  $U_p = \{[1], [z]\}$  with  $z = pz_0$  and  $z_0 \in \mathbb{Z}_p^\times$ , then  $[z]$  has coordinates  $(v_p(z), \chi_p(z)) = (1, \chi_p(z_0))$ , and the linear map  $\chi_p + \chi_p(z_0) v_p$  vanishes on  $U_p$ . At  $p = 2$ , the coordinates are  $e_1, e_2, e_3$  of Lemma 3.2(b), and at  $\infty$  the only nonzero linear map is the sign coordinate  $\text{sgn}$ , which vanishes on  $U_\infty = \{[1]\}$ .

*Remark 3.11* (What the upper bounds measure). The classes in  $\mathbb{Q}^\times / \mathbb{Q}^{\times 2}$  whose localization lies in  $\delta_v(E(\mathbb{Q}_v))$  for every place  $v$  form the Selmer group of the isogeny  $\hat{\phi}$  [43, Section X.4], and  $\delta(E(\mathbb{Q}))$  is contained in it. A matrix  $\mathbf{M}$  as in Lemma 3.10 imposes conditions at finitely many places only, with subgroups  $U_v$  that may be larger than  $\delta_v(E(\mathbb{Q}_v))$ . Its kernel contains the coordinate vectors of the classes of this Selmer group that lie in the span of  $\mathcal{B}$ . We use only the inclusion of  $\delta(E(\mathbb{Q}))$  in  $\ker \mathbf{M}$ . Together with explicit points (Corollary 3.13), this determines  $\delta(E(\mathbb{Q}))$ ; no separate Selmer-group computation is needed, and the finiteness of the Tate–Shafarevich group is not used.

**Lemma 3.12** (A triangular criterion for independence). *Let  $\mathbf{w}_1, \dots, \mathbf{w}_k \in \mathbb{F}_2^n$ . Suppose that there exist distinct indices  $j_1, \dots, j_k \in \{1, \dots, n\}$  such that, for each  $s$ , the  $j_s$ -th entry of  $\mathbf{w}_s$  is 1 and the  $j_s$ -th entry of  $\mathbf{w}_t$  is 0 for every  $t > s$ . Then  $\mathbf{w}_1, \dots, \mathbf{w}_k$  are linearly independent. In particular, if  $\mathcal{B}$  is an ambient basis for  $E$ , the classes  $[\mathbf{w}_1]_{\mathcal{B}}, \dots, [\mathbf{w}_k]_{\mathcal{B}}$  are linearly independent.*

*Proof.* Suppose that  $\sum_t c_t \mathbf{w}_t = 0$  with  $c_t \in \mathbb{F}_2$ , and that  $c_1 = \dots = c_{s-1} = 0$  for some  $s \leq k$ . Then  $\sum_{t \geq s} c_t \mathbf{w}_t = 0$ , and its  $j_s$ -th entry is  $c_s$ , which gives  $c_s = 0$ . By induction on  $s$ , all  $c_t$  vanish. The last statement holds because  $\mathbf{w} \mapsto [\mathbf{w}]_{\mathcal{B}}$  is injective and linear.  $\square$

When  $g_j$  is a prime  $q$  that divides none of the other entries of  $\mathcal{B}$ , the  $j$ -th coordinate of a class is its  $q$ -adic valuation modulo 2. In Sections 6 to 8, the indices  $j_s$  in Lemma 3.12

are such primes, and the lemma amounts to eliminating the coefficients of a relation one at a time by their valuations at these primes.

**Corollary 3.13** (Exact dimension). *Let  $\mathcal{B}$  be an ambient basis for  $E = E_{\alpha,\beta}$  with  $n$  entries, and let  $\mathbf{M}$  be a matrix whose rows are rows in the sense of Definition 3.9. Suppose that  $\mathbf{w}_1, \dots, \mathbf{w}_k \in \mathbb{F}_2^n$  are linearly independent, that  $[\mathbf{w}_s]_{\mathcal{B}} \in \delta(E(\mathbb{Q}))$  for every  $s$ , and that  $\text{rank } \mathbf{M} = n - k$ . Then  $\dim_{\mathbb{F}_2} \delta(E(\mathbb{Q})) = k$ , and  $\delta(E(\mathbb{Q}))$  is the span of  $[\mathbf{w}_1]_{\mathcal{B}}, \dots, [\mathbf{w}_k]_{\mathcal{B}}$ . It consists of the classes  $[\mathbf{w}]_{\mathcal{B}}$  with  $\mathbf{w} \in \ker \mathbf{M}$ .*

*Proof.* Let  $V_0$  be the span of  $\mathbf{w}_1, \dots, \mathbf{w}_k$ , and let  $V_1$  be the subspace of coordinate vectors of the classes in  $\delta(E(\mathbb{Q}))$ . Since  $\delta(E(\mathbb{Q}))$  is a group, we have  $V_0 \subseteq V_1$ , and Lemma 3.10 implies that  $V_1 \subseteq \ker \mathbf{M}$ . The dimensions of  $V_0$  and  $\ker \mathbf{M}$  are both  $k$ , which implies that  $V_0 = V_1 = \ker \mathbf{M}$ .  $\square$

## Families with twelve linear factors

In this section, we set up the framework shared by the three families of Sections 6 to 8 and prove once the steps that are common to them. A twelve-form datum (Definition 4.1) consists of twelve binary linear forms and three integers  $A, B, C$  satisfying the identity  $A^2F + 4BH = CJ$ , where  $F, H, J$  are products of four of the forms each. For each  $(M, N) \in \mathbb{Z}^2$  with  $F(M, N)H(M, N)J(M, N) \neq 0$ , it gives a pair of 2-isogenous curves  $E_{M,N}$  and  $E'_{M,N}$ . In Section 4.1, we compute their basic invariants (Lemmas 4.2 and 4.3). In Section 4.2, we introduce prime specializations, at which the twelve forms take prime values up to fixed cofactors (Definition 4.6), show that a congruence condition on  $(M, N)$  forces the divisibility  $c_i \mid L_i(M, N)$  and fixes the residues of the quotients (Lemma 4.7), and determine the local images of the descent maps at these twelve primes (Lemma 4.9). Section 4.3 turns these local images into linear conditions (Lemma 4.11). The coefficients of these conditions are quadratic characters, and Section 4.4 shows that quadratic reciprocity determines them through fixed residues and a single sign  $\varepsilon$  (Lemma 4.12 and Corollary 4.14). Finally, Section 4.5 proves the rank criterion (Proposition 4.18), which reduces the rank of  $E_{M,N}(\mathbb{Q})$  at all prime specializations in a given set to finitely many checks, for both values of  $\varepsilon$ .

This section uses the results of Section 3. Section 5 uses Definitions 4.1 and 4.6 and Lemmas 4.3 and 4.8 to produce infinitely many prime specializations, and Sections 6 to 8 verify the hypotheses of Proposition 4.18 for the three families.

### 4.1 Twelve-form data

**Definition 4.1** (Twelve-form datum). A *twelve-form datum*  $\mathfrak{D}$  consists of the following.

- (a) Pairs  $(a_i, b_i) \in \mathbb{Z}^2$  for  $0 \leq i \leq 11$ , with  $\gcd(a_i, b_i) = 1$  for every  $i$ ,  $(a_0, b_0) = (1, 0)$ ,  $b_i \neq 0$  for  $1 \leq i \leq 11$ , and  $\Delta_{ij} = a_i b_j - a_j b_i \neq 0$  for all  $i \neq j$ .
- (b) Nonzero integers  $A, B, C$  such that

$$A^2F + 4BH = CJ \tag{4.1}$$

in  $\mathbb{Z}[M, N]$ , where  $L_i = a_i M + b_i N$  for  $0 \leq i \leq 11$  and

$$F = L_0 L_1 L_2 L_3, \quad H = L_4 L_5 L_6 L_7, \quad J = L_8 L_9 L_{10} L_{11}. \tag{4.2}$$

- (c) Positive integers  $c_0, \dots, c_{11}$ , the *cofactors*, with  $\min_i c_i = 1$ .

(d) Two finite ordered lists  $\Gamma_E$  and  $\Gamma_{E'}$  of nonzero integers.

For  $(M, N) \in \mathbb{Z}^2$  with  $F(M, N)H(M, N)J(M, N) \neq 0$ , the curves of  $\mathfrak{D}$  are

$$E_{M,N}: y^2 = x^3 + AFx^2 - BFHx, \quad E'_{M,N}: y^2 = x^3 - 2AFx^2 + CFJx, \quad (4.3)$$

where  $F, H, J$  are evaluated at  $(M, N)$ .

Throughout this section, we fix a twelve-form datum  $\mathfrak{D}$ . We write

$$I_F = \{0, 1, 2, 3\}, \quad I_H = \{4, 5, 6, 7\}, \quad I_J = \{8, 9, 10, 11\}, \quad (4.4)$$

so that  $F = \prod_{i \in I_F} L_i$ ,  $H = \prod_{i \in I_H} L_i$  and  $J = \prod_{i \in I_J} L_i$ . The moving index sets and the opposite index sets of the two curves are

$$G_E = I_F \cup I_H, \quad G_{E'} = I_F \cup I_J, \quad O_E = I_J, \quad O_{E'} = I_H. \quad (4.5)$$

The symbol  $\star$  stands for either  $E$  or  $E'$ . When  $(M, N)$  is fixed, we write  $E = E_{M,N}$  and  $E' = E'_{M,N}$ , and we write

$$\alpha = AF, \quad \beta = -BFH, \quad \alpha' = -2AF, \quad \beta' = CFJ \quad (4.6)$$

for their coefficients, so that  $E = E_{\alpha,\beta}$  and  $E' = E_{\alpha',\beta'}$  in the notation of (3.6). We let  $\delta_E, \delta_{E'}$  be their descent maps (Definition 3.3),  $\delta_{E,v}, \delta_{E',v}$  the local descent maps, and

$$d_E = \dim_{\mathbb{F}_2} \delta_E(E(\mathbb{Q})), \quad d_{E'} = \dim_{\mathbb{F}_2} \delta_{E'}(E'(\mathbb{Q})). \quad (4.7)$$

Condition (a) of Definition 4.1 says that the twelve forms are primitive and pairwise nonproportional, so that their zeros are twelve distinct points of  $\mathbb{P}^1$ . The cofactors and the lists  $\Gamma_E, \Gamma_{E'}$  are used only from Section 4.2 on.

**Lemma 4.2** (Basic properties of the curves). *Let  $(M, N) \in \mathbb{Z}^2$  with  $FHJ \neq 0$ .*

- (a) *We have  $\alpha^2 - 4\beta = CFJ = \beta'$  and  $\alpha'^2 - 4\beta' = 16\beta$ . In particular,  $E'_{M,N}$  is the curve  $E_{\alpha',\beta'}$  of (3.7), and the maps  $\phi$  and  $\hat{\phi}$  of (3.8) are the 2-isogenies between  $E_{M,N}$  and  $E'_{M,N}$ .*
- (b) *The discriminants of the models (4.3) are*

$$\Delta(E_{M,N}) = 16B^2CF^3H^2J, \quad \Delta(E'_{M,N}) = -256BC^2F^3HJ^2. \quad (4.8)$$

*Both are nonzero, and  $E_{M,N}$  and  $E'_{M,N}$  are elliptic curves over  $\mathbb{Q}$ .*

- (c) *Let  $(M_1, N_1) = (\lambda M, \lambda N) \in \mathbb{Z}^2$  with  $\lambda \in \mathbb{Q}^\times$ . Then  $(x, y) \mapsto (\lambda^4 x, \lambda^6 y)$  is an isomorphism over  $\mathbb{Q}$  from  $E_{M,N}$  to  $E_{M_1,N_1}$ , and from  $E'_{M,N}$  to  $E'_{M_1,N_1}$ . It preserves the class  $[x]$  of every point with  $x \neq 0$ .*

*Proof.* By (4.1), we have

$$\alpha^2 - 4\beta = A^2F^2 + 4BFH = F(A^2F + 4BH) = CFJ, \quad (4.9)$$

and then  $\alpha'^2 - 4\beta' = 4\alpha^2 - 4(\alpha^2 - 4\beta) = 16\beta$ . This proves (a). For a curve  $y^2 = x^3 + ax^2 + bx$ , the standard formulas [43, Section III.1] give

$$c_4 = 16(a^2 - 3b), \quad \Delta = 16b^2(a^2 - 4b). \quad (4.10)$$

For  $E_{M,N}$ , we obtain  $\Delta = 16\beta^2(\alpha^2 - 4\beta) = 16B^2F^2H^2 \cdot CFJ$ , and for  $E'_{M,N}$ , we obtain  $\Delta = 16\beta'^2(\alpha'^2 - 4\beta') = 16C^2F^2J^2 \cdot 16\beta = -256BC^2F^3HJ^2$ . These are nonzero because  $B$ ,  $C$  and  $FHJ$  are nonzero. For (c), since each of  $F$ ,  $H$ ,  $J$  is homogeneous of degree four, the coefficients of  $E_{M_1,N_1}$  are  $\lambda^4\alpha$  and  $\lambda^8\beta$ . Then

$$(\lambda^6y)^2 - (\lambda^4x)^3 - \lambda^4\alpha(\lambda^4x)^2 - \lambda^8\beta(\lambda^4x) = \lambda^{12}(y^2 - x^3 - \alpha x^2 - \beta x), \quad (4.11)$$

and the same computation applies to  $E'$ . Finally,  $[\lambda^4x] = [x]$ .  $\square$

**Lemma 4.3** (The  $j$ -invariant). *Let  $\mathcal{N}$  and  $\mathcal{D}$  be the binary forms of degree 12 given by*

$$\mathcal{N} = 256(A^2F + 3BH)^3, \quad \mathcal{D} = B^2CH^2J. \quad (4.12)$$

- (a) *For  $(M, N) \in \mathbb{Z}^2$  with  $FHJ \neq 0$ , we have  $j(E_{M,N}) = \mathcal{N}(M, N) / \mathcal{D}(M, N)$ .*
- (b) *The forms  $\mathcal{N}$  and  $\mathcal{D}$  have no common zero in  $\mathbb{P}^1(\overline{\mathbb{Q}})$ , and  $[M : N] \mapsto [\mathcal{N}(M, N) : \mathcal{D}(M, N)]$  is a morphism  $\mathbb{P}^1 \rightarrow \mathbb{P}^1$  of degree 12. For every  $j_0 \in \mathbb{Q}$ , at most 12 points  $[M : N] \in \mathbb{P}^1(\mathbb{Q})$  with  $FHJ(M, N) \neq 0$  satisfy  $j(E_{M,N}) = j_0$ .*
- (c) *Let  $\mathcal{Q} \subseteq \mathbb{Z}^2$  be a set of pairs with  $FHJ \neq 0$  at every point of  $\mathcal{Q}$ , such that the points  $[M : N]$  with  $(M, N) \in \mathcal{Q}$  are infinitely many. Then the curves  $E_{M,N}$  with  $(M, N) \in \mathcal{Q}$  lie in infinitely many isomorphism classes over  $\overline{\mathbb{Q}}$ .*

*Proof.* By (4.10), we have  $j = c_4^3 / \Delta = 256(a^2 - 3b)^3 / (b^2(a^2 - 4b))$  for the curve  $y^2 = x^3 + ax^2 + bx$ . For  $E_{M,N}$ , we have  $\alpha^2 - 3\beta = A^2F^2 + 3BFH = F(A^2F + 3BH)$ ,  $\beta^2 = B^2F^2H^2$  and  $\alpha^2 - 4\beta = CFJ$ . Inserting these into the formula for  $j$ , we obtain

$$j(E_{M,N}) = \frac{256F^3(A^2F + 3BH)^3}{B^2F^2H^2 \cdot CFJ} = \frac{256(A^2F + 3BH)^3}{B^2CH^2J}. \quad (4.13)$$

This proves (a).

The zero of  $L_i$  in  $\mathbb{P}^1(\overline{\mathbb{Q}})$  is the point  $[b_i : -a_i]$ , and these twelve points are distinct because  $\Delta_{ij} \neq 0$  for  $i \neq j$ . Since  $B, C \neq 0$ , the zeros of  $\mathcal{D}$  are the zeros of  $L_i$  with  $i \in I_H \cup I_J$ . At a zero of  $L_i$  with  $i \in I_H$ , we have  $H = 0$  and  $F \neq 0$ , which gives  $A^2F + 3BH = A^2F \neq 0$ . At a zero of  $L_i$  with  $i \in I_J$ , we have  $J = 0$  and  $H \neq 0$ , and (4.1) implies that  $A^2F = -4BH$ ; then  $A^2F + 3BH = -BH \neq 0$ . We conclude that  $\mathcal{N}$  and  $\mathcal{D}$  have no common zero. As both

have degree 12, the map has degree 12. Let  $j_0 \in \mathbb{Q}$ . The form  $\mathcal{N} - j_0\mathcal{D}$  is not zero, since otherwise  $\mathcal{N}$  would vanish at the zeros of  $\mathcal{D}$ . As a nonzero binary form of degree 12, it has at most 12 zeros in  $\mathbb{P}^1(\overline{\mathbb{Q}})$ . If  $FHJ(M, N) \neq 0$  and  $j(E_{M,N}) = j_0$ , then  $\mathcal{D}(M, N) \neq 0$ , and (a) implies that  $(\mathcal{N} - j_0\mathcal{D})(M, N) = 0$ . This proves (b).

For (c), two elliptic curves over  $\overline{\mathbb{Q}}$  are isomorphic if and only if they have the same  $j$ -invariant [43, Proposition III.1.4(b)]. If the curves  $E_{M,N}$  with  $(M, N) \in \mathcal{Q}$  lay in finitely many classes, then  $j(E_{M,N})$  would take finitely many values on  $\mathcal{Q}$ , and by (b) the points  $[M : N]$  would be finitely many.  $\square$

*Remark 4.4* (The  $j$ -invariants of the three families). For the data of Sections 6 to 8, Lemma 4.3(a) gives the following  $j$ -invariants; in the rank-seven family,  $33124 = 182^2$ .

| Family     | $(A, B, C)$           | $j(E_{M,N})$                                                                 |
|------------|-----------------------|------------------------------------------------------------------------------|
| Rank five  | $(1500, 2700, 57600)$ | $\frac{4}{9} \cdot \frac{(2500F + 9H)^3}{H^2J}$                              |
| Rank six   | $(70, 784, 1764)$     | $\frac{16}{9} \cdot \frac{(25F + 12H)^3}{H^2J}$                              |
| Rank seven | $(91205, 33124, 9)$   | $\frac{256}{9 \cdot 182^4} \cdot \frac{(91205^2F + 3 \cdot 182^2H)^3}{H^2J}$ |

For example, in the rank-five family  $A^2F + 3BH = 900(2500F + 9H)$  and  $256 \cdot 900^3 / (2700^2 \cdot 57600) = 4/9$ .

*Remark 4.5* (The associated elliptic surfaces). The homogeneous equations define Weierstrass models over the projective parameter line, with coefficients  $\alpha$  and  $\beta$  of degrees four and eight. In either projective chart, the formulas in (4.10) give

$$c_4(E) = 16F(A^2F + 3BH), \quad \Delta(E) = 16B^2CF^3H^2J.$$

The twelve forms have distinct zeros. At the zeros of  $F$ ,  $H$  and  $J$ , the orders of  $(c_4, \Delta)$  are  $(1, 3)$ ,  $(0, 2)$  and  $(0, 1)$ , respectively; at a zero of  $J$ , we use  $A^2F + 3BH = -BH$ . These models are minimal because the discriminant orders are less than 12 [49, p. 40, Remark 1]. Tate's algorithm gives four fibers of type III, four of type  $I_2$  and four of type  $I_1$  [49, p. 34]; see also [40, §4.5, Table 1]. For  $E'$ , the types at  $H$  and  $J$  are interchanged. There are no other singular fibers, and the minimal discriminant divisor has degree 24. Thus the relatively minimal smooth elliptic surfaces have  $\chi(\mathcal{O}) = 2$ . Over the base  $\mathbb{P}^1$ , the canonical bundle formula and  $h^1(\mathcal{O}) = 0$  then show that they are K3 surfaces [40, Theorems 6.8 and 6.12 and §8.2].

## 4.2 Prime specializations

**Definition 4.6** (Prime specializations). Let  $S$  be a finite set of primes that contains every prime dividing

$$6ABC \prod_{i=0}^{11} c_i \prod_{i=1}^{11} b_i \prod_{0 \leq i < j \leq 11} \Delta_{ij} \quad (4.14)$$

and every prime dividing an entry of  $\Gamma_E$  or  $\Gamma_{E'}$ . A pair  $(M, N) \in \mathbb{Z}^2$  is a *prime specialization* of  $\mathfrak{D}$  (with respect to  $S$ ) if  $c_i$  divides  $L_i(M, N)$  for  $0 \leq i \leq 11$  and the twelve numbers

$$p_i = \frac{L_i(M, N)}{c_i}, \quad 0 \leq i \leq 11, \quad (4.15)$$

are distinct primes, none of which lies in  $S$ .

In Sections 6 to 8, the divisibility  $c_i \mid L_i(M, N)$  and the residues of the numbers  $L_i(M, N)/c_i$  come from a congruence condition on  $(M, N)$ , through the following elementary fact.

**Lemma 4.7** (Divisibility and residues on a congruence class). *Let  $L = aM + bN$  with  $a, b \in \mathbb{Z}$ , let  $W_0$  be a positive integer, and let  $(m, n) \in \mathbb{Z}^2$ . Let  $c$  be a positive integer that divides both  $W_0$  and  $L(m, n)$ . Then every  $(M, N) \in \mathbb{Z}^2$  with  $(M, N) \equiv (m, n) \pmod{W_0}$  satisfies  $c \mid L(M, N)$  and*

$$\frac{L(M, N)}{c} \equiv \frac{L(m, n)}{c} \pmod{W_0/c}. \quad (4.16)$$

*In particular, if  $q$  is a prime that divides  $W_0/c$  and does not divide  $L(m, n)/c$ , then  $v_q(L(M, N)) = v_q(c)$ .*

*Proof.* Since  $M - m$  and  $N - n$  are divisible by  $W_0$ , there exists  $s \in \mathbb{Z}$  such that  $L(M, N) = L(m, n) + W_0 s$ . Dividing by  $c$ , we obtain

$$\frac{L(M, N)}{c} = \frac{L(m, n)}{c} + \frac{W_0}{c} s, \quad (4.17)$$

where both terms on the right are integers. This proves that  $c$  divides  $L(M, N)$  and that (4.16) holds. If  $q \mid W_0/c$  and  $q \nmid L(m, n)/c$ , then (4.16) shows that  $L(M, N)/c$  is an integer prime to  $q$ , which implies that  $v_q(L(M, N)) = v_q(c)$ .  $\square$

At a prime specialization, we write  $\lambda_i$  for the restriction of the character  $\chi_{p_i}$  of (3.1) to the integers prime to  $p_i$ , so that  $(z/p_i) = (-1)^{\lambda_i(z)}$  for such integers  $z$ . We set

$$\kappa_E = -B \prod_{j \in G_E} c_j, \quad \kappa_{E'} = C \prod_{j \in G_{E'}} c_j. \quad (4.18)$$

The *ambient list*  $\mathcal{B}_\star$  consists of the entries of  $\Gamma_\star$ , in their order, followed by the primes  $p_j$  with  $j \in G_\star$ , in increasing order of  $j$ ; its length is  $n_\star = |\Gamma_\star| + 8$ . We index the entries of

a vector in  $\mathbb{F}_2^{n_\star}$  by the entries  $g$  of  $\Gamma_\star$ , which we call the constant columns, and by the indices  $j \in G_\star$ , which we call the moving columns. We let  $u_\star \in \mathbb{F}_2^{n_\star}$  be the vector with entry 0 at each constant column and 1 at each moving column.

**Lemma 4.8** (Basic properties of prime specializations). *Let  $(M, N)$  be a prime specialization.*

- (a) *The product  $FHJ$  is nonzero, and  $E = E_{M,N}$  and  $E' = E'_{M,N}$  are elliptic curves. Each  $p_i$  is odd, and it divides none of the integers  $A, B, C, c_j$  (for all  $j$ ),  $b_j$  (for  $j \geq 1$ ) and  $\Delta_{jk}$  (for  $j \neq k$ ), and no entry of  $\Gamma_E$  or  $\Gamma_{E'}$ .*
- (b) *For all  $i$  and  $j$ , the valuation  $v_{p_i}(L_j)$  is 1 if  $i = j$  and 0 if  $i \neq j$ .*
- (c) *The integers  $M$  and  $N$  are coprime,  $M = c_0 p_0$ , and  $p_0 \nmid N$ .*
- (d) *The valuation  $v_{p_0}(CFJ)$  is 1. In particular,  $CFJ = \alpha^2 - 4\beta$  is not a square in  $\mathbb{Q}$ , and  $E(\mathbb{Q})[2] = \{O, T\}$ .*
- (e) *The coefficients satisfy  $\beta = \kappa_E \prod_{j \in G_E} p_j$  and  $\beta' = \kappa_{E'} \prod_{j \in G_{E'}} p_j$ .*
- (f) *If  $\Gamma_\star$  consists of  $-1$  and distinct primes, then the classes of the entries of  $\mathcal{B}_\star$  are linearly independent in  $\mathbb{Q}^\times / \mathbb{Q}^{\times 2}$ .*
- (g) *If  $\Gamma_\star$  contains  $-1$  and every prime dividing  $\kappa_\star$ , then  $\delta_\star(\star(\mathbb{Q}))$  is contained in the span of the classes of the entries of  $\mathcal{B}_\star$ .*

*In particular, if  $\Gamma_\star$  consists of  $-1$  and distinct primes, including every prime dividing  $\kappa_\star$ , then  $\mathcal{B}_\star$  is an ambient basis for  $\star$  in the sense of Definition 3.9.*

*Proof.* We have  $L_i(M, N) = c_i p_i \neq 0$  for every  $i$ . Then  $FHJ \neq 0$ , and Lemma 4.2(b) shows that  $E$  and  $E'$  are elliptic curves. The prime 2 divides (4.14) and lies in  $S$ , and each  $p_i$  is odd. The rest of (a) holds because  $p_i \notin S$ . For (b), we have  $L_j = c_j p_j$  with  $p_i \nmid c_j$  by (a), and  $p_i \neq p_j$  for  $j \neq i$ .

For (c), let  $q$  be a prime dividing both  $M$  and  $N$ . Then  $q$  divides  $L_i = c_i p_i$  for every  $i$ . By Definition 4.1(c), there exists  $i_1$  with  $c_{i_1} = 1$ , and then  $q = p_{i_1}$ . For  $i \neq i_1$ , we have  $q \neq p_i$ , so that  $q$  divides  $c_i$ ; this contradicts (a) for the prime  $p_{i_1}$ . Hence  $\gcd(M, N) = 1$ . Since  $(a_0, b_0) = (1, 0)$ , we have  $M = L_0 = c_0 p_0$ , and then  $p_0 \nmid N$ .

For (d), part (b) implies that  $v_{p_0}(F) = 1$  and  $v_{p_0}(J) = 0$ , and  $p_0 \nmid C$  by (a). Then  $v_{p_0}(CFJ) = 1$  is odd, and  $CFJ$  is not a square in  $\mathbb{Q}$ . By Lemma 4.2(a),  $CFJ = \alpha^2 - 4\beta$ , and Lemma 3.7 with  $K = \mathbb{Q}$  shows that  $T$  is the only point of order two in  $E(\mathbb{Q})$ .

Part (e) follows from  $L_j = c_j p_j$  and the definitions (4.6) and (4.18). For (f), suppose that a product of entries of  $\mathcal{B}_\star$  is a square in  $\mathbb{Q}$ . For  $j \in G_\star$ , the prime  $p_j$  divides no other entry of  $\mathcal{B}_\star$ , by (a) and since the  $p_i$  are distinct. The valuation at  $p_j$  then shows that  $p_j$  occurs to an even power. The valuations at the primes of  $\Gamma_\star$  show the same for these primes, and then the sign shows it for  $-1$ .

For (g), the coefficients  $\alpha, \beta$  and  $\alpha', \beta'$  are integers with  $\beta(\alpha^2 - 4\beta) \neq 0$  and  $\beta'(\alpha'^2 - 4\beta') \neq 0$ . By Lemma 3.6, every class in  $\delta_E(E(\mathbb{Q}))$  is the class of  $\pm 1$  times a product of distinct primes dividing  $\beta$ , and by (e) these primes divide  $\kappa_E$  or are equal to  $p_j$  with

$j \in G_E$ . The same argument applies to  $E'$  with  $\beta'$  and  $\kappa_{E'}$ . The final statement combines (f) and (g).  $\square$

**Lemma 4.9** (Local images at the moving primes). *Let  $(M, N)$  be a prime specialization, let  $0 \leq i \leq 11$ , and let  $p = p_i$ .*

- (a) *If  $i \in I_F$ , then  $\delta_{E,p}(E(\mathbb{Q}_p)) = \{[1], [\beta]\}$  and  $\delta_{E',p}(E'(\mathbb{Q}_p)) = \{[1], [\beta']\}$ .*
- (b) *If  $i \in I_J$ , then  $\delta_{E,p}(E(\mathbb{Q}_p)) = \{[1]\}$ .*
- (c) *If  $i \in I_H$ , then  $\delta_{E',p}(E'(\mathbb{Q}_p)) = \{[1]\}$ .*

*Proof.* By Lemma 4.8(a) and (b), the prime  $p$  is odd and does not divide  $ABC$ . Further,  $v_p(F) = 1$  if  $i \in I_F$  and  $v_p(F) = 0$  otherwise, and similarly for  $H$  with  $I_H$  and for  $J$  with  $I_J$ . By (4.6) and Lemma 4.2(a), the valuations of the coefficients are as follows.

| $i \in$ | $v_p(\alpha) = v_p(\alpha')$ | $v_p(\beta)$ | $v_p(\beta')$ | Case of Lemma 3.8                                    |
|---------|------------------------------|--------------|---------------|------------------------------------------------------|
| $I_F$   | 1                            | 1            | 1             | (a) for $E$ and for $E'$                             |
| $I_J$   | 0                            | 0            | 1             | (b) for $E$ , since $\alpha^2 - 4\beta = \beta'$     |
| $I_H$   | 0                            | 1            | 0             | (b) for $E'$ , since $\alpha'^2 - 4\beta' = 16\beta$ |

If  $i \in I_F$ , then  $v_p(\alpha) \geq 1$  and  $v_p(\beta) = 1$ , and Lemma 3.8(a) shows that  $\delta_{E,p}(E(\mathbb{Q}_p)) = \{[1], [\beta]\}$ ; the same holds for  $E'$ , with  $\alpha', \beta'$  in place of  $\alpha, \beta$ . If  $i \in I_J$ , then  $\alpha$  and  $\beta$  are units and  $v_p(\alpha^2 - 4\beta) = v_p(\beta') = 1$ , and Lemma 3.8(b) gives (b). If  $i \in I_H$ , then  $\alpha'$  and  $\beta'$  are units and  $v_p(\alpha'^2 - 4\beta') = v_p(16\beta) = 1$ , and (c) follows from Lemma 3.8(b).  $\square$

### 4.3 Rows at the moving primes

The following rows encode Lemma 4.9 in the coordinates of Lemma 3.2(a). By Lemma 4.8(a) and (b), every integer to which we apply  $\lambda_i$  below is prime to  $p_i$ .

**Definition 4.10** (Moving rows). Let  $(M, N)$  be a prime specialization and  $\star \in \{E, E'\}$ . For  $i \in I_F$ , the moving row  $r_i^\star \in \mathbb{F}_2^{n_\star}$  has the entries

$$\begin{array}{ll}
 \lambda_i(g) & \text{at each constant column } g, \\
 \lambda_i(p_j) & \text{at each moving column } j \in G_\star \setminus \{i\}, \\
 \lambda_i(\kappa_\star) + \sum_{j \in G_\star \setminus \{i\}} \lambda_i(p_j) & \text{at the moving column } i.
 \end{array} \tag{4.19}$$

For  $i \in O_\star$ , the moving row  $r_i^\star$  has entry  $\lambda_i(g)$  at each constant column  $g$  and entry  $\lambda_i(p_j)$  at each moving column  $j \in G_\star$ .

**Lemma 4.11** (Conditions at the moving primes). *Let  $(M, N)$  be a prime specialization,  $\star \in \{E, E'\}$  and  $i \in I_F \cup O_\star$ . Then  $r_i^\star$  is a row for  $\star$  and  $\mathcal{B}_\star$  at the place  $p_i$ , in the sense of Definition 3.9. In particular,  $r_i^\star \cdot \mathbf{w} = 0$  for every  $\mathbf{w} \in \mathbb{F}_2^{n_\star}$  such that  $[\mathbf{w}]_{\mathcal{B}_\star} \in \delta_\star(\star(\mathbb{Q}))$ .*

*Proof.* Let  $p = p_i$ . We use the coordinates  $[z] \mapsto (\nu_p(z), \chi_p(z))$  of (3.3), so that  $[p^k u_0] \mapsto (k \bmod 2, \chi_p(u_0))$  for  $u_0 \in \mathbb{Z}_p^\times$ . Every entry of  $\mathcal{B}_\star$  other than  $p_i$  is a  $p$ -adic unit, and its class has coordinates  $(0, \lambda_i(g))$  or  $(0, \lambda_i(p_j))$ ; if  $p_i$  is an entry of  $\mathcal{B}_\star$ , its class has coordinates  $(1, 0)$ .

Let  $i \in I_F$ , and take  $\star = E$ ; for  $\star = E'$ , replace  $\beta$  and  $\kappa_E$  by  $\beta'$  and  $\kappa_{E'}$ . By Lemma 4.9(a), the local image  $\delta_{E,p}(E(\mathbb{Q}_p))$  is the subgroup  $U_p = \{[1], [\beta]\}$ . By Lemma 4.8(e), we have  $\beta = p_i w$  with  $w = \kappa_E \prod_{j \in G_E \setminus \{i\}} p_j$  a  $p$ -adic unit. The class  $[\beta]$  has coordinates  $(1, h)$  with

$$h = \lambda_i(w) = \lambda_i(\kappa_E) + \sum_{j \in G_E \setminus \{i\}} \lambda_i(p_j). \quad (4.20)$$

The linear map  $f(k, \ell) = \ell + hk$  vanishes on  $U_p = \{(0, 0), (1, h)\}$ . Its values at the classes of the entries of  $\mathcal{B}_E$  are  $\lambda_i(g)$  at a constant column  $g$ ,  $\lambda_i(p_j)$  at a moving column  $j \neq i$ , and  $h$  at the moving column  $i$ . These are the entries (4.19), and  $r_i^E$  is the row defined by  $(p_i, U_p, f)$ .

Let  $i \in O_\star$ . Then  $i \notin G_\star$ , and Lemma 4.9(b) (for  $\star = E$ ) or (c) (for  $\star = E'$ ) shows that the local image at  $p$  is  $U_p = \{[1]\}$ . The map  $f(k, \ell) = \ell$  vanishes on  $U_p$ , and its values at the entries of  $\mathcal{B}_\star$  are the entries of  $r_i^\star$ . (The other coordinate  $k$  vanishes at every entry of  $\mathcal{B}_\star$  and gives the zero row.) The last statement of the lemma is Lemma 3.10.  $\square$

#### 4.4 Reciprocity and the sign $\varepsilon$

The entries of the moving rows are characters  $\lambda_i(g)$  and  $\lambda_i(\kappa_\star)$  of fixed integers, and characters  $\lambda_i(p_j)$  of one moving prime at another. We now express the latter through characters of fixed integers and the single sign

$$\varepsilon = \left( \frac{N}{p_0} \right) = (-1)^\eta, \quad \eta \in \mathbb{F}_2, \quad (4.21)$$

which is defined at every prime specialization because  $p_0 \nmid N$  (Lemma 4.8(c)). We use quadratic reciprocity and its two supplementary laws [21, Chapter 5, Section 2, Theorem 1, p. 53]. In the notation (3.1), they state that, for distinct odd primes  $p$  and  $q$ ,

$$\begin{aligned} \chi_p(-1) &= \frac{p-1}{2} \bmod 2, & \chi_p(2) &= \frac{p^2-1}{8} \bmod 2, \\ \chi_p(q) + \chi_q(p) &= \chi_p(-1)\chi_q(-1). \end{aligned} \quad (4.22)$$

The determinant elimination and one-sign reduction below are analogous to the Gaussian reciprocity calculation in [38, Lemma 4.1].

**Lemma 4.12** (Reciprocity for the prime values). *Let  $(M, N)$  be a prime specialization, and let  $\varepsilon = (N/p_0)$ .*

- (a) For  $1 \leq i \leq 11$ , the symbol  $(p_i/p_0)$  is equal to  $(b_i c_i/p_0)\varepsilon$ .  
 (b) For  $1 \leq i \leq 11$ , we have  $(p_0/p_i) = (-1)^{(p_0-1)(p_i-1)/4}(p_i/p_0)$ .  
 (c) For distinct  $i, j$  with  $1 \leq i, j \leq 11$ , we have  $b_i L_j \equiv \Delta_{ji} M \pmod{p_i}$ , and hence

$$\left(\frac{p_j}{p_i}\right) = \left(\frac{c_0 c_j b_i \Delta_{ji}}{p_i}\right) \left(\frac{p_0}{p_i}\right). \quad (4.23)$$

*Proof.* For (a), recall that  $M = c_0 p_0$  (Lemma 4.8(c)). Reducing  $c_i p_i = a_i M + b_i N$  modulo  $p_0$ , we find  $c_i p_i \equiv b_i N \pmod{p_0}$ . The integers  $c_i$ ,  $b_i$  and  $N$  are prime to  $p_0$ , by Lemma 4.8(a) and (c). Taking Legendre symbols, we have  $(c_i/p_0)(p_i/p_0) = (b_i/p_0)\varepsilon$ , and multiplying by  $(c_i/p_0) = (c_i/p_0)^{-1}$ , we obtain (a). Part (b) is quadratic reciprocity for the distinct odd primes  $p_0$  and  $p_i$ .

For (c), we have  $a_i M + b_i N = c_i p_i \equiv 0 \pmod{p_i}$ , that is,  $b_i N \equiv -a_i M \pmod{p_i}$ . Then

$$b_i L_j = a_j b_i M + b_j (b_i N) \equiv (a_j b_i - a_i b_j) M = \Delta_{ji} M \pmod{p_i}. \quad (4.24)$$

Inserting  $L_j = c_j p_j$  and  $M = c_0 p_0$ , we obtain  $b_i c_j p_j \equiv \Delta_{ji} c_0 p_0 \pmod{p_i}$ . All factors are prime to  $p_i$  by Lemma 4.8(a), and taking Legendre symbols and multiplying by  $(b_i c_j/p_i)$ , we find (4.23).  $\square$

The characters of fixed integers are determined by residues, by the following consequence of (4.22).

**Lemma 4.13** (Characters of fixed integers). *Let  $z = (-1)^\sigma 2^e \prod_q q^{f_q}$  be a nonzero integer, where  $\sigma \in \{0, 1\}$ ,  $e \geq 0$ , and  $q$  runs over the odd primes dividing  $z$ . Let  $p$  be an odd prime not dividing  $z$ . Then*

$$\chi_p(z) = \sigma \chi_p(-1) + e \chi_p(2) + \sum_q f_q (\chi_q(p) + \chi_p(-1) \chi_q(-1)). \quad (4.25)$$

*In particular,  $\chi_p(z)$  depends only on the residues of  $p$  modulo 8 and modulo the odd primes that divide  $z$  to an odd power.*

*Proof.* The map  $\chi_p$  is additive, and (4.22) gives  $\chi_p(q) = \chi_q(p) + \chi_p(-1) \chi_q(-1)$  for each odd prime  $q \neq p$ . This proves (4.25). By (4.22),  $\chi_p(-1)$  and  $\chi_p(2)$  depend only on  $p$  modulo 8, and  $\chi_q(p)$  depends only on  $p$  modulo  $q$ . The terms with  $f_q$  even vanish in  $\mathbb{F}_2$ .  $\square$

At a prime specialization, we define the following bits. For  $1 \leq i \leq 11$ , let

$$\theta_i = \lambda_0(b_i c_i) + \lambda_0(-1) \lambda_i(-1). \quad (4.26)$$

For distinct  $i, j \in \{0, \dots, 11\}$ , let

$$\gamma_{ij} = \begin{cases} \lambda_0(b_j c_j) & \text{if } i = 0, \\ \theta_i & \text{if } j = 0, \\ \lambda_i(c_0 c_j b_i \Delta_{ji}) + \theta_i & \text{if } i, j \geq 1, \end{cases} \quad (4.27)$$

and for  $\star \in \{E, E'\}$  and  $i \in I_F$ , let

$$\gamma_{ii}^* = \lambda_i(\kappa_\star) + \sum_{j \in G_\star \setminus \{i\}} \gamma_{ij}. \quad (4.28)$$

**Corollary 4.14** (The moving rows as functions of  $\varepsilon$ ). *Let  $(M, N)$  be a prime specialization, and let  $\varepsilon = (-1)^\eta$  be as in (4.21). Then  $\lambda_i(p_j) = \gamma_{ij} + \eta$  for all distinct  $i, j \in \{0, \dots, 11\}$ . For  $\star \in \{E, E'\}$  and  $i \in I_F \cup O_\star$ , the moving row  $r_i^*$  has entry  $\lambda_i(g)$  at each constant column  $g$ , entry  $\gamma_{ij} + \eta$  at each moving column  $j \neq i$ , and, if  $i \in I_F$ , entry  $\gamma_{ii}^* + \eta$  at the moving column  $i$ . In other words,*

$$r_i^* = r_i^*(0) + \eta u_\star, \quad (4.29)$$

where  $r_i^*(0) \in \mathbb{F}_2^{n_\star}$  is the vector with entries  $\lambda_i(g)$  at the constant columns,  $\gamma_{ij}$  at the moving columns  $j \neq i$ , and  $\gamma_{ii}^*$  at the moving column  $i$  if  $i \in I_F$ .

*Proof.* Let  $j \geq 1$ . Then Lemma 4.12(a) implies that  $\lambda_0(p_j) = \lambda_0(b_j c_j) + \eta = \gamma_{0j} + \eta$ . Let  $i \geq 1$ . By Lemma 4.12(b) and (4.22), we have  $\lambda_i(p_0) = \lambda_0(p_i) + \lambda_0(-1)\lambda_i(-1)$ , which is  $\theta_i + \eta = \gamma_{i0} + \eta$  by the case just treated. For distinct  $i, j \geq 1$ , we find from (4.23) that

$$\lambda_i(p_j) = \lambda_i(c_0 c_j b_i \Delta_{ji}) + \lambda_i(p_0) = \lambda_i(c_0 c_j b_i \Delta_{ji}) + \theta_i + \eta = \gamma_{ij} + \eta. \quad (4.30)$$

This proves the first statement. The entries of  $r_i^*$  at the moving columns  $j \neq i$  are  $\lambda_i(p_j) = \gamma_{ij} + \eta$ , by Definition 4.10. For  $i \in I_F$ , the entry at the moving column  $i$  is

$$\lambda_i(\kappa_\star) + \sum_{j \in G_\star \setminus \{i\}} (\gamma_{ij} + \eta) = \gamma_{ii}^* + 7\eta = \gamma_{ii}^* + \eta, \quad (4.31)$$

since  $G_\star$  has eight elements and contains  $i$ . The entries at the constant columns do not involve  $\eta$ . Since  $u_\star$  has entry 1 exactly at the moving columns, this proves (4.29).  $\square$

**Remark 4.15** (Which characters must be controlled). The bits  $\lambda_i(g)$ ,  $\lambda_i(\kappa_\star)$ ,  $\theta_i$ ,  $\gamma_{ij}$  and  $\gamma_{ii}^*$  are characters at  $p_0$  or  $p_i$  of the fixed integers  $-1$ ,  $g \in \Gamma_\star$ ,  $\kappa_\star$ ,  $b_j c_j$  and  $c_0 c_j b_i \Delta_{ji}$ , together with the products  $\lambda_0(-1)\lambda_i(-1)$ . By Lemma 4.13, they are determined by the residues of  $p_0, \dots, p_{11}$  modulo 8 and modulo the odd primes that divide one of these integers to an odd power; in Sections 6 to 8, a congruence condition on  $(M, N)$  fixes the residues that are needed. Only the pairs  $(i, j)$  with  $i \in I_F \cup O_\star$  and  $j \in G_\star \setminus \{i\}$  occur in the moving rows of  $\star$ . For  $\star = E$ , these pairs lie in  $I_F \times I_F$ ,  $I_F \times I_H$ ,  $I_J \times I_F$  or  $I_J \times I_H$ , and for  $\star = E'$ , they lie in  $I_F \times I_F$ ,  $I_F \times I_J$ ,  $I_H \times I_F$  or  $I_H \times I_J$ . No pair with both indices in  $I_H$ , or both in  $I_J$ , occurs. The determinants  $\Delta_{ji}$  of such pairs do not enter any moving row, and an odd prime that divides the integers above, for the pairs that occur, only to even powers needs no congruence condition.

**Remark 4.16** (The three families). The results of this section make no assumption on  $p_0$  modulo 4 or on the form  $L_1$ , and they apply to the three families without change. In

the families of Sections 6 to 8, we have  $c_0 = 54, 1$  and  $18$ , and  $p_0 \equiv 1, 3$  and  $1 \pmod{8}$ , respectively. Then  $\lambda_0(-1) = 0$  and  $\theta_i = \lambda_0(b_i c_i)$  in the rank-five and rank-seven families, while  $\theta_i = \lambda_0(b_i c_i) + \lambda_i(-1)$  in the rank-six family. In the rank-six and rank-seven families,  $L_1 = N$  and  $c_1 = 1$ , so that  $p_1 = N$  and  $\varepsilon = (p_1/p_0)$ .

## 4.5 The rank criterion

With the vectors  $r_i^*(0)$  held fixed, Corollary 4.14 shows that changing  $\varepsilon$  adds the same vector  $u_*$  to every moving row. The following lemma gives a condition under which this does not change the kernel. Its hypothesis cannot be omitted: a moving row equal to  $u_*$  becomes zero when  $\eta$  changes. A related common-kernel calculation for two quadratic-residue Laplacians is given in [38, Lemma 4.2].

**Lemma 4.17** (Both signs give the same kernel). *Let  $\mathbf{M}(0)$  and  $\mathbf{M}(1)$  be matrices over  $\mathbb{F}_2$  with  $n$  columns, whose rows are indexed by the same set  $R = R_f \sqcup R_m$  of fixed and moving rows. Write  $r_k(\eta)$  for the row of  $\mathbf{M}(\eta)$  with index  $k$ . Suppose that there exists  $u \in \mathbb{F}_2^n$  such that  $r_k(1) = r_k(0)$  for  $k \in R_f$  and  $r_k(1) = r_k(0) + u$  for  $k \in R_m$ , and that*

$$u = \sum_{k \in K} r_k(0) \quad (4.32)$$

for a set  $K \subseteq R$  such that  $K \cap R_m$  has an even number of elements. Then  $\mathbf{M}(0)$  and  $\mathbf{M}(1)$  have the same row space. In particular,  $\ker \mathbf{M}(1) = \ker \mathbf{M}(0)$  and  $\text{rank } \mathbf{M}(1) = \text{rank } \mathbf{M}(0)$ .

*Proof.* By the hypotheses, we have

$$\sum_{k \in K} r_k(1) = \sum_{k \in K} r_k(0) + |K \cap R_m| u = u, \quad (4.33)$$

since  $|K \cap R_m|$  is even. Together with (4.32), this shows that  $u$  lies in the row spaces of both matrices. Each row of  $\mathbf{M}(1)$  is the corresponding row of  $\mathbf{M}(0)$ , or that row plus  $u$ , and it lies in the row space of  $\mathbf{M}(0)$ . By symmetry, the two row spaces are equal. The kernel of a matrix consists of the vectors  $\mathbf{w}$  with  $r \cdot \mathbf{w} = 0$  for every  $r$  in its row space. Hence the kernels are equal, and so are the ranks.  $\square$

We now define the matrices of the rank criterion. Let  $\mathcal{P}$  be a set of prime specializations, and let  $\star \in \{E, E'\}$ . Suppose that we are given vectors  $f_1^*, \dots, f_{m_\star}^* \in \mathbb{F}_2^{n_\star}$ , and that the bits

$$\lambda_i(g) \ (i \in I_F \cup O_\star, g \in \Gamma_\star), \quad \lambda_i(\kappa_\star) \ (i \in I_F), \quad \gamma_{ij} \ (i \in I_F \cup O_\star, j \in G_\star \setminus \{i\}) \quad (4.34)$$

take the same values at every  $(M, N) \in \mathcal{P}$ . Then the vectors  $r_i^*(0)$  of Corollary 4.14 are the same at every  $(M, N) \in \mathcal{P}$ . For  $\eta \in \mathbb{F}_2$ , we let  $\mathbf{M}_\star(\eta)$  be the matrix with  $n_\star$  columns whose rows are

$$f_1^*, \dots, f_{m_\star}^*, \text{ then } r_i^*(0) + \eta u_\star \text{ for } i \in I_F, \text{ then } r_i^*(0) + \eta u_\star \text{ for } i \in O_\star, \quad (4.35)$$

with  $i$  increasing in each group. We call the first  $m_\star$  rows the fixed rows and the last eight rows the moving rows of  $\mathbf{M}_\star(\eta)$ . By Corollary 4.14, at a point of  $\mathcal{P}$  with  $\varepsilon = (-1)^\eta$ , the moving rows of  $\mathbf{M}_\star(\eta)$  are the moving rows  $r_i^\star$  of Definition 4.10.

**Proposition 4.18** (Rank criterion). *Let  $\mathfrak{D}$  be a twelve-form datum, let  $S$  be a set of primes as in Definition 4.6, and let  $\mathcal{P}$  be a set of prime specializations. Suppose that, for  $\star = E$  and for  $\star = E'$ , the list  $\Gamma_\star$  consists of  $-1$  and distinct primes, including every prime dividing  $\kappa_\star$ , and that the following hold.*

- (i) *Fixed rows. There exist vectors  $f_1^\star, \dots, f_{m_\star}^\star \in \mathbb{F}_2^{n_\star}$  such that, for every  $(M, N) \in \mathcal{P}$ , each  $f_k^\star$  is a row for  $\star_{M,N}$  and  $\mathcal{B}_\star$  in the sense of Definition 3.9.*
- (ii) *Constant characters. The bits (4.34) take the same values at every  $(M, N) \in \mathcal{P}$ . Let  $\mathbf{M}_\star(0)$  and  $\mathbf{M}_\star(1)$  be the matrices (4.35).*
- (iii) *Points. There exists an integer  $k_\star \geq 0$  such that, for every  $(M, N) \in \mathcal{P}$ , the image  $\delta_\star(\star_{M,N}(\mathbb{Q}))$  contains  $k_\star$  linearly independent classes.*
- (iv) *Rank. We have  $\text{rank } \mathbf{M}_\star(0) = n_\star - k_\star$ , and  $u_\star$  is the sum of a set of rows of  $\mathbf{M}_\star(0)$  that contains an even number of moving rows.*

Then every  $(M, N) \in \mathcal{P}$  satisfies  $d_E = k_E$ ,  $d_{E'} = k_{E'}$  and

$$\text{rank } E_{M,N}(\mathbb{Q}) = k_E + k_{E'} - 2. \quad (4.36)$$

Moreover,  $\delta_\star(\star_{M,N}(\mathbb{Q}))$  consists of the classes  $[\mathbf{w}]_{\mathcal{B}_\star}$  with  $\mathbf{w} \in \ker \mathbf{M}_\star(0)$ .

*Proof.* Fix  $(M, N) \in \mathcal{P}$  and  $\star \in \{E, E'\}$ , and let  $\eta \in \mathbb{F}_2$  be such that  $\varepsilon = (-1)^\eta$  at  $(M, N)$ . By Lemma 4.8, the list  $\mathcal{B}_\star$  is an ambient basis for  $\star$ . We first show that every row of  $\mathbf{M}_\star(\eta)$  is a row in the sense of Definition 3.9 at  $(M, N)$ . For the fixed rows, this is hypothesis (i). By hypothesis (ii) and Corollary 4.14, the moving rows of  $\mathbf{M}_\star(\eta)$  are the rows  $r_i^\star$  of Definition 4.10 at  $(M, N)$ , and these are rows by Lemma 4.11. By Lemma 3.10, the coordinate vectors of the classes in  $\delta_\star(\star(\mathbb{Q}))$  lie in  $\ker \mathbf{M}_\star(\eta)$ .

The matrices  $\mathbf{M}_\star(0)$  and  $\mathbf{M}_\star(1)$  satisfy the hypotheses of Lemma 4.17, with  $u = u_\star$ , by (4.35) and hypothesis (iv). This lemma implies that  $\ker \mathbf{M}_\star(\eta) = \ker \mathbf{M}_\star(0)$  and  $\text{rank } \mathbf{M}_\star(\eta) = n_\star - k_\star$ . By hypothesis (iii), there are  $k_\star$  linearly independent classes in  $\delta_\star(\star(\mathbb{Q}))$ , and their coordinate vectors are linearly independent. Applying Corollary 3.13 to  $\mathbf{M}_\star(\eta)$ , we find that  $d_\star = k_\star$  and that  $\delta_\star(\star(\mathbb{Q}))$  consists of the classes  $[\mathbf{w}]_{\mathcal{B}_\star}$  with  $\mathbf{w} \in \ker \mathbf{M}_\star(\eta) = \ker \mathbf{M}_\star(0)$ . Finally, by Lemma 3.5, we have  $\text{rank } E_{M,N}(\mathbb{Q}) = d_E + d_{E'} - 2 = k_E + k_{E'} - 2$ .  $\square$

In Sections 6 to 8, hypothesis (i) is a lemma on the local images at the fixed places, hypothesis (ii) follows from a congruence condition on  $(M, N)$  and Remark 4.15, hypothesis (iii) is verified with explicit points and Lemma 3.12, and hypothesis (iv) is a finite computation with a certificate that can be checked by hand. Since the criterion holds for

both values of  $\varepsilon$ , the prime specializations produced in Section 5 need not satisfy any condition on  $(N/p_0)$ .

## Linear equations in primes

The goal of this section is to prove Proposition 5.5. It states that a twelve-form datum has infinitely many prime specializations in a given congruence class and a given open cone, under conditions on the class and the cone that reduce to finite computations. The analytic input is the theorem of Green and Tao on linear equations in primes [18], which became unconditional through the work of Green and Tao [16] and of Green, Tao, and Ziegler [17]. In Section 5.1, we state the form of this theorem that we use, Theorem 5.1, and deduce it from the Main Theorem of [18]. In Section 5.2, we show that the main term in Theorem 5.1 does not change when we count only the points at which the values of the forms are distinct primes outside a finite set (Lemma 5.3). In Section 5.3, we compute the local factors of the affine forms obtained from binary linear forms by restricting the variables to a congruence class (Lemma 5.4). Section 5.4 combines these results. Apart from the analytic input, the section uses only the notions of Section 4: twelve-form data (Definition 4.1), prime specializations (Definition 4.6), and Lemmas 4.3 and 4.8. We use Proposition 5.5 to prove the infinitude statements in Theorems 6.7, 7.8, and 8.9.

Simultaneous prime values of linear forms have been used before to choose specializations of families. Harpaz, Skorobogatov, and Wittenberg [19] adapted the fibration method over  $\mathbb{Q}$  by replacing Schinzel’s hypothesis with the theorem of Green, Tao, and Ziegler. Their results concern suitable fibrations over the projective line whose degenerate fibers lie over rational points, and [19, Theorem 1.1 and Proposition 1.2] are two-variable statements of the kind we use. Zywna [55, Proposition 5.9] chose the specializations in his construction of elliptic curves of prescribed rank over number fields with the number-field version of this theorem due to Kai [23, Proposition 13.2]. Over  $\mathbb{Q}$ , we can use the theorem of Green, Tao, and Ziegler directly. We describe this history in more detail in Section 1.

**Notation.** Throughout this section, the letter  $q$  denotes a prime; we reserve  $p_i$  for the prime values of a datum. We write  $\Lambda$  for the von Mangoldt function, so that  $\Lambda(n) = \log q$  if  $n = q^k$  for a prime  $q$  and an integer  $k \geq 1$ , and  $\Lambda(n) = 0$  otherwise; in particular,  $\Lambda(n) = 0$  for  $n \leq 0$ . An affine-linear form on  $\mathbb{Z}^2$  is a map  $\ell: \mathbb{Z}^2 \rightarrow \mathbb{Z}$  of the form  $\ell(\mathbf{n}) = \langle \mathbf{w}, \mathbf{n} \rangle + \ell(\mathbf{0})$  with  $\mathbf{w} \in \mathbb{Z}^2$  and  $\ell(\mathbf{0}) \in \mathbb{Z}$ . Its linear part is  $\dot{\ell}(\mathbf{n}) = \langle \mathbf{w}, \mathbf{n} \rangle$ , and we extend  $\ell$  and  $\dot{\ell}$  to  $\mathbb{R}^2$  by the same formulas. For a set  $K \subset \mathbb{R}^2$  and  $R > 0$ , we write  $RK = \{R\mathbf{x} : \mathbf{x} \in K\}$ , and when  $K$  is convex, we write  $\text{area}(K)$  for its Lebesgue measure.

For affine-linear forms  $\ell_1, \dots, \ell_t$  and a prime  $q$ , the reductions of the  $\ell_i$  modulo  $q$  are functions on  $\mathbb{F}_q^2$ , and we define the local factor

$$\beta_q = \left( \frac{q}{q-1} \right)^t \frac{1}{q^2} \# \{ \mathbf{n} \in \mathbb{F}_q^2 : \ell_i(\mathbf{n}) \neq 0 \text{ for } 1 \leq i \leq t \}. \quad (5.1)$$

This is the local factor of [18, (1.6)], written as a count: there,  $\beta_q$  is the average over  $\mathbf{n} \in (\mathbb{Z}/q\mathbb{Z})^2$  of  $\prod_i \Lambda_{\mathbb{Z}/q\mathbb{Z}}(\ell_i(\mathbf{n}))$ , where  $\Lambda_{\mathbb{Z}/q\mathbb{Z}}(m) = q/(q-1)$  if  $q \nmid m$  and  $\Lambda_{\mathbb{Z}/q\mathbb{Z}}(m) = 0$  otherwise.

## 5.1 The theorem of Green, Tao, and Ziegler

We use the theorem in the following form. It is a special case of the generalized Hardy–Littlewood conjecture for systems of finite complexity [18, Conjecture 1.2], with two variables, fixed forms, and a region on which all the forms are eventually positive. The qualitative consequence [18, Corollary 1.9], whose two-variable case is [19, Theorem 1.1], gives infinitely many points at which all the forms are prime. We need the asymptotic form to show, in Section 5.2, that infinitely many of these points have distinct prime values outside a given finite set.

**Theorem 5.1** (Linear equations in primes). *Let  $t \geq 2$ , and let  $\ell_1, \dots, \ell_t$  be affine-linear forms on  $\mathbb{Z}^2$  with linear parts  $\dot{\ell}_i(\mathbf{n}) = \langle \mathbf{w}_i, \mathbf{n} \rangle$  such that  $\det(\mathbf{w}_i, \mathbf{w}_j) \neq 0$  for all  $i \neq j$ . Let  $K \subset \mathbb{R}^2$  be a nonempty bounded convex set whose closure  $\bar{K}$  is contained in the open cone*

$$\mathcal{C} = \{ \mathbf{x} \in \mathbb{R}^2 : \dot{\ell}_i(\mathbf{x}) > 0 \text{ for } 1 \leq i \leq t \}.$$

*Then the following statements hold.*

- (1) *The product  $\mathfrak{S} = \prod_q \beta_q$  over all primes  $q$  converges. It is positive if  $\beta_q > 0$  for all primes  $q$ , and zero otherwise.*
- (2) *As  $R \rightarrow \infty$ , we have*

$$\sum_{\mathbf{n} \in RK \cap \mathbb{Z}^2} \prod_{i=1}^t \Lambda(\ell_i(\mathbf{n})) = \text{area}(K) \mathfrak{S} R^2 + o(R^2), \quad (5.2)$$

*where the term  $o(R^2)$  depends on  $\ell_1, \dots, \ell_t$  and  $K$ .*

*Proof.* The asymptotic (5.2) is an instance of the Main Theorem of [18], whose two conditional inputs are now theorems. We first bound the complexity of the system and check these inputs. We then fix the scale at which we apply the Main Theorem, compute the archimedean factor, and finally prove (1).

**Complexity.** By [18, Definition 1.5], the system  $(\ell_1, \dots, \ell_t)$  has complexity at most  $s$  if, for each  $i$ , the forms  $\ell_j$  with  $j \neq i$  can be covered by  $s + 1$  classes such that  $\ell_i$  does not lie in the affine-linear span of any of the classes. Fix  $i$ , and cover the  $t - 1$  forms  $\ell_j$  with  $j \neq i$  by the singleton classes  $\{\ell_j\}$ . If  $\ell_i$  lay in the affine-linear span of  $\{\ell_j\}$ , then  $\ell_i$  would be a rational multiple of  $\ell_j$ , which contradicts  $\det(\mathbf{w}_i, \mathbf{w}_j) \neq 0$ . This shows that the system has complexity at most  $t - 2$ , which is also the bound of [18, Lemma 1.6]:  $t$  minus the dimension of the span of the linear parts. The same hypothesis implies that the forms are nonconstant and that no two of them are rational multiples of each other, as required in [18, Definition 1.1].

Let  $s = \max(t - 2, 3)$ . A system of complexity at most  $t - 2$  also has complexity at most  $s$ . The inverse conjecture  $\text{GI}(s)$  for the Gowers norm [18, Conjecture 8.3] holds by [17, Theorem 1.3], since  $s \geq 3$ . The Möbius and nilsequences conjecture  $\text{MN}(s)$  [18, Conjecture 8.5] holds for every  $s$  by [16, Theorem 1.1] (see the remark that follows that theorem). The Main Theorem of [18] then implies that [18, Conjecture 1.2] holds for our system. For two variables, this conjecture states the following. We write  $\mathbf{w}_i = (w_{i,1}, w_{i,2})$ , and let  $N$  and  $L$  be positive integers such that

$$\sum_{i=1}^t (|w_{i,1}| + |w_{i,2}|) + \frac{1}{N} \sum_{i=1}^t |\ell_i(\mathbf{0})| \leq L; \quad (5.3)$$

the left side is the size of the system at scale  $N$ , defined in [18, (1.1)]. Then for every convex set  $K' \subset [-N, N]^2$ , we have

$$\sum_{\mathbf{n} \in K' \cap \mathbb{Z}^2} \prod_{i=1}^t \Lambda(\ell_i(\mathbf{n})) = \beta_\infty(K') \prod_q \beta_q + o_{t,L}(N^2), \quad (5.4)$$

where  $\beta_\infty(K')$  is the area of  $\{\mathbf{x} \in K' : \ell_i(\mathbf{x}) > 0 \text{ for } 1 \leq i \leq t\}$  [18, (1.4)], the  $\beta_q$  are the local factors (5.1), and the error term is at most  $\rho_{t,L}(N)N^2$  for a function  $\rho_{t,L}$  with  $\rho_{t,L}(N) \rightarrow 0$  as  $N \rightarrow \infty$ .

**The scale.** Fix a positive integer  $h$  such that  $K \subset [-h, h]^2$ , and let  $L = \sum_i (|w_{i,1}| + |w_{i,2}| + |\ell_i(\mathbf{0})|)$ , which is a positive integer. For  $R \geq 1$ , let  $N_R = \lceil hR \rceil$ . Then  $RK \subset [-N_R, N_R]^2$ , and (5.3) holds with  $N = N_R$  because  $N_R \geq 1$ . We use (5.4) with  $N = N_R$  and  $K' = RK$ . Because  $N_R \leq 2hR$ , the error term is at most  $4h^2 \rho_{t,L}(N_R)R^2$ , which is  $o(R^2)$  as  $R \rightarrow \infty$ . Note that the coefficients of the forms enter only through  $L$ , which does not depend on  $R$ , and that they may be large.

**The archimedean factor.** Since  $\bar{K}$  is compact and contained in the open cone  $\mathcal{C}$ , the number

$$\delta = \min_{1 \leq i \leq t} \min_{\mathbf{y} \in \bar{K}} \ell_i(\mathbf{y})$$

is positive. Let  $G = \max_i |\ell_i(\mathbf{0})|$ . For  $\mathbf{x} = R\mathbf{y}$  with  $\mathbf{y} \in K$ , we have

$$\ell_i(\mathbf{x}) = R\ell_i(\mathbf{y}) + \ell_i(\mathbf{0}) \geq \delta R - G, \quad (5.5)$$

which is positive when  $R > G/\delta$ . For such  $R$ , all the forms are positive on  $RK$ , and  $\beta_\infty(RK) = \text{area}(RK) = \text{area}(K)R^2$ . Inserting this into (5.4), we obtain (5.2).

**The singular product.** Let  $D = \prod_{i < j} \det(\mathbf{w}_i, \mathbf{w}_j)$ , which is a nonzero integer, and let  $q$  be a prime with  $q \nmid D$  and  $q \geq 2t$ . Then  $\mathbf{w}_i \not\equiv \mathbf{0} \pmod{q}$  for every  $i$ , since otherwise  $q$  would divide  $\det(\mathbf{w}_i, \mathbf{w}_j)$  for  $j \neq i$ . We see that the zero set  $Z_i \subset \mathbb{F}_q^2$  of  $\ell_i$  modulo  $q$  is an affine line, with  $q$  points. For  $i \neq j$ , the lines  $Z_i$  and  $Z_j$  meet in exactly one point, because  $\det(\mathbf{w}_i, \mathbf{w}_j) \not\equiv 0 \pmod{q}$ . By inclusion and exclusion, truncated after the second term, we have

$$tq - \binom{t}{2} \leq \left| \bigcup_{i=1}^t Z_i \right| \leq tq.$$

By (5.1), we have  $\beta_q = (1 - 1/q)^{-t} (1 - q^{-2} |\bigcup_i Z_i|)$ , and the previous display implies that

$$\left(1 - \frac{1}{q}\right)^{-t} \left(1 - \frac{t}{q}\right) \leq \beta_q \leq \left(1 - \frac{1}{q}\right)^{-t} \left(1 - \frac{t}{q} + \frac{t^2}{2q^2}\right). \quad (5.6)$$

For the lower bound, we use  $(1 - 1/q)^{-t} \geq (1 + 1/q)^t \geq 1 + t/q$ , and find  $\beta_q \geq 1 - t^2/q^2$ . For the upper bound, we use  $-\log(1 - u) \leq u + u^2$  for  $0 \leq u \leq 1/2$  and  $1 + v \leq e^v$ , and find

$$\beta_q \leq \exp\left(\frac{t}{q} + \frac{t}{q^2} - \frac{t}{q} + \frac{t^2}{2q^2}\right) \leq \exp\left(\frac{t^2}{q^2}\right) \leq 1 + \frac{2t^2}{q^2},$$

where in the second step we used  $t \geq 2$ , and in the last step  $e^v \leq 1 + 2v$  for  $0 \leq v \leq 1$ . Combining the two bounds, we find that  $|\beta_q - 1| \leq 2t^2/q^2 \leq 1/2$ . This is the estimate  $\beta_q = 1 + O(q^{-2})$  of [18, Lemma 1.3], with explicit constants. Using  $|\log(1 + x)| \leq 2|x|$  for  $|x| \leq 1/2$ , we obtain  $|\log \beta_q| \leq 4t^2/q^2$ . Because  $\sum_q q^{-2} < \infty$ , the product of the  $\beta_q$  over the primes  $q \nmid D$  with  $q \geq 2t$  converges absolutely to a positive number. The remaining factors are finitely many nonnegative numbers. This proves (1) and completes the proof.  $\square$

*Remark 5.2.* In Theorem 5.1, we fix the forms and the set  $K$ , and the error term depends on them. In Section 5.4, the linear coefficients of the forms contain the factors  $W/c_i$ , which are large in our applications, but they do not depend on  $R$ . No uniformity in the coefficients is needed.

Kai [23, Theorem 12.1] proved an analogue of (5.4) over number fields, with an error term  $O(N^2(\log N)^{-A})$ . For the field  $\mathbb{Q}$  and the ideal  $\mathbb{Z}$ , his weight at an integer  $m$  is  $\Lambda(|m|)$ , which agrees with  $\Lambda(m)$  at the values  $m = \ell_i(\mathbf{n})$  with  $\mathbf{n} \in RK$  and  $R > G/\delta$ , since these values are positive by (5.5). His local factors are those of (5.1), since the

residue of the Riemann zeta function at 1 is 1. His hypothesis that  $\ell_i$  restricted to  $\ker \ell_j$  has finite cokernel holds because  $\det(\mathbf{w}_i, \mathbf{w}_j) \neq 0$ : the image of  $\ker \ell_j \cap \mathbb{Z}^2$  under  $\ell_i$  is a nonzero subgroup of  $\mathbb{Z}$ . His theorem, applied with  $N = N_R$  and the region  $RK$ , also gives (5.2).

## 5.2 Distinct prime values

The sum in (5.2) also counts points at which some  $\ell_i(\mathbf{n})$  is a power of a prime with exponent at least two, points at which two forms take the same value, and points at which a form takes a value in a given finite set. We now show that these points, which lie on few lines, do not contribute to the main term.

**Lemma 5.3** (Distinct prime values). *Assume the hypotheses of Theorem 5.1, let  $S$  be a finite set of primes, and let  $\mathcal{A}$  be a finite set of lines in  $\mathbb{R}^2$ . For  $R \geq 1$ , let  $\mathcal{N}(R)$  be the set of  $\mathbf{n} \in RK \cap \mathbb{Z}^2$  such that  $\ell_1(\mathbf{n}), \dots, \ell_t(\mathbf{n})$  are  $t$  distinct primes not in  $S$  and  $\mathbf{n}$  lies on no line of  $\mathcal{A}$ . Then, as  $R \rightarrow \infty$ ,*

$$\sum_{\mathbf{n} \in \mathcal{N}(R)} \prod_{i=1}^t \Lambda(\ell_i(\mathbf{n})) = \text{area}(K) \mathfrak{S} R^2 + o(R^2). \quad (5.7)$$

*If moreover  $\text{area}(K) > 0$  and  $\beta_q > 0$  for all primes  $q$ , then there exists  $c > 0$  such that  $|\mathcal{N}(R)| \geq cR^2(\log R)^{-t}$  for all sufficiently large  $R$ . In particular, for every  $R_1 \geq 1$ , the set  $\bigcup_{R \geq R_1} \mathcal{N}(R)$  is infinite.*

*Proof.* Let  $\Sigma(R)$  and  $\Sigma'(R)$  denote the left sides of (5.2) and (5.7). By Theorem 5.1, it suffices to show that  $\Sigma(R) - \Sigma'(R) = o(R^2)$ .

We keep the notation  $h, N_R, \delta$ , and  $G$  of the proof of Theorem 5.1, and set

$$\Theta = G + \max_{1 \leq i \leq t} \max_{\mathbf{y} \in \overline{K}} \ell_i(\mathbf{y}).$$

Note that  $\Theta \geq \delta > 0$ . Let  $R > \max(1, G/\delta, 2/\Theta)$ , so that  $\Theta R \geq 2$ , and let  $\mathbf{n} \in RK \cap \mathbb{Z}^2$ . By (5.5), every  $\ell_i(\mathbf{n})$  is a positive integer, and  $\ell_i(\mathbf{n}) \leq \Theta R$ . Using  $\Lambda(m) \leq \log m$  for  $m \geq 1$ , we find that every term of  $\Sigma(R)$  is at most  $(\log \Theta R)^t$ .

A point  $\mathbf{n}$  contributes to  $\Sigma(R)$  but not to  $\Sigma'(R)$  only if  $\Lambda(\ell_i(\mathbf{n})) > 0$  for every  $i$  and one of the following holds:

- (i)  $\ell_i(\mathbf{n}) = q^k$  for some  $i$ , some prime  $q$ , and some  $k \geq 2$ ;
- (ii)  $\ell_i(\mathbf{n}) = \ell_j(\mathbf{n})$  for some  $i < j$ ;
- (iii)  $\ell_i(\mathbf{n}) \in S$  for some  $i$ ;
- (iv)  $\mathbf{n}$  lies on a line of  $\mathcal{A}$ .

Indeed, if  $\Lambda(\ell_i(\mathbf{n})) > 0$ , then  $\ell_i(\mathbf{n})$  is a power of a prime, and it is a prime if (i) fails; if (ii)–(iv) fail as well, then  $\mathbf{n} \in \mathcal{N}(R)$ .

Each of these conditions places  $\mathbf{n}$  on one of a finite set of lines. Since  $\mathbf{w}_i \neq \mathbf{0}$ , every set  $\{\ell_i = m\}$  with  $m \in \mathbb{Z}$  is a line. In case (i),  $\mathbf{n}$  lies on the line  $\{\ell_i = q^k\}$ , where  $q^k \leq \Theta R$ . Only the exponents  $k \leq \log_2(\Theta R)$  occur, and for each of them there are at most  $(\Theta R)^{1/k} \leq (\Theta R)^{1/2}$  primes  $q$ . Altogether, there are at most  $t(\Theta R)^{1/2} \log_2(\Theta R)$  such lines. In case (ii),  $\mathbf{n}$  lies on the set  $\{\ell_i - \ell_j = 0\}$ , which is a line because  $\mathbf{w}_i$  and  $\mathbf{w}_j$  are linearly independent; there are  $\binom{t}{2}$  such lines. In case (iii),  $\mathbf{n}$  lies on one of the  $t|S|$  lines  $\{\ell_i = q\}$  with  $q \in S$ , and in case (iv), on one of the  $|\mathcal{A}|$  lines of  $\mathcal{A}$ . A line  $\{\mathbf{x} \in \mathbb{R}^2 : a_1 x_1 + a_2 x_2 = b\}$  with  $(a_1, a_2) \neq (0, 0)$  contains at most  $2N_R + 1$  points of  $[-N_R, N_R]^2 \cap \mathbb{Z}^2$ : if  $a_2 \neq 0$ , then  $x_1$  determines  $x_2$ , and otherwise  $x_1 = b/a_1$  is fixed. Since  $RK \subset [-N_R, N_R]^2$ , we obtain

$$0 \leq \Sigma(R) - \Sigma'(R) \leq (2N_R + 1) \left( t(\Theta R)^{1/2} \log_2(\Theta R) + \binom{t}{2} + t|S| + |\mathcal{A}| \right) (\log \Theta R)^t.$$

The right side is  $O(R^{3/2}(\log R)^{t+1}) = o(R^2)$ , because  $N_R \leq 2hR$ . This proves (5.7).

Now assume that  $\text{area}(K) > 0$  and that  $\beta_q > 0$  for all primes  $q$ . Then  $\mathfrak{S} > 0$  by Theorem 5.1, and (5.7) implies that  $\Sigma'(R) \geq \text{area}(K) \mathfrak{S} R^2 / 2$  for all large  $R$ . Each term of  $\Sigma'(R)$  is at most  $(\log \Theta R)^t$ , and  $\log \Theta R \leq 2 \log R$  for  $R \geq \Theta$ . We conclude that

$$|\mathcal{N}(R)| \geq \frac{\text{area}(K) \mathfrak{S} R^2}{2(\log \Theta R)^t} \geq \frac{\text{area}(K) \mathfrak{S}}{2^{t+1}} \frac{R^2}{(\log R)^t}$$

for all large  $R$ . Since  $|\mathcal{N}(R)| \rightarrow \infty$ , the last claim follows.  $\square$

### 5.3 Local factors in a congruence class

We now compute the local factors of the forms that arise from a datum. Let  $t \geq 2$ , let  $(a_i, b_i) \in \mathbb{Z}^2$  for  $0 \leq i \leq t-1$  be primitive vectors, that is,  $\gcd(a_i, b_i) = 1$ , and let  $L_i(M, N) = a_i M + b_i N$ . In Section 5.4, we take for them the twelve forms of a datum. We write  $\Delta_{ij} = a_i b_j - a_j b_i$ . Let  $c_0, \dots, c_{t-1}$  and  $W$  be positive integers, and let  $(M_0, N_0) \in \mathbb{Z}^2$ .

For a prime  $q$ , let  $Z_i(q) = \{(m, n) \in \mathbb{F}_q^2 : a_i m + b_i n = 0\}$ . Since  $(a_i, b_i)$  is primitive, it is nonzero modulo  $q$ , and  $Z_i(q)$  is a line through the origin of  $\mathbb{F}_q^2$ . Recall that  $\mathbb{F}_q^2$  has exactly  $q+1$  lines through the origin, and that two nonzero vectors span the same line if and only if their determinant vanishes. In particular,  $Z_i(q) = Z_j(q)$  if and only if  $q \mid \Delta_{ij}$ . We let  $d_q$  be the number of distinct lines among  $Z_0(q), \dots, Z_{t-1}(q)$ .

**Lemma 5.4** (Local factors in a congruence class). *With the notation above, assume that*

- (i) *every prime dividing  $c_0 c_1 \cdots c_{t-1}$  divides  $W$ , and  $v_q(W) > v_q(c_i)$  for every prime  $q \mid W$  and every  $i$ ;*
- (ii)  *$c_i \mid L_i(M_0, N_0)$  and  $\gcd(L_i(M_0, N_0)/c_i, W) = 1$  for every  $i$ .*

Then  $c_i \mid W$  for every  $i$ , and

$$\ell_i(X, Y) = \frac{L_i(M_0 + WX, N_0 + WY)}{c_i} = \ell_i(\mathbf{0}) + \frac{W}{c_i}(a_i X + b_i Y), \quad \ell_i(\mathbf{0}) = \frac{L_i(M_0, N_0)}{c_i}, \quad (5.8)$$

are affine-linear forms on  $\mathbb{Z}^2$ . Their local factors (5.1) are as follows.

(a) If  $q \mid W$ , then  $\beta_q = (q/(q-1))^t$ .

(b) If  $q \nmid W$ , then

$$\beta_q = \left(\frac{q}{q-1}\right)^t \frac{(q-1)(q+1-d_q)}{q^2}. \quad (5.9)$$

In particular,  $\beta_q > 0$  if  $q \mid W$  or  $q \geq t$ . If  $q \nmid W$ , then  $\beta_q > 0$  if and only if there exists  $(m, n) \in \mathbb{F}_q^2$  with  $\prod_i L_i(m, n) \neq 0$ . If  $q \nmid W \prod_{i < j} \Delta_{ij}$ , then  $d_q = t$ .

*Proof.* By (i), every prime  $q$  dividing  $c_i$  divides  $W$  and satisfies  $v_q(c_i) < v_q(W)$ . This implies that  $c_i \mid W$ . We have  $L_i(M_0 + WX, N_0 + WY) = L_i(M_0, N_0) + W(a_i X + b_i Y)$ , which gives the second equality in (5.8). Its coefficients  $\ell_i(\mathbf{0})$ ,  $Wa_i/c_i$ , and  $Wb_i/c_i$  are integers by (ii) and  $c_i \mid W$ .

**Primes dividing  $W$ .** Let  $q \mid W$ . By (i), we have  $v_q(W/c_i) \geq 1$ , and (5.8) implies that  $\ell_i(X, Y) \equiv \ell_i(\mathbf{0}) \pmod{q}$  for all  $(X, Y)$ . Also,  $q \nmid \ell_i(\mathbf{0})$  by (ii). Every point of  $\mathbb{F}_q^2$  is therefore counted in (5.1), and we have  $\beta_q = (q/(q-1))^t$ .

**Primes not dividing  $W$ .** Let  $q \nmid W$ . Then (i) implies that  $q \nmid c_i$  for all  $i$ . The map  $(X, Y) \mapsto (M_0 + WX, N_0 + WY)$  is a bijection of  $\mathbb{F}_q^2$ , and  $\ell_i(X, Y) \equiv c_i^{-1} L_i(M_0 + WX, N_0 + WY) \pmod{q}$ . We find that the count in (5.1) equals the number of points of  $\mathbb{F}_q^2$  outside  $Z_0(q) \cup \cdots \cup Z_{t-1}(q)$ . Distinct lines through the origin meet only at the origin, and each of them contains  $q-1$  nonzero points. The union therefore has  $1 + d_q(q-1)$  points, and its complement has

$$q^2 - 1 - d_q(q-1) = (q-1)(q+1-d_q)$$

points. Inserting this count into (5.1) gives (5.9).

It remains to prove the last three claims. If  $q \nmid W$  and  $q \geq t$ , then  $q+1-d_q \geq q+1-t \geq 1$ , and we have  $\beta_q > 0$  by (5.9). For  $q \nmid W$ , the count of points outside the union is positive if and only if some  $(m, n) \in \mathbb{F}_q^2$  satisfies  $\prod_i L_i(m, n) \neq 0$ . Finally, if  $q$  divides no  $\Delta_{ij}$ , then the lines  $Z_i(q)$  are pairwise distinct, and  $d_q = t$ .  $\square$

When  $d_q = t$ , we see from (5.9) that  $\beta_q = (q/(q-1))^{t-1}(1 - (t-1)/q)$ , which is  $1 + O(q^{-2})$ , in accordance with (5.6).

## 5.4 Prime specializations of a twelve-form datum

We now return to a twelve-form datum  $\mathfrak{D}$  (Definition 4.1), with forms  $L_i = a_i M + b_i N$  and cofactors  $c_i$  for  $0 \leq i \leq 11$ , and to a finite set  $S$  of primes as in Definition 4.6. In

Sections 6 to 8, we apply the next proposition to a congruence class  $(M_0, N_0)$  modulo  $W$  chosen with the Chinese remainder theorem and to a cone  $\mathcal{K}$  on which the twelve forms are positive. By an open convex cone, we mean an open convex subset of  $\mathbb{R}^2$  that is closed under multiplication by positive real numbers.

**Proposition 5.5** (Infinitely many prime specializations). *Let  $\mathfrak{D}$  be a twelve-form datum with forms  $L_0, \dots, L_{11}$  and cofactors  $c_0, \dots, c_{11}$ , and let  $S$  be a finite set of primes as in Definition 4.6. Let  $W$  be a positive integer, let  $(M_0, N_0) \in \mathbb{Z}^2$ , and let  $\mathcal{K} \subset \mathbb{R}^2$  be a nonempty open convex cone. Assume that*

- (a) *every prime dividing  $c_0 c_1 \cdots c_{11}$  divides  $W$ ;  $v_q(W) > v_q(c_i)$  for all primes  $q \mid W$  and all  $i$ ; and  $c_i \mid L_i(M_0, N_0)$  and  $\gcd(L_i(M_0, N_0)/c_i, W) = 1$  for all  $i$ ;*
- (b) *for every prime  $q \leq 11$  with  $q \nmid W$ , there exists  $(m, n) \in \mathbb{F}_q^2$  such that  $\prod_{i=0}^{11} L_i(m, n) \neq 0$ ;*
- (c)  *$L_i(\mathbf{x}) > 0$  for all  $\mathbf{x} \in \mathcal{K}$  and  $0 \leq i \leq 11$ .*

*Then there exist infinitely many prime specializations  $(M, N) \in \mathcal{K}$  with  $M \equiv M_0$  and  $N \equiv N_0 \pmod{W}$ . Every such pair satisfies  $\gcd(M, N) = 1$  and  $N \neq 0$ . The ratios  $M/N$  of these pairs take infinitely many values, and so do the  $j$ -invariants  $j(E_{M,N})$ .*

*Proof.* We use Theorem 5.1 and Lemma 5.3 for the forms  $\ell_0, \dots, \ell_{11}$  of (5.8), with  $t = 12$ . We first check that their linear parts are pairwise independent and that their local factors are positive. We then choose a convex set  $K_0$  whose large dilates correspond to pairs in  $\mathcal{K}$ , and deduce the claims about prime specializations, ratios, and  $j$ -invariants.

**The forms.** Hypothesis (a) consists of the conditions (i) and (ii) of Lemma 5.4 for the forms  $L_0, \dots, L_{11}$ , whose coefficient vectors are primitive by Definition 4.1. That lemma shows that the  $\ell_i$  are affine-linear forms with  $\mathbf{w}_i = (W/c_i)(a_i, b_i)$ , and for  $i \neq j$  we have

$$\det(\mathbf{w}_i, \mathbf{w}_j) = \frac{W^2 \Delta_{ij}}{c_i c_j} \neq 0,$$

because  $\Delta_{ij} \neq 0$  by Definition 4.1.

**Local factors.** Let  $q$  be a prime. If  $q \mid W$ , then  $\beta_q > 0$  by Lemma 5.4(a). If  $q \nmid W$  and  $q \leq 11$ , then  $\beta_q > 0$  by hypothesis (b) and Lemma 5.4. If  $q \nmid W$  and  $q \geq 13$ , then  $\beta_q > 0$  by Lemma 5.4, since  $q \geq t$ : each  $L_i$  vanishes modulo  $q$  on a single line through the origin, and twelve lines cannot exhaust the  $q + 1 \geq 14$  lines of  $\mathbb{F}_q^2$ . By Theorem 5.1, we have  $\mathfrak{S} > 0$ .

**The region.** Since  $\mathcal{K}$  is open and nonempty, there exist  $\mathbf{x}_0 \in \mathcal{K}$  and  $r > 0$  such that the closed disk of radius  $2r$  about  $\mathbf{x}_0$  is contained in  $\mathcal{K}$ . Let  $K_0$  be the closed disk of radius  $r$  about  $\mathbf{x}_0$ . Then  $K_0$  is compact and convex, and  $\text{area}(K_0) = \pi r^2 > 0$ . By (c), we have

$\dot{\ell}_i(\mathbf{x}) = (W/c_i)L_i(\mathbf{x}) > 0$  for  $\mathbf{x} \in K_0$ . In other words,  $K_0$  is contained in the cone  $\mathcal{C}$  of Theorem 5.1. For  $R > 0$  and  $\mathbf{n} = (X, Y) \in RK_0$ , we have

$$(M_0 + WX, N_0 + WY) = WR \left( R^{-1}\mathbf{n} + (WR)^{-1}(M_0, N_0) \right). \quad (5.10)$$

Let  $R_1 = \max(1, |(M_0, N_0)|/(Wr))$ , where  $|\cdot|$  is the Euclidean norm. Let  $R \geq R_1$ . The point  $R^{-1}\mathbf{n}$  lies in  $K_0$ , and the shift  $(WR)^{-1}(M_0, N_0)$  has norm at most  $r$ . The point in parentheses in (5.10) therefore lies in the disk of radius  $2r$  about  $\mathbf{x}_0$ , which is contained in  $\mathcal{K}$ . As  $\mathcal{K}$  is a cone and  $WR > 0$ , the pair  $(M_0 + WX, N_0 + WY)$  lies in  $\mathcal{K}$  as well.

**Prime specializations.** By the last two paragraphs, Lemma 5.3 applies to  $\ell_0, \dots, \ell_{11}$ , the set  $K_0$ , the set  $S$ , and  $\mathcal{A} = \emptyset$ . We obtain infinitely many  $\mathbf{n} = (X, Y) \in \mathbb{Z}^2$ , each in  $RK_0$  for some  $R \geq R_1$ , such that  $\ell_0(\mathbf{n}), \dots, \ell_{11}(\mathbf{n})$  are twelve distinct primes not in  $S$ . For each such  $\mathbf{n}$ , let  $(M, N) = (M_0 + WX, N_0 + WY)$ . Then  $M \equiv M_0$  and  $N \equiv N_0 \pmod{W}$ , and  $(M, N) \in \mathcal{K}$  by the previous paragraph. By (5.8), we have  $L_i(M, N) = c_i \ell_i(\mathbf{n})$  for all  $i$ . This shows that  $c_i \mid L_i(M, N)$  and that the numbers  $L_i(M, N)/c_i = \ell_i(\mathbf{n})$  are twelve distinct primes not in  $S$ , that is,  $(M, N)$  is a prime specialization in the sense of Definition 4.6. Distinct points  $\mathbf{n}$  give distinct pairs  $(M, N)$ , which proves the first claim.

**Ratios and  $j$ -invariants.** By Lemma 4.8, every prime specialization  $(M, N)$  satisfies  $\gcd(M, N) = 1$  and  $p_0 \nmid N$ , so that  $N \neq 0$ . A rational number has exactly two representations  $m/n$  with  $m, n \in \mathbb{Z}$  and  $\gcd(m, n) = 1$ . It follows that infinitely many such pairs give infinitely many ratios  $M/N$ . By Lemma 4.3,  $j(E_{M,N})$  depends only on  $M/N$ , and each value of  $j$  occurs for at most twelve ratios. If the  $j(E_{M,N})$  took only  $k$  values, at most  $12k$  ratios would occur. Therefore the  $j$ -invariants take infinitely many values, which completes the proof.  $\square$

*Remark 5.6.* By Lemma 5.4, hypothesis (b) says that  $d_q \leq q$  for every prime  $q \leq 11$  with  $q \nmid W$ . As we saw in the proof, larger primes need no check. At  $q = 11$ , the check is needed even when 11 divides no  $\Delta_{ij}$ . For example, the twelve forms  $M + iN$  with  $0 \leq i \leq 10$  and  $N$  have pairwise determinants in  $\{\pm 1, \dots, \pm 10\}$ , but their zero sets modulo 11 are all twelve lines of  $\mathbb{F}_{11}^2$ , and Lemma 5.4 gives  $\beta_{11} = 0$  when  $11 \nmid W$ . In the three families, every prime  $q \leq 11$  divides  $W$ , except  $q = 5$  in the rank-seven family.

*Remark 5.7.* Elliptic curves that are isomorphic over  $\overline{\mathbb{Q}}$  have the same  $j$ -invariant [43, Proposition III.1.4(b)]. Hence the curves  $E_{M,N}$  at the prime specializations of Proposition 5.5 represent infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes.

PART II

The three families

## The rank-five family

In this section, we prove Theorem 6.7. It states that the twelve-form datum  $\mathfrak{D}_5$  defined below has infinitely many prime specializations in a fixed congruence class and a fixed cone, that the curve  $E_{M,N}$  has rank exactly five at each of them, and that these curves represent infinitely many isomorphism classes over  $\overline{\mathbb{Q}}$ . The proof consists of checking the hypotheses of Proposition 4.18 and Proposition 5.5 for  $\mathfrak{D}_5$ . We do not repeat the general arguments of Sections 3 to 5; instead, we give the data of the family together with the tables needed to recompute every entry of the matrices by hand. Theorem 6.7 is used in Section 9 to prove Theorem 1.1 for  $r = 5$ .

The family is a base change, along a conic, of a rank-four family of Zywina [55, §6.5]. We explain this origin in Appendix B.1.

The section is organized as follows. In Section 6.1, we define  $\mathfrak{D}_5$ , the set  $S$ , and the bases  $\mathcal{B}_E$  and  $\mathcal{B}_{E'}$ . In Section 6.2, we exhibit three points on  $E$  and four points on  $E'$  whose classes are independent at every prime specialization (Lemmas 6.1 and 6.2). In Section 6.3, we fix the congruence class and the cone, and we compute the residues of the primes  $p_i$  (Lemmas 6.3 and 6.4). Section 6.4 bounds the local images at 2, 3, 5 and the real place (Lemma 6.5), and Section 6.5 computes the quadratic characters that enter the rows at the twelve primes  $p_i$ . In Section 6.6, we display the matrices  $\mathbf{M}_E(0)$  and  $\mathbf{M}_{E'}(0)$  and certify their ranks (Lemma 6.6). Section 6.7 proves Theorem 6.7. Finally, in Section 6.8, we use the dual isogeny to write down five independent points of  $E_{M,N}(\mathbb{Q})$  (Proposition 6.9); this is not needed for Theorem 6.7.

### 6.1 The datum

Let  $L_i = a_i M + b_i N$  for  $0 \leq i \leq 11$ , with the coefficients  $a_i, b_i$  and the cofactors  $c_i$  given in Table 6.1. As in Section 4, we set  $I_F = \{0, 1, 2, 3\}$ ,  $I_H = \{4, 5, 6, 7\}$ ,  $I_J = \{8, 9, 10, 11\}$ , and

$$F = L_0 L_1 L_2 L_3, \quad H = L_4 L_5 L_6 L_7, \quad J = L_8 L_9 L_{10} L_{11}.$$

Expanding the products, we find the coefficients of  $F$ ,  $H$  and  $J$  listed in the first three rows of Table 6.4 below. Comparing the five coefficients, we obtain the identity

$$625F + 3H = 16J. \tag{6.1}$$

Table 6.1. The linear forms  $L_i = a_i M + b_i N$  of the rank-five family, the quartic to which each belongs, and the cofactors  $c_i$ .

| $i$   | 0   | 1   | 2   | 3   | 4   | 5   | 6   | 7   | 8   | 9   | 10  | 11  |
|-------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| group | $F$ | $F$ | $F$ | $F$ | $H$ | $H$ | $H$ | $H$ | $J$ | $J$ | $J$ | $J$ |
| $a_i$ | 1   | 22  | 9   | 143 | -55 | 3   | 138 | 55  | 99  | 5   | 32  | 55  |
| $b_i$ | 0   | -1  | -2  | 155 | 62  | -1  | -31 | 64  | 62  | -1  | 31  | -12 |
| $c_i$ | 54  | 1   | 8   | 1   | 8   | 1   | 1   | 2   | 4   | 1   | 1   | 6   |

For example, the coefficients of  $M^4$  give  $625 \cdot 28314 - 3 \cdot 1252350 = 13939200 = 16 \cdot 871200$ . We set

$$A = 1500, \quad B = 2700, \quad C = 57600. \quad (6.2)$$

Since  $A^2 = 3600 \cdot 625$ ,  $4B = 3600 \cdot 3$  and  $C = 3600 \cdot 16$ , multiplying (6.1) by 3600 gives  $A^2 F + 4BH = CJ$ . The curves of Definition 4.1 are

$$\begin{aligned} E = E_{M,N} : y^2 &= x^3 + 1500F x^2 - 2700FH x, \\ E' = E'_{M,N} : y^2 &= x^3 - 3000F x^2 + 57600FJ x. \end{aligned} \quad (6.3)$$

In the notation of Section 3, we have  $\alpha = 1500F$ ,  $\beta = -2700FH$ ,  $\alpha' = -3000F$  and  $\beta' = \alpha^2 - 4\beta = 57600FJ$ . We write  $T = (0,0) \in E$  and  $T' = (0,0) \in E'$ .

The coefficient vectors  $(a_i, b_i)$  in Table 6.1 are primitive,  $(a_0, b_0) = (1,0)$ , and  $b_i \neq 0$  for  $i \geq 1$ . The sixty-six determinants  $\Delta_{ij} = a_i b_j - a_j b_i$  are factored in Table 6.2; none of them vanishes. The cofactors are positive and  $c_1 = 1$ . The forms  $L_i$ , the constants (6.2), the cofactors  $c_i$  and the constant lists

$$\Gamma_E = \Gamma_{E'} = (-1, 2, 3, 5) \quad (6.4)$$

therefore form a twelve-form datum in the sense of Definition 4.1, which we denote by  $\mathfrak{D}_5$ .

We define

$$S = \{2, 3, 5, 7, 11, 13, 17, 19, 31, 41, 131, 257, 409, 2089\}. \quad (6.5)$$

By Table 6.2,  $S$  is exactly the set of primes dividing some  $\Delta_{ij}$ . The other integers in Definition 4.6, and the entries of the lists (6.4), have prime factors in  $\{2, 3, 5, 31\}$ : we have  $A = 2^2 \cdot 3 \cdot 5^3$ ,  $B = 2^2 \cdot 3^3 \cdot 5^2$ ,  $C = 2^8 \cdot 3^2 \cdot 5^2$ , every  $c_i$  divides  $2^3 \cdot 3^3$ , and

$$(b_1, \dots, b_{11}) = (-1, -2, 5 \cdot 31, 2 \cdot 31, -1, -31, 2^6, 2 \cdot 31, -1, 31, -2^2 \cdot 3).$$

We conclude that  $S$  satisfies the conditions of Definition 4.6. Throughout this section, a prime specialization is a prime specialization of  $\mathfrak{D}_5$  with respect to this set  $S$ . At a prime specialization we write  $p_i = L_i(M, N)/c_i$  and

$$\pi_F = p_0 p_1 p_2 p_3, \quad \pi_H = p_4 p_5 p_6 p_7, \quad \pi_J = p_8 p_9 p_{10} p_{11}, \quad (6.6)$$

Table 6.2. The determinants  $\Delta_{ij} = a_i b_j - a_j b_i$  for  $0 \leq i < j \leq 11$ , factored.

| $(i, j)$ | $\Delta_{ij}$                | $(i, j)$ | $\Delta_{ij}$                           | $(i, j)$ | $\Delta_{ij}$                    |
|----------|------------------------------|----------|-----------------------------------------|----------|----------------------------------|
| (0, 1)   | -1                           | (2, 4)   | $2^6 \cdot 7$                           | (4, 11)  | $-2 \cdot 5^3 \cdot 11$          |
| (0, 2)   | -2                           | (2, 5)   | -3                                      | (5, 6)   | $3^2 \cdot 5$                    |
| (0, 3)   | $5 \cdot 31$                 | (2, 6)   | -3                                      | (5, 7)   | $13 \cdot 19$                    |
| (0, 4)   | $2 \cdot 31$                 | (2, 7)   | $2 \cdot 7^3$                           | (5, 8)   | $3 \cdot 5 \cdot 19$             |
| (0, 5)   | -1                           | (2, 8)   | $2^2 \cdot 3^3 \cdot 7$                 | (5, 9)   | 2                                |
| (0, 6)   | -31                          | (2, 9)   | 1                                       | (5, 10)  | $5^3$                            |
| (0, 7)   | $2^6$                        | (2, 10)  | $7^3$                                   | (5, 11)  | 19                               |
| (0, 8)   | $2 \cdot 31$                 | (2, 11)  | 2                                       | (6, 7)   | $41 \cdot 257$                   |
| (0, 9)   | -1                           | (3, 4)   | $3 \cdot 11 \cdot 17 \cdot 31$          | (6, 8)   | $3 \cdot 5^3 \cdot 31$           |
| (0, 10)  | 31                           | (3, 5)   | $-2^5 \cdot 19$                         | (6, 9)   | 17                               |
| (0, 11)  | $-2^2 \cdot 3$               | (3, 6)   | $-7^2 \cdot 17 \cdot 31$                | (6, 10)  | $2 \cdot 5 \cdot 17 \cdot 31$    |
| (1, 2)   | $-5 \cdot 7$                 | (3, 7)   | $3 \cdot 11 \cdot 19$                   | (6, 11)  | $7^2$                            |
| (1, 3)   | $11 \cdot 17 \cdot 19$       | (3, 8)   | $-11 \cdot 19 \cdot 31$                 | (7, 8)   | $-2 \cdot 7 \cdot 11 \cdot 19$   |
| (1, 4)   | $7 \cdot 11 \cdot 17$        | (3, 9)   | $-2 \cdot 3^3 \cdot 17$                 | (7, 9)   | $-3 \cdot 5^3$                   |
| (1, 5)   | -19                          | (3, 10)  | $-17 \cdot 31$                          | (7, 10)  | $-7^3$                           |
| (1, 6)   | $-2^5 \cdot 17$              | (3, 11)  | $-7^2 \cdot 11 \cdot 19$                | (7, 11)  | $-2^2 \cdot 5 \cdot 11 \cdot 19$ |
| (1, 7)   | $7 \cdot 11 \cdot 19$        | (4, 5)   | -131                                    | (8, 9)   | -409                             |
| (1, 8)   | $7 \cdot 11 \cdot 19$        | (4, 6)   | $-13 \cdot 17 \cdot 31$                 | (8, 10)  | $5 \cdot 7 \cdot 31$             |
| (1, 9)   | -17                          | (4, 7)   | $-2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ | (8, 11)  | $-2 \cdot 11^2 \cdot 19$         |
| (1, 10)  | $2 \cdot 3 \cdot 7 \cdot 17$ | (4, 8)   | $-2^2 \cdot 7 \cdot 11 \cdot 31$        | (9, 10)  | $11 \cdot 17$                    |
| (1, 11)  | $-11 \cdot 19$               | (4, 9)   | $-3 \cdot 5 \cdot 17$                   | (9, 11)  | -5                               |
| (2, 3)   | $41^2$                       | (4, 10)  | $-7 \cdot 17 \cdot 31$                  | (10, 11) | -2089                            |

so that  $F = 432\pi_F$ ,  $H = 16\pi_H$  and  $J = 24\pi_J$ , since  $c_0c_1c_2c_3 = 432$ ,  $c_4c_5c_6c_7 = 16$  and  $c_8c_9c_{10}c_{11} = 24$ .

The moving index sets are  $G_E = I_F \cup I_H = \{0, \dots, 7\}$  and  $G_{E'} = I_F \cup I_J$ , and the ordered bases are

$$\begin{aligned}\mathcal{B}_E &= (-1, 2, 3, 5, p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7), \\ \mathcal{B}_{E'} &= (-1, 2, 3, 5, p_0, p_1, p_2, p_3, p_8, p_9, p_{10}, p_{11}).\end{aligned}\tag{6.7}$$

We have  $n_E = n_{E'} = 12$ . The constants of Definition 4.10 are

$$\begin{aligned}\kappa_E &= -B \prod_{j \in G_E} c_j = -2700 \cdot 6912 = -4320^2, \\ \kappa_{E'} &= C \prod_{j \in G_{E'}} c_j = 57600 \cdot 10368 = 2 \cdot 17280^2,\end{aligned}\tag{6.8}$$

so that  $[\kappa_E] = [-1]$  and  $[\kappa_{E'}] = [2]$ . Since  $\kappa_E$  and  $\kappa_{E'}$  have no prime factors other than 2, 3 and 5, each of the lists (6.4) consists of  $-1$  and distinct primes, including every prime dividing  $\kappa_E$  and  $\kappa_{E'}$ . By Lemma 4.8, at every prime specialization,  $\mathcal{B}_E$  and  $\mathcal{B}_{E'}$  are ambient bases for  $E$  and  $E'$  in the sense of Definition 3.9, and  $E(\mathbb{Q})[2] = \{O, T\}$ .

## 6.2 Rational points and the lower bound

We use the binary quadratic forms

$$\begin{aligned}D &= -165M^2 - 226MN + 62N^2, & D_1 &= -8745M^2 - 5440MN + 1550N^2, \\ V &= -7755M^2 - 3187MN + 1240N^2,\end{aligned}\tag{6.9}$$

and the two combinations

$$\begin{aligned}2D_1 - 55D &= -8415M^2 + 1550MN - 310N^2, \\ 3D_1 + 65D &= -36960M^2 - 31010MN + 8680N^2.\end{aligned}$$

The forms  $D$  and  $D_1$  come from the parametrization of a conic (see Appendix B.1). Table 6.3 lists five points; for each, the table gives the abscissa  $x$  and the ratio  $y/x$ .

**Lemma 6.1** (Points). *For every  $(M, N) \in \mathbb{Z}^2$  with  $FHJ \neq 0$ , the points  $P_1, P_2$  of Table 6.3 lie in  $E_{M,N}(\mathbb{Q})$ , and the points  $Q_1, Q_2, Q_3$  lie in  $E'_{M,N}(\mathbb{Q})$ .*

*Proof.* Consider a curve  $y^2 = x^3 + \alpha x^2 + \beta x$  and a pair  $(x, y)$  with  $y = \rho x$ . Then

$$y^2 - x^3 - \alpha x^2 - \beta x = x^2 \left( \rho^2 - x - \alpha - \frac{\beta}{x} \right).$$

In each of the five cases,  $\beta/x$  is a polynomial in  $M$  and  $N$ , and it suffices to check that  $\rho^2 = x + \alpha + \beta/x$  as polynomials. For  $P_1$ , we have  $\rho = -24D$ ,  $x = -150F$  and  $\beta/x = 18H$ , and

Table 6.3. Points on  $E$  and  $E'$ . The ordinate is  $y = x \cdot (y/x)$ .

| point        | $x$                              | $y/x$                     |
|--------------|----------------------------------|---------------------------|
| $P_1 \in E$  | $-150F$                          | $-24D$                    |
| $P_2 \in E$  | $\frac{10}{49}L_2L_3L_6L_7$      | $\frac{8}{7}(2D_1 - 55D)$ |
| $Q_1 \in E'$ | $24J$                            | $12D$                     |
| $Q_2 \in E'$ | $120L_0L_1L_8L_9$                | $\frac{6}{7}(3D_1 + 65D)$ |
| $Q_3 \in E'$ | $\frac{1600}{49}L_1L_2L_8L_{10}$ | $\frac{2}{7}V$            |

the condition reads  $576D^2 = 1350F + 18H$ . For  $P_2$ , we have  $\beta/x = -13230 L_0L_1L_4L_5$ , and after multiplication by 49 the condition becomes the second identity in (6.10) below. For the points on  $E'$ , we have  $\beta'/x = 2400F$ ,  $480L_2L_3L_{10}L_{11}$  and  $1764L_0L_3L_9L_{11}$ , respectively. After dividing by 18, 1, 24, 1 and 1, and multiplying by 1, 49, 1, 49 and 49, respectively, the five conditions become

$$\begin{aligned}
32D^2 &= 75F + H, \\
64(2D_1 - 55D)^2 &= 10L_2L_3L_6L_7 + 73500F - 648270L_0L_1L_4L_5, \\
6D^2 &= J - 25F, \\
36(3D_1 + 65D)^2 &= 5880L_0L_1L_8L_9 - 147000F + 23520L_2L_3L_{10}L_{11}, \\
4V^2 &= 1600L_1L_2L_8L_{10} - 147000F + 86436L_0L_3L_9L_{11}.
\end{aligned} \tag{6.10}$$

Both sides of each line are binary quartic forms, and each line amounts to five equalities between integers, which follow from Table 6.4. For instance, the coefficients of  $M^4$  in the first line are  $32 \cdot 27225 = 871200$  and  $75 \cdot 28314 - 1252350 = 871200$ .  $\square$

Next, we compute the classes of these points and of the 2-torsion points  $T$  and  $T'$  at a prime specialization. By Definition 3.3, we have  $\delta_E(T) = [\beta]$ ,  $\delta_{E'}(T') = [\beta']$ , and  $\delta_E(P) = [x(P)]$  for the other points. We substitute  $L_i = c_i p_i$  and remove square factors from the constants. For example,

$$\begin{aligned}
\beta &= -2700FH = -2700 \cdot 432 \cdot 16 \pi_F \pi_H = -4320^2 \pi_F \pi_H, \\
\frac{10}{49}L_2L_3L_6L_7 &= \frac{10}{49} \cdot 16 p_2 p_3 p_6 p_7 = 10 \left(\frac{4}{7}\right)^2 p_2 p_3 p_6 p_7.
\end{aligned}$$

Table 6.5 lists all seven classes, and (6.11) gives their coordinate vectors in the bases (6.7).

Table 6.4. Coefficients of the binary quartic forms in (6.1) and (6.10), in the monomials  $M^4$ ,  $M^3N$ ,  $M^2N^2$ ,  $MN^3$ ,  $N^4$ .

| form                 | $M^4$      | $M^3N$     | $M^2N^2$  | $MN^3$     | $N^4$    |
|----------------------|------------|------------|-----------|------------|----------|
| $F$                  | 28314      | 23111      | -7929     | 310        | 0        |
| $H$                  | -1252350   | 653235     | 1574387   | -920018    | 123008   |
| $J$                  | 871200     | 1025255    | -14529    | -160394    | 23064    |
| $D^2$                | 27225      | 74580      | 30616     | -28024     | 3844     |
| $(2D_1 - 55D)^2$     | 70812225   | -26086500  | 7619800   | -961000    | 96100    |
| $(3D_1 + 65D)^2$     | 1366041600 | 2292259200 | 319994500 | -538333600 | 75342400 |
| $V^2$                | 60140025   | 49430370   | -9075431  | -7903760   | 1537600  |
| $L_0L_1L_4L_5$       | -3630      | 5467       | -1605     | 62         | 0        |
| $L_2L_3L_6L_7$       | 9768330    | 17589759   | 2997535   | -4409626   | 615040   |
| $L_0L_1L_8L_9$       | 10890      | 4147       | -1575     | 62         | 0        |
| $L_2L_3L_{10}L_{11}$ | 2265120    | 3651967    | 440625    | -822058    | 115320   |
| $L_1L_2L_8L_{10}$    | 627264     | 832590     | 119083    | -91760     | 3844     |
| $L_0L_3L_9L_{11}$    | 39325      | 26180      | -16109    | 1860       | 0        |

Table 6.5. Classes of the points at a prime specialization. The class is  $[g \prod_j p_j]$ , where  $g$  is the constant and  $j$  runs over the moving support.

| point        | class               | constant after $L_i = c_i p_i$        | $g$ | moving support           |
|--------------|---------------------|---------------------------------------|-----|--------------------------|
| $T \in E$    | $[-2700FH]$         | $-2700 \cdot 6912 = -4320^2$          | -1  | 0, 1, 2, 3, 4, 5, 6, 7   |
| $P_1 \in E$  | $[-150F]$           | $-150 \cdot 432 = -2 \cdot 180^2$     | -2  | 0, 1, 2, 3               |
| $P_2 \in E$  | $[10L_2L_3L_6L_7]$  | $10 \cdot 16 = 10 \cdot 4^2$          | 10  | 2, 3, 6, 7               |
| $T' \in E'$  | $[57600FJ]$         | $57600 \cdot 10368 = 2 \cdot 17280^2$ | 2   | 0, 1, 2, 3, 8, 9, 10, 11 |
| $Q_1 \in E'$ | $[24J]$             | $24 \cdot 24 = 24^2$                  | 1   | 8, 9, 10, 11             |
| $Q_2 \in E'$ | $[120L_0L_1L_8L_9]$ | $120 \cdot 216 = 5 \cdot 72^2$        | 5   | 0, 1, 8, 9               |
| $Q_3 \in E'$ | $[L_1L_2L_8L_{10}]$ | $32 = 2 \cdot 4^2$                    | 2   | 1, 2, 8, 10              |

In coordinates, the classes are

$$\begin{aligned}
\mathbf{v}_1 &= \delta_E(T) = (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1), \\
\mathbf{v}_2 &= \delta_E(P_1) = (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0), \\
\mathbf{v}_3 &= \delta_E(P_2) = (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1), \\
\mathbf{w}_1 &= \delta_{E'}(T') = (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1), \\
\mathbf{w}_2 &= \delta_{E'}(Q_1) = (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1), \\
\mathbf{w}_3 &= \delta_{E'}(Q_2) = (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0), \\
\mathbf{w}_4 &= \delta_{E'}(Q_3) = (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0).
\end{aligned} \tag{6.11}$$

**Lemma 6.2** (Lower bound). *At every prime specialization, the classes  $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$  are independent elements of  $\delta_E(E(\mathbb{Q}))$ , and the classes  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3, \mathbf{w}_4$  are independent elements of  $\delta_{E'}(E'(\mathbb{Q}))$ . In particular,  $d_E \geq 3$  and  $d_{E'} \geq 4$ .*

*Proof.* At a prime specialization, we have  $FHJ \neq 0$  by Lemma 4.8, and Lemma 6.1 implies that the points of Table 6.3 are rational points. Their classes, and those of  $T$  and  $T'$ , lie in  $\delta_E(E(\mathbb{Q}))$  and  $\delta_{E'}(E'(\mathbb{Q}))$ , and they are given by (6.11). By Lemma 3.12, it suffices to find suitable columns. On  $E$ , we take the columns  $p_4, p_0, p_6$  for  $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ : the vector  $\mathbf{v}_1$  has entry 1 at  $p_4$ , where  $\mathbf{v}_2$  and  $\mathbf{v}_3$  vanish;  $\mathbf{v}_2$  has entry 1 at  $p_0$ , where  $\mathbf{v}_3$  vanishes; and  $\mathbf{v}_3$  has entry 1 at  $p_6$ . On  $E'$ , the columns  $p_3, p_{11}, p_0, p_2$  for  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3, \mathbf{w}_4$  have the same property, as one reads off from (6.11).  $\square$

### 6.3 The congruence class and the real cone

We impose the congruences in Table 6.6. The moduli are pairwise coprime, and their product is

$$W = 2^6 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 31 = 19984345920.$$

By the Chinese remainder theorem, the congruences are equivalent to

$$M \equiv M_0, \quad N \equiv N_0 \pmod{W}, \quad M_0 = 6555660534, \quad N_0 = -1. \tag{6.12}$$

One checks directly that  $M_0 \equiv 54 \pmod{2^6 \cdot 3^4 \cdot 5}$  (note  $2^6 \cdot 3^4 \cdot 5 = 25920$  and  $54 \equiv 4 \pmod{5}$ ), and that  $M_0 \equiv 3, 5, 4, 18, 14 \pmod{7, 11, 17, 19, 31}$ , respectively. We write  $\mathcal{P}_5$  for the set of  $(M, N) \in \mathbb{Z}^2$  satisfying (6.12).

Table 6.6. The congruences defining  $\mathcal{P}_5$ .

| modulus   | $2^6$ | $3^4$ | 5  | 7  | 11 | 17 | 19 | 31 |
|-----------|-------|-------|----|----|----|----|----|----|
| $M \bmod$ | 54    | 54    | 4  | 3  | 5  | 4  | 18 | 14 |
| $N \bmod$ | -1    | -1    | -1 | -1 | -1 | -1 | -1 | -1 |

**Lemma 6.3** (Residues on the progression). *Let  $(M, N) \in \mathcal{P}_5$ . For every  $i$ , the cofactor  $c_i$  divides  $L_i(M, N)$ , and the integer  $p_i = L_i(M, N)/c_i$  satisfies the congruences of Table 6.7. In particular, every  $p_i$  is prime to  $W$ , and  $FHJ \neq 0$ .*

Table 6.7. Residues of  $p_i = L_i(M, N)/c_i$  modulo  $q$ , for  $(M, N) \in \mathcal{P}_5$ .

| $q \backslash i$ | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 |
|------------------|----|----|----|----|----|----|----|----|----|----|----|----|
| 8                | 1  | 5  | 5  | 7  | 5  | 3  | 3  | 5  | 1  | 7  | 1  | 1  |
| 3                | 1  | 1  | 1  | 1  | 2  | 1  | 1  | 1  | 1  | 1  | 2  | 2  |
| 5                | 1  | 4  | 1  | 2  | 1  | 3  | 3  | 3  | 1  | 1  | 2  | 2  |
| 7                | 2  | 4  | 1  | 1  | 4  | 3  | 4  | 5  | 1  | 2  | 2  | 5  |
| 11               | 6  | 1  | 10 | 10 | 6  | 5  | 6  | 1  | 1  | 4  | 8  | 2  |
| 17               | 7  | 4  | 9  | 9  | 3  | 13 | 5  | 10 | 7  | 4  | 12 | 16 |
| 19               | 13 | 17 | 11 | 6  | 11 | 17 | 7  | 7  | 12 | 15 | 13 | 15 |
| 31               | 6  | 30 | 16 | 18 | 20 | 12 | 10 | 12 | 21 | 9  | 14 | 27 |

*Proof.* We begin with the moduli 8, 3 and 5. Since  $M_0 \equiv 54 \pmod{25920}$ ,  $N_0 = -1$  and  $25920 = 2^6 \cdot 3^4 \cdot 5$  divides  $W$ , every  $(M, N) \in \mathcal{P}_5$  satisfies  $(M, N) \equiv (54, -1) \pmod{25920}$ . The values  $L_i(54, -1) = 54a_i - b_i$  are

$$54, 1189, 488, 7567, -3032, 163, 7483, 2906, 5284, 271, 1697, 2982,$$

and their quotients by  $c_i$  are the integers

$$1, 1189, 61, 7567, -379, 163, 7483, 1453, 1321, 271, 1697, 497. \quad (6.13)$$

Each  $c_i$  divides  $2^3 \cdot 3^3$ . Hence  $c_i$  divides 25920, and  $25920/c_i$  is an integer divisible by  $2^3 \cdot 3 \cdot 5 = 120$ . By Lemma 4.7 with  $W_0 = 25920$  and  $(m, n) = (54, -1)$ , the cofactor  $c_i$  divides  $L_i(M, N)$ , and  $p_i$  is congruent modulo  $25920/c_i$ , and hence modulo 120, to the  $i$ -th integer in (6.13). Reducing (6.13) modulo 8, 3 and 5 gives the first three rows of Table 6.7. All entries in these rows are nonzero. We note that the integer of index 4 in (6.13) is negative: the residues of  $p_4$  are those of  $-379$ , not those of 379 (for instance,  $-379 \equiv 5$  and  $379 \equiv 3 \pmod{8}$ ).

Now let  $q \in \{7, 11, 17, 19, 31\}$ . Then  $q \nmid c_i$ , and by (6.12) we have  $(M, N) \equiv (r_q, -1) \pmod{q}$ , where  $r_q = 3, 5, 4, 18, 14$ , respectively. We obtain

$$p_i \equiv (a_i r_q - b_i) c_i^{-1} \pmod{q},$$

which gives the remaining rows of Table 6.7. For example, for  $q = 7$  and  $i = 4$ , we have  $(-55 \cdot 3 - 62) \cdot 8^{-1} \equiv (-227) \cdot 1 \equiv 4 \pmod{7}$ . All entries are nonzero, which implies that every  $p_i$  is prime to  $W$ . Then  $L_i(M, N) \neq 0$  for every  $i$ , and  $FHJ \neq 0$ .  $\square$

The cone is

$$\mathcal{K}_5 = \left\{ (M, N) \in \mathbb{R}^2 : M > 0, \frac{19}{20}M < N < \frac{11}{10}M \right\}. \quad (6.14)$$

It is an open convex cone.

**Lemma 6.4** (Positivity on the cone). *Every  $L_i$  is positive on  $\mathcal{K}_5$ . In particular,  $F$ ,  $H$  and  $J$  are positive on  $\mathcal{K}_5$ .*

*Proof.* Let  $(M, N) \in \mathcal{K}_5$  and  $t = N/M$ , so that  $19/20 < t < 11/10$ . Then  $L_i = M(a_i + b_i t)$ , and  $L_0 = M > 0$ . If  $b_i > 0$ , then  $a_i + b_i t > 0$  if and only if  $t > -a_i/b_i$ ; the largest of these thresholds is  $-a_4/b_4 = 55/62 < 19/20$ . If  $b_i < 0$ , then  $a_i + b_i t > 0$  if and only if  $t < a_i/|b_i|$ ; the smallest of these thresholds is  $a_5/|b_5| = 3 > 11/10$ . Hence  $a_i + b_i t > 0$  for every  $i$ .  $\square$

The proof shows that the twelve forms are positive exactly when  $M > 0$  and  $55/62 < N/M < 3$ . We note that  $(54, -1)$  and  $(M_0, N_0)$  are not in  $\mathcal{K}_5$ ; this does not matter, because Lemma 6.3 concerns residues only.

## 6.4 Local conditions at the fixed places

We now bound the local images at the places 2, 3, 5 and  $\infty$ . Recall from Definition 3.3 that  $\delta_{E,v}$  denotes the local descent map on  $E(\mathbb{Q}_v)$ .

**Lemma 6.5** (Local images at the fixed places). *Let  $(M, N) \in \mathcal{P}_5$ . Then  $FHJ \neq 0$ , and the local images satisfy the inclusions in Table 6.8, at the places 2, 3 and 5. If moreover  $(M, N) \in \mathcal{K}_5$ , then they also satisfy the inclusions in the last line of Table 6.8.*

Table 6.8. Upper bounds for the local images at the fixed places.

| $v$      | $\delta_{E,v}(E(\mathbb{Q}_v))$                       | $\delta_{E',v}(E'(\mathbb{Q}_v))$                         |
|----------|-------------------------------------------------------|-----------------------------------------------------------|
| 2        | $\subseteq \{[1], [2]\}$                              | $\subseteq \{[1], [-1], [2], [-2]\}$                      |
| 3        | $\subseteq \{[1]\}$                                   | $\subseteq \mathbb{Q}_3^\times / \mathbb{Q}_3^{\times 2}$ |
| 5        | $\subseteq \{[1], [5]\}$                              | $\subseteq \{[1], [5]\}$                                  |
| $\infty$ | $\subseteq \mathbb{R}^\times / \mathbb{R}^{\times 2}$ | $\subseteq \{[1]\}$                                       |

The entries  $\mathbb{Q}_3^\times / \mathbb{Q}_3^{\times 2}$  and  $\mathbb{R}^\times / \mathbb{R}^{\times 2}$  impose no condition; we list them for completeness. The proof below uses the parameters at the finite places only through the residues of the numbers  $L_i(M, N)/c_i$  modulo 8, 3 and 5. By Lemma 4.7, applied with  $W_0 = 25920$  to the values at  $(54, -1)$ , these residues are already fixed when  $M \equiv 54$  and  $N \equiv -1 \pmod{25920}$ , so the bounds at 2, 3 and 5 hold for all such pairs. We use them only on  $\mathcal{P}_5$ .

*Proof.* The proof has five parts: the prime 2 for  $E$  and for  $E'$ , the prime 3 for  $E$ , the prime 5 for both curves, and the real place for  $E'$ . In each part, we first rescale the curve. We then treat the points of the local curve in turn: the point at infinity  $O$ , the point  $T$  (or  $T'$ ), the other points with  $y = 0$ , whose existence we decide with Lemma 3.7, and the points with  $y \neq 0$ , sorted by the valuation of  $x$ . The descent class of  $O$  is always  $[1]$ .

**Preliminaries.** By Lemma 6.3, we have  $FHJ \neq 0$ , and  $F = 432\pi_F$ ,  $H = 16\pi_H$ ,  $J = 24\pi_J$ , where  $\pi_F, \pi_H, \pi_J$  are the products (6.6) of integers with the residues of Table 6.7. Multiplying these residues, we find

$$\begin{aligned} (\pi_F, \pi_H, \pi_J) &\equiv (7, 1, 7) \pmod{8}, \\ (\pi_F, \pi_H, \pi_J) &\equiv (1, 2, 1) \pmod{3}, \\ (\pi_F, \pi_H, \pi_J) &\equiv (3, 2, 4) \pmod{5}. \end{aligned} \tag{6.15}$$

These residues are the same for all  $(M, N) \in \mathcal{P}_5$ , and they are the only properties of  $(M, N)$  that we use at 2, 3 and 5. A change of coordinates  $x = \lambda^2 \tilde{x}$ ,  $y = \lambda^3 \tilde{y}$  with  $\lambda \in \mathbb{Q}^\times$  divides the coefficients of  $x^2$  and  $x$  by  $\lambda^2$  and  $\lambda^4$ , and it multiplies  $x$  by a square. It therefore does not change the descent class of any point, including the class  $[\beta]$  of  $T$ . For a point with  $\tilde{y} \neq 0$ , the right side of the rescaled equation is the square  $\tilde{y}^2$ , and we use Lemma 3.2: an element of  $\mathbb{Q}_p^\times$  is a square only if its valuation is even and its unit part is congruent to 1 (mod 8) (if  $p = 2$ ) or to a square modulo  $p$  (if  $p$  is odd). We use Lemma 3.1(a) for valuations, and Lemma 3.1(b) for unit parts: if the other terms have valuation at least  $h$  more than the dominant term, then the unit part of the sum is congruent to that of the dominant term modulo  $p^h$ .

**The prime 2, curve  $E$ .** Let  $F = 16F_2$ ,  $H = 16H_2$  and  $J = 8J_2$ , where  $F_2 = 27\pi_F$ ,  $H_2 = \pi_H$  and  $J_2 = 3\pi_J$  are odd. By (6.15), we have  $F_2 \equiv 5$ ,  $H_2 \equiv 1$  and  $J_2 \equiv 5 \pmod{8}$ . We set

$$\alpha_2 = 375F_2, \quad \beta_2 = -675F_2H_2, \quad \beta'_2 = 225F_2J_2,$$

so that  $\alpha_2 \equiv 3$ ,  $\beta_2 \equiv 1$  and  $\beta'_2 \equiv 1 \pmod{8}$ . The identity (6.1) implies that  $1875F + 9H = 3(625F + 3H) = 48J$ , which gives

$$\alpha_2^2 - \beta_2 = 75F_2(1875F_2 + 9H_2) = \frac{75F_2}{16}(1875F + 9H) = 225F_2J = 8\beta'_2. \tag{6.16}$$

The change of coordinates  $x = 16\tilde{x}$ ,  $y = 64\tilde{y}$  transforms  $E$  into

$$\tilde{y}^2 = g(\tilde{x}), \quad g(\tilde{x}) = \tilde{x}^3 + 4\alpha_2\tilde{x}^2 + 4\beta_2\tilde{x},$$

since  $1500F/16 = 1500F_2 = 4\alpha_2$  and  $-2700FH/16^2 = -2700F_2H_2 = 4\beta_2$ .

The point  $T$  has class  $[4\beta_2] = [\beta_2] = [1]$ , since  $\beta_2 \equiv 1 \pmod{8}$ . By Lemma 3.7, points  $(\tilde{x}_0, 0)$  with  $\tilde{x}_0 \neq 0$  exist only if  $(4\alpha_2)^2 - 16\beta_2 = 16(\alpha_2^2 - \beta_2) = 128\beta'_2$  is a square in  $\mathbb{Q}_2$ . By (6.16), this number has odd valuation 7, and there are no such points.

Now let  $(\tilde{x}, \tilde{y})$  be a point with  $\tilde{y} \neq 0$ , and let  $\tilde{x} = 2^r u$  with  $r = v_2(\tilde{x})$  and  $u \in \mathbb{Z}_2^\times$ . The three terms of  $g(\tilde{x})$  have valuations  $3r, 2r + 2$  and  $r + 2$ .

- If  $r < 0$ , then  $\tilde{x}^3$  is the only term of least valuation, and  $v_2(g(\tilde{x})) = 3r$ . Since this valuation is even, we have  $r \leq -2$ . The other two terms then have valuation at least  $3r + 4$ , and the unit part of  $g(\tilde{x})$  is congruent to  $u^3 \equiv u \pmod{8}$ . Since  $g(\tilde{x})$  is a square, we have  $u \equiv 1 \pmod{8}$  and  $[\tilde{x}] = [1]$ .
- If  $r = 0$ , then  $g(\tilde{x}) = u(u^2 + 4(\alpha_2 u + \beta_2))$ , where  $\alpha_2 u + \beta_2$  is even. Then  $g(\tilde{x}) \equiv u^3 \equiv u \pmod{8}$ , which implies that  $u \equiv 1 \pmod{8}$  and  $[\tilde{x}] = [1]$ .
- If  $r \geq 2$ , then  $4\beta_2 \tilde{x}$  is the only term of least valuation, and  $r$  is even. For  $r = 2$ , we have  $g(4u) = 16u(\beta_2 + 4u(\alpha_2 + u))$ , where  $\alpha_2 + u$  is even. For even  $r \geq 4$ , the other two terms have valuation at least  $(r + 2) + 4$ . In both cases the unit part of  $g(\tilde{x})$  is congruent to  $\beta_2 u \equiv u \pmod{8}$ , and we find  $u \equiv 1 \pmod{8}$  and  $[\tilde{x}] = [1]$ .
- If  $r = 1$ , then (6.16) implies that

$$g(2u) = 8u(u^2 + 2\alpha_2 u + \beta_2) = 8u((u + \alpha_2)^2 - 8\beta'_2).$$

If  $u \equiv 3$  or  $7 \pmod{8}$ , then  $u + \alpha_2 \equiv 2 \pmod{4}$ , and  $(u + \alpha_2)^2$  has valuation 2. By Lemma 3.1, the bracket also has valuation 2, and  $v_2(g(\tilde{x})) = 5$  is odd, a contradiction. If  $u \equiv 5 \pmod{8}$ , then  $8 \mid u + \alpha_2$  and  $(u + \alpha_2)^2 \in 2^6 \mathbb{Z}_2$ . The bracket is then  $-8\beta'_2$  times an element of  $1 + 8\mathbb{Z}_2$ , and the unit part of  $g(\tilde{x})$  is congruent to  $-u\beta'_2 \equiv 3 \pmod{8}$ , which is not a square. The remaining case  $u \equiv 1 \pmod{8}$  gives  $[\tilde{x}] = [2u] = [2]$ .

This shows that  $\delta_{E,2}(E(\mathbb{Q}_2)) \subseteq \{[1], [2]\}$ .

**The prime 2, curve  $E'$ .** The change of coordinates  $x = 64\tilde{x}, y = 512\tilde{y}$  transforms  $E'$  into

$$\tilde{y}^2 = g'(\tilde{x}), \quad g'(\tilde{x}) = \tilde{x}^3 - 2\alpha_2 \tilde{x}^2 + 8\beta'_2 \tilde{x},$$

since  $-3000F/64 = -750F_2 = -2\alpha_2$  and  $57600FJ/64^2 = 1800F_2J_2 = 8\beta'_2$ .

The point  $T'$  has class  $[8\beta'_2] = [2]$ , since  $\beta'_2 \equiv 1 \pmod{8}$ . By (6.16), the discriminant of  $\tilde{x}^2 - 2\alpha_2 \tilde{x} + 8\beta'_2$  is  $4\alpha_2^2 - 32\beta'_2 = 4\beta_2$ , and  $\beta_2 \equiv 1 \pmod{8}$  is a square in  $\mathbb{Q}_2$ . By Lemma 3.7, there are two points  $(\tilde{x}_1, 0)$  and  $(\tilde{x}_2, 0)$  with  $\tilde{x}_1 \tilde{x}_2 \neq 0$ . Their abscissas are  $\alpha_2 \pm s$ , where  $s^2 = \beta_2$  and we choose the sign of  $s$  with  $s \equiv 1 \pmod{4}$ . Then  $\alpha_2 - s \equiv 2 \pmod{4}$ , and  $(\alpha_2 - s)(\alpha_2 + s) = 8\beta'_2$  has valuation 3. We obtain  $\alpha_2 - s = 2u_1$  and  $\alpha_2 + s = 4u_2$  with  $u_1, u_2 \in \mathbb{Z}_2^\times$ , and these satisfy  $u_1 u_2 = \beta'_2 \equiv 1$  and  $u_1 + 2u_2 = \alpha_2 \equiv 3 \pmod{8}$ . Since  $u_1^2 \equiv 1 \pmod{8}$ , the first congruence implies that  $u_2 \equiv u_1 \pmod{8}$ , and the second then reads  $3u_1 \equiv 3 \pmod{8}$ , that is,  $u_1 \equiv u_2 \equiv 1 \pmod{8}$ . The two points have the classes  $[2u_1] = [2]$  and  $[4u_2] = [1]$ .

Now let  $(\tilde{x}, \tilde{y})$  be a point with  $\tilde{y} \neq 0$ , and let  $\tilde{x} = 2^r u$  with  $r = v_2(\tilde{x})$  and  $u \in \mathbb{Z}_2^\times$ . The three terms of  $g'(\tilde{x})$  have valuations  $3r, 2r + 1$  and  $r + 3$ .

- If  $r < 0$ , then  $\tilde{x}^3$  is the only term of least valuation, and as before  $r \leq -2$ . The other two terms have valuation at least  $3r + 3$ , and the unit part of  $g'(\tilde{x})$  is congruent to  $u \pmod{8}$ . We find  $u \equiv 1 \pmod{8}$  and  $[\tilde{x}] = [1]$ .
- If  $r = 0$ , then  $g'(u) = u^3 - 2\alpha_2 u^2 + 8\beta'_2 u \equiv u - 6 \pmod{8}$ , where we used  $u^2 \equiv 1$  and  $2\alpha_2 \equiv 6 \pmod{8}$ . This is a square only if  $u \equiv 7 \pmod{8}$ , which gives  $[\tilde{x}] = [-1]$ .
- If  $r \geq 3$ , then  $8\beta'_2 \tilde{x}$  is the only term of least valuation, and  $r$  is odd. For  $r = 3$ , we have  $g'(8u) = 64u(\beta'_2 - 2\alpha_2 u + 8u^2)$ , whose unit part is congruent to  $u(1 - 6u) \equiv u - 6 \pmod{8}$ ; this implies that  $u \equiv 7 \pmod{8}$  and  $[\tilde{x}] = [8 \cdot 7] = [-2]$ . For odd  $r \geq 5$ , the other two terms have valuation at least  $(r + 3) + 3$ , the unit part of  $g'(\tilde{x})$  is congruent to  $\beta'_2 u \equiv u \pmod{8}$ , and we find  $u \equiv 1 \pmod{8}$  and  $[\tilde{x}] = [2]$ .
- If  $r = 1$  or  $r = 2$ , then

$$\begin{aligned} g'(2u) &= 2^3 u g_1(u), & g_1(u) &= u^2 - \alpha_2 u + 2\beta'_2, \\ g'(4u) &= 2^5 u g_2(u), & g_2(u) &= 2u^2 - \alpha_2 u + \beta'_2. \end{aligned}$$

Since  $u^2 \equiv 1$ ,  $\alpha_2 \equiv 3$  and  $\beta'_2 \equiv 1 \pmod{8}$ , we have  $g_1(u) \equiv g_2(u) \equiv 3 - 3u \pmod{8}$ . If  $u \equiv 5 \pmod{8}$ , then  $g_1(u) \equiv g_2(u) \equiv 4 \pmod{8}$  have valuation 2, and  $v_2(g'(\tilde{x}))$  is 5 or 7, which is odd. If  $u \equiv 3 \pmod{8}$ , then  $g_i(u) \equiv 2 \pmod{8}$ . In that case  $g_i(u) = 2w$  with  $w \equiv 1 \pmod{4}$ , and the unit part  $uw$  of  $g'(\tilde{x})$  is congruent to 3  $\pmod{4}$ ; it is not a square. Only the residues of  $u$ ,  $\alpha_2$  and  $\beta'_2$  modulo 8 enter this argument, and it applies to every  $u$  in the residue class and every parameter in  $\mathcal{P}_5$ . The remaining residues  $u \equiv 1, 7 \pmod{8}$  give  $[\tilde{x}] \in \{[\pm 2], [\pm 1]\}$ .

Altogether, every point of  $E'(\mathbb{Q}_2)$  has one of the classes  $[1], [-1], [2], [-2]$ , which proves the inclusion for  $E'$  at 2.

**The prime 3, curve  $E$ .** We have  $F = 27F_3$  with  $F_3 = 16\pi_F \equiv 1 \pmod{3}$ , and  $H = 16\pi_H \equiv 2 \pmod{3}$  by (6.15). The change of coordinates  $x = 9\tilde{x}$ ,  $y = 27\tilde{y}$  transforms  $E$  into

$$\tilde{y}^2 = h(\tilde{x}), \quad h(\tilde{x}) = \tilde{x}^3 + 9\alpha_3 \tilde{x}^2 + 9\beta_3 \tilde{x}, \quad \alpha_3 = 500F_3, \quad \beta_3 = -100F_3H,$$

where  $\alpha_3 \equiv 2$  and  $\beta_3 \equiv 1 \pmod{3}$ . The point  $T$  has class  $[9\beta_3] = [1]$ , since  $\beta_3$  is a unit congruent to a square modulo 3. The discriminant of  $\tilde{x}^2 + 9\alpha_3 \tilde{x} + 9\beta_3$  is  $9(9\alpha_3^2 - 4\beta_3)$ , and  $9\alpha_3^2 - 4\beta_3 \equiv 2 \pmod{3}$  is not a square modulo 3. By Lemma 3.7, there are no points  $(\tilde{x}_0, 0)$  with  $\tilde{x}_0 \neq 0$ .

Let  $(\tilde{x}, \tilde{y})$  be a point with  $\tilde{y} \neq 0$ , and let  $\tilde{x} = 3^r u$  with  $r = v_3(\tilde{x})$  and  $u \in \mathbb{Z}_3^\times$ . The three terms of  $h(\tilde{x})$  have valuations  $3r$ ,  $2r + 2$  and  $r + 2$ .

- If  $r \leq 0$ , then  $\tilde{x}^3$  is the only term of least valuation, and the other two terms have valuation at least  $3r + 2$ . We find that  $r$  is even and that the unit part of  $h(\tilde{x})$  is congruent to  $u^3 \equiv u \pmod{3}$ . This implies that  $u \equiv 1 \pmod{3}$  and  $[\tilde{x}] = [1]$ .

- If  $r \geq 2$ , then  $9\beta_3\tilde{x}$  is the only term of least valuation, and the other two terms have valuation at least  $(r+2)+2$ . As before,  $r$  is even and the unit part of  $h(\tilde{x})$  is congruent to  $\beta_3u \equiv u \pmod{3}$ , which gives  $[\tilde{x}] = [1]$ .
- If  $r = 1$ , then  $h(3u) = 27u(u^2 + 3\alpha_3u + \beta_3)$ , and the bracket is congruent to  $1 + 1 = 2 \pmod{3}$ . Then  $v_3(h(\tilde{x})) = 3$  is odd, a contradiction.

Every point of  $E(\mathbb{Q}_3)$  has class  $[1]$ , and  $\delta_{E,3}(E(\mathbb{Q}_3)) = \{[1]\}$ .

**The prime 5.** By (6.15),  $F, H$  and  $J$  are units at 5, with  $F \equiv 432 \cdot 3 \equiv 1$ ,  $H \equiv 16 \cdot 2 \equiv 2$  and  $J \equiv 24 \cdot 4 \equiv 1 \pmod{5}$ . For either curve, we denote its coefficients by  $125\alpha_5$  and  $25\beta_5$ : for  $E$ , we have  $\alpha_5 = 12F$  and  $\beta_5 = -108FH \equiv 4 \pmod{5}$ , and for  $E'$ , we have  $\alpha_5 = -24F$  and  $\beta_5 = 2304FJ \equiv 4 \pmod{5}$ . Both curves have the form

$$y^2 = k(x), \quad k(x) = x^3 + 125\alpha_5x^2 + 25\beta_5x, \quad \alpha_5 \in \mathbb{Z}_5, \quad \beta_5 \equiv 4 \pmod{5}.$$

The point  $(0,0)$  has class  $[25\beta_5] = [1]$ , since 4 is a square modulo 5. The discriminant  $25(625\alpha_5^2 - 4\beta_5)$  is 25 times a unit congruent to 4  $\pmod{5}$ , and it is a square. By Lemma 3.7, there are two points  $(x_0, 0)$  with  $x_0 \neq 0$ . Let  $(x_0, 0)$  be one of them, and let  $r = v_5(x_0)$ . If  $r \leq 0$ , the term  $x_0^2$  is the only term of least valuation in  $x_0^2 + 125\alpha_5x_0 + 25\beta_5$ , and if  $r \geq 2$ , the term  $25\beta_5$  is; in both cases Lemma 3.1 shows that the sum is not zero. The only possibility is  $r = 1$ , that is,  $x_0 = 5u$  with  $u \in \mathbb{Z}_5^\times$  and  $u^2 + 25\alpha_5u + \beta_5 = 0$ , which gives  $u^2 \equiv -\beta_5 \equiv 1 \pmod{5}$ . Then  $u \equiv \pm 1$  is a square modulo 5, and  $[x_0] = [5]$ .

Let  $(x, y)$  be a point with  $y \neq 0$ , and let  $x = 5^r u$  with  $r = v_5(x)$  and  $u \in \mathbb{Z}_5^\times$ . The three terms of  $k(x)$  have valuations  $3r$ , at least  $2r + 3$ , and  $r + 2$ .

- If  $r \leq 0$ , then  $x^3$  is the only term of least valuation, and the unit part of  $k(x)$  is congruent to  $u^3 \pmod{5}$ . We find that  $r$  is even and that  $u$  is a square modulo 5, and  $[x] = [1]$ .
- If  $r \geq 2$ , then  $25\beta_5x$  is the only term of least valuation, and the unit part of  $k(x)$  is congruent to  $4u \pmod{5}$ . Again  $r$  is even and  $u$  is a square modulo 5, and  $[x] = [1]$ .
- If  $r = 1$ , then  $k(5u) = 125u(u^2 + \beta_5 + 25\alpha_5u)$ . If  $u \not\equiv \pm 1 \pmod{5}$ , then  $u^2 \equiv 4$ , the bracket is congruent to 3  $\pmod{5}$ , and  $v_5(k(x)) = 3$  is odd, a contradiction. If  $u \equiv \pm 1 \pmod{5}$ , then  $u$  is a square and  $[x] = [5]$ .

We conclude that  $\delta_{E,5}(E(\mathbb{Q}_5))$  and  $\delta_{E',5}(E'(\mathbb{Q}_5))$  are contained in  $\{[1], [5]\}$ .

**The real place, curve  $E'$ .** Let  $(M, N) \in \mathcal{K}_5$ . By Lemma 6.4, we have  $F, H, J > 0$ . The point  $T'$  has class  $[57600FJ] = [1]$ . The discriminant of  $x^2 - 3000Fx + 57600FJ$  is  $16\beta = -43200FH < 0$ , and there are no other real points with  $y = 0$ . If  $(x, y)$  is a real point with  $y \neq 0$  and  $x < 0$ , then  $x^2 - 3000Fx + 57600FJ > 0$  and  $y^2 = x(x^2 - 3000Fx + 57600FJ) < 0$ , which is impossible. Every point with  $y \neq 0$  therefore has  $x > 0$ , and  $\delta_{E',\infty}(E'(\mathbb{R})) = \{[1]\}$ . This completes the proof.  $\square$

We now turn the inclusions of Lemma 6.5 into rows in the sense of Definition 3.9. We use the coordinates of Section 3.1: a class in  $\mathbb{Q}_2^\times / \mathbb{Q}_2^{\times 2}$  has coordinates  $(e_1, e_2, e_3)$  with respect to  $[-1], [2], [5]$ , a class in  $\mathbb{Q}_q^\times / \mathbb{Q}_q^{\times 2}$  for odd  $q$  has the valuation coordinate  $v_q$  and the character coordinate  $\chi_q$  of (3.3), and in  $\mathbb{R}^\times / \mathbb{R}^{\times 2}$  we use the sign coordinate  $\text{sgn}$ . Let  $U_v$  be the subgroup in the row of Table 6.8 for the place  $v$ . The linear maps vanishing on  $U_2 = \{[1], [2]\}$  (for  $E$ ) are spanned by  $e_1$  and  $e_3$ ; on  $U_2 = \{[\pm 1], [\pm 2]\}$  (for  $E'$ ), by  $e_3$ ; on  $U_3 = \{[1]\}$ , by  $\chi_3$  and  $v_3$ ; on  $U_5 = \{[1], [5]\}$ , by  $\chi_5$ ; and on  $U_\infty = \{[1]\}$ , by  $\text{sgn}$ . The rows defined by these triples  $(v, U_v, f)$  are the five fixed rows  $f_1^E, \dots, f_5^E$  for  $E$  and the three fixed rows  $f_1^{E'}, f_2^{E'}, f_3^{E'}$  for  $E'$  in Table 6.9, in the notation of Proposition 4.18. By (3.27), their entries are the values of these coordinates at the entries of  $\mathcal{B}_E$  and  $\mathcal{B}_{E'}$ . At the constants  $-1, 2, 3, 5$ , the values follow from  $3 \equiv 3 \pmod{8}$ ,  $5 \equiv 5 \pmod{8}$  and the Legendre symbols modulo 3 and 5. At  $p_j$ , the entries of the rows at the finite places depend only on the residues of  $p_j$  modulo 8, 3 and 5 in Table 6.7, and the entries of the real row  $f_3^{E'}$  are zero at every prime specialization, since the  $p_j$  are positive. The fixed rows are therefore the same at every prime specialization in  $\mathcal{P}_5$ .

Table 6.9. The fixed rows, as functions of the basis elements. The last column gives the entry at  $p_j$  in terms of the residues of  $p_j$ .

| row        | place    | coordinate   | -1 | 2 | 3 | 5 | entry at $p_j$                  |
|------------|----------|--------------|----|---|---|---|---------------------------------|
| $f_1^E$    | 2        | $e_1$        | 1  | 0 | 1 | 0 | 1 if $p_j \equiv 3, 7 \pmod{8}$ |
| $f_2^E$    | 2        | $e_3$        | 0  | 0 | 1 | 1 | 1 if $p_j \equiv 3, 5 \pmod{8}$ |
| $f_3^E$    | 3        | $\chi_3$     | 1  | 1 | 0 | 1 | 1 if $p_j \equiv 2 \pmod{3}$    |
| $f_4^E$    | 3        | $v_3$        | 0  | 0 | 1 | 0 | 0                               |
| $f_5^E$    | 5        | $\chi_5$     | 0  | 1 | 1 | 0 | 1 if $p_j \equiv 2, 3 \pmod{5}$ |
| $f_1^{E'}$ | 2        | $e_3$        | 0  | 0 | 1 | 1 | 1 if $p_j \equiv 3, 5 \pmod{8}$ |
| $f_2^{E'}$ | 5        | $\chi_5$     | 0  | 1 | 1 | 0 | 1 if $p_j \equiv 2, 3 \pmod{5}$ |
| $f_3^{E'}$ | $\infty$ | $\text{sgn}$ | 1  | 0 | 0 | 0 | 0                               |

## 6.5 Characters at the moving primes

The moving rows are given by Definition 4.10: they are the rows  $r_i^E$  with  $i \in I_F \cup I_J$  for  $E$ , and the rows  $r_i^{E'}$  with  $i \in I_F \cup I_H$  for  $E'$ . By Corollary 4.14, the entries of these rows are the constant characters  $\lambda_i(g)$  with  $g \in \Gamma_E = \Gamma_{E'}$ , the bits  $\gamma_{ij} + \eta$  at the moving columns  $j \neq i$ , and, for  $i \in I_F$ , the diagonal entries  $\gamma_{ii}^* + \eta$ , where  $\theta_i$ ,  $\gamma_{ij}$  and  $\gamma_{ii}^*$  are defined in (4.26), (4.27) and (4.28), and  $\varepsilon = (N/p_0) = (-1)^\eta$ . We now compute these bits from the residues in Table 6.7 and check that they are the same at all prime specializations in  $\mathcal{P}_5$ .

**Constant characters.** We write  $\sigma_i = \lambda_i(-1)$ . By (4.22),  $\sigma_i = 1$  if and only if  $p_i \equiv 3 \pmod{4}$ , and  $\lambda_i(2) = 1$  if and only if  $p_i \equiv 3, 5 \pmod{8}$ . For an odd prime  $q \neq p_i$ , we have  $\lambda_i(q) = \chi_q(p_i) + \sigma_i \chi_q(-1)$  by Lemma 4.13. We see that  $\lambda_i(q)$  is determined by the residue of  $p_i$  modulo  $q$  and by  $\sigma_i$ , and that the correction  $\sigma_i$  enters only when  $q \equiv 3 \pmod{4}$ . The nonzero squares modulo 7, 11, 17, 19 and 31 are  $\{1, 2, 4\}$ ,  $\{1, 3, 4, 5, 9\}$ ,  $\{1, 2, 4, 8, 9, 13, 15, 16\}$ ,  $\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$  and  $\{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\}$ . Applying these rules to Table 6.7, we find the entries of Table 6.10. The rows for  $-1, 2, 3, 5$  give the entries of the moving rows in the constant columns; the other rows are used for the bits  $\gamma_{ij}$  below.

Table 6.10. The constant characters  $\lambda_i(g)$ , where  $(g/p_i) = (-1)^{\lambda_i(g)}$ .

| $g \backslash i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|------------------|---|---|---|---|---|---|---|---|---|---|----|----|
| -1               | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0  | 0  |
| 2                | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0  | 0  |
| 3                | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1  | 1  |
| 5                | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1  | 1  |
| 7                | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0  | 1  |
| 11               | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1  | 1  |
| 17               | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1  | 0  |
| 19               | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1  | 1  |
| 31               | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0  | 1  |

**Cross symbols.** By Table 6.7, we have  $p_0 \equiv 1 \pmod{8}$  on  $\mathcal{P}_5$ , and  $\lambda_0(-1) = 0$ . Then (4.26) and (4.27) read

$$\theta_i = \lambda_0(b_i c_i), \quad \gamma_{0j} = \theta_j, \quad \gamma_{i0} = \theta_i, \quad \gamma_{ij} = \lambda_i(K_{ij}) + \theta_i \quad (i, j \geq 1), \quad (6.17)$$

where  $K_{ij} = c_0 c_j b_i \Delta_{ji} = 54 c_j b_i (a_j b_i - a_i b_j)$ . The numbers  $b_i c_i$  have the square-free parts

$$-1, -1, 5 \cdot 31, 31, -1, -31, 2, 2 \cdot 31, -1, 31, -2 \quad (i = 1, \dots, 11),$$

and since  $\lambda_0(-1) = \lambda_0(2) = \lambda_0(5) = 0$  and  $\lambda_0(31) = 1$  by Table 6.10, we find

$$(\theta_1, \dots, \theta_{11}) = (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0). \quad (6.18)$$

By Remark 4.15, the bits  $\gamma_{ij}$  are needed for  $i \in I_F$  and every  $j \neq i$ , and for the pairs with one index in  $I_H$  and the other in  $I_J$ . In Table 6.11, we list the square-free part  $s_{ij}$  of  $K_{ij}$  for every needed pair with  $1 \leq i < j$ , together with  $\lambda_i(K_{ij})$ , which is the sum of the entries of Table 6.10 in column  $i$  over the prime factors of  $s_{ij}$  (and over  $-1$  if  $s_{ij} < 0$ ).

For example, for  $(i, j) = (1, 3)$ , we have  $\lambda_1(2) + \lambda_1(3) + \lambda_1(11) + \lambda_1(17) + \lambda_1(19) = 1 + 0 + 0 + 0 + 0 = 1$ . For  $1 \leq i < j$ , the bit  $\gamma_{ji}$  can be computed in the same way from  $K_{ji}$ , but it is quicker to use reciprocity. At a prime specialization, Corollary 4.14 and (4.22) show that  $\gamma_{ji} + \eta = \lambda_j(p_i) = \lambda_i(p_j) + \sigma_i \sigma_j = \gamma_{ij} + \eta + \sigma_i \sigma_j$ , and we obtain

$$\gamma_{ji} = \gamma_{ij} + \sigma_i \sigma_j, \quad (6.19)$$

and  $\sigma_i \sigma_j = 1$  only when  $i, j \in \{3, 5, 6, 9\}$ . Combining (6.17), (6.18), Table 6.11 and (6.19), we obtain the bits  $\gamma_{ij}$  of Table 6.12.

Table 6.11. The square-free parts  $s_{ij}$  of  $K_{ij} = 54c_j b_i(a_j b_i - a_i b_j)$  for the needed pairs  $1 \leq i < j$ , and the characters  $\lambda_i(K_{ij}) = \lambda_i(s_{ij})$ .

| $(i, j)$ | $s_{ij}$                               | $\lambda_i$ | $(i, j)$ | $s_{ij}$                              | $\lambda_i$ | $(i, j)$ | $s_{ij}$                      | $\lambda_i$ |
|----------|----------------------------------------|-------------|----------|---------------------------------------|-------------|----------|-------------------------------|-------------|
| (1, 2)   | $-3 \cdot 5 \cdot 7$                   | 0           | (2, 8)   | 7                                     | 0           | (4, 11)  | $5 \cdot 11 \cdot 31$         | 1           |
| (1, 3)   | $2 \cdot 3 \cdot 11 \cdot 17 \cdot 19$ | 1           | (2, 9)   | 3                                     | 0           | (5, 8)   | $2 \cdot 5 \cdot 19$          | 1           |
| (1, 4)   | $3 \cdot 7 \cdot 11 \cdot 17$          | 0           | (2, 10)  | $3 \cdot 7$                           | 0           | (5, 9)   | 3                             | 1           |
| (1, 5)   | $-2 \cdot 3 \cdot 19$                  | 1           | (2, 11)  | 1                                     | 0           | (5, 10)  | $2 \cdot 3 \cdot 5$           | 1           |
| (1, 6)   | $-3 \cdot 17$                          | 0           | (3, 4)   | $-5 \cdot 11 \cdot 17$                | 0           | (5, 11)  | 19                            | 1           |
| (1, 7)   | $3 \cdot 7 \cdot 11 \cdot 19$          | 0           | (3, 5)   | $3 \cdot 5 \cdot 19 \cdot 31$         | 0           | (6, 8)   | $2 \cdot 5$                   | 0           |
| (1, 8)   | $2 \cdot 3 \cdot 7 \cdot 11 \cdot 19$  | 1           | (3, 6)   | $2 \cdot 3 \cdot 5 \cdot 17$          | 0           | (6, 9)   | $2 \cdot 3 \cdot 17 \cdot 31$ | 0           |
| (1, 9)   | $-2 \cdot 3 \cdot 17$                  | 1           | (3, 7)   | $-5 \cdot 11 \cdot 19 \cdot 31$       | 0           | (6, 10)  | $3 \cdot 5 \cdot 17$          | 1           |
| (1, 10)  | $7 \cdot 17$                           | 0           | (3, 8)   | $2 \cdot 3 \cdot 5 \cdot 11 \cdot 19$ | 1           | (6, 11)  | 31                            | 1           |
| (1, 11)  | $-11 \cdot 19$                         | 0           | (3, 9)   | $5 \cdot 17 \cdot 31$                 | 0           | (7, 8)   | $3 \cdot 7 \cdot 11 \cdot 19$ | 1           |
| (2, 3)   | 3                                      | 0           | (3, 10)  | $2 \cdot 3 \cdot 5 \cdot 17$          | 0           | (7, 9)   | $2 \cdot 5$                   | 0           |
| (2, 4)   | $2 \cdot 3 \cdot 7$                    | 1           | (3, 11)  | $5 \cdot 11 \cdot 19 \cdot 31$        | 1           | (7, 10)  | $2 \cdot 3 \cdot 7$           | 0           |
| (2, 5)   | -1                                     | 0           | (4, 8)   | $3 \cdot 7 \cdot 11$                  | 0           | (7, 11)  | $5 \cdot 11 \cdot 19$         | 1           |
| (2, 6)   | -1                                     | 0           | (4, 9)   | $5 \cdot 17 \cdot 31$                 | 1           |          |                               |             |
| (2, 7)   | $3 \cdot 7$                            | 0           | (4, 10)  | $3 \cdot 7 \cdot 17$                  | 0           |          |                               |             |

For example,  $\gamma_{13} = \lambda_1(K_{13}) + \theta_1 = 1 + 0 = 1$ , and  $\gamma_{31} = \gamma_{13} + \sigma_1 \sigma_3 = 1$ .

**Primes outside the modulus.** By Lemma 4.13, the characters in Tables 6.10 and 6.11 depend only on the residues of the  $p_i$  modulo 8 and modulo the odd primes 3, 5, 7, 11, 17, 19, 31, which are fixed on  $\mathcal{P}_5$ . Six primes of  $S$  do not divide  $W$ : 13, 41, 131, 257, 409 and 2089. By Table 6.2, they divide only  $\Delta_{46}$ ,  $\Delta_{57}$ ,  $\Delta_{23} = 41^2$ ,  $\Delta_{67}$ ,  $\Delta_{45}$ ,  $\Delta_{89}$  and  $\Delta_{10,11}$ . Except for  $\Delta_{23}$ , these belong to pairs of two indices in  $I_H$  or two in  $I_J$ , which enter no row by Remark 4.15, and  $\Delta_{23}$  is a square. The square-free parts in Table 6.11 have prime factors in  $\{2, 3, 5, 7, 11, 17, 19, 31\}$  only, as the table shows. Every character in this section is therefore the same for all prime specializations in  $\mathcal{P}_5$ . The only quantity that is not determined by the congruence class is  $\eta$ .

Table 6.12. The constants  $\gamma_{ij}$  with  $\lambda_i(p_j) = \gamma_{ij} + \eta$ . Row  $i$ , column  $j$ . A dash marks a pair that enters no row.

| $i \setminus j$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|-----------------|---|---|---|---|---|---|---|---|---|---|----|----|
| 0               | . | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1  | 0  |
| 1               | 0 | . | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0  | 0  |
| 2               | 0 | 0 | . | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0  | 0  |
| 3               | 1 | 1 | 0 | . | 1 | 1 | 1 | 1 | 0 | 1 | 1  | 0  |
| 4               | 1 | 0 | 1 | 1 | . | – | – | – | 1 | 0 | 1  | 0  |
| 5               | 0 | 1 | 0 | 0 | – | . | – | – | 1 | 1 | 1  | 1  |
| 6               | 1 | 0 | 0 | 0 | – | – | . | – | 1 | 1 | 0  | 0  |
| 7               | 0 | 0 | 0 | 1 | – | – | – | . | 1 | 0 | 0  | 1  |
| 8               | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | . | – | –  | –  |
| 9               | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | – | . | –  | –  |
| 10              | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | – | – | .  | –  |
| 11              | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | – | – | –  | .  |

## 6.6 The matrices and the upper bound

We now assemble the rows. The matrix  $\mathbf{M}_E(\eta)$  has the fixed rows  $f_1^E, \dots, f_5^E$  of Table 6.9, followed by the moving rows  $r_0^E, r_1^E, r_2^E, r_3^E$  (at  $p_i, i \in I_F$ ) and  $r_8^E, r_9^E, r_{10}^E, r_{11}^E$  (at  $p_i, i \in I_I$ ). The matrix  $\mathbf{M}_{E'}(\eta)$  has the fixed rows  $f_1^{E'}, f_2^{E'}, f_3^{E'}$ , followed by the moving rows  $r_0^{E'}, \dots, r_3^{E'}$  and  $r_4^{E'}, \dots, r_7^{E'}$ . The columns are indexed by the bases (6.7).

By Corollary 4.14 and Section 6.5, the entries of a moving row  $r_i^*$  are as follows. In the constant columns  $-1, 2, 3, 5$ , they are the entries of Table 6.10 in column  $i$ . In a moving column  $p_j$  with  $j \neq i$ , the entry is  $\gamma_{ij} + \eta$ , with  $\gamma_{ij}$  from Table 6.12. For  $i \in I_F$ , the entry in the column  $p_i$  is  $\gamma_{ii}^* + \eta$ , where

$$\gamma_{ii}^* = \lambda_i(\kappa_*) + \sum_{j \in G_* \setminus \{i\}} \gamma_{ij}, \quad \lambda_i(\kappa_E) = \lambda_i(-1), \quad \lambda_i(\kappa_{E'}) = \lambda_i(2),$$

by (4.28) and (6.8). Table 6.13 evaluates these sums.

The resulting matrices at  $\eta = 0$  are displayed in Tables 6.14 and 6.15. A vertical and a horizontal rule separate the block of moving rows and moving columns. When  $\eta = 1$ , that is, when  $\varepsilon = -1$ , every entry of this block changes, and no other entry changes: the fixed rows do not depend on  $\eta$ , and neither do the entries of the moving rows in the columns  $-1, 2, 3, 5$ . In accordance with Corollary 4.14, we have

$$\begin{aligned} r_i^E(\eta) &= r_i^E(0) + \eta u_E, & r_i^{E'}(\eta) &= r_i^{E'}(0) + \eta u_{E'}, \\ u_E &= u_{E'} = (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1), \end{aligned} \tag{6.20}$$

Table 6.13. The diagonal bits  $\gamma_{ii}^E$  and  $\gamma_{ii}^{E'}$  of the moving rows.

| $i$ | curve $E$       |                                                |                 |  | curve $E'$     |                                                   |                    |  |
|-----|-----------------|------------------------------------------------|-----------------|--|----------------|---------------------------------------------------|--------------------|--|
|     | $\lambda_i(-1)$ | $\sum_{j \in G_E \setminus \{i\}} \gamma_{ij}$ | $\gamma_{ii}^E$ |  | $\lambda_i(2)$ | $\sum_{j \in G_{E'} \setminus \{i\}} \gamma_{ij}$ | $\gamma_{ii}^{E'}$ |  |
| 0   | 0               | 3                                              | 1               |  | 0              | 3                                                 | 1                  |  |
| 1   | 0               | 2                                              | 0               |  | 1              | 3                                                 | 0                  |  |
| 2   | 0               | 1                                              | 1               |  | 1              | 0                                                 | 1                  |  |
| 3   | 1               | 6                                              | 1               |  | 0              | 4                                                 | 0                  |  |

where  $r_i^*(\eta)$  denotes the moving row of  $\mathbf{M}_*(\eta)$  at  $p_i$ , and  $u_E = u_{E'}$  is the indicator vector of the eight moving columns. The row codes that the verification scripts use for these matrices are listed in Appendix A.

Table 6.14. The matrix  $\mathbf{M}_E(0)$ .

|               |               | -1 | 2 | 3 | 5 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $p_7$ |
|---------------|---------------|----|---|---|---|-------|-------|-------|-------|-------|-------|-------|-------|
| $f_1^E$       | $(2, e_1)$    | 1  | 0 | 1 | 0 | 0     | 0     | 0     | 1     | 0     | 1     | 1     | 0     |
| $f_2^E$       | $(2, e_3)$    | 0  | 0 | 1 | 1 | 0     | 1     | 1     | 0     | 1     | 1     | 1     | 1     |
| $f_3^E$       | $(3, \chi_3)$ | 1  | 1 | 0 | 1 | 0     | 0     | 0     | 0     | 1     | 0     | 0     | 0     |
| $f_4^E$       | $(3, \nu_3)$  | 0  | 0 | 1 | 0 | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     |
| $f_5^E$       | $(5, \chi_5)$ | 0  | 1 | 1 | 0 | 0     | 0     | 0     | 1     | 0     | 1     | 1     | 1     |
| $r_0^E(0)$    | $p_0$         | 0  | 0 | 0 | 0 | 1     | 0     | 0     | 1     | 1     | 0     | 1     | 0     |
| $r_1^E(0)$    | $p_1$         | 0  | 1 | 0 | 0 | 0     | 0     | 0     | 1     | 0     | 1     | 0     | 0     |
| $r_2^E(0)$    | $p_2$         | 0  | 1 | 0 | 0 | 0     | 0     | 1     | 0     | 1     | 0     | 0     | 0     |
| $r_3^E(0)$    | $p_3$         | 1  | 0 | 1 | 1 | 1     | 1     | 0     | 1     | 1     | 1     | 1     | 1     |
| $r_8^E(0)$    | $p_8$         | 0  | 0 | 0 | 0 | 1     | 1     | 0     | 0     | 1     | 1     | 1     | 1     |
| $r_9^E(0)$    | $p_9$         | 1  | 0 | 1 | 0 | 0     | 1     | 0     | 0     | 0     | 0     | 0     | 0     |
| $r_{10}^E(0)$ | $p_{10}$      | 0  | 0 | 1 | 1 | 1     | 0     | 0     | 1     | 1     | 1     | 0     | 0     |
| $r_{11}^E(0)$ | $p_{11}$      | 0  | 0 | 1 | 1 | 0     | 0     | 0     | 0     | 0     | 1     | 0     | 1     |

**Lemma 6.6** (Rank certificates). *The matrices of Tables 6.14 and 6.15 have the following properties.*

- (a)  $\text{rank } \mathbf{M}_E(0) = 9$  and  $\text{rank } \mathbf{M}_{E'}(0) = 8$ . The kernel of  $\mathbf{M}_E(0)$  is spanned by  $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ , and the kernel of  $\mathbf{M}_{E'}(0)$  is spanned by  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3, \mathbf{w}_4$  (see (6.11)).
- (b) We have

$$\begin{aligned}
 u_E &= f_3^E + f_4^E + r_2^E(0) + r_3^E(0), \\
 u_{E'} &= r_1^{E'}(0) + r_2^{E'}(0) + r_5^{E'}(0) + r_6^{E'}(0).
 \end{aligned} \tag{6.21}$$

Table 6.15. The matrix  $\mathbf{M}_{E'}(0)$ .

|               |                        | -1 | 2 | 3 | 5 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_8$ | $p_9$ | $p_{10}$ | $p_{11}$ |
|---------------|------------------------|----|---|---|---|-------|-------|-------|-------|-------|-------|----------|----------|
| $f_1^{E'}$    | $(2, e_3)$             | 0  | 0 | 1 | 1 | 0     | 1     | 1     | 0     | 0     | 0     | 0        | 0        |
| $f_2^{E'}$    | $(5, \chi_5)$          | 0  | 1 | 1 | 0 | 0     | 0     | 0     | 1     | 0     | 0     | 1        | 1        |
| $f_3^{E'}$    | $(\infty, \text{sgn})$ | 1  | 0 | 0 | 0 | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| $r_0^{E'}(0)$ | $p_0$                  | 0  | 0 | 0 | 0 | 1     | 0     | 0     | 1     | 1     | 0     | 1        | 0        |
| $r_1^{E'}(0)$ | $p_1$                  | 0  | 1 | 0 | 0 | 0     | 0     | 0     | 1     | 1     | 1     | 0        | 0        |
| $r_2^{E'}(0)$ | $p_2$                  | 0  | 1 | 0 | 0 | 0     | 0     | 1     | 0     | 0     | 0     | 0        | 0        |
| $r_3^{E'}(0)$ | $p_3$                  | 1  | 0 | 1 | 1 | 1     | 1     | 0     | 0     | 0     | 1     | 1        | 0        |
| $r_4^{E'}(0)$ | $p_4$                  | 0  | 1 | 1 | 0 | 1     | 0     | 1     | 1     | 1     | 0     | 1        | 0        |
| $r_5^{E'}(0)$ | $p_5$                  | 1  | 1 | 1 | 1 | 0     | 1     | 0     | 0     | 1     | 1     | 1        | 1        |
| $r_6^{E'}(0)$ | $p_6$                  | 1  | 1 | 1 | 1 | 1     | 0     | 0     | 0     | 1     | 1     | 0        | 0        |
| $r_7^{E'}(0)$ | $p_7$                  | 0  | 1 | 0 | 1 | 0     | 0     | 0     | 1     | 1     | 0     | 0        | 1        |

In particular,  $u_E$  is the sum of a set of rows of  $\mathbf{M}_E(0)$  containing two moving rows, and  $u_{E'}$  is the sum of a set of rows of  $\mathbf{M}_{E'}(0)$  containing four moving rows.

*Proof.* For (a), we exhibit minors that are lower triangular with ones on the diagonal. In Table 6.16, we display the submatrix of  $\mathbf{M}_E(0)$  formed by the rows  $f_4^E, f_1^E, r_1^E(0), f_5^E, r_{11}^E(0), f_3^E, r_0^E(0), r_3^E(0), r_2^E(0)$  and the columns 3, -1, 2,  $p_7, 5, p_4, p_0, p_1, p_2$ , in these orders, and the submatrix of  $\mathbf{M}_{E'}(0)$  formed by the rows  $f_3^{E'}, r_0^{E'}(0), r_1^{E'}(0), r_2^{E'}(0), r_4^{E'}(0), r_6^{E'}(0), r_3^{E'}(0), r_7^{E'}(0)$  and the columns -1,  $p_0, 2, p_2, 3, 5, p_1, p_{11}$ . Each entry can be read off from Tables 6.14 and 6.15. Both submatrices have ones on the diagonal and zeros above it, and their determinants are 1. This implies that  $\text{rank } \mathbf{M}_E(0) \geq 9$  and  $\text{rank } \mathbf{M}_{E'}(0) \geq 8$ .

Next, the vectors  $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$  are orthogonal to every row of  $\mathbf{M}_E(0)$ , and  $\mathbf{w}_1, \dots, \mathbf{w}_4$  are orthogonal to every row of  $\mathbf{M}_{E'}(0)$ ; this is a direct check of  $13 \cdot 3 + 11 \cdot 4 = 83$  scalar products over  $\mathbb{F}_2$ . For example,  $r_3^E(0)$  and  $\mathbf{v}_2$  both have the entry 1 exactly in the columns -1,  $p_0, p_1, p_3$ , so  $r_3^E(0) \cdot \mathbf{v}_2 = 1 + 1 + 1 + 1 = 0$ . These vectors are independent by the proof of Lemma 6.2, and the kernels have dimensions at least 3 and 4. We find that  $\text{rank } \mathbf{M}_E(0) \leq 9$  and  $\text{rank } \mathbf{M}_{E'}(0) \leq 8$ , which together with the previous paragraph proves (a).

For (b), we add the rows column by column. On  $E$ , the four rows  $f_3^E, f_4^E, r_2^E(0), r_3^E(0)$  have the entries  $(1, 1, 0, 1), (0, 0, 1, 0), (0, 1, 0, 0)$  and  $(1, 0, 1, 1)$  in the columns -1, 2, 3, 5, which add to zero. In the columns  $p_0, \dots, p_7$ , the entries of  $f_3^E$  and  $f_4^E$  are zero except for  $f_3^E$  at  $p_4$ , and the entries of  $r_2^E(0) + r_3^E(0)$  are  $(1, 1, 1, 1, 0, 1, 1, 1)$ ; adding  $f_3^E$  gives all ones. On  $E'$ , the rows  $r_1^{E'}(0), r_2^{E'}(0), r_5^{E'}(0), r_6^{E'}(0)$  have the entries  $(0, 1, 0, 0), (0, 1, 0, 0), (1, 1, 1, 1)$  and  $(1, 1, 1, 1)$  in the columns -1, 2, 3, 5, which add to zero, and their sum in

the moving columns is

$$(0, 0, 0, 1, 1, 1, 0, 0) + (0, 0, 1, 0, 0, 0, 0, 0) \\ + (0, 1, 0, 0, 1, 1, 1, 1) + (1, 0, 0, 0, 1, 1, 0, 0) = (1, 1, 1, 1, 1, 1, 1, 1).$$

This proves (6.21).  $\square$

Table 6.16. Lower-triangular minors with unit diagonal of  $\mathbf{M}_E(0)$  (top) and  $\mathbf{M}_{E'}(0)$  (bottom).

|               | 3 | -1 | 2 | $p_7$ | 5 | $p_4$ | $p_0$ | $p_1$ | $p_2$ |
|---------------|---|----|---|-------|---|-------|-------|-------|-------|
| $f_4^E$       | 1 | 0  | 0 | 0     | 0 | 0     | 0     | 0     | 0     |
| $f_1^E$       | 1 | 1  | 0 | 0     | 0 | 0     | 0     | 0     | 0     |
| $r_1^E(0)$    | 0 | 0  | 1 | 0     | 0 | 0     | 0     | 0     | 0     |
| $f_5^E$       | 1 | 0  | 1 | 1     | 0 | 0     | 0     | 0     | 0     |
| $r_{11}^E(0)$ | 1 | 0  | 0 | 1     | 1 | 0     | 0     | 0     | 0     |
| $f_3^E$       | 0 | 1  | 1 | 0     | 1 | 1     | 0     | 0     | 0     |
| $r_0^E(0)$    | 0 | 0  | 0 | 0     | 0 | 1     | 1     | 0     | 0     |
| $r_3^E(0)$    | 1 | 1  | 0 | 1     | 1 | 1     | 1     | 1     | 0     |
| $r_2^E(0)$    | 0 | 0  | 1 | 0     | 0 | 1     | 0     | 0     | 1     |

  

|               | -1 | $p_0$ | 2 | $p_2$ | 3 | 5 | $p_1$ | $p_{11}$ |
|---------------|----|-------|---|-------|---|---|-------|----------|
| $f_3^{E'}$    | 1  | 0     | 0 | 0     | 0 | 0 | 0     | 0        |
| $r_0^{E'}(0)$ | 0  | 1     | 0 | 0     | 0 | 0 | 0     | 0        |
| $r_1^{E'}(0)$ | 0  | 0     | 1 | 0     | 0 | 0 | 0     | 0        |
| $r_2^{E'}(0)$ | 0  | 0     | 1 | 1     | 0 | 0 | 0     | 0        |
| $r_4^{E'}(0)$ | 0  | 1     | 1 | 1     | 1 | 0 | 0     | 0        |
| $r_6^{E'}(0)$ | 1  | 1     | 1 | 0     | 1 | 1 | 0     | 0        |
| $r_3^{E'}(0)$ | 1  | 1     | 0 | 0     | 1 | 1 | 1     | 0        |
| $r_7^{E'}(0)$ | 0  | 0     | 1 | 0     | 0 | 1 | 0     | 1        |

## 6.7 Exact rank and infinitude

We can now prove the main result of this section.

**Theorem 6.7** (Exact rank five). *Let  $(M, N) \in \mathcal{P}_5 \cap \mathcal{K}_5$  be a prime specialization of  $\mathfrak{D}_5$  with respect to the set  $S$  of (6.5). Then  $\text{rank } E_{M,N}(\mathbb{Q}) = 5$ . Moreover, there exist infinitely many such  $(M, N)$ , and the curves  $E_{M,N}$  obtained from them represent infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes.*

*Proof.* We first prove the rank statement with Proposition 4.18, and then the infinitude statements with Proposition 5.5.

**The rank.** Let  $\mathcal{P}$  be the set of prime specializations in  $\mathcal{P}_5 \cap \mathcal{K}_5$ . We apply Proposition 4.18 to the datum  $\mathfrak{D}_5$ , the set  $S$  of (6.5) and the set  $\mathcal{P}$ . As noted at the end of Section 6.1, the lists  $\Gamma_E$  and  $\Gamma_{E'}$  consist of  $-1$  and distinct primes, including every prime dividing  $\kappa_E$  and  $\kappa_{E'}$ . We check the four hypotheses.

- (i) By Lemma 6.5, the vectors  $f_1^E, \dots, f_5^E$  and  $f_1^{E'}, f_2^{E'}, f_3^{E'}$  of Table 6.9 are rows for  $E_{M,N}$  and  $E'_{M,N}$  at every  $(M, N) \in \mathcal{P}$ , in the sense of Definition 3.9. They do not depend on  $(M, N)$ , because their entries depend only on the residues of the  $p_j$  modulo 8, 3 and 5, which are the same for all  $(M, N) \in \mathcal{P}$  by Lemma 6.3.
- (ii) By Section 6.5, the bits (4.34), namely  $\lambda_i(g)$  for  $g \in \Gamma_*$ ,  $\lambda_i(\kappa_*)$  and  $\gamma_{ij}$ , are given by Tables 6.10 and 6.12, and they are the same for all  $(M, N) \in \mathcal{P}$ . The matrices  $\mathbf{M}_E(\eta)$  and  $\mathbf{M}_{E'}(\eta)$  of (4.35) are given by Tables 6.14 and 6.15 and (6.20).
- (iii) By Lemma 6.2, the image  $\delta_E(E(\mathbb{Q}))$  contains the three independent classes  $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ , and  $\delta_{E'}(E'(\mathbb{Q}))$  contains the four independent classes  $\mathbf{w}_1, \dots, \mathbf{w}_4$ , at every  $(M, N) \in \mathcal{P}$ . We take  $k_E = 3$  and  $k_{E'} = 4$ .
- (iv) By Lemma 6.6, we have  $\text{rank } \mathbf{M}_E(0) = 9 = n_E - k_E$  and  $\text{rank } \mathbf{M}_{E'}(0) = 8 = n_{E'} - k_{E'}$ , and  $u_E$  and  $u_{E'}$  are sums of rows of  $\mathbf{M}_E(0)$  and of  $\mathbf{M}_{E'}(0)$ , respectively, each containing an even number of moving rows.

Proposition 4.18 implies that every  $(M, N) \in \mathcal{P}$  has  $d_E = 3$ ,  $d_{E'} = 4$  and

$$\text{rank } E_{M,N}(\mathbb{Q}) = d_E + d_{E'} - 2 = 5.$$

**Infinitude.** We check the hypotheses of Proposition 5.5 for  $W$ ,  $(M_0, N_0)$  and  $\mathcal{K}_5$ . For hypothesis (a), the primes dividing  $c_0 \cdots c_{11}$  are 2 and 3, which divide  $W$ . Every  $c_i$  divides  $2^3 \cdot 3^3$ , and  $v_2(W) = 6$ ,  $v_3(W) = 4$ , so  $v_q(W) > v_q(c_i)$  for  $q = 2, 3$ ; for the other primes  $q \mid W$ , we have  $v_q(c_i) = 0 < 1 = v_q(W)$ . Since  $(M_0, N_0) \in \mathcal{P}_5$ , Lemma 6.3 shows that  $c_i \mid L_i(M_0, N_0)$  and that  $L_i(M_0, N_0)/c_i$  is prime to  $W$ . Hypothesis (b) is empty, because every prime  $q \leq 11$  divides  $W$ . Hypothesis (c) is Lemma 6.4. Proposition 5.5 now gives infinitely many prime specializations  $(M, N) \in \mathcal{K}_5$  with  $M \equiv M_0$  and  $N \equiv N_0 \pmod{W}$ , and it shows that the  $j$ -invariants  $j(E_{M,N})$  of these curves take infinitely many values. Curves with distinct  $j$ -invariants are not isomorphic over  $\overline{\mathbb{Q}}$  (Remark 5.7). This completes the proof.  $\square$

*Remark 6.8.* The  $j$ -invariant of  $E_{M,N}$  is  $\frac{4}{9}(2500F + 9H)^3/(H^2J)$ , by Remark 4.4. In the proof of Theorem 6.7, we did not need to examine the primes  $q \nmid W$  at which the zero lines of two of the forms  $L_i$  coincide modulo  $q$ , because  $d_q \leq 12 < q + 1$  for every such  $q$  (see Lemma 5.4). For the record, by Table 6.2, these primes are 13, 41, 131, 257, 409 and 2089. The pairs of forms whose zero lines coincide modulo these primes are  $\{L_4, L_6\}$  and

$\{L_5, L_7\}$  modulo 13;  $\{L_2, L_3\}$  and  $\{L_6, L_7\}$  modulo 41; and  $\{L_4, L_5\}$ ,  $\{L_6, L_7\}$ ,  $\{L_8, L_9\}$  and  $\{L_{10}, L_{11}\}$  modulo 131, 257, 409 and 2089, respectively. Hence  $d_{13} = d_{41} = 10$  and  $d_q = 11$  for the other four primes.

## 6.8 Five independent points on $E$

The proof of Theorem 6.7 uses points on both curves. Using the dual isogeny  $\hat{\phi}: E' \rightarrow E$ , we now write down five independent points on  $E$  itself. By (3.8), for a point  $(x', y')$  of  $E'$  with  $x' \neq 0$  and  $\rho = y'/x'$ , we have

$$\hat{\phi}(x', y') = \left( \frac{y'^2}{4x'^2}, \frac{y'}{8} \left( 1 - \frac{\beta'}{x'^2} \right) \right) = \left( \frac{\rho^2}{4}, \frac{\rho}{8} \left( x' - \frac{\beta'}{x'} \right) \right). \quad (6.22)$$

**Proposition 6.9** (Five independent points). *Let  $(M, N)$  be as in Theorem 6.7. Then the points*

$$\begin{aligned} P_1 &= (-150F, 3600DF), \\ P_2 &= \left( \frac{10}{49}L_2L_3L_6L_7, \frac{80}{343}L_2L_3L_6L_7(2D_1 - 55D) \right), \\ \hat{\phi}(Q_1) &= (36D^2, 36D(J - 100F)), \\ \hat{\phi}(Q_2) &= \left( \frac{9}{49}(3D_1 + 65D)^2, \frac{90}{7}(3D_1 + 65D)(L_0L_1L_8L_9 - 4L_2L_3L_{10}L_{11}) \right), \\ \hat{\phi}(Q_3) &= \left( \frac{1}{49}V^2, \frac{1}{343}V(400L_1L_2L_8L_{10} - 21609L_0L_3L_9L_{11}) \right) \end{aligned} \quad (6.23)$$

of  $E_{M,N}(\mathbb{Q})$  are independent.

*Proof.* We first check the formulas. For the three points  $(x', y') = Q_1, Q_2, Q_3$ , Table 6.3 and  $\beta' = 57600FJ$  give

$$\begin{aligned} Q_1 : \quad \rho &= 12D, & x' - \beta'/x' &= 24J - 2400F, \\ Q_2 : \quad \rho &= \frac{6}{7}(3D_1 + 65D), & x' - \beta'/x' &= 120L_0L_1L_8L_9 - 480L_2L_3L_{10}L_{11}, \\ Q_3 : \quad \rho &= \frac{2}{7}V, & x' - \beta'/x' &= \frac{1600}{49}L_1L_2L_8L_{10} - 1764L_0L_3L_9L_{11}. \end{aligned}$$

Inserting these values into (6.22) gives (6.23), where in the last line we used  $1764 \cdot 49/4 = 21609$ .

By the proof of Theorem 6.7, we have  $d_E = 3$  and  $d_{E'} = 4$ . The classes in (6.11) are independent by Lemma 6.2, and since there are three of them on  $E$  and four on  $E'$ , they form bases of  $\delta_E(E(\mathbb{Q}))$  and  $\delta_{E'}(E'(\mathbb{Q}))$ . By Proposition 3.4, the kernel of  $\delta_E$  is  $\hat{\phi}(E'(\mathbb{Q}))$  and the kernel of  $\delta_{E'}$  is  $\phi(E(\mathbb{Q}))$ , and we obtain

$$E(\mathbb{Q}) = \hat{\phi}(E'(\mathbb{Q})) + \langle T, P_1, P_2 \rangle, \quad E'(\mathbb{Q}) = \phi(E(\mathbb{Q})) + \langle T', Q_1, Q_2, Q_3 \rangle.$$

Applying  $\hat{\phi}$  to the second equality, and using  $\hat{\phi} \circ \phi = [2]$  and  $\hat{\phi}(T') = O$  (Proposition 3.4), we find  $\hat{\phi}(E'(\mathbb{Q})) = 2E(\mathbb{Q}) + \langle \hat{\phi}(Q_1), \hat{\phi}(Q_2), \hat{\phi}(Q_3) \rangle$ . Inserting this into the first equality,

we find  $E(\mathbb{Q}) = \mathcal{G} + 2E(\mathbb{Q})$ , where  $\mathcal{G}$  is the subgroup generated by  $T$  and the five points (6.23). By the Mordell–Weil theorem [43, Theorem VIII.6.7], the quotient  $E(\mathbb{Q})/\mathcal{G}$  is a finitely generated abelian group, and it equals twice itself. If  $E(\mathbb{Q})/\mathcal{G} \cong \mathbb{Z}^m \oplus \mathcal{T}$  with  $\mathcal{T}$  finite, then  $(\mathbb{Z}/2\mathbb{Z})^m \oplus \mathcal{T}/2\mathcal{T} = 0$ , which implies that  $m = 0$ . The group  $E(\mathbb{Q})/\mathcal{G}$  is therefore finite, and  $\mathcal{G}$  has rank  $\text{rank } E(\mathbb{Q}) = 5$ . Since  $T$  has finite order, the subgroup generated by the five points (6.23) also has rank five, and the five points are independent.  $\square$

The abscissas of the three points  $\hat{\phi}(Q_k)$  are the squares  $(6D)^2$ ,  $(3(3D_1 + 65D)/7)^2$  and  $(V/7)^2$ , as they must be, since  $\hat{\phi}(E'(\mathbb{Q}))$  is the kernel of  $\delta_E$ .

## The rank-six family

The goal of this section is to prove Theorem 7.8, which states that every prime specialization of the datum  $\mathfrak{D}_6$  defined below that lies in a progression  $\mathcal{P}_6$  and a real cone  $\mathcal{K}_6$  gives an elliptic curve over  $\mathbb{Q}$  of rank exactly six, and that these curves represent infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes. The proof consists of checking the hypotheses of two general results. The rank comes from Proposition 4.18, which requires four points on each of the two curves, local conditions at the fixed places 2, 3, 7 and  $\infty$ , the quadratic characters at the moving primes, and the ranks of two  $12 \times 12$  matrices over  $\mathbb{F}_2$ . The infinitude comes from Proposition 5.5. Besides these two propositions, we use the lemmas of Sections 3 and 4, cited where they enter. Theorem 7.8 is used in Section 9 for the case  $r = 6$  of Theorem 1.1. Appendix B.2 explains how the family was obtained from a rank-four surface of Zywina [55, §6.5].

The section is organized as follows. In Section 7.1, we define the datum and the two curves and fix the set  $S$  and the bases. Section 7.2 gives three points on each curve besides  $(0, 0)$  and proves that the four resulting classes on each side are independent. Section 7.3 defines  $\mathcal{P}_6$  and  $\mathcal{K}_6$  and computes the residues of the primes  $p_i$  on  $\mathcal{P}_6$ . Section 7.4 proves the local conditions at the fixed places, and Section 7.5 computes the characters at the moving primes. In Section 7.6, we assemble the two matrices and show that they have rank eight. Section 7.7 contains the proof of Theorem 7.8.

Throughout this section,  $E = E_{M,N}$  and  $E' = E'_{M,N}$  are the curves of  $\mathfrak{D}_6$ , given in (7.5) below, and  $T$  and  $T'$  are their points  $(0, 0)$ . We write

$$\alpha = 70F, \quad \beta = -784FH, \quad \alpha' = -140F, \quad \beta' = 1764FJ,$$

so that  $E = E_{\alpha,\beta}$  and  $E' = E_{\alpha',\beta'}$  in the notation of Section 3. The index sets  $I_F, I_H, I_J, G_E, G_{E'}$  are those of Section 4, and for a prime specialization  $(M, N)$  we write  $p_i = L_i(M, N)/c_i$ .

### 7.1 The datum

The twelve linear forms are  $L_i = a_iM + b_iN$ , with the coefficients  $a_i, b_i$  and the cofactors  $c_i$  listed in Table 7.1. As in Section 4, we set  $F = L_0L_1L_2L_3$ ,  $H = L_4L_5L_6L_7$  and  $J =$

$L_8L_9L_{10}L_{11}$ . Multiplying out these products, we have

$$\begin{aligned} F &= 4225M^3N - 9811M^2N^2 - 126750MN^3, \\ H &= 126M^4 - 4225M^3N + 17371M^2N^2 + 126750MN^3 + 113400N^4, \\ J &= 224M^4 + 4225M^3N + 3629M^2N^2 - 126750MN^3 + 201600N^4. \end{aligned} \quad (7.1)$$

Let  $D_0 = M^2 + 30N^2$ , so that  $D_0^2 = M^4 + 60M^2N^2 + 900N^4$ . Comparing coefficients in (7.1), we find

$$F + H = 126D_0^2, \quad J - F = 224D_0^2. \quad (7.2)$$

Using (7.2) twice, we have  $25F + 16H = 9F + 16(F + H) = 9F + 2016D_0^2 = 9(F + 224D_0^2)$ , that is,

$$25F + 16H = 9J. \quad (7.3)$$

Table 7.1. The linear forms  $L_i = a_iM + b_iN$  of  $\mathfrak{D}_6$ , their groups, the factorizations of the  $b_i$ , and the cofactors  $c_i$ .

| $i$ | group | $a_i$ | $b_i$ | $b_i$ factored        | $c_i$ |
|-----|-------|-------|-------|-----------------------|-------|
| 0   | $F$   | 1     | 0     |                       | 1     |
| 1   | $F$   | 0     | 1     | 1                     | 1     |
| 2   | $F$   | 169   | 750   | $2 \cdot 3 \cdot 5^3$ | 1     |
| 3   | $F$   | 25    | -169  | $-13^2$               | 8     |
| 4   | $H$   | 1     | -27   | $-3^3$                | 2     |
| 5   | $H$   | 7     | 20    | $2^2 \cdot 5$         | 1     |
| 6   | $H$   | 2     | -21   | $-3 \cdot 7$          | 1     |
| 7   | $H$   | 9     | 10    | $2 \cdot 5$           | 1     |
| 8   | $J$   | 1     | 15    | $3 \cdot 5$           | 8     |
| 9   | $J$   | 7     | 64    | $2^6$                 | 27    |
| 10  | $J$   | 1     | -2    | -2                    | 3     |
| 11  | $J$   | 32    | -105  | $-3 \cdot 5 \cdot 7$  | 1     |

We define  $\mathfrak{D}_6$  to be the twelve-form datum (Definition 4.1) with the forms and cofactors of Table 7.1, the constants

$$A = 70, \quad B = 784, \quad C = 1764,$$

and the lists  $\Gamma_E = \Gamma_{E'} = (-1, 2, 3, 7)$ . We check the conditions of Definition 4.1. We have  $(a_0, b_0) = (1, 0)$ , each pair  $(a_i, b_i)$  is primitive,  $b_i \neq 0$  for  $i \geq 1$ , and  $\min_i c_i = 1$ . The identity  $A^2F + 4BH = CJ$ , that is,  $4900F + 3136H = 1764J$ , is 196 times (7.3). Finally, every determinant  $\Delta_{ij} = a_ib_j - a_jb_i$  with  $i \neq j$  is nonzero. To see this, note that  $\Delta_{0j} = b_j$ ,

and that the determinants  $\Delta_{ji}$  with  $1 \leq i < j$  and  $\{i, j\}$  contained in neither  $I_H$  nor  $I_J$  are factored in Table 7.11 below. The remaining twelve determinants are

$$\begin{aligned}\Delta_{4,5} &= \Delta_{6,7} = 11 \cdot 19, & \Delta_{4,6} &= 3 \cdot 11, & \Delta_{4,7} &= 11 \cdot 23, & \Delta_{5,6} &= -11 \cdot 17, \\ \Delta_{5,7} &= -2 \cdot 5 \cdot 11, & \Delta_{8,9} &= \Delta_{10,11} = -41, & \Delta_{8,10} &= -17, \\ \Delta_{8,11} &= -3^2 \cdot 5 \cdot 13, & \Delta_{9,10} &= -2 \cdot 3 \cdot 13, & \Delta_{9,11} &= -11^2 \cdot 23.\end{aligned}\tag{7.4}$$

The curves of  $\mathfrak{D}_6$  are

$$E : y^2 = x^3 + 70Fx^2 - 784FHx, \quad E' : y^2 = x^3 - 140Fx^2 + 1764FJx. \tag{7.5}$$

By Lemma 4.2, we have  $\beta' = \alpha^2 - 4\beta$ ; this means that  $E'$  is the curve 2-isogenous to  $E$  considered in Section 3. The discriminant of  $E$  is  $16\beta^2\beta' = 2^{14}3^27^6F^3H^2J$ .

We take

$$S = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 41\}. \tag{7.6}$$

We note that  $S$  satisfies the requirement of Definition 4.6: we have  $6ABC = 2^83^35 \cdot 7^5$ , the cofactors are products of 2 and 3, the  $b_i$  have their prime factors in  $\{2, 3, 5, 7, 13\}$  by Table 7.1, and the determinants have their prime factors in  $S$  by (7.4) and Table 7.11. The primes in  $\Gamma_E \cup \Gamma_{E'}$  are 2, 3 and 7. In fact  $S$  is exactly the set of primes dividing  $6ABC \prod_i c_i \prod_{i \geq 1} b_i \prod_{i < j} \Delta_{ij}$ . Throughout this section, prime specializations of  $\mathfrak{D}_6$  are taken with respect to this set  $S$ .

The ambient bases of Section 4 are

$$\mathcal{B}_E = (-1, 2, 3, 7; p_0, p_1, \dots, p_7), \quad \mathcal{B}_{E'} = (-1, 2, 3, 7; p_0, p_1, p_2, p_3, p_8, p_9, p_{10}, p_{11}), \tag{7.7}$$

so that  $n_E = n_{E'} = 12$ . The cofactors of Table 7.1 satisfy  $\prod_{i \in I_F} c_i = 8$ ,  $\prod_{i \in I_H} c_i = 2$  and  $\prod_{i \in I_J} c_i = 648 = 2^33^4$ . Inserting  $L_i = c_i p_i$ , we find

$$F = 8p_0p_1p_2p_3, \quad H = 2p_4p_5p_6p_7, \quad J = 648p_8p_9p_{10}p_{11}, \tag{7.8}$$

and the constants of Definition 4.10 are

$$\kappa_E = -784 \cdot 16 = -112^2, \quad \kappa_{E'} = 1764 \cdot 8 \cdot 648 = 3024^2. \tag{7.9}$$

The primes dividing  $\kappa_E$  and  $\kappa_{E'}$  belong to  $\{2, 3, 7\}$ , and  $\Gamma_E = \Gamma_{E'}$  consists of  $-1$  and the distinct primes 2, 3, 7. By Lemma 4.8, at every prime specialization of  $\mathfrak{D}_6$  the lists  $\mathcal{B}_E$  and  $\mathcal{B}_{E'}$  are ambient bases for  $E$  and  $E'$  in the sense of Definition 3.9, and  $E(\mathbb{Q})[2] = \{O, T\}$ . Since the prime 3 divides neither  $\kappa_E$  nor  $\beta$ , the entry 3 of  $\Gamma_E$  is not needed for  $\mathcal{B}_E$  to contain  $\delta_E(E(\mathbb{Q}))$  in its span. It does no harm: the local condition at 3 forces its coefficient to vanish (see the fixed row  $f_3^E$ , defined at 3 by the coordinate  $v_3$ , in Table 7.13).

## 7.2 Rational points and the lower bound

Besides  $D_0 = M^2 + 30N^2$ , we use the quadratic forms

$$\begin{aligned} D_1 &= 25M^2 - 338MN - 750N^2, & D_2 &= 52M^2 + 375MN - 975N^2, \\ D_3 &= 39M^2 - 500MN + 4550N^2. \end{aligned} \quad (7.10)$$

Table 7.2 defines three points on each curve. For each point, it gives the  $x$ -coordinate and the ratio  $y/x$ .

Table 7.2. Three points on  $E$  and three points on  $E'$ . The  $y$ -coordinate is the product of the last two columns.

| curve | point | $x$                      | $y/x$             |
|-------|-------|--------------------------|-------------------|
| $E$   | $P_1$ | $14H$                    | $42D_0$           |
| $E$   | $P_2$ | $-2L_1L_2L_4L_5$         | $3(3D_1 + 65D_0)$ |
| $E$   | $P_3$ | $-175L_1L_3L_4L_6$       | $(21/5)D_2$       |
| $E'$  | $Q_1$ | $14F$                    | $-168D_0$         |
| $E'$  | $Q_2$ | $2L_0L_3L_{10}L_{11}$    | $8(2D_1 - 55D_0)$ |
| $E'$  | $Q_3$ | $(18/25)L_0L_2L_8L_{11}$ | $(8/5)D_3$        |

**Lemma 7.1** (Rational points). *Let  $(M, N) \in \mathbb{Z}^2$  with  $FHJ \neq 0$ . Then  $P_1, P_2, P_3 \in E(\mathbb{Q})$  and  $Q_1, Q_2, Q_3 \in E'(\mathbb{Q})$ , and each of these six points has nonzero  $x$ -coordinate.*

*Proof.* Every  $x$ -coordinate in Table 7.2 is a nonzero constant times a product of four of the forms  $L_i$ ; it does not vanish when  $FHJ \neq 0$ . A point  $(x, y)$  with  $x \neq 0$  and  $y = xr$  lies on  $E$  if and only if  $r^2 = x + \alpha + \beta/x$ , and it lies on  $E'$  if and only if  $r^2 = x + \alpha' + \beta'/x$ . For each point of the table,  $x$  divides  $\beta$  (respectively  $\beta'$ ) in  $\mathbb{Q}[M, N]$ . For example, for  $P_3$  we have

$$\frac{\beta}{x} = \frac{-784FH}{-175L_1L_3L_4L_6} = \frac{112}{25}L_0L_2L_5L_7.$$

After we multiply by 25 for  $P_3$  and  $Q_3$ , the six conditions become the following identities between binary quartic forms:

$$\begin{aligned} (P_1) \quad & 1764D_0^2 = 14F + 14H, \\ (P_2) \quad & 9(3D_1 + 65D_0)^2 = -2L_1L_2L_4L_5 + 70F + 392L_0L_3L_6L_7, \\ (P_3) \quad & 441D_2^2 = -4375L_1L_3L_4L_6 + 1750F + 112L_0L_2L_5L_7, \\ (Q_1) \quad & 28224D_0^2 = -126F + 126J, \\ (Q_2) \quad & 64(2D_1 - 55D_0)^2 = 2L_0L_3L_{10}L_{11} - 140F + 882L_1L_2L_8L_9, \\ (Q_3) \quad & 64D_3^2 = 18L_0L_2L_8L_{11} - 3500F + 61250L_1L_3L_9L_{10}. \end{aligned} \quad (7.11)$$

The identities for  $P_1$  and  $Q_1$  are 14 and 126 times the two identities in (7.2). We check each identity in (7.11) by expanding both sides and comparing the coefficients of  $M^4$ ,  $M^3N$ ,  $M^2N^2$ ,  $MN^3$  and  $N^4$ ; Table 7.3 lists the common values. This completes the proof.  $\square$

Table 7.3. The coefficients of  $M^4, M^3N, M^2N^2, MN^3, N^4$ , in this order, common to both sides of each identity in (7.11).

| point | $M^4$   | $M^3N$   | $M^2N^2$ | $MN^3$     | $N^4$      |
|-------|---------|----------|----------|------------|------------|
| $P_1$ | 1764    | 0        | 105840   | 0          | 1587600    |
| $P_2$ | 176400  | -2555280 | 8497764  | 5475600    | 810000     |
| $P_3$ | 1192464 | 17199000 | 17298225 | -322481250 | 419225625  |
| $Q_1$ | 28224   | 0        | 1693440  | 0          | 25401600   |
| $Q_2$ | 1600    | 432640   | 31262464 | 272563200  | 635040000  |
| $Q_3$ | 97344   | -2496000 | 38713600 | -291200000 | 1324960000 |

At a prime specialization, we compute the classes of these points by inserting  $L_i = c_i p_i$  and (7.8). We collect the results in Table 7.4.

Table 7.4. The classes of  $T, P_1, P_2, P_3$  under  $\delta_E$  and of  $T', Q_1, Q_2, Q_3$  under  $\delta_{E'}$  at a prime specialization. The second column is  $\beta$  or  $\beta'$  for  $T$  and  $T'$  and the  $x$ -coordinate otherwise.

| point | $x$ (or $\beta, \beta'$ )   | in terms of the $p_i$                      | class                                 | moving support             |
|-------|-----------------------------|--------------------------------------------|---------------------------------------|----------------------------|
| $T$   | $-784FH$                    | $-112^2 p_0 p_1 \cdots p_7$                | $[-p_0 p_1 \cdots p_7]$               | $0, 1, \dots, 7$           |
| $P_1$ | $14H$                       | $2^2 \cdot 7 p_4 p_5 p_6 p_7$              | $[7p_4 p_5 p_6 p_7]$                  | $4, 5, 6, 7$               |
| $P_2$ | $-2L_1 L_2 L_4 L_5$         | $-2^2 p_1 p_2 p_4 p_5$                     | $[-p_1 p_2 p_4 p_5]$                  | $1, 2, 4, 5$               |
| $P_3$ | $-175L_1 L_3 L_4 L_6$       | $-20^2 \cdot 7 p_1 p_3 p_4 p_6$            | $[-7p_1 p_3 p_4 p_6]$                 | $1, 3, 4, 6$               |
| $T'$  | $1764FJ$                    | $3024^2 p_0 p_1 p_2 p_3 p_8 \cdots p_{11}$ | $[p_0 p_1 p_2 p_3 p_8 \cdots p_{11}]$ | $0, 1, 2, 3, 8, 9, 10, 11$ |
| $Q_1$ | $14F$                       | $4^2 \cdot 7 p_0 p_1 p_2 p_3$              | $[7p_0 p_1 p_2 p_3]$                  | $0, 1, 2, 3$               |
| $Q_2$ | $2L_0 L_3 L_{10} L_{11}$    | $4^2 \cdot 3 p_0 p_3 p_{10} p_{11}$        | $[3p_0 p_3 p_{10} p_{11}]$            | $0, 3, 10, 11$             |
| $Q_3$ | $(18/25)L_0 L_2 L_8 L_{11}$ | $(12/5)^2 p_0 p_2 p_8 p_{11}$              | $[p_0 p_2 p_8 p_{11}]$                | $0, 2, 8, 11$              |

**Lemma 7.2** (Independent classes). *Let  $(M, N)$  be a prime specialization of  $\mathfrak{D}_6$ . Then the classes  $\delta_E(T)$ ,  $\delta_E(P_1)$ ,  $\delta_E(P_2)$ ,  $\delta_E(P_3)$  and  $\delta_{E'}(T')$ ,  $\delta_{E'}(Q_1)$ ,  $\delta_{E'}(Q_2)$ ,  $\delta_{E'}(Q_3)$  are those listed in Table 7.4, and the four classes on each side are independent. In particular,  $d_E \geq 4$  and  $d_{E'} \geq 4$ .*

*Proof.* By Definition 3.3, we have  $\delta_E(T) = [\beta]$  and  $\delta_{E'}(T') = [\beta']$ , and every other point is sent to the class of its  $x$ -coordinate, which is nonzero by Lemma 7.1. Inserting  $L_i = c_i p_i$  and (7.8), we obtain the third column of Table 7.4. For example,  $P_3$  has  $x = -175L_1 L_3 L_4 L_6 = -175 \cdot c_1 c_3 c_4 c_6 p_1 p_3 p_4 p_6 = -2800 p_1 p_3 p_4 p_6$ , and  $2800 = 20^2 \cdot 7$ . Removing the square factor gives the class in the fourth column.

Since the  $p_j$  are distinct primes outside  $S$ , the coordinate of each class at the column  $p_j$  of  $\mathcal{B}_E$  or  $\mathcal{B}_{E'}$  is 1 if  $j$  belongs to its moving support and 0 otherwise. The coordinates of the four classes on  $E$  at the columns  $p_0, p_7, p_2, p_3$ , and those of the four classes on  $E'$  at the columns  $p_9, p_1, p_3, p_2$ , are

|                 | $p_0$ | $p_7$ | $p_2$ | $p_3$ |                    | $p_9$ | $p_1$ | $p_3$ | $p_2$ |
|-----------------|-------|-------|-------|-------|--------------------|-------|-------|-------|-------|
| $\delta_E(T)$   | 1     | 1     | 1     | 1     | $\delta_{E'}(T')$  | 1     | 1     | 1     | 1     |
| $\delta_E(P_1)$ | 0     | 1     | 0     | 0     | $\delta_{E'}(Q_1)$ | 0     | 1     | 1     | 1     |
| $\delta_E(P_2)$ | 0     | 0     | 1     | 0     | $\delta_{E'}(Q_2)$ | 0     | 0     | 1     | 0     |
| $\delta_E(P_3)$ | 0     | 0     | 0     | 1     | $\delta_{E'}(Q_3)$ | 0     | 0     | 0     | 1     |

Both arrays are upper triangular with ones on the diagonal, and Lemma 3.12 implies that the four classes on each side are independent. Since they are classes of points of  $E(\mathbb{Q})$  and  $E'(\mathbb{Q})$  (Lemma 7.1), we have  $d_E \geq 4$  and  $d_{E'} \geq 4$ .  $\square$

### 7.3 The congruence class and the real cone

We impose the congruences of Table 7.5. The moduli are pairwise coprime, and their product is

$$W = 2^6 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 23 = 780373440.$$

By the Chinese remainder theorem, the congruences of Table 7.5 hold if and only if  $(M, N) \equiv (M_0, N_0) \pmod{W}$ , where

$$M_0 = 416513683, \quad N_0 = 91046603. \quad (7.12)$$

We define the progression and the cone

$$\begin{aligned} \mathcal{P}_6 &= \{(M, N) \in \mathbb{Z}^2 : M \equiv M_0 \text{ and } N \equiv N_0 \pmod{W}\}, \\ \mathcal{K}_6 &= \{(M, N) \in \mathbb{R}^2 : N > 0 \text{ and } 29N < M < 31N\}. \end{aligned} \quad (7.13)$$

Equivalently,  $\mathcal{P}_6$  consists of the pairs  $(M_0 + WX, N_0 + WY)$  with  $(X, Y) \in \mathbb{Z}^2$ .

Table 7.5. The congruences defining  $\mathcal{P}_6$ .

| modulus                  | 64 | 81 | 5 | 7 | 11 | 17 | 23 |
|--------------------------|----|----|---|---|----|----|----|
| $M \bmod \text{modulus}$ | 19 | 19 | 3 | 5 | 3  | 15 | 13 |
| $N \bmod \text{modulus}$ | 11 | 11 | 3 | 4 | 10 | 9  | 22 |

**Lemma 7.3** (Residues on the progression). *Let  $(M, N) \in \mathcal{P}_6$ . Then  $c_i$  divides  $L_i(M, N)$  for every  $i$ , and the integers  $p_i = L_i(M, N)/c_i$  satisfy the congruences of Table 7.6 modulo 8, 3, 5, 7, 11, 17 and 23. In particular, every  $p_i$  is prime to  $W$ , we have  $v_2(L_i(M, N)) = v_2(c_i)$  and  $v_3(L_i(M, N)) = v_3(c_i)$  for every  $i$ , and  $FHJ \neq 0$ .*

Table 7.6. The values  $L_i(19, 11)$  and  $L_i(19, 11)/c_i$ , and the residues of  $p_i = L_i(M, N)/c_i$  for  $(M, N) \in \mathcal{P}_6$  (Lemma 7.3).

| $i$ | $L_i(19, 11)$ | $L_i(19, 11)/c_i$ | $p_i \bmod 8$ | $\bmod 3$ | $\bmod 5$ | $\bmod 7$ | $\bmod 11$ | $\bmod 17$ | $\bmod 23$ |
|-----|---------------|-------------------|---------------|-----------|-----------|-----------|------------|------------|------------|
| 0   | 19            | 19                | 3             | 1         | 3         | 5         | 3          | 15         | 13         |
| 1   | 11            | 11                | 3             | 2         | 3         | 4         | 10         | 9          | 22         |
| 2   | 11461         | 11461             | 5             | 1         | 2         | 2         | 10         | 3          | 21         |
| 3   | -1384         | -173              | 3             | 1         | 1         | 2         | 3          | 14         | 10         |
| 4   | -278          | -139              | 5             | 2         | 1         | 1         | 4          | 5          | 20         |
| 5   | 353           | 353               | 1             | 2         | 1         | 3         | 1          | 13         | 2          |
| 6   | -193          | -193              | 7             | 2         | 3         | 3         | 5          | 11         | 1          |
| 7   | 281           | 281               | 1             | 2         | 2         | 1         | 6          | 4          | 15         |
| 8   | 184           | 23                | 7             | 2         | 1         | 2         | 4          | 6          | 17         |
| 9   | 837           | 31                | 7             | 1         | 4         | 3         | 9          | 12         | 1          |
| 10  | -3            | -1                | 7             | 2         | 4         | 6         | 9          | 16         | 5          |
| 11  | -547          | -547              | 5             | 2         | 1         | 6         | 3          | 11         | 15         |

*Proof.* We begin with the primes 2 and 3. Note that  $M_0 \equiv 19$  and  $N_0 \equiv 11$  modulo  $2^6$  and modulo  $3^4$ , which implies that  $(M, N) \equiv (19, 11) \pmod{2^6 3^4}$ . We read off from the second and third columns of Table 7.6 that  $L_i(19, 11)/c_i$  is an integer prime to 6. By Table 7.1, every  $c_i$  divides  $2^3 3^3$ , hence  $2^6 3^4$ , and  $2^6 3^4/c_i$  is divisible by  $2^3 \cdot 3$ . By Lemma 4.7 with  $W_0 = 2^6 3^4$  and  $(m, n) = (19, 11)$ , the cofactor  $c_i$  divides  $L_i(M, N)$ , and  $p_i \equiv L_i(19, 11)/c_i$  modulo  $2^6 3^4/c_i$ , and hence modulo 8 and modulo 3; this gives the columns for 8 and 3. The integer  $p_i$  is then prime to 6, and  $v_2(L_i(M, N)) = v_2(c_i)$ ,  $v_3(L_i(M, N)) = v_3(c_i)$ .

Next, let  $q \in \{5, 7, 11, 17, 23\}$ . Every  $c_i$  is invertible modulo  $q$ , and Table 7.5 prescribes  $(M, N)$  modulo  $q$ . We find that  $p_i \equiv c_i^{-1}(a_i M + b_i N) \pmod{q}$  is determined by the prescribed residues, which gives the remaining columns of Table 7.6. All entries of the table are nonzero, which shows that  $p_i$  is prime to every prime divisor of  $W$ . Finally,  $L_i(M, N) = c_i p_i \neq 0$  for every  $i$ , and  $FHJ \neq 0$ .  $\square$

Several of the quotients  $L_i(19, 11)/c_i$  are negative, and their residues must be computed with the sign. For example,  $L_3(19, 11)/8 = -173 \equiv 3 \pmod{8}$ , whereas  $173 \equiv 5 \pmod{8}$ . The pair  $(19, 11)$  represents only the classes modulo  $2^6$  and  $3^4$ , and it does not lie in  $\mathcal{K}_6$ . At the points of  $\mathcal{P}_6 \cap \mathcal{K}_6$  the  $p_i$  are positive and have the residues of Table 7.6.

**Lemma 7.4** (Positivity on the cone). *Every form  $L_i$  is positive on  $\mathcal{K}_6$ . In particular,  $F$ ,  $H$  and  $J$  are positive on  $\mathcal{K}_6$ .*

*Proof.* For  $N > 0$ , we have  $L_i/N = a_it + b_i$  with  $t = M/N$ , which is an affine function of  $t$ . Its values at the endpoints  $t = 29$  and  $t = 31$  are

| $i$      | 0  | 1 | 2    | 3   | 4 | 5   | 6  | 7   | 8  | 9   | 10 | 11  |
|----------|----|---|------|-----|---|-----|----|-----|----|-----|----|-----|
| $t = 29$ | 29 | 1 | 5651 | 556 | 2 | 223 | 37 | 271 | 44 | 267 | 27 | 823 |
| $t = 31$ | 31 | 1 | 5989 | 606 | 4 | 237 | 41 | 289 | 46 | 281 | 29 | 887 |

All of these values are positive. An affine function that is positive at both endpoints of an interval is positive on the whole interval. Then  $a_it + b_i > 0$  for  $29 \leq t \leq 31$ , and  $L_i = N(a_it + b_i) > 0$  on  $\mathcal{K}_6$ .  $\square$

Among the forms with  $a_i \neq 0$ , the largest root  $-b_i/a_i$  is 27, from  $L_4 = M - 27N$ , and  $L_1 = N$ . All forms are therefore positive whenever  $N > 0$  and  $M > 27N$ , and the cone  $\mathcal{K}_6$  lies inside this region.

## 7.4 Local conditions at the fixed places

We now prove the local conditions at the fixed places 2, 3, 7 and  $\infty$  and derive the fixed rows of the matrices of Section 7.6. We use the coordinates on  $\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2}$  of Section 3.1. At 2, every class is  $[(-1)^{e_1}2^{e_2}5^{e_3}]$  for a unique  $(e_1, e_2, e_3) \in \mathbb{F}_2^3$ , and an odd unit  $w$  has  $(e_1, e_3) = (0, 0), (1, 1), (0, 1), (1, 0)$  according as  $w \equiv 1, 3, 5, 7 \pmod{8}$ . At an odd prime  $q$ , we write a class as  $[q^k w]$  with  $w$  a  $q$ -adic unit and use the coordinates  $v_q(q^k w) = k \pmod{2}$  and  $\chi_q(q^k w) = \chi_q(w)$  of (3.3), where  $(w/q) = (-1)^{\chi_q(w)}$ . At  $\infty$ , we use the sign coordinate  $\text{sgn}$ , which is 1 on  $[-1]$  and 0 on  $[1]$ .

**Lemma 7.5** (Local images at the fixed places). *Let  $(M, N) \in \mathcal{P}_6$ . Then  $FHJ \neq 0$ , and*

$$\begin{aligned} \delta_{E,2}(E(\mathbb{Q}_2)) &\subseteq \langle [-1], [5] \rangle, & \delta_{E',2}(E'(\mathbb{Q}_2)) &\subseteq \{[1], [5]\}, \\ \delta_{E,3}(E(\mathbb{Q}_3)) &= \{[1]\}, \\ \delta_{E,7}(E(\mathbb{Q}_7)) &\subseteq \{[1], [7]\}, & \delta_{E',7}(E'(\mathbb{Q}_7)) &\subseteq \{[1], [21]\}. \end{aligned}$$

*If moreover  $(M, N) \in \mathcal{K}_6$ , then  $\delta_{E',\infty}(E'(\mathbb{R})) = \{[1]\}$ .*

We use no condition at 3 on  $E'$  and no condition at  $\infty$  on  $E$ .

*Proof.* We have  $FHJ \neq 0$  by Lemma 7.3. We first compute the valuations and unit residues of the four coefficients  $\alpha, \beta, \alpha', \beta'$  on  $\mathcal{P}_6$ . We then treat the places 2, 3, 7 and  $\infty$  in turn. At each place we consider the point  $O$ , the point  $(0, 0)$ , the other points with  $y = 0$ , and the points with  $y \neq 0$ , the last according to the valuation of  $x$ .

**The coefficients.** Let  $\pi_F = p_0 p_1 p_2 p_3$ ,  $\pi_H = p_4 p_5 p_6 p_7$  and  $\pi_J = p_8 p_9 p_{10} p_{11}$ , where  $p_i = L_i(M, N)/c_i$  are the integers of Lemma 7.3. The computation leading to (7.8) applies to every  $(M, N) \in \mathcal{P}_6$  and gives  $F = 8\pi_F$ ,  $H = 2\pi_H$  and  $J = 648\pi_J$ . Multiplying the residues of Table 7.6, we find

$$\begin{aligned} \pi_F &\equiv 7, \quad \pi_H \equiv 3, \quad \pi_J \equiv 3 & (\text{mod } 8), \\ \pi_F &\equiv 2, \quad \pi_H \equiv 1, \quad \pi_J \equiv 2 & (\text{mod } 3), \\ \pi_F &\equiv 3, \quad \pi_H \equiv 2, \quad \pi_J \equiv 6 & (\text{mod } 7). \end{aligned}$$

We have  $\alpha = 560\pi_F$ ,  $\beta = -12544\pi_F\pi_H$ ,  $\alpha' = -1120\pi_F$  and  $\beta' = 9144576\pi_F\pi_J$ , where  $560 = 2^4 \cdot 5 \cdot 7$ ,  $12544 = 2^8 7^2$ ,  $1120 = 2^5 \cdot 5 \cdot 7$  and  $9144576 = 2^8 3^6 7^2$ . Inserting the residues above, we obtain Table 7.7. Together with  $\alpha' = -2\alpha$  and  $\beta' = \alpha^2 - 4\beta$ , these are the only properties of the coefficients that we use below, and by Lemma 7.3 they hold for every  $(M, N) \in \mathcal{P}_6$ .

Table 7.7. Valuations of the coefficients at 2, 3, 7, and their unit parts  $z p^{-v_p(z)}$  modulo 8, 3, 7, for  $(M, N) \in \mathcal{P}_6$ .

| coefficient       | $v_2$ | unit mod 8 | $v_3$ | unit mod 3 | $v_7$ | unit mod 7 |
|-------------------|-------|------------|-------|------------|-------|------------|
| $\alpha = 70F$    | 4     | 5          | 0     | 1          | 1     | 2          |
| $\beta = -784FH$  | 8     | 3          | 0     | 1          | 2     | 4          |
| $\alpha' = -140F$ | 5     | 3          | 0     | 1          | 1     | 3          |
| $\beta' = 1764FJ$ | 8     | 5          | 6     | 1          | 2     | 2          |

**The prime 2, curve  $E$ .** The change of variables  $x = 2^4 \tilde{x}$ ,  $y = 2^6 \tilde{y}$  is a bijection from the affine points of  $E(\mathbb{Q}_2)$  to those of

$$\tilde{y}^2 = \tilde{x}^3 + \alpha_2 \tilde{x}^2 + \beta_2 \tilde{x}, \quad \alpha_2 = 2^{-4}\alpha, \quad \beta_2 = 2^{-8}\beta,$$

and  $[x] = [\tilde{x}]$  since  $2^4$  is a square. Using Table 7.7, we see that  $\alpha_2$  and  $\beta_2$  are 2-adic units with  $\alpha_2 \equiv 5$  and  $\beta_2 \equiv 3 \pmod{8}$ . The point  $O$  has class  $[1]$ , and  $\delta_{E,2}(T) = [\beta] = [\beta_2] = [3] = [-5]$ . The discriminant of  $\tilde{x}^2 + \alpha_2 \tilde{x} + \beta_2$  is  $\alpha_2^2 - 4\beta_2 = 2^{-8}\beta'$ , which is a unit congruent to 5 modulo 8 and hence not a square in  $\mathbb{Q}_2$  by Lemma 3.2(b). By Lemma 3.7,  $E$  has no other point with  $y = 0$ . Now let  $(\tilde{x}, \tilde{y})$  be a point such that  $\tilde{y} \neq 0$ , and let  $r = v_2(\tilde{x})$ . If  $r < 0$ , the term  $\tilde{x}^3$  has strictly smaller valuation than  $\alpha_2 \tilde{x}^2$  and  $\beta_2 \tilde{x}$ , since  $3r < 2r < r$ . Lemma 3.1(a) implies that  $v_2(\tilde{y}^2) = 3r$ , and since  $v_2(\tilde{y}^2)$  is even,  $r$  is even. If  $r > 0$ , the term  $\beta_2 \tilde{x}$  has the strictly smallest valuation  $r$ ; as before,  $r$  is even. If  $r = 0$ , then  $r$  is even. In every case  $[\tilde{x}]$  has  $e_2 = 0$ , which shows that  $\delta_{E,2}(E(\mathbb{Q}_2)) \subseteq \langle [-1], [5] \rangle$ .

**The prime 2, curve  $E'$ .** The same change of variables transforms  $E'$  into

$$\tilde{y}^2 = \tilde{x}^3 - 2\alpha_2\tilde{x}^2 + \beta'_2\tilde{x}, \quad \beta'_2 = 2^{-8}\beta' = \alpha_2^2 - 4\beta_2,$$

and we have  $\beta'_2 \equiv 5 \pmod{8}$  by Table 7.7. The point  $O$  has class  $[1]$ , and  $\delta_{E',2}(T') = [\beta'_2] = [5]$ . The discriminant of  $\tilde{x}^2 - 2\alpha_2\tilde{x} + \beta'_2$  is  $4\alpha_2^2 - 4\beta'_2 = 16\beta_2$ , whose class  $[\beta_2] = [3]$  is not trivial. By Lemma 3.7, there is no other point with  $\tilde{y} = 0$ . Let  $(\tilde{x}, \tilde{y})$  be a point with  $\tilde{y} \neq 0$ , and write  $\tilde{x} = 2^r w$  with  $w$  a unit. Recall from Lemma 3.2(b) that a unit of  $\mathbb{Z}_2$  is a square in  $\mathbb{Q}_2$  if and only if it is congruent to 1 modulo 8.

Suppose that  $r < 0$ . The valuations of  $\tilde{x}^3$ ,  $-2\alpha_2\tilde{x}^2$  and  $\beta'_2\tilde{x}$  are  $3r$ ,  $1 + 2r$  and  $r$ , and  $3r$  is the strictly smallest. By Lemma 3.1(a), we have  $v_2(\tilde{y}^2) = 3r$ , which implies that  $r$  is even, and  $r \leq -2$ . The other two terms then have valuations  $1 + 2r \geq 3r + 3$  and  $r \geq 3r + 4$ , and by Lemma 3.1(b) with  $h = 3$  we have  $\tilde{y}^2 = \tilde{x}^3(1 + 8t)$  with  $t \in \mathbb{Z}_2$ . The factor  $1 + 8t$  is a square by Lemma 3.2(c). Then  $\tilde{x}^3$  is a square, and  $[\tilde{x}] = [\tilde{x}^3] = [1]$ .

Suppose that  $r > 0$ . Now  $\beta'_2\tilde{x}$  has the strictly smallest valuation  $r$ , and as before  $r$  is even, so that  $r \geq 2$ . The other two terms have valuations  $1 + 2r \geq r + 3$  and  $3r \geq r + 4$ , and Lemma 3.1(b) gives  $\tilde{y}^2 = \beta'_2\tilde{x}(1 + 8t)$  with  $t \in \mathbb{Z}_2$ . We see that  $\beta'_2\tilde{x}$  is a square, and  $[\tilde{x}] = [\beta'_2] = [5]$ .

Suppose that  $r = 0$ , so that  $\tilde{x} = w$ . Since  $\beta'_2 = \alpha_2^2 - 4\beta_2$ , we have

$$\tilde{x}^2 - 2\alpha_2\tilde{x} + \beta'_2 = (w - \alpha_2)^2 - 4\beta_2 = 4\left(\left(\frac{w - \alpha_2}{2}\right)^2 - \beta_2\right),$$

where  $(w - \alpha_2)/2$  belongs to  $\mathbb{Z}_2$  because  $w$  and  $\alpha_2$  are odd. If  $w \equiv 3 \pmod{4}$ , then  $w - \alpha_2 \equiv 2 \pmod{4}$ , because  $\alpha_2 \equiv 1 \pmod{4}$ . Then  $(w - \alpha_2)/2$  is odd, its square is congruent to 1 modulo 8, and the bracket is congruent to  $1 - 3 \equiv 6 \pmod{8}$  and has valuation one. It follows that  $\tilde{y}^2 = w(\tilde{x}^2 - 2\alpha_2\tilde{x} + \beta'_2)$  has valuation three, which is impossible. Therefore  $w \equiv 1 \pmod{4}$ , that is,  $w \equiv 1$  or  $5 \pmod{8}$ , and  $[\tilde{x}] = [w] \in \{[1], [5]\}$ .

Combining the three cases with the classes of  $O$  and  $T'$ , we obtain  $\delta_{E',2}(E'(\mathbb{Q}_2)) \subseteq \{[1], [5]\}$ .

**The prime 3, curve  $E$ .** By Table 7.7,  $\alpha$  and  $\beta$  are 3-adic units with  $\alpha \equiv \beta \equiv 1 \pmod{3}$ , and  $\beta' = 3^6 w'$  with a unit  $w' \equiv 1 \pmod{3}$ . The point  $O$  has class  $[1]$ , and  $\delta_{E,3}(T) = [\beta] = [1]$ , since  $\beta$  is a unit congruent to 1 modulo 3 (Lemma 3.2(a)). Let  $(x, y) \in E(\mathbb{Q}_3)$  be a point such that  $x \neq 0$ , and let  $r = v_3(x)$ .

If  $r < 0$ , the term  $x^3$  has valuation  $3r$ , and the other two terms have valuations  $2r$  and  $r$ , which are at least  $3r + 1$ . By Lemma 3.1(b), we have  $y^2 = x^3(1 + 3t)$  with  $t \in \mathbb{Z}_3$ . Then  $y \neq 0$ , and  $r$  is even because  $v_3(y^2) = 3r$  is even. The factor  $1 + 3t$  is a square by Lemma 3.2(c), and  $[x] = [x^3] = [1]$ . If  $r > 0$ , the term  $\beta x$  has valuation  $r$ , and the other two have valuations  $2r$  and  $3r$ , which are at least  $r + 1$ . As before,  $y \neq 0$ ,  $r$  is even, and  $y^2 = \beta x(1 + 3t)$ ; then  $\beta x$  is a square, and  $[x] = [\beta] = [1]$ . If  $r = 0$  and  $x \equiv 1 \pmod{3}$ ,

then  $[x] = [1]$ . If  $r = 0$  and  $x \equiv 2 \pmod{3}$ , then  $x^2 + \alpha x + \beta \equiv 4 + 2 + 1 \equiv 1 \pmod{3}$ , and  $x^3 + \alpha x^2 + \beta x \equiv 2 \pmod{3}$  is a unit that is not a square; there is no point with such an  $x$ .

The discriminant  $\alpha^2 - 4\beta = \beta' = 3^6 w'$  is a square in  $\mathbb{Q}_3$ . By Lemma 3.7, the curve  $E$  has two points  $(x_0, 0)$  and  $(x_1, 0)$  with  $x_0 x_1 = \beta$ . The case analysis above shows that a point with  $x \neq 0$  and  $y = 0$  has  $r = 0$  and  $x \equiv 1 \pmod{3}$ , and these two points have class  $[1]$ . We conclude that  $\delta_{E,3}(E(\mathbb{Q}_3)) = \{[1]\}$ .

**The prime 7.** Let  $(\alpha_*, \beta_*)$  be  $(\alpha, \beta)$  or  $(\alpha', \beta')$ , so that  $y^2 = x^3 + \alpha_* x^2 + \beta_* x$  is  $E$  or  $E'$ . Using Table 7.7, we find that  $v_7(\alpha_*) = 1$ ,  $v_7(\beta_*) = 2$ , and

$$\left(\frac{\alpha_*}{7}, \frac{\beta_*}{49}\right) \equiv (2, 4) \text{ on } E, \quad \left(\frac{\alpha_*}{7}, \frac{\beta_*}{49}\right) \equiv (3, 2) \text{ on } E' \pmod{7}.$$

The nonzero squares modulo 7 are 1, 2 and 4. The point  $O$  has class  $[1]$ , and  $[\beta_*] = [\beta_*/49] = [1]$ , since  $\beta_*/49$  is a unit congruent to a nonzero square. Let  $(x, y)$  be a point such that  $x \neq 0$ , and let  $r = v_7(x)$ . The three terms  $x^3$ ,  $\alpha_* x^2$  and  $\beta_* x$  have valuations  $3r$ ,  $2r + 1$  and  $r + 2$ .

If  $r \leq 0$ , then  $2r + 1$  and  $r + 2$  are at least  $3r + 1$ . Using Lemma 3.1(b), we may write  $y^2 = x^3(1 + 7t)$  with  $t \in \mathbb{Z}_7$ . Then  $y \neq 0$ , the valuation  $3r$  of  $y^2$  is even, and  $r$  is even. We also have  $[x] = [x^3] = [1]$ , because  $1 + 7t$  is a square (Lemma 3.2(c)). If  $r \geq 2$ , then  $3r$  and  $2r + 1$  are at least  $(r + 2) + 1$ , and Lemma 3.1(b) gives  $y^2 = \beta_* x(1 + 7t)$  with  $t \in \mathbb{Z}_7$ . As before,  $y \neq 0$ ,  $r$  is even, and  $[x] = [\beta_*] = [1]$ .

If  $r = 1$ , write  $x = 7w$  with  $w$  a unit. Then

$$y^2 = 7^3 w h_*(w), \quad h_*(w) = w^2 + \frac{\alpha_*}{7} w + \frac{\beta_*}{49} \in \mathbb{Z}_7.$$

If  $h_*(w)$  were a unit, then  $y \neq 0$  and  $v_7(y^2) = 3$ , which is impossible. Hence  $h_*(w) \equiv 0 \pmod{7}$ , both when  $y \neq 0$  and when  $y = 0$ . Modulo 7, we have  $h_*(w) \equiv w^2 + 2w + 4 \equiv (w - 1)(w - 4)$  on  $E$  and  $h_*(w) \equiv w^2 + 3w + 2 \equiv (w + 1)(w + 2)$  on  $E'$ . On  $E$ , the residue of  $w$  is 1 or 4, which is a square; then  $[x] = [7w] = [7]$ . On  $E'$ , the residue of  $w$  is 5 or 6, which is not a square modulo 7; then  $[w] = [3]$  and  $[x] = [21]$ .

The points with  $y = 0$  and  $x \neq 0$  have  $r = 1$ , since  $y \neq 0$  in the other cases; they are covered by the last paragraph. By Lemma 3.7, such points exist on both curves: the discriminants are  $\beta' = 49 \cdot (\beta'/49)$  on  $E$  and  $16\beta = 49 \cdot (16\beta/49)$  on  $E'$ , and the units  $\beta'/49 \equiv 2$  and  $16\beta/49 \equiv 16 \cdot 4 \equiv 1$  are squares modulo 7. We conclude that  $\delta_{E,7}(E(\mathbb{Q}_7)) \subseteq \{[1], [7]\}$  and  $\delta_{E',7}(E'(\mathbb{Q}_7)) \subseteq \{[1], [21]\}$ .

**The real place, curve  $E'$ .** Let  $(M, N) \in \mathcal{K}_6$ . Then  $F$ ,  $H$  and  $J$  are positive by Lemma 7.4, so that  $\alpha' = -140F < 0$  and  $\beta' = 1764FJ > 0$ . For  $x < 0$ , the three terms  $x^3$ ,  $\alpha' x^2$  and  $\beta' x$  are negative, and  $E'(\mathbb{R})$  has no point with  $x < 0$ . The points  $O$  and  $T'$  have classes  $[1]$  and  $[\beta'] = [1]$ , and therefore  $\delta_{E',\infty}(E'(\mathbb{R})) = \{[1]\}$ . This completes the proof.  $\square$

**The fixed rows.** In the coordinates above, the subgroups of Lemma 7.5 are

$$\begin{aligned} \langle [-1], [5] \rangle &= \{e_2 = 0\}, & \{[1], [5]\} &= \{e_1 = e_2 = 0\} && \text{in } \mathbb{Q}_2^\times / \mathbb{Q}_2^{\times 2}, \\ \{[1]\} &= \{v_3 = \chi_3 = 0\} &&&& \text{in } \mathbb{Q}_3^\times / \mathbb{Q}_3^{\times 2}, \\ \{[1], [7]\} &= \{\chi_7 = 0\}, & \{[1], [21]\} &= \{\chi_7 + v_7 = 0\} && \text{in } \mathbb{Q}_7^\times / \mathbb{Q}_7^{\times 2}, \\ \{[1]\} &= \{\text{sgn} = 0\} &&&& \text{in } \mathbb{R}^\times / \mathbb{R}^{\times 2}, \end{aligned}$$

where we used that  $[21] = [7 \cdot 3]$  has  $v_7 = 1$  and  $\chi_7 = 1$ . By Lemma 3.10, the following linear maps give rows for  $\delta_E(E(\mathbb{Q}))$  and  $\delta_{E'}(E'(\mathbb{Q}))$ , which we name as in Proposition 4.18: on  $E$ , the fixed rows  $f_1^E, f_2^E, f_3^E, f_4^E$  are given by the linear map  $e_2$  at 2, the linear maps  $\chi_3$  and  $v_3$  at 3, and  $\chi_7$  at 7; on  $E'$ , the fixed rows  $f_1^{E'}, f_2^{E'}, f_3^{E'}, f_4^{E'}$  are given by the linear maps  $e_1$  and  $e_2$  at 2,  $\chi_7 + v_7$  at 7, and  $\text{sgn}$  at  $\infty$ . To write the rows, we evaluate each linear map at the local coordinates of the basis elements. Table 7.8 lists these coordinates for  $-1, 2, 3$  and  $7$ . For the moving basis elements  $p_j$  with  $(M, N) \in \mathcal{P}_6 \cap \mathcal{K}_6$ , we have  $e_1(p_j) = 1$  if and only if  $p_j \equiv 3 \pmod{4}$ ,  $e_2(p_j) = v_3(p_j) = v_7(p_j) = \text{sgn}(p_j) = 0$ ,  $\chi_3(p_j) = 1$  if and only if  $p_j \equiv 2 \pmod{3}$ , and  $\chi_7(p_j) = 1$  if and only if  $p_j \equiv 3, 5, 6 \pmod{7}$ . Since these values depend only on the residues of Table 7.6, the fixed rows are the same at every point of  $\mathcal{P}_6 \cap \mathcal{K}_6$ . They are the first four rows of Tables 7.13 and 7.14.

Table 7.8. Local coordinates of the constant basis elements.

|      | $\mathbb{Q}_2$ |       |       | $\mathbb{Q}_3$ |          | $\mathbb{Q}_7$ |          | $\mathbb{R}$ |
|------|----------------|-------|-------|----------------|----------|----------------|----------|--------------|
|      | $e_1$          | $e_2$ | $e_3$ | $v_3$          | $\chi_3$ | $v_7$          | $\chi_7$ | $\text{sgn}$ |
| $-1$ | 1              | 0     | 0     | 0              | 1        | 0              | 1        | 1            |
| $2$  | 0              | 1     | 0     | 0              | 1        | 0              | 0        | 0            |
| $3$  | 1              | 0     | 1     | 1              | 0        | 0              | 1        | 0            |
| $7$  | 1              | 0     | 0     | 0              | 0        | 1              | 0        | 0            |

## 7.5 Characters at the moving primes

Fix a prime specialization  $(M, N)$  of  $\mathcal{D}_6$  with  $(M, N) \in \mathcal{P}_6$ . We compute the characters  $\lambda_i(z)$  that enter the moving rows of Lemma 4.11. Recall that  $\lambda_i(z) \in \mathbb{F}_2$  is defined by  $(z/p_i) = (-1)^{\lambda_i(z)}$  for  $z$  prime to  $p_i$ . Since  $(a_0, b_0) = (1, 0)$ ,  $(a_1, b_1) = (0, 1)$  and  $c_0 = c_1 = 1$ , we have  $p_0 = M$  and  $p_1 = N$ . As in Lemma 4.12, we define  $\eta \in \mathbb{F}_2$  by

$$\varepsilon = \left( \frac{N}{p_0} \right) = (-1)^\eta;$$

here  $\varepsilon \neq 0$  because  $p_1 \neq p_0$ .

**Constant characters.** By Lemma 4.13, that is, by quadratic reciprocity and its supplementary laws (4.22), we have, for every odd prime  $q \neq p_i$ ,

$$\begin{aligned}\lambda_i(-1) &= \mathbf{1}[p_i \equiv 3 \pmod{4}], & \lambda_i(2) &= \mathbf{1}[p_i \equiv \pm 3 \pmod{8}], \\ \lambda_i(q) &= \mathbf{1}[p_i \pmod{q} \text{ is a nonsquare}] + \mathbf{1}[q \equiv 3 \pmod{4}] \lambda_i(-1).\end{aligned}\tag{7.14}$$

Combined with Table 7.6, these rules give Table 7.9 for  $q \in \{3, 5, 7, 11, 17, 23\}$ . For checking the table, the nonzero squares modulo these primes are

$$\begin{aligned}3 : 1; & \quad 5 : 1, 4; & 7 : 1, 2, 4; & \quad 11 : 1, 3, 4, 5, 9; \\ 17 : 1, 2, 4, 8, 9, 13, 15, 16; & \quad 23 : 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.\end{aligned}$$

We write  $\sigma_i = \lambda_i(-1)$ ; this is the first row of Table 7.9.

Table 7.9. The characters  $\lambda_i(g)$  for the constants  $g$  that occur in the rows.

| $g \backslash i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|------------------|---|---|---|---|---|---|---|---|---|---|----|----|
| -1               | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1  | 0  |
| 2                | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0  | 1  |
| 3                | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0  | 1  |
| 5                | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0  | 0  |
| 7                | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0  | 1  |
| 11               | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1  | 0  |
| 17               | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0  | 1  |
| 23               | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0  | 1  |

**Cross symbols.** By Corollary 4.14, we have  $\lambda_i(p_j) = \gamma_{ij} + \eta$  for all distinct  $i, j$ , with the constants  $\gamma_{ij}$  of (4.26) and (4.27). Recall from Table 7.6 that  $p_0 \equiv 3 \pmod{4}$ , that is,  $\lambda_0(-1) = 1$ . Since  $c_0 = 1$ , these constants are

$$\begin{aligned}\gamma_{0j} &= \lambda_0(b_j c_j), & \gamma_{j0} &= \theta_j = \lambda_0(b_j c_j) + \sigma_j & (j \geq 1), \\ \gamma_{ij} &= \lambda_i(K_{ij}) + \theta_i, & \text{where } K_{ij} &= c_j b_i \Delta_{ji} & (i, j \geq 1, i \neq j).\end{aligned}\tag{7.15}$$

For  $1 \leq i < j$ , we compute  $\gamma_{ij}$  from (7.15). The reverse constant follows from quadratic reciprocity: by (4.22),  $\lambda_j(p_i) = \lambda_i(p_j) + \sigma_i \sigma_j$ , which gives

$$\gamma_{ji} = \gamma_{ij} + \sigma_i \sigma_j \quad (1 \leq i < j).\tag{7.16}$$

In this way, we only need to factor the constants  $K_{ij}$  with  $i < j$ . By Remark 4.15, the moving rows involve  $\gamma_{ij}$  only for  $i \neq j$  with  $\{i, j\}$  contained in neither  $I_H$  nor  $I_J$ . We list  $\lambda_0(b_j c_j)$  and  $\theta_j$  in Table 7.10, and  $\gamma_{ij}$  for the needed pairs with  $1 \leq i < j$  in Table 7.11; Table 7.12 collects all the constants.

The constants  $b_j c_j$  and  $K_{ij}$  in Tables 7.10 and 7.11 are a square times their squarefree part  $\text{sf}$ , and  $\lambda_i$  of a constant equals  $\lambda_i$  of its squarefree part. Every squarefree part listed is  $\pm 1$  times a product of primes in  $\{2, 3, 5, 7, 11, 17, 23\}$ , and its character is the sum of the corresponding entries of Table 7.9. The primes 13, 19 and 41 of  $S$ , which do not divide  $W$ , occur in these constants only to even powers:  $13^2$  divides  $b_3$  and  $\Delta_{21}$ , while every other determinant divisible by 13, 19 or 41 belongs to a pair inside  $I_H$  or inside  $I_J$  by (7.4), and such pairs do not occur. No congruence modulo 13, 19 or 41 is needed.

Table 7.10. The constants  $b_i c_i$ , their squarefree parts, and the bits  $\gamma_{0i} = \lambda_0(b_i c_i)$ ,  $\sigma_i = \lambda_i(-1)$  and  $\gamma_{i0} = \theta_i = \lambda_0(b_i c_i) + \sigma_i$ .

| $i$ | $b_i c_i$ | factored              | $\text{sf}(b_i c_i)$ | $\lambda_0(b_i c_i)$ | $\sigma_i$ | $\theta_i$ |
|-----|-----------|-----------------------|----------------------|----------------------|------------|------------|
| 1   | 1         | 1                     | 1                    | 0                    | 1          | 1          |
| 2   | 750       | $2 \cdot 3 \cdot 5^3$ | 30                   | 1                    | 0          | 1          |
| 3   | -1352     | $-2^3 \cdot 13^2$     | -2                   | 0                    | 1          | 1          |
| 4   | -54       | $-2 \cdot 3^3$        | -6                   | 1                    | 0          | 1          |
| 5   | 20        | $2^2 \cdot 5$         | 5                    | 1                    | 0          | 1          |
| 6   | -21       | $-3 \cdot 7$          | -21                  | 0                    | 1          | 1          |
| 7   | 10        | $2 \cdot 5$           | 10                   | 0                    | 0          | 0          |
| 8   | 120       | $2^3 \cdot 3 \cdot 5$ | 30                   | 1                    | 1          | 0          |
| 9   | 1728      | $2^6 \cdot 3^3$       | 3                    | 1                    | 1          | 0          |
| 10  | -6        | $-2 \cdot 3$          | -6                   | 1                    | 1          | 0          |
| 11  | -105      | $-3 \cdot 5 \cdot 7$  | -105                 | 1                    | 0          | 1          |

**Lemma 7.6** (Characters at the moving primes). *Let  $(M, N) \in \mathcal{P}_6$  be a prime specialization of  $\mathfrak{D}_6$ , and define  $\eta$  by  $(N/p_0) = (-1)^\eta$ . Then  $\lambda_i(g)$  is given by Table 7.9 for  $g \in \{-1, 2, 3, 5, 7, 11, 17, 23\}$ , and  $\lambda_i(p_j) = \gamma_{ij} + \eta$  with  $\gamma_{ij}$  given by Table 7.12, for all  $i \neq j$  with  $\{i, j\}$  contained in neither  $I_H$  nor  $I_J$ . In particular, the characters  $\lambda_i(g)$  and the constants  $\gamma_{ij}$  are the same for all prime specializations of  $\mathfrak{D}_6$  in  $\mathcal{P}_6$ , and the characters  $\lambda_i(p_j)$  depend on the specialization only through  $\eta$ .*

*Proof.* The first claim follows from (7.14) and Table 7.6. For the second, we have  $\lambda_i(p_j) = \gamma_{ij} + \eta$  by Corollary 4.14, and the constants  $\gamma_{ij}$  are given by (7.15) and (7.16). In these formulas,  $\lambda_0(b_j c_j)$  and  $\lambda_i(K_{ij})$  are computed from the squarefree parts in Tables 7.10 and 7.11 and the characters in Table 7.9. For example, for  $(i, j) = (2, 3)$  we have  $\text{sf}(K_{23}) = 5865 = 3 \cdot 5 \cdot 17 \cdot 23$ . This gives  $\lambda_2(K_{23}) = 0 + 1 + 1 + 1 = 1$  and  $\gamma_{23} = 1 + \theta_2 = 0$ , and (7.16) gives  $\gamma_{32} = \gamma_{23} + \sigma_2 \sigma_3 = 0$ . All these numbers depend only on the residues in Table 7.6, which are the same at every point of  $\mathcal{P}_6$ .  $\square$

Table 7.11. For the pairs  $1 \leq i < j$  that occur in the rows: the determinant  $\Delta_{ji} = a_j b_i - a_i b_j$ , the factor  $c_j b_i$ , the squarefree part of  $K_{ij} = c_j b_i \Delta_{ji}$ , the bit  $\lambda_i(K_{ij})$ , and  $\gamma_{ij} = \lambda_i(K_{ij}) + \theta_i$ .

| $(i, j)$ | $\Delta_{ji}$                   | $c_j b_i$ | sf   | $\lambda_i$ | $\gamma_{ij}$ | $(i, j)$ | $\Delta_{ji}$                 | $c_j b_i$ | sf    | $\lambda_i$ | $\gamma_{ij}$ |
|----------|---------------------------------|-----------|------|-------------|---------------|----------|-------------------------------|-----------|-------|-------------|---------------|
| (1, 2)   | $13^2$                          | 1         | 1    | 0           | 1             | (3, 7)   | $-7 \cdot 11 \cdot 23$        | -169      | 1771  | 0           | 1             |
| (1, 3)   | $5^2$                           | 8         | 2    | 1           | 0             | (3, 8)   | $-2^5 \cdot 17$               | -1352     | 17    | 1           | 0             |
| (1, 4)   | 1                               | 2         | 2    | 1           | 0             | (3, 9)   | $-11^2 \cdot 23$              | -4563     | 69    | 1           | 0             |
| (1, 5)   | 7                               | 1         | 7    | 1           | 0             | (3, 10)  | $-7 \cdot 17$                 | -507      | 357   | 1           | 0             |
| (1, 6)   | 2                               | 1         | 2    | 1           | 0             | (3, 11)  | $-11^2 \cdot 23$              | -169      | 23    | 0           | 1             |
| (1, 7)   | $3^2$                           | 1         | 1    | 0           | 1             | (4, 8)   | $-2 \cdot 3 \cdot 7$          | -216      | 7     | 0           | 1             |
| (1, 8)   | 1                               | 8         | 2    | 1           | 0             | (4, 9)   | $-11 \cdot 23$                | -729      | 253   | 1           | 0             |
| (1, 9)   | 7                               | 27        | 21   | 1           | 0             | (4, 10)  | $-5^2$                        | -81       | 1     | 0           | 1             |
| (1, 10)  | 1                               | 3         | 3    | 0           | 1             | (4, 11)  | $-3 \cdot 11 \cdot 23$        | -27       | 253   | 1           | 0             |
| (1, 11)  | $2^5$                           | 1         | 2    | 1           | 0             | (5, 8)   | $-5 \cdot 17$                 | 160       | -34   | 0           | 1             |
| (2, 3)   | $11^2 \cdot 17 \cdot 23$        | 6000      | 5865 | 1           | 0             | (5, 9)   | $-2^2 \cdot 7 \cdot 11$       | 540       | -1155 | 0           | 1             |
| (2, 4)   | $3 \cdot 7 \cdot 11 \cdot 23$   | 1500      | 8855 | 1           | 0             | (5, 10)  | $2 \cdot 17$                  | 60        | 510   | 1           | 0             |
| (2, 5)   | $2 \cdot 5 \cdot 11 \cdot 17$   | 750       | 561  | 0           | 1             | (5, 11)  | $5^3 \cdot 11$                | 20        | 11    | 0           | 1             |
| (2, 6)   | $3^3 \cdot 11 \cdot 17$         | 750       | 1870 | 0           | 1             | (6, 8)   | $-3 \cdot 17$                 | -168      | 238   | 1           | 0             |
| (2, 7)   | $2^2 \cdot 5 \cdot 11 \cdot 23$ | 750       | 1518 | 1           | 0             | (6, 9)   | $-5^2 \cdot 11$               | -567      | 77    | 1           | 0             |
| (2, 8)   | $-3 \cdot 5 \cdot 7 \cdot 17$   | 6000      | -119 | 1           | 0             | (6, 10)  | -17                           | -63       | 119   | 1           | 0             |
| (2, 9)   | $-2 \cdot 11^2 \cdot 23$        | 20250     | -115 | 0           | 1             | (6, 11)  | $-2 \cdot 3 \cdot 7 \cdot 11$ | -21       | 22    | 1           | 0             |
| (2, 10)  | $2^6 \cdot 17$                  | 2250      | 170  | 1           | 0             | (7, 8)   | $-5^3$                        | 80        | -1    | 0           | 0             |
| (2, 11)  | $3 \cdot 5 \cdot 11^2 \cdot 23$ | 750       | 46   | 0           | 1             | (7, 9)   | $-2 \cdot 11 \cdot 23$        | 270       | -3795 | 0           | 0             |
| (3, 4)   | $2 \cdot 11 \cdot 23$           | -338      | -253 | 0           | 1             | (7, 10)  | $2^2 \cdot 7$                 | 30        | 210   | 0           | 0             |
| (3, 5)   | $-3^2 \cdot 11 \cdot 17$        | -169      | 187  | 0           | 1             | (7, 11)  | $5 \cdot 11 \cdot 23$         | 10        | 506   | 0           | 0             |
| (3, 6)   | $11 \cdot 17$                   | -169      | -187 | 1           | 0             |          |                               |           |       |             |               |

Table 7.12. The constants  $\gamma_{ij}$ , defined by  $\lambda_i(p_j) = \gamma_{ij} + \eta$ . Row  $i$ , column  $j$ . A dot marks a pair inside  $I_H$  or inside  $I_J$ , which does not occur in the rows.

| $i \setminus j$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|-----------------|---|---|---|---|---|---|---|---|---|---|----|----|
| 0               | * | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1  | 1  |
| 1               | 1 | * | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1  | 0  |
| 2               | 1 | 1 | * | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0  | 1  |
| 3               | 1 | 1 | 0 | * | 1 | 1 | 0 | 1 | 0 | 0 | 0  | 1  |
| 4               | 1 | 0 | 0 | 1 | * | . | . | . | 1 | 0 | 1  | 0  |
| 5               | 1 | 0 | 1 | 1 | . | * | . | . | 1 | 1 | 0  | 1  |
| 6               | 1 | 1 | 1 | 1 | . | . | * | . | 0 | 0 | 0  | 0  |
| 7               | 0 | 1 | 0 | 1 | . | . | . | * | 0 | 0 | 0  | 0  |
| 8               | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | * | . | .  | .  |
| 9               | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | . | * | .  | .  |
| 10              | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | . | . | *  | .  |
| 11              | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | . | . | .  | *  |

## 7.6 The matrices and the upper bound

We now assemble the matrices  $\mathbf{M}_E(\eta)$  and  $\mathbf{M}_{E'}(\eta)$  of (4.35). We index the columns by the bases (7.7). The first four rows are the fixed rows of Section 7.4. The remaining eight rows are the moving rows  $r_i^E(0) + \eta u_E$  for  $i \in I_F$  and then  $i \in I_J$ , respectively  $r_i^{E'}(0) + \eta u_{E'}$  for  $i \in I_F$  and then  $i \in I_H$ . By Corollary 4.14, the entries of  $r_i^*(0)$  are as follows: at a constant column  $g \in \{-1, 2, 3, 7\}$ , the entry is  $\lambda_i(g)$ , from Table 7.9; at a moving column  $j \neq i$ , it is  $\gamma_{ij}$ , from Table 7.12; and for  $i \in I_F$ , the entry at the moving column  $i$  is  $\gamma_{ii}^* = \lambda_i(\kappa_*) + \sum_{j \in G_* \setminus \{i\}} \gamma_{ij}$ , as in (4.28). Using (7.9), we find  $\lambda_i(\kappa_E) = \lambda_i(-1) = \sigma_i$  and  $\lambda_i(\kappa_{E'}) = 0$ . The diagonal constants are

| $i$ | $\sum_{j \in G_E \setminus \{i\}} \gamma_{ij}$ | $\sigma_i$ | $\gamma_{ii}^E$ | $\sum_{j \in G_{E'} \setminus \{i\}} \gamma_{ij}$ | $\gamma_{ii}^{E'}$ |
|-----|------------------------------------------------|------------|-----------------|---------------------------------------------------|--------------------|
| 0   | 3                                              | 1          | 0               | 5                                                 | 1                  |
| 1   | 3                                              | 1          | 0               | 3                                                 | 1                  |
| 2   | 4                                              | 0          | 0               | 4                                                 | 0                  |
| 3   | 5                                              | 1          | 0               | 3                                                 | 1                  |

Tables 7.13 and 7.14 display  $\mathbf{M}_E(0)$  and  $\mathbf{M}_{E'}(0)$ . Recall from (4.35) that  $\mathbf{M}_*(1)$  is obtained by adding the vector  $u_E = u_{E'} = (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$  to each of the eight moving rows; that is, the entries of a moving row in a moving column are complemented, and all other entries are unchanged. The row codes used by the certificate are listed in Appendix A.

Table 7.13. The matrix  $\mathbf{M}_E(0)$ . The rows above the rule are the fixed rows  $f_k^E$ , with the place and the linear map that define them; the rows below are the moving rows  $r_i^E(0)$  at  $p_0, \dots, p_3$  and  $p_8, \dots, p_{11}$ . The entries that lie both in a moving row and in one of the columns  $p_0, \dots, p_7$  are those at  $\eta = 0$ ; for  $\eta = 1$  each of them is replaced by 1 minus its value, and all other entries are unchanged.

|               |               | -1 | 2 | 3 | 7 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $p_7$ |
|---------------|---------------|----|---|---|---|-------|-------|-------|-------|-------|-------|-------|-------|
| $f_1^E$       | $(2, e_2)$    | 0  | 1 | 0 | 0 | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     |
| $f_2^E$       | $(3, \chi_3)$ | 1  | 1 | 0 | 0 | 0     | 1     | 0     | 0     | 1     | 1     | 1     | 1     |
| $f_3^E$       | $(3, v_3)$    | 0  | 0 | 1 | 0 | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     |
| $f_4^E$       | $(7, \chi_7)$ | 1  | 0 | 1 | 0 | 1     | 0     | 0     | 0     | 0     | 1     | 1     | 0     |
| $r_0^E(0)$    | $p_0$         | 1  | 1 | 1 | 0 | 0     | 0     | 1     | 0     | 1     | 1     | 0     | 0     |
| $r_1^E(0)$    | $p_1$         | 1  | 1 | 0 | 1 | 1     | 0     | 1     | 0     | 0     | 0     | 0     | 1     |
| $r_2^E(0)$    | $p_2$         | 0  | 1 | 0 | 0 | 1     | 1     | 0     | 0     | 0     | 1     | 1     | 0     |
| $r_3^E(0)$    | $p_3$         | 1  | 1 | 1 | 1 | 1     | 1     | 0     | 0     | 1     | 1     | 0     | 1     |
| $r_8^E(0)$    | $p_8$         | 1  | 0 | 0 | 1 | 0     | 1     | 0     | 1     | 1     | 1     | 1     | 0     |
| $r_9^E(0)$    | $p_9$         | 1  | 0 | 1 | 0 | 0     | 1     | 1     | 1     | 0     | 1     | 1     | 0     |
| $r_{10}^E(0)$ | $p_{10}$      | 1  | 0 | 0 | 0 | 0     | 0     | 0     | 1     | 1     | 0     | 1     | 0     |
| $r_{11}^E(0)$ | $p_{11}$      | 0  | 1 | 1 | 1 | 1     | 0     | 1     | 1     | 0     | 1     | 0     | 0     |

Table 7.14. The matrix  $\mathbf{M}_{E'}(0)$ , with the conventions of Table 7.13. The moving rows  $r_i^{E'}(0)$  are at  $p_0, \dots, p_3$  and  $p_4, \dots, p_7$ , and the moving columns are  $p_0, \dots, p_3, p_8, \dots, p_{11}$ .

|               |                        | -1 | 2 | 3 | 7 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_8$ | $p_9$ | $p_{10}$ | $p_{11}$ |
|---------------|------------------------|----|---|---|---|-------|-------|-------|-------|-------|-------|----------|----------|
| $f_1^{E'}$    | $(2, e_1)$             | 1  | 0 | 1 | 1 | 1     | 1     | 0     | 1     | 1     | 1     | 1        | 0        |
| $f_2^{E'}$    | $(2, e_2)$             | 0  | 1 | 0 | 0 | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| $f_3^{E'}$    | $(7, \chi_7 + v_7)$    | 1  | 0 | 1 | 1 | 1     | 0     | 0     | 0     | 0     | 1     | 1        | 1        |
| $f_4^{E'}$    | $(\infty, \text{sgn})$ | 1  | 0 | 0 | 0 | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| $r_0^{E'}(0)$ | $p_0$                  | 1  | 1 | 1 | 0 | 1     | 0     | 1     | 0     | 1     | 1     | 1        | 1        |
| $r_1^{E'}(0)$ | $p_1$                  | 1  | 1 | 0 | 1 | 1     | 1     | 1     | 0     | 0     | 0     | 1        | 0        |
| $r_2^{E'}(0)$ | $p_2$                  | 0  | 1 | 0 | 0 | 1     | 1     | 0     | 0     | 0     | 1     | 0        | 1        |
| $r_3^{E'}(0)$ | $p_3$                  | 1  | 1 | 1 | 1 | 1     | 1     | 0     | 1     | 0     | 0     | 0        | 1        |
| $r_4^{E'}(0)$ | $p_4$                  | 0  | 1 | 1 | 0 | 1     | 0     | 0     | 1     | 1     | 0     | 1        | 0        |
| $r_5^{E'}(0)$ | $p_5$                  | 0  | 0 | 1 | 1 | 1     | 0     | 1     | 1     | 1     | 1     | 0        | 1        |
| $r_6^{E'}(0)$ | $p_6$                  | 1  | 0 | 0 | 0 | 1     | 1     | 1     | 1     | 0     | 0     | 0        | 0        |
| $r_7^{E'}(0)$ | $p_7$                  | 0  | 0 | 1 | 0 | 0     | 1     | 0     | 1     | 0     | 0     | 0        | 0        |

**Lemma 7.7** (Rank of the matrices). *The matrices  $\mathbf{M}_E(0)$  and  $\mathbf{M}_{E'}(0)$  of Tables 7.13 and 7.14 have rank 8. Moreover,*

$$u_E = f_1^E + r_1^E(0) + r_8^E(0), \quad u_{E'} = f_3^{E'} + r_1^{E'}(0) + r_4^{E'}(0). \quad (7.17)$$

Each of these two sums contains exactly two moving rows.

*Proof.* The two sums are computed directly from Tables 7.13 and 7.14:

| rows of $\mathbf{M}_E(0)$ |    |   |   |   |       |       |       |       |       |       |       |       |
|---------------------------|----|---|---|---|-------|-------|-------|-------|-------|-------|-------|-------|
|                           | -1 | 2 | 3 | 7 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $p_7$ |
| $f_1^E$                   | 0  | 1 | 0 | 0 | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     |
| $r_1^E(0)$                | 1  | 1 | 0 | 1 | 1     | 0     | 1     | 0     | 0     | 0     | 0     | 1     |
| $r_8^E(0)$                | 1  | 0 | 0 | 1 | 0     | 1     | 0     | 1     | 1     | 1     | 1     | 0     |
| sum                       | 0  | 0 | 0 | 0 | 1     | 1     | 1     | 1     | 1     | 1     | 1     | 1     |

| rows of $\mathbf{M}_{E'}(0)$ |    |   |   |   |       |       |       |       |       |       |          |          |
|------------------------------|----|---|---|---|-------|-------|-------|-------|-------|-------|----------|----------|
|                              | -1 | 2 | 3 | 7 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_8$ | $p_9$ | $p_{10}$ | $p_{11}$ |
| $f_3^{E'}$                   | 1  | 0 | 1 | 1 | 1     | 0     | 0     | 0     | 0     | 1     | 1        | 1        |
| $r_1^{E'}(0)$                | 1  | 1 | 0 | 1 | 1     | 1     | 1     | 0     | 0     | 0     | 1        | 0        |
| $r_4^{E'}(0)$                | 0  | 1 | 1 | 0 | 1     | 0     | 0     | 1     | 1     | 0     | 1        | 0        |
| sum                          | 0  | 0 | 0 | 0 | 1     | 1     | 1     | 1     | 1     | 1     | 1        | 1        |

To bound the ranks from below, we exhibit an  $8 \times 8$  submatrix of each matrix that becomes lower triangular with ones on the diagonal after reordering its rows and columns. In  $\mathbf{M}_E(0)$ , take the rows  $f_1^E, f_3^E, f_4^E, r_0^E(0), r_2^E(0), f_2^E, r_{10}^E(0), r_8^E(0)$  and the columns 2, 3,  $p_0, p_2, p_1, p_7, p_3, 7$ , in these orders. In  $\mathbf{M}_{E'}(0)$ , take the rows  $f_2^{E'}, f_4^{E'}, r_6^{E'}(0), r_1^{E'}(0), r_7^{E'}(0), r_4^{E'}(0), f_1^{E'}, f_3^{E'}$  and the columns 2, -1,  $p_2, 7, 3, p_8, p_9, p_{11}$ , in these orders. Reading the entries off Tables 7.13 and 7.14, we find the two submatrices

|               | 2 | 3 | $p_0$ | $p_2$ | $p_1$ | $p_7$ | $p_3$ | 7 |
|---------------|---|---|-------|-------|-------|-------|-------|---|
| $f_1^E$       | 1 | 0 | 0     | 0     | 0     | 0     | 0     | 0 |
| $f_3^E$       | 0 | 1 | 0     | 0     | 0     | 0     | 0     | 0 |
| $f_4^E$       | 0 | 1 | 1     | 0     | 0     | 0     | 0     | 0 |
| $r_0^E(0)$    | 1 | 1 | 0     | 1     | 0     | 0     | 0     | 0 |
| $r_2^E(0)$    | 1 | 0 | 1     | 0     | 1     | 0     | 0     | 0 |
| $f_2^E$       | 1 | 0 | 0     | 0     | 1     | 1     | 0     | 0 |
| $r_{10}^E(0)$ | 0 | 0 | 0     | 0     | 0     | 0     | 1     | 0 |
| $r_8^E(0)$    | 0 | 0 | 0     | 0     | 1     | 0     | 1     | 1 |

|               | 2 | -1 | $p_2$ | 7 | 3 | $p_8$ | $p_9$ | $p_{11}$ |
|---------------|---|----|-------|---|---|-------|-------|----------|
| $f_2^{E'}$    | 1 | 0  | 0     | 0 | 0 | 0     | 0     | 0        |
| $f_4^{E'}$    | 0 | 1  | 0     | 0 | 0 | 0     | 0     | 0        |
| $r_6^{E'}(0)$ | 0 | 1  | 1     | 0 | 0 | 0     | 0     | 0        |
| $r_1^{E'}(0)$ | 1 | 1  | 1     | 1 | 0 | 0     | 0     | 0        |
| $r_7^{E'}(0)$ | 0 | 0  | 0     | 0 | 1 | 0     | 0     | 0        |
| $r_4^{E'}(0)$ | 1 | 0  | 0     | 0 | 1 | 1     | 0     | 0        |
| $f_1^{E'}$    | 0 | 1  | 0     | 1 | 1 | 1     | 1     | 0        |
| $f_3^{E'}$    | 0 | 1  | 0     | 1 | 1 | 0     | 1     | 1        |

Both are lower triangular with ones on the diagonal, and they have determinant 1 over  $\mathbb{F}_2$ . This implies that both matrices have rank at least 8.

To bound the ranks from above, consider the coordinate vectors of the four classes of Lemma 7.2 in the bases (7.7):

|                 | -1 | 2 | 3 | 7 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $p_7$ |
|-----------------|----|---|---|---|-------|-------|-------|-------|-------|-------|-------|-------|
| $\delta_E(T)$   | 1  | 0 | 0 | 0 | 1     | 1     | 1     | 1     | 1     | 1     | 1     | 1     |
| $\delta_E(P_1)$ | 0  | 0 | 0 | 1 | 0     | 0     | 0     | 0     | 1     | 1     | 1     | 1     |
| $\delta_E(P_2)$ | 1  | 0 | 0 | 0 | 0     | 1     | 1     | 0     | 1     | 1     | 0     | 0     |
| $\delta_E(P_3)$ | 1  | 0 | 0 | 1 | 0     | 1     | 0     | 1     | 1     | 0     | 1     | 0     |

  

|                    | -1 | 2 | 3 | 7 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_8$ | $p_9$ | $p_{10}$ | $p_{11}$ |
|--------------------|----|---|---|---|-------|-------|-------|-------|-------|-------|----------|----------|
| $\delta_{E'}(T')$  | 0  | 0 | 0 | 0 | 1     | 1     | 1     | 1     | 1     | 1     | 1        | 1        |
| $\delta_{E'}(Q_1)$ | 0  | 0 | 0 | 1 | 1     | 1     | 1     | 1     | 0     | 0     | 0        | 0        |
| $\delta_{E'}(Q_2)$ | 0  | 0 | 1 | 0 | 1     | 0     | 0     | 1     | 0     | 0     | 1        | 1        |
| $\delta_{E'}(Q_3)$ | 0  | 0 | 0 | 0 | 1     | 0     | 1     | 0     | 1     | 0     | 0        | 1        |

We check directly that each of these vectors has zero dot product with every row of the corresponding matrix in Tables 7.13 and 7.14. The four vectors on each side are independent by Lemma 7.2. This implies that the kernel of each matrix has dimension at least 4, and each rank is at most  $12 - 4 = 8$ . This completes the proof.  $\square$

Since every moving support in Table 7.4 has four or eight elements, each class vector also has zero dot product with  $u_\star$ , and hence with every row of  $\mathbf{M}_\star(1)$ . Together with Lemmas 4.17 and 7.7, this shows that the kernel of  $\mathbf{M}_\star(\eta)$  is spanned by the four class vectors for both values of  $\eta$ . The proof of Theorem 7.8 does not need this, but it is a useful check on the tables: an error in an entry of a row would typically make one of these dot products nonzero.

## 7.7 Exact rank and infinitude

**Theorem 7.8** (Exact rank six). *Let  $(M, N) \in \mathcal{P}_6 \cap \mathcal{K}_6$  be a prime specialization of  $\mathfrak{D}_6$  with respect to the set  $S$  of (7.6). Then  $\text{rank } E_{M,N}(\mathbb{Q}) = 6$ . Moreover, there exist infinitely many such  $(M, N)$ , and the curves  $E_{M,N}$  obtained from them represent infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes.*

*Proof.* We prove the rank statement with Proposition 4.18, and then the infinitude statements with Proposition 5.5.

**The rank.** Let  $\mathcal{P}$  be the set of prime specializations of  $\mathfrak{D}_6$  that lie in  $\mathcal{P}_6 \cap \mathcal{K}_6$ . We apply Proposition 4.18 to the datum  $\mathfrak{D}_6$ , the set  $S$  of (7.6) and the set  $\mathcal{P}$ , with  $n_E = n_{E'} = 12$  and  $k_E = k_{E'} = 4$ . The lists  $\Gamma_E = \Gamma_{E'} = (-1, 2, 3, 7)$  consist of  $-1$  and distinct primes, including every prime dividing  $\kappa_E = -2^8 7^2$  and  $\kappa_{E'} = 2^8 3^6 7^2$ . We check the four hypotheses.

- (i) *Fixed rows.* Let  $f_1^E, \dots, f_4^E$  and  $f_1^{E'}, \dots, f_4^{E'}$  be the first four rows of Tables 7.13 and 7.14. By Lemma 7.5 and the discussion of the fixed rows after it, at every  $(M, N) \in \mathcal{P}$  each of them is the row defined, in the sense of Definition 3.9, by a place  $v \in \{2, 3, 7, \infty\}$ , the subgroup  $U_v$  of Lemma 7.5, and one of the listed linear maps.
- (ii) *Constant characters.* By Lemma 7.6, the bits  $\lambda_i(g)$  with  $g \in \{-1, 2, 3, 7\}$  and  $\gamma_{ij}$  are the same at every  $(M, N) \in \mathcal{P}$ , and so are  $\lambda_i(\kappa_E) = \sigma_i$  and  $\lambda_i(\kappa_{E'}) = 0$ . In other words, the bits (4.34) are constant on  $\mathcal{P}$ , and the matrices  $\mathbf{M}_E(0)$  and  $\mathbf{M}_{E'}(0)$  of (4.35) are those of Tables 7.13 and 7.14.
- (iii) *Points.* By Lemmas 7.1 and 7.2, at every  $(M, N) \in \mathcal{P}$  the image  $\delta_E(E(\mathbb{Q}))$  contains the four independent classes of  $T, P_1, P_2, P_3$ , and  $\delta_{E'}(E'(\mathbb{Q}))$  contains the four independent classes of  $T', Q_1, Q_2, Q_3$ .
- (iv) *Rank.* By Lemma 7.7,  $\text{rank } \mathbf{M}_E(0) = \text{rank } \mathbf{M}_{E'}(0) = 8 = 12 - 4$ , and  $u_E$  and  $u_{E'}$  are sums of rows of  $\mathbf{M}_E(0)$  and  $\mathbf{M}_{E'}(0)$ , respectively, in each of which exactly two moving rows occur.

By Proposition 4.18, every  $(M, N) \in \mathcal{P}$  has  $d_E = d_{E'} = 4$  and  $\text{rank } E_{M,N}(\mathbb{Q}) = 4 + 4 - 2 = 6$ . The last statement of Proposition 4.18 also shows that  $\delta_E(E(\mathbb{Q}))$  and  $\delta_{E'}(E'(\mathbb{Q}))$  are spanned by the four classes of Table 7.4 on the respective sides.

**Infinitude.** We check the hypotheses of Proposition 5.5 for  $W$ , the pair  $(M_0, N_0)$  of (7.12), and the cone  $\mathcal{K}_6$ . For (a), the primes dividing  $c_0 c_1 \cdots c_{11}$  are 2 and 3, which divide  $W$ . Every  $c_i$  divides  $2^3 \cdot 3^3$ , while  $v_2(W) = 6$  and  $v_3(W) = 4$ , and we have  $v_q(W) > v_q(c_i)$  for  $q = 2, 3$ ; for the other primes  $q \mid W$ , we have  $v_q(c_i) = 0 < 1 = v_q(W)$ . Applying Lemma 7.3 to  $(M_0, N_0) \in \mathcal{P}_6$ , we find that  $c_i \mid L_i(M_0, N_0)$  and that  $L_i(M_0, N_0)/c_i$  is prime to  $W$ . Hypothesis (b) is empty, because every prime  $q \leq 11$  divides  $W$ . Hypothesis (c) is Lemma 7.4. By Proposition 5.5, there exist infinitely many prime specializations  $(M, N) \in \mathcal{K}_6$  with  $M \equiv M_0$  and  $N \equiv N_0 \pmod{W}$ , that is, infinitely many elements of  $\mathcal{P}$ , and their  $j$ -invariants  $j(E_{M,N})$  take infinitely many values. Each of these curves has rank six by the first part. Curves with distinct  $j$ -invariants are not isomorphic over  $\overline{\mathbb{Q}}$  (Remark 5.7). This completes the proof.  $\square$

*Remark 7.9.* By Remark 4.4, we have  $j(E_{M,N}) = (16/9)(25F + 12H)^3 / (H^2 J)$ ; here  $A^2 F + 3BH = 196(25F + 12H)$  and  $B^2 C = 144 \cdot 196^3$ . The primes of  $S$  that do not divide  $W$  are 13, 19 and 41; Proposition 5.5 needs no check at them. For comparison with Lemma 5.4, the twelve forms define 8 distinct lines through the origin in  $\mathbb{F}_{13}^2$  (the zero lines of the pairs  $\{0, 3\}$ ,  $\{1, 2\}$ ,  $\{8, 11\}$ ,  $\{9, 10\}$  coincide), 10 in  $\mathbb{F}_{19}^2$  (the pairs  $\{4, 5\}$ ,  $\{6, 7\}$ ), and 10 in  $\mathbb{F}_{41}^2$  (the pairs  $\{8, 9\}$ ,  $\{10, 11\}$ ). At every other prime not dividing  $W$ , they define 12 distinct lines.

## The rank-seven family

In this section we prove Theorem 8.9, the case  $r = 7$  of Theorem 1.1. It concerns the twelve-form datum  $\mathfrak{D}_7$  of Section 8.1, the progression  $\mathcal{P}_7$  modulo  $W = 308403583488$  of Section 8.3, and the cone  $\mathcal{K}_7 = \{(M, N) \in \mathbb{R}^2 : N > 0, 2999N < M < 3001N\}$ . Theorem 8.9 states that, for every prime specialization  $(M, N) \in \mathcal{P}_7 \cap \mathcal{K}_7$  of  $\mathfrak{D}_7$ , the curve  $E_{M,N}$  has rank exactly seven, and that these curves represent infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes. It is used, together with Theorems 6.7 and 7.8, in Section 9.

The proof follows the scheme of Part I, and this section supplies the data of the family and checks hypotheses. In Sections 8.1 and 8.2 we define the datum and exhibit four rational points on  $E$  and three on  $E'$ . Together with the points of order two, their classes show that  $d_E \geq 5$  and  $d_{E'} \geq 4$  (Lemma 8.3). In Section 8.3 we show that the residues of the prime values  $p_i$  are constant on  $\mathcal{P}_7$  (Lemma 8.4). The local computations are Lemma 8.6, at the fixed places 2, 3, 7, 13 and  $\infty$ , and Lemma 8.7, at the moving primes. In Section 8.6 we display the matrices  $\mathbf{M}_E(0)$  and  $\mathbf{M}_{E'}(0)$  and prove that their ranks are  $8 = 13 - 5$  and  $9 = 13 - 4$  (Lemma 8.8). Finally, in Section 8.7 we check the hypotheses of Propositions 4.18 and 5.5 and prove Theorem 8.9. From Section 3 we use Lemmas 3.1, 3.2, 3.7, 3.10, and 3.12, and from Section 4 we use Lemmas 4.2, 4.3, 4.7 to 4.9, 4.11 to 4.13, and 4.17 and Corollary 4.14.

The family comes from a conic base change of a 2-isogeny pair of the same split-factor form as the rank-four pair of Zywina [55, §6.5]. Appendix B.3 explains this.

**Notation.** In this section,  $A = 91205$ ,  $B = 33124 = 182^2$  and  $C = 9$ . For  $(M, N) \in \mathbb{Z}^2$  with  $FHJ \neq 0$ , we write  $E = E_{M,N}$  and  $E' = E'_{M,N}$ . We set

$$\alpha = AF, \quad \beta = -BFH, \quad \alpha' = -2AF, \quad \beta' = CFJ,$$

so that  $E = E_{\alpha,\beta}$  and  $E' = E_{\alpha',\beta'}$ . Let  $T = (0,0)$  on  $E$  and  $T' = (0,0)$  on  $E'$ , and let  $\delta_{E,v}$  and  $\delta_{E',v}$  be the descent maps over  $\mathbb{Q}_v$ . At a prime specialization,  $p_i = L_i(M, N)/c_i$ , and  $\lambda_i$  is the additive Legendre symbol at  $p_i$ , defined by  $(z/p_i) = (-1)^{\lambda_i(z)}$ . As in Section 4, the fixed rows of  $\mathbf{M}_E(\eta)$  and  $\mathbf{M}_{E'}(\eta)$  are denoted  $f_k^E$  and  $f_k^{E'}$ , and their moving rows are denoted  $r_i^E$  ( $i \in I_F \cup I_J$ ) and  $r_i^{E'}$  ( $i \in I_F \cup I_H$ ).

### 8.1 The datum

The coefficients of the twelve forms  $L_i = a_iM + b_iN$  and the cofactors  $c_i$  are listed in Table 8.1. The index sets are  $I_F = \{0, 1, 2, 3\}$ ,  $I_H = \{4, 5, 6, 7\}$  and  $I_J = \{8, 9, 10, 11\}$ , and we have  $L_0 = M$  and  $L_1 = N$ .

Table 8.1. The forms  $L_i = a_iM + b_iN$  of  $\mathfrak{D}_7$ , their groups, and the cofactors  $c_i$ .

| $i$ | group | $a_i$ | $b_i$ | $c_i$ | $i$ | group | $a_i$ | $b_i$  | $c_i$ |
|-----|-------|-------|-------|-------|-----|-------|-------|--------|-------|
| 0   | $F$   | 1     | 0     | 18    | 6   | $H$   | 2     | -5589  | 9     |
| 1   | $F$   | 0     | 1     | 1     | 7   | $H$   | 8     | 425    | 1     |
| 2   | $F$   | 1     | -182  | 64    | 8   | $J$   | 13    | 2688   | 6     |
| 3   | $F$   | 182   | 10557 | 9     | 9   | $J$   | 325   | 49266  | 1728  |
| 4   | $H$   | 9     | 34    | 8     | 10  | $J$   | 14    | -975   | 3     |
| 5   | $H$   | 25    | -4968 | 18    | 11  | $J$   | 896   | -45747 | 9     |

Expanding the products of the four forms in each group, we find

$$\begin{aligned}
 F &= 182M^3N - 22567M^2N^2 - 1921374MN^3, \\
 H &= 3600M^4 - 10570742M^3N + 1386724327M^2N^2 \\
 &\quad + 111595323294MN^3 + 401220896400N^4, \\
 J &= 52998400M^4 + 12595448502M^3N - 442758190887M^2N^2 \\
 &\quad - 132970149835614MN^3 + 5906684876601600N^4.
 \end{aligned} \tag{8.1}$$

Comparing the five coefficients of each side, we obtain the identity

$$91205^2F + 4 \cdot 33124H = 9J, \tag{8.2}$$

that is,  $A^2F + 4BH = CJ$ . For instance, since  $F$  has no  $M^4$  term, the coefficients of  $M^4$  give  $4 \cdot 33124 \cdot 3600 = 476985600 = 9 \cdot 52998400$ . The two curves are

$$\begin{aligned}
 E_{M,N} : \quad y^2 &= x^3 + 91205Fx^2 - 33124FHx, \\
 E'_{M,N} : \quad y^2 &= x^3 - 182410Fx^2 + 9FJx.
 \end{aligned} \tag{8.3}$$

**Lemma 8.1** (The datum). *The forms and cofactors of Table 8.1, the constants  $A = 91205$ ,  $B = 33124$  and  $C = 9$ , and the lists  $\Gamma_E = \Gamma_{E'} = (-1, 2, 3, 7, 13)$  form a twelve-form datum  $\mathfrak{D}_7$ . The set*

$$S = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 37, 41, 47, 59, 61, 109, 241, 409\} \tag{8.4}$$

*satisfies the requirement of Definition 4.6.*

*Proof.* We check the conditions of Definition 4.1. We have  $(a_0, b_0) = (1, 0)$  and  $b_i \neq 0$  for  $i \geq 1$ . The 66 determinants  $\Delta_{ij} = a_i b_j - a_j b_i$  with  $i < j$  are listed, factored, in Table 8.2; none of them vanishes. Each pair  $(a_i, b_i)$  is primitive. Indeed,  $(a_0, b_0) = (1, 0)$  and  $(a_1, b_1) = (0, 1)$ ; for  $i \geq 2$  the coefficients  $a_i$  are

$$1, 2 \cdot 7 \cdot 13, 3^2, 5^2, 2, 2^3, 13, 5^2 \cdot 13, 2 \cdot 7, 2^7 \cdot 7,$$

the coefficients  $b_i = \Delta_{0i}$  are factored in the first eleven entries of Table 8.2, and for each  $i$  the two factorizations have no prime in common. The identity  $A^2 F + 4BH = CJ$  is (8.2), the cofactors are positive with  $c_1 = 1$ , and  $\Gamma_E$  and  $\Gamma_{E'}$  consist of  $-1$  and distinct primes.

Table 8.2 shows that the primes dividing some  $b_i$  with  $i \geq 1$  or some  $\Delta_{ij}$  with  $i < j$  are exactly the elements of  $S$ . The other primes that Definition 4.6 requires also lie in  $S$ : we have  $6ABC = 2 \cdot 3 \cdot (5 \cdot 17 \cdot 29 \cdot 37) \cdot (2^2 \cdot 7^2 \cdot 13^2) \cdot 3^2$ , every  $c_i$  is of the form  $2^a 3^b$ , and the primes in  $\Gamma_E \cup \Gamma_{E'}$  are 2, 3, 7 and 13.  $\square$

Table 8.2. The determinants  $\Delta_{ij} = a_i b_j - a_j b_i$  for  $i < j$ , factored. Since  $(a_0, b_0) = (1, 0)$ , the first eleven entries are  $\Delta_{0j} = b_j$ .

| $(i, j)$ $\Delta_{ij}$                           | $(i, j)$ $\Delta_{ij}$                                        | $(i, j)$ $\Delta_{ij}$                                |
|--------------------------------------------------|---------------------------------------------------------------|-------------------------------------------------------|
| $(0, 1)$ 1                                       | $(2, 4)$ $2^3 \cdot 11 \cdot 19$                              | $(4, 11)$ $-17 \cdot 19 \cdot 37^2$                   |
| $(0, 2)$ $-2 \cdot 7 \cdot 13$                   | $(2, 5)$ $-2 \cdot 11 \cdot 19$                               | $(5, 6)$ $-3^3 \cdot 11 \cdot 19 \cdot 23$            |
| $(0, 3)$ $3^3 \cdot 17 \cdot 23$                 | $(2, 6)$ $-5^2 \cdot 11 \cdot 19$                             | $(5, 7)$ $11 \cdot 19 \cdot 241$                      |
| $(0, 4)$ $2 \cdot 17$                            | $(2, 7)$ $3^2 \cdot 11 \cdot 19$                              | $(5, 8)$ $2^3 \cdot 3 \cdot 17^2 \cdot 19$            |
| $(0, 5)$ $-2^3 \cdot 3^3 \cdot 23$               | $(2, 8)$ $2 \cdot 7 \cdot 19^2$                               | $(5, 9)$ $2 \cdot 3^2 \cdot 5^4 \cdot 11 \cdot 23$    |
| $(0, 6)$ $-3^5 \cdot 23$                         | $(2, 9)$ $2^7 \cdot 7 \cdot 11^2$                             | $(5, 10)$ $3 \cdot 11 \cdot 37^2$                     |
| $(0, 7)$ $5^2 \cdot 17$                          | $(2, 10)$ $11^2 \cdot 13$                                     | $(5, 11)$ $3^2 \cdot 19 \cdot 23 \cdot 29^2$          |
| $(0, 8)$ $2^7 \cdot 3 \cdot 7$                   | $(2, 11)$ $5^2 \cdot 13 \cdot 19^2$                           | $(6, 7)$ $2 \cdot 11 \cdot 19 \cdot 109$              |
| $(0, 9)$ $2 \cdot 3^2 \cdot 7 \cdot 17 \cdot 23$ | $(3, 4)$ $-5^2 \cdot 11 \cdot 17 \cdot 19$                    | $(6, 8)$ $3 \cdot 19 \cdot 37^2$                      |
| $(0, 10)$ $-3 \cdot 5^2 \cdot 13$                | $(3, 5)$ $-3^5 \cdot 11 \cdot 19 \cdot 23$                    | $(6, 9)$ $3^2 \cdot 11 \cdot 23 \cdot 29^2$           |
| $(0, 11)$ $-3^2 \cdot 13 \cdot 17 \cdot 23$      | $(3, 6)$ $-2^3 \cdot 3^3 \cdot 11 \cdot 19 \cdot 23$          | $(6, 10)$ $2^3 \cdot 3 \cdot 11 \cdot 17^2$           |
| $(1, 2)$ $-1$                                    | $(3, 7)$ $-2 \cdot 11 \cdot 17 \cdot 19$                      | $(6, 11)$ $2 \cdot 3^2 \cdot 5^4 \cdot 19 \cdot 23$   |
| $(1, 3)$ $-2 \cdot 7 \cdot 13$                   | $(3, 8)$ $3 \cdot 5^2 \cdot 13 \cdot 19^2$                    | $(7, 8)$ $19 \cdot 29^2$                              |
| $(1, 4)$ $-3^2$                                  | $(3, 9)$ $3^2 \cdot 11^2 \cdot 13 \cdot 17 \cdot 23$          | $(7, 9)$ $11 \cdot 17 \cdot 37^2$                     |
| $(1, 5)$ $-5^2$                                  | $(3, 10)$ $-2^7 \cdot 3 \cdot 7 \cdot 11^2$                   | $(7, 10)$ $-2 \cdot 5^4 \cdot 11$                     |
| $(1, 6)$ $-2$                                    | $(3, 11)$ $-2 \cdot 3^2 \cdot 7 \cdot 17 \cdot 19^2 \cdot 23$ | $(7, 11)$ $-2^3 \cdot 17^3 \cdot 19$                  |
| $(1, 7)$ $-2^3$                                  | $(4, 5)$ $-2 \cdot 11 \cdot 19 \cdot 109$                     | $(8, 9)$ $-2 \cdot 3 \cdot 7^2 \cdot 13 \cdot 61$     |
| $(1, 8)$ $-13$                                   | $(4, 6)$ $-11 \cdot 19 \cdot 241$                             | $(8, 10)$ $-3 \cdot 41 \cdot 409$                     |
| $(1, 9)$ $-5^2 \cdot 13$                         | $(4, 7)$ $11 \cdot 17 \cdot 19$                               | $(8, 11)$ $-3 \cdot 19^2 \cdot 47 \cdot 59$           |
| $(1, 10)$ $-2 \cdot 7$                           | $(4, 8)$ $2 \cdot 5^4 \cdot 19$                               | $(9, 10)$ $-3 \cdot 11^2 \cdot 47 \cdot 59$           |
| $(1, 11)$ $-2^7 \cdot 7$                         | $(4, 9)$ $2^3 \cdot 11 \cdot 17^3$                            | $(9, 11)$ $-3^2 \cdot 17 \cdot 23 \cdot 41 \cdot 409$ |
| $(2, 3)$ $11^2 \cdot 19^2$                       | $(4, 10)$ $-11 \cdot 29^2$                                    | $(10, 11)$ $2 \cdot 3 \cdot 7^2 \cdot 13 \cdot 61$    |

Lemma 4.2 implies that  $\beta' = \alpha^2 - 4\beta$ , that the curves (8.3) are nonsingular exactly when  $FHJ \neq 0$ , that  $E'_{M,N}$  is the curve 2-isogenous to  $E_{M,N}$  of Section 3, and that replacing  $(M, N)$  by  $(\lambda M, \lambda N)$  with  $\lambda \in \mathbb{Q}^\times$  gives  $\mathbb{Q}$ -isomorphic curves.

At a prime specialization, the ambient bases of Section 4 are

$$\mathcal{B}_E = (-1, 2, 3, 7, 13, p_0, p_1, \dots, p_7), \quad \mathcal{B}_{E'} = (-1, 2, 3, 7, 13, p_0, p_1, p_2, p_3, p_8, p_9, p_{10}, p_{11}),$$

so  $n_E = n_{E'} = 13$ . The products of the cofactors over the three groups are

$$\prod_{i \in I_F} c_i = 2^7 3^4 = 2 \cdot 72^2, \quad \prod_{i \in I_H} c_i = 2^4 3^4 = 36^2, \quad \prod_{i \in I_J} c_i = 2^7 3^7 = 6 \cdot 216^2. \quad (8.5)$$

With these products, the constants of (4.18) are

$$\kappa_E = -B \prod_{j \in G_E} c_j = -2^{13} 3^{87} 2^{13} 13^2, \quad \kappa_{E'} = C \prod_{j \in G_{E'}} c_j = 2^{14} 3^{13}, \quad (8.6)$$

with squareclasses  $[\kappa_E] = [-2]$  and  $[\kappa_{E'}] = [3]$ . The list  $\Gamma_E$  contains  $-1$  and the primes  $2, 3, 7, 13$  dividing  $\kappa_E$ , and  $\Gamma_{E'}$  contains  $-1$  and the primes  $2, 3$  dividing  $\kappa_{E'}$ , as Lemma 4.8 requires. The entries  $7$  and  $13$  of  $\Gamma_{E'}$  are not needed there. We keep them so that both bases have the same constant part; the conditions at  $7$  and  $13$  in Lemma 8.6 force their exponents to vanish.

## 8.2 Rational points and the lower bound

We define the binary quadratic forms

$$\begin{aligned} D_0 &= M^2 + 10557N^2, & D_1 &= 175M^2 + 10738MN + 2470338N^2, \\ D_2 &= 364M^2 + 36639MN - 2825550N^2, & D_3 &= 728M^2 - 592647MN + 28820610N^2, \\ V_1 &= 49M^2 - 43862MN - 2026944N^2, & V_2 &= 2912M^2 + 2544237MN - 432309150N^2, \end{aligned} \quad (8.7)$$

and we abbreviate products of the forms  $L_i$  by their indices, so that  $L_{0,2,6,7} = L_0 L_2 L_6 L_7$ , for example.

**Lemma 8.2** (Rational points). *Let  $(M, N) \in \mathbb{Z}^2$  with  $FHJ \neq 0$ . Then the points  $P_1, \dots, P_4$  of Table 8.3 lie on  $E$ , and the points  $Q_1, Q_2, Q_3$  lie on  $E'$ .*

*Proof.* Every  $L_i(M, N)$  is nonzero because  $FHJ \neq 0$ , and each abscissa  $x$  in Table 8.3 is nonzero. For  $y = xr$  with  $x \neq 0$ , the equation  $y^2 = x^3 + \alpha x^2 + \beta x$  is equivalent to

$$r^2 = x + \alpha + \beta/x, \quad (8.8)$$

and similarly on  $E'$  with  $\alpha', \beta'$  in place of  $\alpha, \beta$ . For each of the seven points,  $\beta/x$  (respectively  $\beta'/x$ ) is a constant times the product of the four forms of  $FH$  (respectively  $FJ$ ) that do not occur in  $x$ ; for  $P_1$  and  $Q_1$ , it is a constant times  $H$  and  $J$ , respectively. Multiplying

Table 8.3. Rational points on  $E = E_{M,N}$  and  $E' = E'_{M,N}$ . The ordinate is the product of the third and fourth columns. The last column is the factor by which (8.8) is multiplied to obtain (8.9).

| curve | point | $x$                    | $y/x$           | multiplier    |
|-------|-------|------------------------|-----------------|---------------|
| $E$   | $P_1$ | $-58081F$              | $10920 D_0/241$ | $58081/33124$ |
| $E$   | $P_2$ | $(1225/9)L_{0,2,6,7}$  | $4D_1/15$       | $225$         |
| $E$   | $P_3$ | $-2275L_{1,2,5,6}$     | $-6D_2/5$       | $25$          |
| $E$   | $P_4$ | $(182/361)L_{2,3,6,7}$ | $D_3/19$        | $361$         |
| $E'$  | $Q_1$ | $3481F$                | $21840 D_0/59$  | $3481$        |
| $E'$  | $Q_2$ | $(49/64)L_{0,2,8,9}$   | $65V_1/56$      | $3136$        |
| $E'$  | $Q_3$ | $(16/225)L_{0,3,8,10}$ | $V_2/60$        | $3600$        |

(8.8) by the factor in the last column of Table 8.3, we find that the seven assertions are equivalent to the identities

$$\begin{aligned}
3600 D_0^2 &= 58081F + H & (P_1), \\
16 D_1^2 &= 30625L_{0,2,6,7} + 20521125F - 54756L_{1,3,4,5} & (P_2), \\
36 D_2^2 &= -56875L_{1,2,5,6} + 2280125F + 364L_{0,3,4,7} & (P_3), \\
D_3^2 &= 182L_{2,3,6,7} + 32925005F - 23718422L_{0,1,4,5} & (P_4), \\
476985600 D_0^2 &= -622851849F + 9J & (Q_1), \\
4225 V_1^2 &= 2401L_{0,2,8,9} - 572037760F + 36864L_{1,3,10,11} & (Q_2), \\
V_2^2 &= 256L_{0,3,8,10} - 656676000F + 455625L_{1,2,9,11} & (Q_3).
\end{aligned} \tag{8.9}$$

For example, for  $P_1$  we have  $x + \alpha = (91205 - 58081)F = 33124F$  and  $\beta/x = 33124H/58081$ . Using  $10920 = 60 \cdot 182$  and  $58081 = 241^2$ , and multiplying (8.8) by  $58081/33124$ , we obtain the first line of (8.9). Each line of (8.9) is an equality of binary quartic forms. It holds if and only if the coefficients of  $M^4, M^3N, M^2N^2, MN^3, N^4$  on the two sides agree. We list these common coefficients in Table 8.4, and expanding both sides of each line confirms them. The program of Appendix A checks the seven point equations by exact coefficient arithmetic.  $\square$

Together with  $T$  and  $T'$ , these points give five classes in  $\delta_E(E(\mathbb{Q}))$  and four in  $\delta_{E'}(E'(\mathbb{Q}))$ . At a prime specialization, Table 8.5 expresses them in terms of the primes  $p_i$ . Each entry follows from  $L_i = c_i p_i$  and (8.5): the abscissa of the point (for  $T$  and  $T'$ , the coefficient  $\beta$  or  $\beta'$ ) equals  $sh^2 \prod_{i \in I} p_i$  with the listed  $s$ ,  $I$  and  $h$ . For example,  $c_2 c_3 c_6 c_7 = 64 \cdot 9 \cdot 9 \cdot 1 = 72^2$ , so that  $x(P_4) = 182 (72/19)^2 p_2 p_3 p_6 p_7$ , and  $\beta = -182^2 \cdot 2^{11} 3^8 p_0 \cdots p_7 = -2 (182 \cdot 2^5 3^4)^2 p_0 \cdots p_7$ .

Table 8.4. The coefficients of both sides of each identity in (8.9).

|       | $M^4$     | $M^3N$       | $M^2N^2$       | $MN^3$            | $N^4$              |
|-------|-----------|--------------|----------------|-------------------|--------------------|
| $P_1$ | 3600      | 0            | 76010400       | 0                 | 401220896400       |
| $P_2$ | 490000    | 60132800     | 15678767104    | 848847662208      | 97641117347904     |
| $P_3$ | 4769856   | 960234912    | -25725026844   | -7453823504400    | 287414380890000    |
| $P_4$ | 529984    | -862894032   | 393193274769   | -34160896109340   | 830627560772100    |
| $Q_1$ | 476985600 | 0            | 10071073958400 | 0                 | 53160163889414400  |
| $Q_2$ | 10144225  | -18161061100 | 7289115897700  | 751254159801600   | 17358420861849600  |
| $Q_3$ | 8479744   | 14817636288  | 3955373422569  | -2199793869737100 | 186891201173722500 |

Table 8.5. At a prime specialization, the class of each point is  $[s \prod_{i \in I} p_i]$ ; the abscissa (for  $T$  and  $T'$ , the coefficient  $\beta$  or  $\beta'$ ) is  $sh^2 \prod_{i \in I} p_i$ .

| curve | point | $s$  | $I$                            | $h$    |
|-------|-------|------|--------------------------------|--------|
| $E$   | $T$   | -2   | $\{0, 1, 2, 3, 4, 5, 6, 7\}$   | 471744 |
| $E$   | $P_1$ | -2   | $\{0, 1, 2, 3\}$               | 17352  |
| $E$   | $P_2$ | 2    | $\{0, 2, 6, 7\}$               | 840    |
| $E$   | $P_3$ | -182 | $\{1, 2, 5, 6\}$               | 360    |
| $E$   | $P_4$ | 182  | $\{2, 3, 6, 7\}$               | 72/19  |
| $E'$  | $T'$  | 3    | $\{0, 1, 2, 3, 8, 9, 10, 11\}$ | 93312  |
| $E'$  | $Q_1$ | 2    | $\{0, 1, 2, 3\}$               | 4248   |
| $E'$  | $Q_2$ | 1    | $\{0, 2, 8, 9\}$               | 3024   |
| $E'$  | $Q_3$ | 1    | $\{0, 3, 8, 10\}$              | 72/5   |

In the bases  $\mathcal{B}_E$  and  $\mathcal{B}_{E'}$ , these classes have the coordinate vectors of Table 8.6. The entry at  $g \in \{-1, 2, 3, 7, 13\}$  is the exponent of  $g$  in the squarefree constant  $s$ , and the entry at  $p_j$  is 1 exactly when  $j \in I$ .

Table 8.6. The coordinate vectors of the classes of Table 8.5 in the bases  $\mathcal{B}_E$  (top) and  $\mathcal{B}_{E'}$  (bottom).

|                 | -1 | 2 | 3 | 7 | 13 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $p_7$ |
|-----------------|----|---|---|---|----|-------|-------|-------|-------|-------|-------|-------|-------|
| $\delta_E(T)$   | 1  | 1 | 0 | 0 | 0  | 1     | 1     | 1     | 1     | 1     | 1     | 1     | 1     |
| $\delta_E(P_1)$ | 1  | 1 | 0 | 0 | 0  | 1     | 1     | 1     | 1     | 0     | 0     | 0     | 0     |
| $\delta_E(P_2)$ | 0  | 1 | 0 | 0 | 0  | 1     | 0     | 1     | 0     | 0     | 0     | 1     | 1     |
| $\delta_E(P_3)$ | 1  | 1 | 0 | 1 | 1  | 0     | 1     | 1     | 0     | 0     | 1     | 1     | 0     |
| $\delta_E(P_4)$ | 0  | 1 | 0 | 1 | 1  | 0     | 0     | 1     | 1     | 0     | 0     | 1     | 1     |

  

|                    | -1 | 2 | 3 | 7 | 13 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_8$ | $p_9$ | $p_{10}$ | $p_{11}$ |
|--------------------|----|---|---|---|----|-------|-------|-------|-------|-------|-------|----------|----------|
| $\delta_{E'}(T')$  | 0  | 0 | 1 | 0 | 0  | 1     | 1     | 1     | 1     | 1     | 1     | 1        | 1        |
| $\delta_{E'}(Q_1)$ | 0  | 1 | 0 | 0 | 0  | 1     | 1     | 1     | 1     | 0     | 0     | 0        | 0        |
| $\delta_{E'}(Q_2)$ | 0  | 0 | 0 | 0 | 0  | 1     | 0     | 1     | 0     | 1     | 1     | 0        | 0        |
| $\delta_{E'}(Q_3)$ | 0  | 0 | 0 | 0 | 0  | 1     | 0     | 0     | 1     | 1     | 0     | 1        | 0        |

**Lemma 8.3** (Independence of the point classes). *Let  $(M, N)$  be a prime specialization of  $\mathfrak{D}_7$ . Then the classes  $\delta_E(T), \delta_E(P_1), \dots, \delta_E(P_4)$  are independent, and the classes  $\delta_{E'}(T'), \delta_{E'}(Q_1), \delta_{E'}(Q_2), \delta_{E'}(Q_3)$  are independent. In particular,  $d_E \geq 5$  and  $d_{E'} \geq 4$ .*

*Proof.* By Lemma 4.8(f), the classes of the entries of  $\mathcal{B}_E$  are independent, and the vectors of Table 8.6 are the coordinate vectors of the five classes on  $E$ . We order the classes as  $T, P_3, P_1, P_2, P_4$  and take the columns  $p_4, p_5, p_1, p_0, p_7$ . The corresponding entries of Table 8.6 form the matrix

|       | $p_4$ | $p_5$ | $p_1$ | $p_0$ | $p_7$ |
|-------|-------|-------|-------|-------|-------|
| $T$   | 1     | 1     | 1     | 1     | 1     |
| $P_3$ | 0     | 1     | 1     | 0     | 0     |
| $P_1$ | 0     | 0     | 1     | 1     | 0     |
| $P_2$ | 0     | 0     | 0     | 1     | 1     |
| $P_4$ | 0     | 0     | 0     | 0     | 1     |

which has ones on the diagonal and zeros below it. Lemma 3.12 implies that the five classes are independent. In words, the valuation at  $p_4$  eliminates  $T$  from a relation, and then the valuations at  $p_5, p_1, p_0$  and  $p_7$  eliminate  $P_3, P_1, P_2$  and  $P_4$  in turn. On  $E'$ , we use the order  $T', Q_2, Q_3, Q_1$  and the columns  $p_{11}, p_9, p_{10}, p_1$ , for which the corresponding

matrix is

|       | $p_{11}$ | $p_9$ | $p_{10}$ | $p_1$ |
|-------|----------|-------|----------|-------|
| $T'$  | 1        | 1     | 1        | 1     |
| $Q_2$ | 0        | 1     | 0        | 0     |
| $Q_3$ | 0        | 0     | 1        | 0     |
| $Q_1$ | 0        | 0     | 0        | 1     |

and Lemma 3.12 applies in the same way.  $\square$

### 8.3 The congruence class and the real cone

We impose the congruences of Table 8.7. The moduli are pairwise coprime, and by the Chinese remainder theorem these congruences are equivalent to  $(M, N) \equiv (M_0, N_0) \pmod{W}$ , where

$$\begin{aligned} W &= 2^9 \cdot 3^4 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 308403583488, \\ M_0 &= 79151095314, \quad N_0 = 151444919819. \end{aligned} \tag{8.10}$$

We write  $\mathcal{P}_7$  for the set of  $(M, N) \in \mathbb{Z}^2$  with  $(M, N) \equiv (M_0, N_0) \pmod{W}$ . As in Section 5, we parametrize  $\mathcal{P}_7$  by  $M = M_0 + WX$  and  $N = N_0 + WY$  with  $(X, Y) \in \mathbb{Z}^2$ . We also set  $\ell_i(X, Y) = L_i(M_0 + WX, N_0 + WY)/c_i$ .

Table 8.7. The congruences defining  $\mathcal{P}_7$ .

| modulus $q^k$ | $2^9$ | $3^4$ | 7 | 11 | 13 | 17 | 19 | 23 |
|---------------|-------|-------|---|----|----|----|----|----|
| $M \bmod q^k$ | 18    | 18    | 4 | 5  | 5  | 3  | 15 | 4  |
| $N \bmod q^k$ | 11    | 11    | 4 | 6  | 11 | 4  | 12 | 6  |

**Lemma 8.4** (Residues on the progression). *Let  $(M, N) \in \mathcal{P}_7$ . For every  $i$ , the cofactor  $c_i$  divides  $L_i(M, N)$ , and the quotient  $L_i(M, N)/c_i$  is prime to  $W$  and has the residues modulo 8, 3, 7, 11, 13, 17, 19, 23 listed in Table 8.8. In particular,  $FHJ \neq 0$  and*

$$F = 2^7 3^4 \prod_{i \in I_F} \frac{L_i}{c_i}, \quad H = 2^4 3^4 \prod_{i \in I_H} \frac{L_i}{c_i}, \quad J = 2^7 3^7 \prod_{i \in I_J} \frac{L_i}{c_i}, \tag{8.11}$$

where all three products are prime to 6.

*Proof.* Every  $(M, N) \in \mathcal{P}_7$  satisfies  $(M, N) \equiv (18, 11) \pmod{2^9}$  and modulo  $3^4$ , that is, modulo  $2^9 3^4$ . Table 8.9 lists the values  $L_i(18, 11)$  and their valuations at 2 and 3. These valuations agree with the exponents of 2 and 3 in  $c_i$ , so that  $c_i$  divides  $L_i(18, 11)$

Table 8.8. The residues of  $p_i = L_i(M, N)/c_i$  for  $(M, N) \in \mathcal{P}_7$ .

| $i$            | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 |
|----------------|----|----|----|----|----|----|----|----|----|----|----|----|
| $p_i \bmod 8$  | 1  | 3  | 1  | 3  | 3  | 5  | 5  | 3  | 7  | 5  | 5  | 7  |
| $p_i \bmod 3$  | 1  | 2  | 2  | 1  | 1  | 1  | 1  | 1  | 2  | 2  | 1  | 2  |
| $p_i \bmod 7$  | 1  | 4  | 4  | 2  | 4  | 6  | 5  | 3  | 4  | 2  | 2  | 3  |
| $p_i \bmod 11$ | 7  | 6  | 10 | 5  | 5  | 4  | 9  | 5  | 2  | 1  | 2  | 9  |
| $p_i \bmod 13$ | 1  | 11 | 8  | 7  | 2  | 5  | 11 | 9  | 1  | 5  | 6  | 11 |
| $p_i \bmod 17$ | 3  | 4  | 7  | 4  | 14 | 8  | 10 | 7  | 5  | 16 | 6  | 4  |
| $p_i \bmod 19$ | 4  | 12 | 5  | 9  | 18 | 18 | 12 | 14 | 3  | 1  | 8  | 18 |
| $p_i \bmod 23$ | 13 | 6  | 6  | 17 | 7  | 3  | 6  | 6  | 21 | 4  | 16 | 20 |

and the quotient  $L_i(18, 11)/c_i$  is prime to 6. They are at most 6 at 2 and at most 3 at 3. Then  $c_i$  divides  $2^9 3^4$ , and  $2^9 3^4/c_i$  is divisible by  $2^3 \cdot 3$ . By Lemma 4.7 with  $W_0 = 2^9 3^4$  and  $(m, n) = (18, 11)$ , the cofactor  $c_i$  divides  $L_i(M, N)$ , and  $L_i(M, N)/c_i \equiv L_i(18, 11)/c_i$  modulo  $2^9 3^4/c_i$ , and hence modulo 8 and modulo 3. Since  $L_i(18, 11)/c_i$  is prime to 6, so is  $L_i(M, N)/c_i$ , and the valuations  $v_2(L_i(M, N))$  and  $v_3(L_i(M, N))$  are those of the table. We obtain the first two rows of Table 8.8 from the last two columns of Table 8.9.

For  $q \in \{7, 11, 13, 17, 19, 23\}$ , the class  $\mathcal{P}_7$  fixes  $(M, N)$  modulo  $q$  to the pair  $(m_q, n_q)$  of Table 8.7, and  $L_i(M, N) \equiv a_i m_q + b_i n_q \pmod{q}$ . These residues are listed in Table 8.10; none of them vanishes. Since  $c_i$  is prime to  $q$ , we find that  $L_i(M, N)/c_i$  is prime to  $q$  and congruent to  $(a_i m_q + b_i n_q)c_i^{-1}$  modulo  $q$ . These are the remaining rows of Table 8.8. Finally, (8.11) follows from  $L_i = c_i \cdot (L_i/c_i)$  and (8.5).  $\square$

Several values in Table 8.9 are negative, and the residues must be computed from the signed values. For example,  $L_2(18, 11)/64 = -31 \equiv 1 \pmod{8}$ , whereas  $31 \equiv 7 \pmod{8}$ . The proof of Lemma 8.4 shows that  $-31$  has the correct residue: for every  $(M, N) \in \mathcal{P}_7$ , including those for which  $L_2(M, N) > 0$ , we have  $L_2(M, N)/64 \equiv 1 \pmod{8}$ .

The real cone is

$$\mathcal{K}_7 = \{(M, N) \in \mathbb{R}^2 : N > 0, 2999N < M < 3001N\}, \quad (8.12)$$

an open convex cone. The pairs  $(18, 11)$  and  $(M_0, N_0)$  do not lie in  $\mathcal{K}_7$ . This does not matter, since Lemma 8.4 holds on all of  $\mathcal{P}_7$ .

**Lemma 8.5** (Positivity on the cone). *Every  $L_i$  is positive on  $\mathcal{K}_7$ . In particular,  $F$ ,  $H$  and  $J$  are positive on  $\mathcal{K}_7$ .*

*Proof.* Let  $(M, N) \in \mathcal{K}_7$  and set  $\rho = M/N > 2999$ . Then  $L_i(M, N) = N(a_i \rho + b_i)$ , and since  $a_i \geq 0$  for all  $i$ , we have  $a_i \rho + b_i \geq 2999a_i + b_i$ . The twelve values  $2999a_i + b_i$  are

$$2999, 1, 2817, 556375, 27025, 70007, 409, 24417, 41675, 1023941, 41011, 2641357,$$

Table 8.9. The values of the forms at  $(18, 11)$ , which fix the exact powers of 2 and 3 and the residues modulo 8 and 3 on  $\mathcal{P}_7$ .

| $i$ | $L_i(18, 11)$ | $v_2$ | $v_3$ | $c_i$ | $L_i(18, 11)/c_i$ | mod 8 | mod 3 |
|-----|---------------|-------|-------|-------|-------------------|-------|-------|
| 0   | 18            | 1     | 2     | 18    | 1                 | 1     | 1     |
| 1   | 11            | 0     | 0     | 1     | 11                | 3     | 2     |
| 2   | -1984         | 6     | 0     | 64    | -31               | 1     | 2     |
| 3   | 119403        | 0     | 2     | 9     | 13267             | 3     | 1     |
| 4   | 536           | 3     | 0     | 8     | 67                | 3     | 1     |
| 5   | -54198        | 1     | 2     | 18    | -3011             | 5     | 1     |
| 6   | -61443        | 0     | 2     | 9     | -6827             | 5     | 1     |
| 7   | 4819          | 0     | 0     | 1     | 4819              | 3     | 1     |
| 8   | 29802         | 1     | 1     | 6     | 4967              | 7     | 2     |
| 9   | 547776        | 6     | 3     | 1728  | 317               | 5     | 2     |
| 10  | -10473        | 0     | 1     | 3     | -3491             | 5     | 1     |
| 11  | -487089       | 0     | 2     | 9     | -54121            | 7     | 2     |

Table 8.10. The residues  $L_i(m_q, n_q) \bmod q$  for  $i = 0, \dots, 11$ .

| $q$ | $(m_q, n_q)$ | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 |
|-----|--------------|----|----|----|----|----|----|----|----|----|----|----|----|
| 7   | (4, 4)       | 4  | 4  | 4  | 4  | 4  | 3  | 3  | 3  | 3  | 5  | 6  | 6  |
| 11  | (5, 6)       | 5  | 6  | 2  | 1  | 7  | 6  | 4  | 5  | 1  | 1  | 6  | 4  |
| 13  | (5, 11)      | 5  | 11 | 5  | 11 | 3  | 12 | 8  | 9  | 6  | 8  | 5  | 8  |
| 17  | (3, 4)       | 3  | 4  | 6  | 2  | 10 | 8  | 5  | 7  | 13 | 6  | 1  | 2  |
| 19  | (15, 12)     | 15 | 12 | 16 | 5  | 11 | 1  | 13 | 14 | 18 | 18 | 5  | 10 |
| 23  | (4, 6)       | 4  | 6  | 16 | 15 | 10 | 8  | 8  | 6  | 11 | 12 | 2  | 19 |

all positive. Then every  $L_i(M, N)$  is positive, because  $N > 0$ .  $\square$

More precisely, the twelve forms are all positive exactly on the region  $\{N > 0, M/N > 5589/2\}$ : the largest of the roots  $-b_i/a_i$  with  $a_i > 0$  is  $5589/2$ , from  $L_6$ , and  $\mathcal{K}_7$  lies inside this region. Finally, since  $L_0 = M$  and  $L_1 = N$ , we have  $p_0 = M/18$  and  $p_1 = N$  at every prime specialization.

## 8.4 Local conditions at the fixed places

We now bound the images of the local descent maps at the places 2 and 3 for  $E$ , and 2, 7, 13 and  $\infty$  for  $E'$ , and write the resulting fixed rows. We use no condition for  $E$  at 7, 13 and  $\infty$ , or for  $E'$  at 3.

**Lemma 8.6** (Local images at the fixed places). *Let  $(M, N) \in \mathcal{P}_7$ . Then  $FHJ \neq 0$ , and the following hold.*

- (a)  $\delta_{E,2}(E(\mathbf{Q}_2)) \subseteq \{[1], [-2]\}$ .
- (b)  $\delta_{E,3}(E(\mathbf{Q}_3)) = \{[1]\}$ .
- (c)  $\delta_{E',2}(E'(\mathbf{Q}_2)) \subseteq \{[1], [2], [3], [6]\}$ .
- (d)  $\delta_{E',q}(E'(\mathbf{Q}_q)) = \{[1]\}$  for  $q = 7$  and  $q = 13$ .
- (e) If moreover  $(M, N) \in \mathcal{K}_7$ , then  $\delta_{E',\infty}(E'(\mathbb{R})) = \{[1]\}$ .

The proof treats the places one at a time. At each place we first find the valuations and residues of  $\alpha$ ,  $\beta$  and  $\beta'$  that we need; by Lemma 8.4, they are the same for all  $(M, N) \in \mathcal{P}_7$ . Then we go through all points of the local curve: the point  $O$ , which has class  $[1]$ ; the point  $T$  or  $T'$ , whose class is  $[\beta]$  or  $[\beta']$ ; the other points with  $y = 0$ , whose existence we decide with Lemma 3.7; and the points with  $y \neq 0$ , sorted by the valuation of  $x$ . In the last step we use Lemma 3.1 to find the valuation of the right side of the equation, and Lemma 3.2 to decide whether it is a square. We may rescale the coordinates by squares, because multiplying  $x$  by a nonzero square does not change its class.

*Proof.* By Lemma 8.4,  $FHJ \neq 0$ . We first collect the coefficient data. Using (8.11) and Table 8.8, we find

$$\begin{aligned} F/2^7 &\equiv 3^4 \cdot 1 \cdot 3 \cdot 1 \cdot 3 \equiv 1, & H/2^4 &\equiv 3^4 \cdot 3 \cdot 5 \cdot 5 \cdot 3 \equiv 1, \\ J/2^7 &\equiv 3^7 \cdot 7 \cdot 5 \cdot 5 \cdot 7 \equiv 3 \pmod{8}, \end{aligned}$$

and  $F/3^4 \equiv 2^7 \cdot 1 \cdot 2 \cdot 2 \cdot 1 \equiv 2$  and  $H/3^4 \equiv 2^4 \equiv 1 \pmod{3}$ . Modulo 7 and 13, the forms are units, and by Table 8.8 we have  $F \equiv 4, H \equiv 3, J \equiv 1 \pmod{7}$  and  $F \equiv 9, H \equiv 5, J \equiv 9 \pmod{13}$ . Recall that  $91205 = 5 \cdot 17 \cdot 29 \cdot 37$  and  $33124 = 2^2 \cdot 7^2 \cdot 13^2$ . Inserting these residues into  $\alpha = 91205F$ ,  $\beta = -33124FH$  and  $\beta' = 9FJ$ , we obtain Table 8.11. For example, at 2 we have  $v_2(\beta) = 2 + 7 + 4 = 13$  and  $\beta/2^{13} = -91^2(F/2^7)(H/2^4) \equiv -1 \pmod{8}$ , since  $91^2 \equiv 1 \pmod{8}$ .

Table 8.11. Valuations and residues of the coefficients at the fixed primes, for  $(M, N) \in \mathcal{P}_7$ . Here  $u$  denotes a unit at the place.

| place | $\alpha$                     | $\beta$                         | $\beta'$                        |
|-------|------------------------------|---------------------------------|---------------------------------|
| 2     | $2^7 u, u \equiv 5 \pmod{8}$ | $2^{13} u, u \equiv 7 \pmod{8}$ | $2^{14} u, u \equiv 3 \pmod{8}$ |
| 3     | $3^4 u, u \equiv 1 \pmod{3}$ | $3^8 u, u \equiv 1 \pmod{3}$    | $v_3(\beta') = 13$              |
| 7     | $\alpha \equiv 1 \pmod{7}$   | $7^2 u, u \equiv 1 \pmod{7}$    | $\beta' \equiv 1 \pmod{7}$      |
| 13    | $\alpha \equiv 12 \pmod{13}$ | $13^2 u, u \equiv 7 \pmod{13}$  | $\beta' \equiv 1 \pmod{13}$     |

**The prime 2, curve  $E$ .** Since  $\beta/2^{13} \equiv 7$  and  $\beta'/2^{14} \equiv 3 \pmod{8}$ , Lemma 3.2 implies that  $[\beta] = [-2]$  and  $[\beta'] = [3]$  in  $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ . We change coordinates by  $x = 2^6 \tilde{x}$  and  $y = 2^9 \tilde{y}$ . The equation of  $E$  becomes

$$\tilde{y}^2 = \tilde{x}^3 + \alpha_2 \tilde{x}^2 + \beta_2 \tilde{x}, \quad \alpha_2 = \alpha/2^6, \quad \beta_2 = \beta/2^{12},$$

and  $[x] = [\tilde{x}]$ . In Table 8.11, we see that  $\alpha_2$  and  $\beta_2$  have valuation 1, with  $\alpha_2/2 \equiv 5$  and  $\beta_2/2 \equiv 7 \pmod{8}$ . Then  $\alpha_2 \equiv 2$  and  $\beta_2 \equiv 6 \pmod{8}$ , and  $[\beta_2] = [-2]$ .

The point  $T$  has class  $[\beta] = [-2]$ . Since  $\alpha^2 - 4\beta = \beta'$  is not a square in  $\mathbb{Q}_2$ , Lemma 3.7 shows that  $E(\mathbb{Q}_2)$  has no other point with  $y = 0$ . Let  $(\tilde{x}, \tilde{y})$  be a point with  $\tilde{y} \neq 0$ , and write  $\tilde{x} = 2^r u$  with  $u \in \mathbb{Z}_2^\times$ . The right side of the equation is the nonzero square  $\tilde{y}^2$ , and its three terms  $\tilde{x}^3$ ,  $\alpha_2 \tilde{x}^2$  and  $\beta_2 \tilde{x}$  have valuations  $3r$ ,  $2r + 1$  and  $r + 1$ .

- If  $r \leq -1$ , then  $\tilde{x}^3$  is the dominant term, and Lemma 3.1 implies that the right side has valuation  $3r$ . This valuation is even, and we have  $r \leq -2$ . The other two terms then have valuations at least  $3r + 3$ , and by Lemma 3.1(b) the right side equals  $\tilde{x}^3(1 + 8t)$  with  $t \in \mathbb{Z}_2$ . By Lemma 3.2(c),  $1 + 8t$  is a square. It follows that  $\tilde{x}^3$  is a square, and so is  $\tilde{x} = \tilde{x}^3/\tilde{x}^2$ .
- If  $r = 0$ , the right side is a unit, congruent to  $u(u^2 + 2u + 6)$  modulo 8. For  $u \equiv 1, 3, 5, 7 \pmod{8}$ , this residue is 1, 7, 5, 3, respectively. A square unit is 1 modulo 8. We conclude that  $u \equiv 1 \pmod{8}$  and  $[\tilde{x}] = [1]$ .
- If  $r = 1$ , the valuations are 3, 3 and 2, and the right side has valuation 2. Dividing it by 4 and using  $u^2 \equiv 1 \pmod{8}$ , we obtain the unit  $2u^3 + \alpha_2 u^2 + (\beta_2/2)u \equiv 2u + 2 + 7u \equiv u + 2 \pmod{8}$ . For  $u \equiv 1, 3, 5, 7 \pmod{8}$ , this is 3, 5, 7, 1. Only  $u \equiv 7 \pmod{8}$  gives a square, and then  $[\tilde{x}] = [2 \cdot 7] = [-2]$ .
- If  $r \geq 2$ , then  $\beta_2 \tilde{x}$  is the dominant term, with valuation  $r + 1$ , and  $r$  is odd; in particular,  $r \geq 3$ . The other two terms have valuations  $2r + 1$  and  $3r$ , which are at least  $(r + 1) + 3$ . As in the first case, we find that  $\beta_2 \tilde{x}$  is a square, and  $[\tilde{x}] = [\beta_2] = [-2]$ .

Together with  $O$  and  $T$ , these cases prove (a).

**The prime 3, curve E.** We change coordinates by  $x = 3^4\tilde{x}$  and  $y = 3^6\tilde{y}$ . The equation becomes

$$\tilde{y}^2 = \tilde{x}^3 + \alpha_3\tilde{x}^2 + \beta_3\tilde{x}, \quad \alpha_3 = \alpha/3^4, \quad \beta_3 = \beta/3^8,$$

where  $\alpha_3$  and  $\beta_3$  are units congruent to 1 modulo 3, by Table 8.11. By Lemma 3.2, a unit at 3 is a square exactly when it is 1 modulo 3. The point  $T$  has class  $[\beta] = [\beta_3] = [1]$ . The element  $\alpha^2 - 4\beta = \beta'$  has odd valuation  $v_3(\beta') = 13$  and is not a square in  $\mathbb{Q}_3$ . Lemma 3.7 then shows that there is no other point with  $y = 0$ . Let  $(\tilde{x}, \tilde{y})$  be a point with  $\tilde{y} \neq 0$ , and write  $\tilde{x} = 3^r u$  with  $u \in \mathbb{Z}_3^\times$ .

- If  $r < 0$ , then  $\tilde{x}^3$  is the dominant term, and the other two terms have valuations at least  $3r + 1$ . By Lemma 3.1, the right side equals  $\tilde{x}^3(1 + 3t)$  with  $t \in \mathbb{Z}_3$ . Its valuation  $3r$  is even, and  $1 + 3t$  is a square, so  $\tilde{x}^3$  and  $\tilde{x}$  are squares.
- If  $r > 0$ , then  $\beta_3\tilde{x}$  is the dominant term, and the other two terms have valuations at least  $r + 1$ . As before,  $\beta_3\tilde{x}$  is a square, and since  $\beta_3$  is a square, so is  $\tilde{x}$ .
- Finally, let  $r = 0$ . If  $u \equiv 1 \pmod{3}$ , then  $\tilde{x}$  is a square. If  $u \equiv 2 \pmod{3}$ , the right side is a unit congruent to  $2(4 + 2 + 1) \equiv 2 \pmod{3}$ , which is not a square. This case does not occur.

These cases and the point  $O$  prove (b).

**The prime 2, curve E'.** We use the following fact: if  $s, t \in \mathbb{Q}_2$  are not both zero, then  $s^2 + 2t^2 \neq 0$  and

$$[s^2 + 2t^2] \in \{[1], [2], [3], [6]\}. \quad (8.13)$$

Indeed,  $s^2 + 2t^2 \neq 0$  because  $-2$  is not a square in  $\mathbb{Q}_2$ . After multiplying  $s$  and  $t$  by a power of 2, which changes  $s^2 + 2t^2$  by a square, we may assume that  $s, t \in \mathbb{Z}_2$  and that one of them is odd. If  $s$  is odd, then  $s^2 \equiv 1$  and  $2t^2 \equiv 0$  or  $2 \pmod{8}$ , and  $s^2 + 2t^2$  is a unit congruent to 1 or 3 modulo 8; by Lemma 3.2, its class is  $[1]$  or  $[3]$ . If  $s$  is even and  $t$  is odd, then  $s^2 + 2t^2 = 2(t^2 + 2(s/2)^2)$ , and the same argument shows that its class is  $[2]$  or  $[6]$ . In other words, the nonzero values of  $s^2 + 2t^2$ , which are the norms from  $\mathbb{Q}_2(\sqrt{-2})$ , have classes in  $\{[1], [2], [3], [6]\}$ .

Since  $[\beta] = [-2]$ , there exists  $w_0 \in \mathbb{Q}_2^\times$  such that  $\beta = -2w_0^2$ . Using  $\alpha' = -2\alpha$  and  $\beta' = \alpha^2 - 4\beta$ , we write the equation of  $E'$  as

$$y^2 = x((x - \alpha)^2 - 4\beta) = x((x - \alpha)^2 + 2(2w_0)^2). \quad (8.14)$$

The point  $T'$  has class  $[\beta'] = [\alpha^2 + 2(2w_0)^2]$ , which lies in the set (8.13); indeed,  $[\beta'] = [3]$ . The class of  $\alpha'^2 - 4\beta' = 16\beta$  is  $[-2] \neq [1]$ , and Lemma 3.7 shows that there is no other point with  $y = 0$ . If  $(x, y)$  is a point with  $x \neq 0$  and  $y \neq 0$ , we have

$$[x] = [y^2/x] = [(x - \alpha)^2 + 2(2w_0)^2],$$

which lies in the set (8.13) with  $s = x - \alpha$  and  $t = 2w_0 \neq 0$ . Together with  $O$ , this proves (c).

**The primes 7 and 13, curve  $E'$ .** Let  $q \in \{7, 13\}$ . By Table 8.11,  $\alpha$  and  $\beta'$  are units at  $q$ ,  $\beta = q^2 b_q$  with  $b_q$  a unit, and  $\beta' \equiv 1 \pmod{q}$ . By Lemma 3.2, a unit at  $q$  is a square exactly when its residue modulo  $q$  is a nonzero square. In particular,  $\beta'$  is a square. Further,  $\alpha$  is congruent to a nonzero square modulo  $q$ : we have  $\alpha \equiv 1 \pmod{7}$  and  $\alpha \equiv 12 \equiv 5^2 \pmod{13}$ .

The point  $T'$  has class  $[\beta'] = [1]$ . The other points with  $y = 0$  have abscissas  $x_0$  with  $x_0^2 - 2\alpha x_0 + \beta' = 0$ , that is,  $(x_0 - \alpha)^2 = 4\beta = 4q^2 b_q$ , and by Lemma 3.7 they exist exactly when  $b_q$  is a square. For  $q = 13$ , we have  $b_q \equiv 7 \pmod{13}$ , which is not a square, and there are no such points. For  $q = 7$ , we have  $b_q \equiv 1 \pmod{7}$ , the two points exist, and  $x_0 = \alpha \pm 2 \cdot 7 \sqrt{b_q} \equiv \alpha \equiv 1 \pmod{7}$ ; their class is  $[1]$ . Let  $(x, y)$  be a point with  $y \neq 0$ , and write  $x = q^r u$  with  $u \in \mathbb{Z}_q^\times$ . The terms  $x^3$ ,  $\alpha' x^2$  and  $\beta' x$  of the right side have valuations  $3r$ ,  $2r$  and  $r$ .

- If  $r < 0$ , then  $x^3$  is the dominant term, and, as at the prime 3, the right side equals  $x^3(1 + qt)$  with  $t \in \mathbb{Z}_q$ . Its valuation  $3r$  is even,  $1 + qt$  is a square, and  $x$  is a square.
- If  $r > 0$ , then  $\beta' x$  is the dominant term. As before,  $\beta' x$  is a square, and since  $\beta'$  is a square, so is  $x$ .
- If  $r = 0$ , the right side is  $x((x - \alpha)^2 - 4\beta)$ , and  $4\beta \equiv 0 \pmod{q}$ . If  $x \not\equiv \alpha \pmod{q}$ , then  $(x - \alpha)^2 - 4\beta$  is a unit congruent to the nonzero square  $(x - \alpha)^2$  modulo  $q$ . It is a square, and therefore  $x$  is a square. If  $x \equiv \alpha \pmod{q}$ , then  $x$  is a square because  $\alpha$  is congruent to a nonzero square modulo  $q$ .

Together with  $O$ , these cases prove (d).

**The real place, curve  $E'$ .** Let  $(M, N) \in \mathcal{K}_7$ . The forms  $F$ ,  $H$  and  $J$  are positive by Lemma 8.5, and  $\alpha > 0$ ,  $\beta < 0$  and  $\beta' > 0$ . If  $x < 0$ , the three terms  $x^3$ ,  $-2\alpha x^2$  and  $\beta' x$  of the right side are negative, and there is no real point with this abscissa. The point  $T'$  has class  $[\beta'] = [1]$  in  $\mathbb{R}^\times / \mathbb{R}^{\times 2}$ . The discriminant  $\alpha'^2 - 4\beta' = 16\beta$  is negative, and Lemma 3.7 shows that there is no other point with  $y = 0$ . Every other point has  $x > 0$ . Together with  $O$ , this proves (e).  $\square$

**The fixed rows.** We write the fixed rows in the coordinates of Section 3.1. At 2, the class of  $z \in \mathbb{Q}_2^\times$  is  $[(-1)^{e_1} 2^{e_2} 5^{e_3}]$ , with coordinates  $e_1(z), e_2(z), e_3(z)$ . At an odd prime  $q$ , we write  $z = q^k z_0$  with  $z_0 \in \mathbb{Z}_q^\times$ , and the coordinates are  $v_q(z) = k \bmod 2$  and  $\chi_q(z) = \chi_q(z_0)$ , as in (3.3). At  $\infty$ , the sign coordinate  $\text{sgn}(z)$  is 0 or 1 according as  $z > 0$  or  $z < 0$ . These coordinates are linear maps on the groups of squareclasses. The subgroups of Lemma 8.6 are annihilated by the following linear maps:

- $e_1 + e_2$  and  $e_3$  (on  $E$  at 2), since  $[-2]$  has coordinates  $(e_1, e_2, e_3) = (1, 1, 0)$ ;
- $\chi_3$  and  $v_3$  (on  $E$  at 3);
- $e_1 + e_3$  (on  $E'$  at 2), since  $[2]$ ,  $[3]$  and  $[6]$  have coordinates  $(0, 1, 0)$ ,  $(1, 0, 1)$  and  $(1, 1, 1)$ ;
- $\chi_q$  and  $v_q$  for  $q = 7, 13$ , and  $\text{sgn}$  (on  $E'$ ).

For each map  $f$  in this list, we obtain a row as in Definition 3.9, whose entry at a basis element  $g$  is  $f(\text{loc}_v([g]))$ , which we denote simply by  $f(g)$ . These are the fixed rows. In the order of this list, we denote them by  $f_1^E, \dots, f_4^E$  (for the maps  $e_1 + e_2, e_3, \chi_3, \nu_3$ ) and  $f_1^{E'}, \dots, f_6^{E'}$  (for the maps  $e_1 + e_3, \chi_7, \nu_7, \chi_{13}, \nu_{13}, \text{sgn}$ ). They are the first four rows of  $\mathbf{M}_E(\eta)$  and the first six rows of  $\mathbf{M}_{E'}(\eta)$  in Tables 8.17 and 8.18. Their entries at the constant columns are given by Table 8.12. At a column  $p_i$ , we note that  $p_i$  is a positive unit at 2, 3, 7, 13. This gives  $e_2(p_i) = \nu_3(p_i) = \nu_7(p_i) = \nu_{13}(p_i) = \text{sgn}(p_i) = 0$ . Further,  $(e_1, e_3)(p_i) = (0, 0), (1, 1), (0, 1), (1, 0)$  for  $p_i \equiv 1, 3, 5, 7 \pmod{8}$  by (3.2), and  $\chi_q(p_i) = 0$  exactly when  $p_i$  is a square modulo  $q$ . By Lemma 8.4, the entries at the finite fixed places are the same for all  $(M, N) \in \mathcal{P}_7$ . The entries of the real row at the columns  $p_i$  are zero at every prime specialization, since the  $p_i$  are positive.

Table 8.12. Local coordinates of the constant basis elements. At 2 we used  $3 \equiv -5, 7 \equiv -1$  and  $13 \equiv 5 \pmod{8}$ .

| $g$                        | $-1$        | $2$         | $3$         | $7$         | $13$        |
|----------------------------|-------------|-------------|-------------|-------------|-------------|
| $(e_1, e_2, e_3)(g)$       | $(1, 0, 0)$ | $(0, 1, 0)$ | $(1, 0, 1)$ | $(1, 0, 0)$ | $(0, 0, 1)$ |
| $(\chi_3, \nu_3)(g)$       | $(1, 0)$    | $(1, 0)$    | $(0, 1)$    | $(0, 0)$    | $(0, 0)$    |
| $(\chi_7, \nu_7)(g)$       | $(1, 0)$    | $(0, 0)$    | $(1, 0)$    | $(0, 1)$    | $(1, 0)$    |
| $(\chi_{13}, \nu_{13})(g)$ | $(0, 0)$    | $(1, 0)$    | $(0, 0)$    | $(1, 0)$    | $(0, 1)$    |
| $\text{sgn}(g)$            | $1$         | $0$         | $0$         | $0$         | $0$         |

## 8.5 Characters at the moving primes

Let  $(M, N)$  be a prime specialization in  $\mathcal{P}_7$ . By Lemma 4.11 and Corollary 4.14, the moving rows of  $\mathbf{M}_E(\eta)$  and  $\mathbf{M}_{E'}(\eta)$  are determined by the bits (4.34): the characters  $\lambda_i(g)$  for  $g \in \{-1, 2, 3, 7, 13\}$ , the characters  $\lambda_i(\kappa_E)$  and  $\lambda_i(\kappa_{E'})$ , and the bits  $\gamma_{ij}$  of (4.27), which satisfy  $\lambda_i(p_j) = \gamma_{ij} + \eta$ . Recall that  $\varepsilon = (N/p_0) = (-1)^\eta$ ; since  $N = p_1$ , we have  $\varepsilon = (p_1/p_0)$ .

**Lemma 8.7** (Characters at the moving primes). *Let  $(M, N)$  be a prime specialization of  $\mathcal{D}_7$  with  $(M, N) \in \mathcal{P}_7$ . Then the following hold.*

- (a) *For  $g \in \{-1, 2, 3, 7, 11, 13, 17, 19, 23\}$  and  $0 \leq i \leq 11$ , the number  $\lambda_i(g)$  is given by Table 8.13. In particular,  $\lambda_i(\kappa_E) = \lambda_i(-1) + \lambda_i(2)$  and  $\lambda_i(\kappa_{E'}) = \lambda_i(3)$ .*
- (b) *For distinct  $i, j$  such that  $\{i, j\}$  is contained neither in  $I_H$  nor in  $I_J$ , the bit  $\gamma_{ij}$  of (4.27) is given by Table 8.14, and  $\lambda_i(p_j) = \gamma_{ij} + \eta$ .*

Table 8.13. The characters  $\lambda_i(g)$ , defined by  $(g/p_i) = (-1)^{\lambda_i(g)}$ . The first five rows give the constant columns of the moving rows; the last four enter the constants of Table 8.15.

| $i$             | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|-----------------|---|---|---|---|---|---|---|---|---|---|----|----|
| $\lambda_i(-1)$ | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0  | 1  |
| $\lambda_i(2)$  | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1  | 0  |
| $\lambda_i(3)$  | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0  | 0  |
| $\lambda_i(7)$  | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0  | 0  |
| $\lambda_i(13)$ | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1  | 1  |
| $\lambda_i(11)$ | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1  | 1  |
| $\lambda_i(17)$ | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1  | 0  |
| $\lambda_i(19)$ | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1  | 0  |
| $\lambda_i(23)$ | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0  | 0  |

Table 8.14. The numbers  $\gamma_{ij}$ , with  $\lambda_i(p_j) = \gamma_{ij} + \eta$ : row  $p_i$ , column  $p_j$ . A dot marks a pair inside  $I_H$  or inside  $I_J$ , which does not occur in any row.

|          | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $p_7$ | $p_8$ | $p_9$ | $p_{10}$ | $p_{11}$ |
|----------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|----------|----------|
| $p_0$    | *     | 0     | 0     | 1     | 1     | 0     | 0     | 1     | 0     | 1     | 0        | 1        |
| $p_1$    | 0     | *     | 1     | 0     | 0     | 0     | 0     | 0     | 1     | 0     | 1        | 1        |
| $p_2$    | 0     | 1     | *     | 1     | 0     | 0     | 0     | 0     | 0     | 0     | 1        | 0        |
| $p_3$    | 1     | 1     | 1     | *     | 0     | 1     | 1     | 0     | 0     | 0     | 1        | 1        |
| $p_4$    | 1     | 1     | 0     | 1     | *     | .     | .     | .     | 0     | 1     | 0        | 1        |
| $p_5$    | 0     | 0     | 0     | 1     | .     | *     | .     | .     | 1     | 1     | 0        | 1        |
| $p_6$    | 0     | 0     | 0     | 1     | .     | .     | *     | .     | 1     | 1     | 0        | 1        |
| $p_7$    | 1     | 1     | 0     | 1     | .     | .     | .     | *     | 0     | 1     | 0        | 1        |
| $p_8$    | 0     | 0     | 0     | 1     | 1     | 1     | 1     | 1     | *     | .     | .        | .        |
| $p_9$    | 1     | 0     | 0     | 0     | 1     | 1     | 1     | 1     | .     | *     | .        | .        |
| $p_{10}$ | 0     | 1     | 1     | 1     | 0     | 0     | 0     | 0     | .     | .     | *        | .        |
| $p_{11}$ | 1     | 0     | 0     | 0     | 0     | 1     | 1     | 0     | .     | .     | .        | *        |

Table 8.15. The squarefree parts  $s_j$  of  $b_j c_j$  and  $s_{ij}$  of  $c_0 c_j b_i \Delta_{ji}$ , for  $1 \leq i < j$  with  $\{i, j\}$  not inside  $I_H$  or  $I_J$ .

| $j$              | 1 | 2    | 3    | 4  | 5   | 6   | 7  | 8 | 9     | 10  | 11    |
|------------------|---|------|------|----|-----|-----|----|---|-------|-----|-------|
| $s_j$            | 1 | -182 | 1173 | 17 | -69 | -69 | 17 | 7 | 16422 | -13 | -5083 |
| $\lambda_0(s_j)$ | 0 | 0    | 1    | 1  | 0   | 0   | 1  | 0 | 1     | 0   | 1     |

  

| $s_{ij}$ | $j = 2$ | 3  | 4     | 5      | 6      | 7     | 8      | 9   | 10   | 11 |
|----------|---------|----|-------|--------|--------|-------|--------|-----|------|----|
| $i = 1$  | 2       | 91 | 1     | 1      | 1      | 1     | 39     | 78  | 21   | 7  |
| 2        |         | 91 | 19019 | -19019 | -19019 | 19019 | 39     | 78  | 21   | 7  |
| 3        |         |    | 14421 | 3553   | 3553   | 14421 | -15249 | -26 | 8211 | 21 |

  

| $s_{ij}$ | $j = 8$ | 9   | 10  | 11 |
|----------|---------|-----|-----|----|
| $i = 4$  | -969    | -66 | 561 | 19 |
| 5        | 1311    | 22  | 759 | 57 |
| 6        | 1311    | 22  | 759 | 57 |
| 7        | -969    | -66 | 561 | 19 |

*Proof.* For (a), recall that every  $p_i$  is an odd prime outside  $S$ ; in particular,  $p_i$  is distinct from 3, 7, 11, 13, 17, 19, 23. By (4.22) and Lemma 4.13, we have, modulo 2,

$$\lambda_i(-1) = \frac{p_i - 1}{2}, \quad \lambda_i(2) = \frac{p_i^2 - 1}{8}, \quad \lambda_i(q) = \chi_q(p_i) + \lambda_i(-1)\chi_q(-1) \quad (8.15)$$

for every odd prime  $q \neq p_i$ . Here  $\chi_q(p_i)$  is 0 or 1 according as  $p_i$  is or is not a square modulo  $q$ , and among the primes  $q \in \{3, 7, 11, 13, 17, 19, 23\}$  used here,  $\chi_q(-1) = 1$  exactly for  $q \in \{3, 7, 11, 19, 23\}$ . The right sides depend only on the residues of  $p_i$  modulo 8 and modulo  $q$ , which are given in Table 8.8. The nonzero squares modulo 3, 7, 11, 13, 17, 19, 23 are

$$\{1\}, \quad \{1, 2, 4\}, \quad \{1, 3, 4, 5, 9\}, \quad \{1, 3, 4, 9, 10, 12\}, \quad \{1, 2, 4, 8, 9, 13, 15, 16\}, \\ \{1, 4, 5, 6, 7, 9, 11, 16, 17\}, \quad \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}.$$

For example, we have  $p_3 \equiv 3 \pmod{8}$  and  $p_3 \equiv 7 \pmod{13}$ , which is not a square modulo 13, and (8.15) gives  $\lambda_3(-1) = \lambda_3(2) = 1$  and  $\lambda_3(13) = 1$ . Inserting the residues of Table 8.8 into (8.15), we obtain Table 8.13. The assertions on  $\kappa_E$  and  $\kappa_{E'}$  follow from  $[\kappa_E] = [-2]$  and  $[\kappa_{E'}] = [3]$ , since  $p_i \nmid \kappa_E \kappa_{E'}$ .

For (b), we evaluate (4.26) and (4.27). Recall from Table 8.8 that  $p_0 \equiv 1 \pmod{8}$ . Then  $\lambda_0(-1) = 0$ , and  $\theta_i = \lambda_0(b_i c_i) = \lambda_0(s_i)$ , where  $s_j$  denotes the squarefree part of  $b_j c_j$ . We obtain

$$\gamma_{0j} = \gamma_{j0} = \lambda_0(s_j) \quad (1 \leq j \leq 11).$$

For distinct  $i, j \geq 1$ , we have

$$\gamma_{ij} = \lambda_i(s_{ij}) + \lambda_0(s_i),$$

where  $s_{ij}$  is the squarefree part of  $c_0 c_j b_i \Delta_{ji}$ . Removing square factors does not change the characters, since every prime factor of  $b_j c_j$  and of  $c_0 c_j b_i \Delta_{ji}$  lies in  $S$ , and  $p_0, p_i \notin S$ . The constants  $s_j$ , and  $s_{ij}$  for  $i < j$ , are listed in Table 8.15. Their prime factors are

$$\begin{aligned} 182 &= 2 \cdot 7 \cdot 13, & 1173 &= 3 \cdot 17 \cdot 23, & 69 &= 3 \cdot 23, & 16422 &= 2 \cdot 3 \cdot 7 \cdot 17 \cdot 23, \\ 5083 &= 13 \cdot 17 \cdot 23, & 91 &= 7 \cdot 13, & 39 &= 3 \cdot 13, & 78 &= 2 \cdot 3 \cdot 13, & 21 &= 3 \cdot 7, \\ 19019 &= 7 \cdot 11 \cdot 13 \cdot 19, & 14421 &= 3 \cdot 11 \cdot 19 \cdot 23, & 3553 &= 11 \cdot 17 \cdot 19, \\ 15249 &= 3 \cdot 13 \cdot 17 \cdot 23, & 26 &= 2 \cdot 13, & 8211 &= 3 \cdot 7 \cdot 17 \cdot 23, & 969 &= 3 \cdot 17 \cdot 19, \\ 66 &= 2 \cdot 3 \cdot 11, & 561 &= 3 \cdot 11 \cdot 17, & 1311 &= 3 \cdot 19 \cdot 23, \\ 22 &= 2 \cdot 11, & 759 &= 3 \cdot 11 \cdot 23, & 57 &= 3 \cdot 19, \end{aligned}$$

so  $\lambda_i(s_{ij})$  and  $\lambda_0(s_j)$  are sums of entries of Table 8.13. For  $i > j \geq 1$ , we use the relation

$$\gamma_{ij} + \gamma_{ji} = \lambda_i(-1)\lambda_j(-1),$$

which follows from (4.22), since  $\lambda_i(p_j) = \gamma_{ij} + \eta$  and  $\lambda_j(p_i) = \gamma_{ji} + \eta$  by Corollary 4.14. For example,  $s_{3,10} = 3 \cdot 7 \cdot 17 \cdot 23$  and  $s_3 = 3 \cdot 17 \cdot 23$  give

$$\begin{aligned} \gamma_{3,10} &= \lambda_3(3) + \lambda_3(7) + \lambda_3(17) + \lambda_3(23) + \lambda_0(3) + \lambda_0(17) + \lambda_0(23) \\ &= 1 + 1 + 0 + 0 + 0 + 1 + 0 = 1, \end{aligned}$$

and then  $\gamma_{10,3} = \gamma_{3,10} + \lambda_{10}(-1)\lambda_3(-1) = 1$ . In this way, we obtain Table 8.14. One finds the same values by computing  $\gamma_{ij}$  for  $i > j$  directly from (4.27). The relation  $\lambda_i(p_j) = \gamma_{ij} + \eta$  is Corollary 4.14.  $\square$

The proof shows that the bits (4.34) are the same at every prime specialization in  $\mathcal{P}_7$ , as Remark 4.15 requires. In more detail, the pairs  $\{i, j\}$  that occur in the rows are the  $66 - 6 - 6 = 54$  pairs not contained in  $I_H$  or in  $I_J$ . Eleven of them contain 0 and enter through  $b_j = \Delta_{0j}$  and Lemma 4.12(a); the other 43 enter through  $\Delta_{ji}$  and Lemma 4.12(c). In Table 8.2, the primes 5, 29, 37 occur in the determinants of these pairs and in the  $b_j$  only to even powers, and the primes 41, 47, 59, 61, 109, 241, 409 occur only in determinants of pairs inside  $I_H$  or  $I_J$ . It follows that all the constants have squarefree parts supported on

$$S_0 = \{2, 3, 7, 11, 13, 17, 19, 23\},$$

and every prime of  $S_0$  divides  $W$ . The primes in  $S \setminus S_0$  are needed in  $S$  only for Definition 4.6.

## 8.6 The matrices and the upper bound

We now assemble the matrices  $\mathbf{M}_E(\eta)$  and  $\mathbf{M}_{E'}(\eta)$  of (4.35). The rows of  $\mathbf{M}_E(\eta)$  are the four fixed rows  $f_1^E, \dots, f_4^E$  of Section 8.4, followed by the moving rows  $r_0^E, r_1^E, r_2^E, r_3^E$  and  $r_8^E, r_9^E, r_{10}^E, r_{11}^E$ ; the rows of  $\mathbf{M}_{E'}(\eta)$  are the six fixed rows  $f_1^{E'}, \dots, f_6^{E'}$ , followed by  $r_0^{E'}, \dots, r_3^{E'}$  and  $r_4^{E'}, \dots, r_7^{E'}$ . The matrix  $\mathbf{M}_E(\eta)$  has  $4 + 4 + 4 = 12$  rows, and  $\mathbf{M}_{E'}(\eta)$  has  $6 + 4 + 4 = 14$  rows; the two counts differ because  $E'$  has conditions at 7, 13 and  $\infty$ . By Corollary 4.14, the entries of the moving rows of  $\mathbf{M}_\star(0)$  are as follows.

- In a constant column  $g$ , the row at  $p_i$  has the entry  $\lambda_i(g)$  of Table 8.13.
- In the row at  $p_i$  and the moving column  $j \neq i$ , the entry is  $\gamma_{ij}$ , from Table 8.14.
- For  $i \in I_F$ , the entry in the moving column  $i$  is the bit  $\gamma_{ii}^\star = \lambda_i(\kappa_\star) + \sum_{j \in G_\star \setminus \{i\}} \gamma_{ij}$  of (4.28); Table 8.16 lists these bits.

The matrices  $\mathbf{M}_E(0)$  and  $\mathbf{M}_{E'}(0)$  are displayed in Tables 8.17 and 8.18. The integer row codes under which the program of Appendix A stores them are listed in Table A.4.

Table 8.16. The diagonal bits  $\gamma_{ii}^E$  and  $\gamma_{ii}^{E'}$  for  $i \in I_F$ . The sums are over  $j \in G_\star \setminus \{i\}$ , modulo 2, and  $\lambda_i(\kappa_E) = \lambda_i(-2)$ ,  $\lambda_i(\kappa_{E'}) = \lambda_i(3)$ .

| $i$ | $E, \kappa_E, G_E = I_F \cup I_H$ |                      |          | $E', \kappa_{E'}, G_{E'} = I_F \cup I_J$ |                      |          |
|-----|-----------------------------------|----------------------|----------|------------------------------------------|----------------------|----------|
|     | $\lambda_i(-2)$                   | $\sum_j \gamma_{ij}$ | diagonal | $\lambda_i(3)$                           | $\sum_j \gamma_{ij}$ | diagonal |
| 0   | 0                                 | 1                    | 1        | 0                                        | 1                    | 1        |
| 1   | 0                                 | 1                    | 1        | 0                                        | 0                    | 0        |
| 2   | 0                                 | 0                    | 0        | 1                                        | 1                    | 0        |
| 3   | 0                                 | 1                    | 1        | 1                                        | 1                    | 0        |

**Dependence on  $\eta$ .** By (4.35), every moving row of  $\mathbf{M}_\star(1)$  is the corresponding row of  $\mathbf{M}_\star(0)$  plus  $u_\star$ , where  $u_E$  and  $u_{E'}$  are the indicator vectors of the eight moving columns:

$$u_E = u_{E'} = (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1).$$

In words,  $\mathbf{M}_\star(1)$  is obtained from  $\mathbf{M}_\star(0)$  by replacing every entry of the lower right block of Table 8.17 or Table 8.18 (moving rows, moving columns) by its complement. The fixed rows and the constant columns do not depend on  $\eta$ . As explained in Corollary 4.14, this reflects the fact that every cross symbol  $\lambda_i(p_j)$  equals  $\gamma_{ij} + \eta$ , and that an odd number (seven) of cross symbols enter each diagonal entry.

**The repeated row.** The rows  $r_5^{E'}(0)$  and  $r_6^{E'}(0)$  of  $\mathbf{M}_{E'}(0)$  are equal. This is not an error: the two rows are the conditions at the two different primes  $p_5$  and  $p_6$ , and they happen to coincide. Indeed,  $p_5$  and  $p_6$  have the same residues modulo 8 and 3, the residues 6 and 5

Table 8.17. The matrix  $\mathbf{M}_E(0)$  in the basis  $\mathcal{B}_E$ : the four fixed rows  $f_k^E$ , with the place and the linear map that define them, and the moving rows  $r_i^E(0)$  at the primes  $p_i$  with  $i \in I_F$  and with  $i \in I_J$ .

|               |                  | -1 | 2 | 3 | 7 | 13 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $p_7$ |
|---------------|------------------|----|---|---|---|----|-------|-------|-------|-------|-------|-------|-------|-------|
| $f_1^E$       | $(2, e_1 + e_2)$ | 1  | 1 | 1 | 1 | 0  | 0     | 1     | 0     | 1     | 1     | 0     | 0     | 1     |
| $f_2^E$       | $(2, e_3)$       | 0  | 0 | 1 | 0 | 1  | 0     | 1     | 0     | 1     | 1     | 1     | 1     | 1     |
| $f_3^E$       | $(3, \chi_3)$    | 1  | 1 | 0 | 0 | 0  | 0     | 1     | 1     | 0     | 0     | 0     | 0     | 0     |
| $f_4^E$       | $(3, \nu_3)$     | 0  | 0 | 1 | 0 | 0  | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     |
| $r_0^E(0)$    | $p_0$            | 0  | 0 | 0 | 0 | 0  | 1     | 0     | 0     | 1     | 1     | 0     | 0     | 1     |
| $r_1^E(0)$    | $p_1$            | 1  | 1 | 0 | 1 | 1  | 0     | 1     | 1     | 0     | 0     | 0     | 0     | 0     |
| $r_2^E(0)$    | $p_2$            | 0  | 0 | 1 | 0 | 1  | 0     | 1     | 0     | 1     | 0     | 0     | 0     | 0     |
| $r_3^E(0)$    | $p_3$            | 1  | 1 | 1 | 1 | 1  | 1     | 1     | 1     | 1     | 0     | 1     | 1     | 0     |
| $r_8^E(0)$    | $p_8$            | 1  | 0 | 0 | 1 | 0  | 0     | 0     | 0     | 1     | 1     | 1     | 1     | 1     |
| $r_9^E(0)$    | $p_9$            | 0  | 1 | 1 | 0 | 1  | 1     | 0     | 0     | 0     | 1     | 1     | 1     | 1     |
| $r_{10}^E(0)$ | $p_{10}$         | 0  | 1 | 0 | 0 | 1  | 0     | 1     | 1     | 1     | 0     | 0     | 0     | 0     |
| $r_{11}^E(0)$ | $p_{11}$         | 1  | 0 | 0 | 0 | 1  | 1     | 0     | 0     | 0     | 0     | 1     | 1     | 0     |

Table 8.18. The matrix  $\mathbf{M}_{E'}(0)$  in the basis  $\mathcal{B}_{E'}$ : the six fixed rows  $f_k^{E'}$ , with the place and the linear map that define them, and the moving rows  $r_i^{E'}(0)$  at the primes  $p_i$  with  $i \in I_F$  and with  $i \in I_H$ .

|               |                        | -1 | 2 | 3 | 7 | 13 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_8$ | $p_9$ | $p_{10}$ | $p_{11}$ |
|---------------|------------------------|----|---|---|---|----|-------|-------|-------|-------|-------|-------|----------|----------|
| $f_1^{E'}$    | $(2, e_1 + e_3)$       | 1  | 0 | 0 | 1 | 1  | 0     | 0     | 0     | 0     | 1     | 1     | 1        | 1        |
| $f_2^{E'}$    | $(7, \chi_7)$          | 1  | 0 | 1 | 0 | 1  | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 1        |
| $f_3^{E'}$    | $(7, \nu_7)$           | 0  | 0 | 0 | 1 | 0  | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| $f_4^{E'}$    | $(13, \chi_{13})$      | 0  | 1 | 0 | 1 | 0  | 0     | 1     | 1     | 1     | 0     | 1     | 1        | 1        |
| $f_5^{E'}$    | $(13, \nu_{13})$       | 0  | 0 | 0 | 0 | 1  | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| $f_6^{E'}$    | $(\infty, \text{sgn})$ | 1  | 0 | 0 | 0 | 0  | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| $r_0^{E'}(0)$ | $p_0$                  | 0  | 0 | 0 | 0 | 0  | 1     | 0     | 0     | 1     | 0     | 1     | 0        | 1        |
| $r_1^{E'}(0)$ | $p_1$                  | 1  | 1 | 0 | 1 | 1  | 0     | 0     | 1     | 0     | 1     | 0     | 1        | 1        |
| $r_2^{E'}(0)$ | $p_2$                  | 0  | 0 | 1 | 0 | 1  | 0     | 1     | 0     | 1     | 0     | 0     | 1        | 0        |
| $r_3^{E'}(0)$ | $p_3$                  | 1  | 1 | 1 | 1 | 1  | 1     | 1     | 1     | 0     | 0     | 0     | 1        | 1        |
| $r_4^{E'}(0)$ | $p_4$                  | 1  | 1 | 1 | 1 | 1  | 1     | 1     | 0     | 1     | 0     | 1     | 0        | 1        |
| $r_5^{E'}(0)$ | $p_5$                  | 0  | 1 | 0 | 1 | 1  | 0     | 0     | 0     | 1     | 1     | 1     | 0        | 1        |
| $r_6^{E'}(0)$ | $p_6$                  | 0  | 1 | 0 | 1 | 1  | 0     | 0     | 0     | 1     | 1     | 1     | 0        | 1        |
| $r_7^{E'}(0)$ | $p_7$                  | 1  | 1 | 1 | 0 | 0  | 1     | 1     | 0     | 1     | 0     | 1     | 0        | 1        |

modulo 7 are both nonsquares, and the residues 5 and 11 modulo 13 are both nonsquares; so the constant entries agree. The cross entries agree because  $s_5 = s_6$ ,  $s_{j5} = s_{j6}$  for  $j = 1, 2, 3$ , and  $s_{5j} = s_{6j}$  for  $j = 8, \dots, 11$  (Table 8.15), and because  $\lambda_5(q) = \lambda_6(q)$  for the primes  $q \in \{2, 3, 11, 19, 23\}$  that divide the last four constants (Table 8.13). Since both rows change by  $u_{E'}$  when  $\eta$  changes, they also coincide at  $\eta = 1$ . This explains the two equal consecutive codes in each of the two lists for  $E'$  in Table A.4. The repeated row adds nothing to the rank, and the certificate below does not use  $r_6^{E'}(0)$ .

**Lemma 8.8** (Rank certificates). *For every prime specialization in  $\mathcal{P}_7 \cap \mathcal{K}_7$ , we have*

$$\text{rank } \mathbf{M}_E(0) = 8 = n_E - 5, \quad \text{rank } \mathbf{M}_{E'}(0) = 9 = n_{E'} - 4.$$

Moreover,

$$u_E = f_4^E + r_9^E(0) + r_{10}^E(0), \quad u_{E'} = f_4^{E'} + f_5^{E'} + r_0^{E'}(0) + r_5^{E'}(0), \quad (8.16)$$

where the rows are those of  $\mathbf{M}_E(0)$  and  $\mathbf{M}_{E'}(0)$ . Each of these sums contains exactly two moving rows.

*Proof.* By Lemmas 8.6 and 8.7, the matrices  $\mathbf{M}_E(0)$  and  $\mathbf{M}_{E'}(0)$  are those of Tables 8.17 and 8.18 for every prime specialization in  $\mathcal{P}_7 \cap \mathcal{K}_7$ .

We begin with the lower bound on the rank of  $\mathbf{M}_E(0)$ . We take the rows  $f_4^E$ ,  $r_0^E(0)$ ,  $r_2^E(0)$ ,  $f_2^E$ ,  $r_{11}^E(0)$ ,  $r_9^E(0)$ ,  $r_{10}^E(0)$ ,  $r_8^E(0)$  and the columns 3,  $p_0$ ,  $p_1$ ,  $p_5$ ,  $-1$ , 2,  $p_2$ , 7 of Table 8.17, in this order. The corresponding submatrix is

|               | 3 | $p_0$ | $p_1$ | $p_5$ | $-1$ | 2 | $p_2$ | 7 |
|---------------|---|-------|-------|-------|------|---|-------|---|
| $f_4^E$       | 1 | 0     | 0     | 0     | 0    | 0 | 0     | 0 |
| $r_0^E(0)$    | 0 | 1     | 0     | 0     | 0    | 0 | 0     | 0 |
| $r_2^E(0)$    | 1 | 0     | 1     | 0     | 0    | 0 | 0     | 0 |
| $f_2^E$       | 1 | 0     | 1     | 1     | 0    | 0 | 0     | 0 |
| $r_{11}^E(0)$ | 0 | 1     | 0     | 1     | 1    | 0 | 0     | 0 |
| $r_9^E(0)$    | 1 | 1     | 0     | 1     | 0    | 1 | 0     | 0 |
| $r_{10}^E(0)$ | 0 | 0     | 1     | 0     | 0    | 1 | 1     | 0 |
| $r_8^E(0)$    | 0 | 0     | 0     | 1     | 1    | 0 | 0     | 1 |

This submatrix has ones on the diagonal and zeros above it. Its determinant is therefore 1, and  $\text{rank } \mathbf{M}_E(0) \geq 8$ . For  $\mathbf{M}_{E'}(0)$ , we take the rows  $f_6^{E'}$ ,  $f_3^{E'}$ ,  $f_5^{E'}$ ,  $f_1^{E'}$ ,  $r_5^{E'}(0)$ ,  $f_2^{E'}$ ,  $r_2^{E'}(0)$ ,  $r_0^{E'}(0)$ ,  $f_4^{E'}$  and the columns  $-1$ , 7, 13,  $p_8$ , 2, 3,  $p_1$ ,  $p_0$ ,  $p_2$  of Table 8.18, in this order. The

corresponding submatrix is

|               | -1 | 7 | 13 | $p_8$ | 2 | 3 | $p_1$ | $p_0$ | $p_2$ |
|---------------|----|---|----|-------|---|---|-------|-------|-------|
| $f_6^{E'}$    | 1  | 0 | 0  | 0     | 0 | 0 | 0     | 0     | 0     |
| $f_3^{E'}$    | 0  | 1 | 0  | 0     | 0 | 0 | 0     | 0     | 0     |
| $f_5^{E'}$    | 0  | 0 | 1  | 0     | 0 | 0 | 0     | 0     | 0     |
| $f_1^{E'}$    | 1  | 1 | 1  | 1     | 0 | 0 | 0     | 0     | 0     |
| $r_5^{E'}(0)$ | 0  | 1 | 1  | 1     | 1 | 0 | 0     | 0     | 0     |
| $f_2^{E'}$    | 1  | 0 | 1  | 0     | 0 | 1 | 0     | 0     | 0     |
| $r_2^{E'}(0)$ | 0  | 0 | 1  | 0     | 0 | 1 | 1     | 0     | 0     |
| $r_0^{E'}(0)$ | 0  | 0 | 0  | 0     | 0 | 0 | 0     | 1     | 0     |
| $f_4^{E'}$    | 0  | 1 | 0  | 0     | 1 | 0 | 1     | 0     | 1     |

which again has ones on the diagonal and zeros above it. This gives  $\text{rank } \mathbf{M}_{E'}(0) \geq 9$ .

For the upper bound, recall from Lemma 3.10 and Lemma 4.11 that every row of  $\mathbf{M}_\star(\eta)$  annihilates every class in  $\delta_\star(\star(\mathbb{Q}))$ , where  $\eta$  is the sign of the specialization. Each vector of Table 8.6 has an even number of entries equal to 1 in the moving columns (four or eight), so its dot product with  $u_\star$  vanishes. Since a moving row of  $\mathbf{M}_\star(\eta)$  differs from the corresponding row of  $\mathbf{M}_\star(0)$  by  $\eta u_\star$ , every row of  $\mathbf{M}_\star(0)$  also annihilates these vectors. By Lemma 8.3, the five vectors of Table 8.6 on  $E$  are therefore independent elements of the kernel of  $\mathbf{M}_E(0)$ , which implies that  $\text{rank } \mathbf{M}_E(0) \leq 13 - 5 = 8$ . Similarly,  $\text{rank } \mathbf{M}_{E'}(0) \leq 13 - 4 = 9$ . One can also check directly that each vector of Table 8.6 has even dot product with each row of Table 8.17 or Table 8.18.

Finally, we verify (8.16). The rows involved, copied from Tables 8.17 and 8.18, and their sums modulo 2 are

|               | -1 | 2 | 3 | 7 | 13 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $p_7$ |
|---------------|----|---|---|---|----|-------|-------|-------|-------|-------|-------|-------|-------|
| $f_4^E$       | 0  | 0 | 1 | 0 | 0  | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     |
| $r_9^E(0)$    | 0  | 1 | 1 | 0 | 1  | 1     | 0     | 0     | 0     | 1     | 1     | 1     | 1     |
| $r_{10}^E(0)$ | 0  | 1 | 0 | 0 | 1  | 0     | 1     | 1     | 1     | 0     | 0     | 0     | 0     |
| sum           | 0  | 0 | 0 | 0 | 0  | 1     | 1     | 1     | 1     | 1     | 1     | 1     | 1     |

and

|               | -1 | 2 | 3 | 7 | 13 | $p_0$ | $p_1$ | $p_2$ | $p_3$ | $p_8$ | $p_9$ | $p_{10}$ | $p_{11}$ |
|---------------|----|---|---|---|----|-------|-------|-------|-------|-------|-------|----------|----------|
| $f_4^{E'}$    | 0  | 1 | 0 | 1 | 0  | 0     | 1     | 1     | 1     | 0     | 1     | 1        | 1        |
| $f_5^{E'}$    | 0  | 0 | 0 | 0 | 1  | 0     | 0     | 0     | 0     | 0     | 0     | 0        | 0        |
| $r_0^{E'}(0)$ | 0  | 0 | 0 | 0 | 0  | 1     | 0     | 0     | 1     | 0     | 1     | 0        | 1        |
| $r_5^{E'}(0)$ | 0  | 1 | 0 | 1 | 1  | 0     | 0     | 0     | 1     | 1     | 1     | 0        | 1        |
| sum           | 0  | 0 | 0 | 0 | 0  | 1     | 1     | 1     | 1     | 1     | 1     | 1        | 1        |

The two sums are  $u_E$  and  $u_{E'}$ . This completes the proof.  $\square$

Since each sum in (8.16) contains two moving rows, Lemma 4.17 shows that  $\mathbf{M}_\star(0)$  and  $\mathbf{M}_\star(1)$  have the same row space, hence the same rank and kernel. This is the equality of the reduced row bases for  $\varepsilon = \pm 1$  that the program of Appendix A checks. Since the kernel of  $\mathbf{M}_E(0)$  has dimension  $13 - 8 = 5$  and contains the five independent vectors of Table 8.6, it is their span; likewise, the kernel of  $\mathbf{M}_{E'}(0)$  is spanned by the four vectors of Table 8.6 on  $E'$ .

## 8.7 Exact rank and infinitude

**Theorem 8.9** (Exact rank seven). *Let  $(M, N) \in \mathcal{P}_7 \cap \mathcal{K}_7$  be a prime specialization of  $\mathfrak{D}_7$  with respect to the set  $S$  of (8.4). Then  $d_E = 5$ ,  $d_{E'} = 4$  and  $\text{rank } E_{M,N}(\mathbb{Q}) = 7$ . Moreover, there exist infinitely many such  $(M, N)$ , and the curves  $E_{M,N}$  obtained from them represent infinitely many  $\overline{\mathbb{Q}}$ -isomorphism classes.*

*Proof.* We apply Proposition 4.18 to the datum  $\mathfrak{D}_7$ , the set  $S$  of (8.4), and the set  $\mathcal{P}$  of prime specializations in  $\mathcal{P}_7 \cap \mathcal{K}_7$ . We check its hypotheses. By Lemma 8.1,  $\Gamma_E = \Gamma_{E'} = (-1, 2, 3, 7, 13)$  consists of  $-1$  and distinct primes, and by (8.6) it contains every prime dividing  $\kappa_E$  and  $\kappa_{E'}$ .

- (i) By Lemma 8.6, at the places 2 and 3 for  $E$  and 2, 7, 13 and  $\infty$  for  $E'$ , the local images lie in subgroups that do not depend on  $(M, N) \in \mathcal{P}$ . The fixed rows of Section 8.4 are the rows in the sense of Definition 3.9 defined by these subgroups and the linear maps listed there. Their entries depend only on the residues of the  $p_i$ , which are constant on  $\mathcal{P}_7$  by Lemma 8.4. This proves (i).
- (ii) By Lemma 8.7, the bits (4.34) are the same for all  $(M, N) \in \mathcal{P}$ , which is (ii). The resulting matrices  $\mathbf{M}_E(0)$  and  $\mathbf{M}_{E'}(0)$  are those of Tables 8.17 and 8.18.
- (iii) The points  $T, P_1, \dots, P_4$  on  $E$  and  $T', Q_1, Q_2, Q_3$  on  $E'$  are given by the formulas of Lemma 8.2, and their classes are independent at every prime specialization by Lemma 8.3. This proves (iii) with  $k_E = 5$  and  $k_{E'} = 4$ .
- (iv) By Lemma 8.8,  $\text{rank } \mathbf{M}_E(0) = 13 - 5$  and  $\text{rank } \mathbf{M}_{E'}(0) = 13 - 4$ , and  $u_E$  and  $u_{E'}$  are sums of rows of  $\mathbf{M}_E(0)$  and  $\mathbf{M}_{E'}(0)$  that contain exactly two moving rows. This is (iv).

Proposition 4.18 now implies that  $d_E = 5$ ,  $d_{E'} = 4$  and  $\text{rank } E_{M,N}(\mathbb{Q}) = 5 + 4 - 2 = 7$  for every  $(M, N) \in \mathcal{P}$ . It also shows that  $\delta_E(E(\mathbb{Q}))$  and  $\delta_{E'}(E'(\mathbb{Q}))$  are spanned by the classes of Table 8.5.

For the infinitude, we check the hypotheses of Proposition 5.5 for  $W$ ,  $(M_0, N_0)$  and the cone  $\mathcal{K}_7$ .

- (a) The primes dividing some  $c_i$  are 2 and 3, and they divide  $W$ . We have  $v_2(W) = 9 > 6 = \max_i v_2(c_i)$  and  $v_3(W) = 4 > 3 = \max_i v_3(c_i)$ , and  $v_q(c_i) = 0$  for the other

primes  $q \mid W$ . By Lemma 8.4 applied to  $(M_0, N_0) \in \mathcal{P}_7$ , every  $c_i$  divides  $L_i(M_0, N_0)$ , and  $L_i(M_0, N_0)/c_i$  is prime to  $W$ .

- (b) The only prime  $q \leq 11$  that does not divide  $W$  is  $q = 5$ . At  $(m, n) = (1, 1)$ , the values  $L_i(1, 1) = a_i + b_i$  are congruent to

$$1, 1, 4, 4, 3, 2, 3, 3, 1, 1, 4, 4$$

modulo 5, and their product is not divisible by 5.

- (c) By Lemma 8.5, every  $L_i$  is positive on  $\mathcal{K}_7$ .

Proposition 5.5 now implies that there exist infinitely many prime specializations  $(M, N) \in \mathcal{K}_7$  with  $(M, N) \equiv (M_0, N_0) \pmod{W}$ , and their ratios  $M/N$  take infinitely many values. By Lemma 4.3(c), the curves  $E_{M,N}$  for these pairs lie in infinitely many isomorphism classes over  $\overline{\mathbb{Q}}$ . In the present case, the  $j$ -invariant of Lemma 4.3 is

$$j(E_{M,N}) = \frac{256 (91205^2 F + 3 \cdot 33124 H)^3}{9 \cdot 33124^2 H^2 J}.$$

This completes the proof. □

## Proof of the main theorem

In this section, we deduce Theorem 1.1 from Theorems 6.7, 7.8, and 8.9, which are proved in Sections 6 to 8. We then list the results on which these three theorems rest, as a guide to the paper.

*Proof of Theorem 1.1.* Let  $r \in \{5, 6, 7\}$ , and let  $\mathfrak{D}_r$ ,  $\mathcal{P}_r$  and  $\mathcal{K}_r$  be the datum, the congruence class and the cone of Section 6, Section 7 or Section 8, respectively. Let  $\mathcal{E}_r$  be the set of curves  $E_{M,N}$ , where  $(M, N)$  runs over the prime specializations of  $\mathfrak{D}_r$  that lie in  $\mathcal{P}_r \cap \mathcal{K}_r$ , with respect to the set  $S$  fixed in that section. Each curve in  $\mathcal{E}_r$  is an elliptic curve over  $\mathbb{Q}$  (Lemma 4.8). By Theorem 6.7 if  $r = 5$ , Theorem 7.8 if  $r = 6$ , and Theorem 8.9 if  $r = 7$ , every curve in  $\mathcal{E}_r$  has rank  $r$  over  $\mathbb{Q}$ , and the curves in  $\mathcal{E}_r$  represent infinitely many isomorphism classes over  $\overline{\mathbb{Q}}$ . Choosing one curve of  $\mathcal{E}_r$  in each of these classes, we obtain infinitely many elliptic curves over  $\mathbb{Q}$  of rank  $r$ , pairwise nonisomorphic over  $\overline{\mathbb{Q}}$ . This completes the proof.  $\square$

*Remark 9.1* (The structure of the proof). In each family, the rank statement is deduced from Proposition 4.18, and the infinitude statement from Proposition 5.5. Table 9.1 lists the results that verify the hypotheses of these two propositions.

The proof of Proposition 4.18 combines the ambient bases of Lemma 4.8, the rows at the moving primes of Lemma 4.11 (which rest on Lemmas 3.8 and 4.9), their dependence on the sign  $\varepsilon$  (Corollary 4.14, which rests on Lemma 4.12), the upper bound of Lemma 3.10, the comparison of the two signs in Lemma 4.17, Corollary 3.13, and the rank formula of Lemma 3.5. The proof of Proposition 5.5 combines Theorem 5.1 with Lemmas 5.3 and 5.4, and it uses Lemma 4.3 for the  $j$ -invariants.

Besides elementary arguments, the proof uses the following results from the literature: the Mordell–Weil theorem [43, Theorem VIII.6.7], in the proof of Lemma 3.5; the basic properties of the isogenies  $\phi$  and  $\hat{\phi}$  in Proposition 3.4(a); the formulas for  $c_4$  and  $\Delta$  and the classification of elliptic curves over  $\overline{\mathbb{Q}}$  by their  $j$ -invariant, in Lemmas 4.2 and 4.3; quadratic reciprocity and its supplementary laws (4.22); and the theorem of Green and Tao on linear equations in primes [18], with its inputs from [16, 17], in Theorem 5.1. The geometric description of the surfaces in Remark 4.5, which is not used in the arithmetic rank or infinitude proof, additionally uses Tate’s algorithm [49] and the elliptic-surface formulas in [40].

Table 9.1. The results that verify the hypotheses of Proposition 4.18 (items (i)–(iv)) and of Proposition 5.5 in the three families.

|                           | Rank five          | Rank six           | Rank seven            |
|---------------------------|--------------------|--------------------|-----------------------|
| Datum and identity        | Section 6.1        | Section 7.1        | Lemma 8.1             |
| (iii) Points              | Lemmas 6.1 and 6.2 | Lemmas 7.1 and 7.2 | Lemmas 8.2 and 8.3    |
| Congruence class          | Lemma 6.3          | Lemma 7.3          | Lemma 8.4             |
| Positivity on the cone    | Lemma 6.4          | Lemma 7.4          | Lemma 8.5             |
| Primes $q \leq 11$        | divide $W$         | divide $W$         | $q = 5$ : Theorem 8.9 |
| (i) Fixed rows            | Lemma 6.5          | Lemma 7.5          | Lemma 8.6             |
| (ii) Characters           | Section 6.5        | Lemma 7.6          | Lemma 8.7             |
| (iv) Ranks                | Lemma 6.6          | Lemma 7.7          | Lemma 8.8             |
| Exact rank and infinitude | Theorem 6.7        | Theorem 7.8        | Theorem 8.9           |

## Computer verification

The finite computations in Sections 6 to 8 are stated there precisely enough to be checked by hand or with any computer algebra system. In this appendix, we describe three programs, one for each family, that check them. The programs and their inputs are available in the GitHub repository <https://github.com/pmaronow/ec567-palomar>. In Appendix A.1, we explain how to run the programs. In Appendix A.2, we describe how they encode squareclasses, matrix rows, and the free sign. In Appendices A.3 and A.4, we list what the programs check and what they do not check. Finally, in Appendix A.5, we give the integer codes under which the programs store the matrices of Sections 6 to 8, so that a reader can match the matrices of the text with the input files.

The programs check finite arithmetic only. The arguments that hold uniformly in the parameters are proved in the text, and the programs do not check them. These arguments are the results of Sections 3 and 4, the fixed-place lemmas Lemmas 6.5, 7.5, and 8.6, and the results of Section 5 on prime values. They also include the fact that the residues used in the fixed-place lemmas are constant on the congruence class of each family (by Lemma 4.7 and the congruences that define the class), and the computation of the  $j$ -invariant (Lemma 4.3). In each family, we deduce the rank from Proposition 4.18. Its proof combines three facts: the image of the descent map lies in the span of the ambient basis, its elements satisfy the local conditions at the fixed places and at the moving primes, and it contains the classes of the rational points. The programs check the finite inputs to this argument, namely the identities satisfied by the points, the matrices and their ranks, and the classes of the points.

### A.1 Running the programs

The programs and their inputs are the following files, relative to the repository directory `manuscript/source/certificates`:

- `rank5/verify_final155_certificate.py`, with input `rank5/final155_certificate.json`, for the rank-five family (Section 6);
- `rank6/verify_rank6_certificate.py`, with input `rank6/rank6_certificate.json`, for the rank-six family (Section 7);
- `rank7/verify_rank7_certificate.py`, with input `rank7/rank7_certificate.json`, for the rank-seven family (Section 8).

Each program reads its input from its own directory and uses only the standard library of Python. The programs require Python 3.10 or later, because they use the method `int.bit_count`, which was introduced in that version; under Python 3.9, the first call to this method raises an `AttributeError`. From the repository directory `manuscript/source`, the commands are

```
python3 -I certificates/rank5/verify_final155_certificate.py
python3 -I certificates/rank6/verify_rank6_certificate.py
python3 -I certificates/rank7/verify_rank7_certificate.py
```

where `python3` denotes an interpreter of version 3.10 or later. The option `-I` runs the interpreter in isolated mode: it ignores the environment variables of Python and does not add the directory of the script or the user's site-packages directory to the module search path.

Each program consists of assertions. If one of them fails, the program stops with an `AssertionError` and a nonzero exit status. If all of them hold, the program prints the ranks of its four matrices and their reduced row bases, followed by a line that begins with `PASS`. The rank-seven program also writes a report, `rank7_certificate_output.json`, into its own directory, replacing the file of that name, so this directory must be writable. The script `manuscript/source/build.py` in the repository runs the three programs in turn, with the interpreter that runs `build.py`, stops at the first failure, and writes their combined output to the file `manuscript/source/verification_output.txt`. It then compiles this paper with `pdflatex` and `bibtex`.

## A.2 Conventions

**Row codes.** The programs store a vector  $r = (r_0, \dots, r_{n-1}) \in \mathbb{F}_2^n$ , either a row of a matrix or the vector of exponents of a squareclass in the ambient basis, as the integer  $\sum_k r_k 2^k$ . Recall that the ambient basis is  $\mathcal{B}_\star = (\Gamma_\star; p_j \ (j \in G_\star))$ . The programs number its elements from 0, first the constants of  $\Gamma_\star$  and then the  $p_j$  in increasing order of  $j$ , and the columns are numbered in the same way. For example, in the rank-five family, the columns of  $\mathbf{M}_E(\eta)$  are  $-1, 2, 3, 5, p_0, \dots, p_7$ , and the code  $267 = 2^0 + 2^1 + 2^3 + 2^8$  is the row with entries 1 in the columns of  $-1, 2, 5$ , and  $p_4$ . This is the condition at 3 on the unit part of a class, that is, the fixed row  $f_3^E$  of Table 6.14: the Legendre symbols modulo 3 of  $-1, 2, 5$ , and  $p_4 \equiv 2 \pmod{3}$  equal  $-1$ , those of  $p_0, \dots, p_3, p_5, p_6, p_7 \equiv 1 \pmod{3}$  equal 1, and 3 has unit part 1. The vector  $u_\star$  of moving columns has code  $2^n - 2^{n-8}$ , that is, 4080 in the rank-five and rank-six families and 8160 in the rank-seven family.

**The free sign.** The programs encode the sign  $\varepsilon$  by a bit  $e \in \{0, 1\}$  with  $\varepsilon = (-1)^e$ , so  $e$  is the number  $\eta$  of Corollary 4.14. The matrices stored under keys ending in 0 ( $E0$  and  $Ep0$ ) are  $\mathbf{M}_E(0)$  and  $\mathbf{M}_{E'}(0)$ , for  $\varepsilon = 1$ ; those under keys ending in 1 are  $\mathbf{M}_E(1)$  and  $\mathbf{M}_{E'}(1)$ ,

for  $\varepsilon = -1$ . The letters  $E$  and  $E_p$  refer to  $E$  and  $E'$ . The program for the rank-five family prints `epsilon=0` and `epsilon=1` for these two cases.

**Local coordinates.** To build the rows at a fixed place  $v$ , the programs give coordinates to each element of the ambient basis in  $\mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2}$ . For an odd prime  $p$ , the class of  $z = p^k u_0$  with  $u_0$  a unit has the code  $\chi_p(z) + 2v_p(z) = \chi_p(u_0) + 2(k \bmod 2)$ , with the coordinates  $v_p$  and  $\chi_p$  of (3.3); these are the coordinates of Lemma 3.2, in the opposite order. For  $p = 2$ , the class  $[(-1)^{e_1} 2^{e_2} 5^{e_3}]$  has the code  $e_1 + 2e_2 + 4e_3$ ; in particular, odd units congruent to 1, 3, 5, and 7 modulo 8 have the codes 0, 5, 4, and 1. A fixed row is the composition of the coordinate map with a linear map that vanishes on the local subgroup given by the fixed-place lemma of the family.

**Characters at the moving primes.** The programs compute the characters  $\lambda_i(-1)$ ,  $\lambda_i(2)$ , and  $\lambda_i(q)$  for the odd primes  $q$  dividing  $W$  from the residues of the  $p_i$  on the congruence class, using quadratic reciprocity. The primes of  $S$  that do not divide  $W$  are not controlled by the congruence class. For these primes, the programs assign auxiliary values to the characters  $\lambda_i(q)$ , computed from a residue class chosen for this purpose. Note that these values are not congruence conditions on  $(M, N)$ , and that the programs check that no row depends on them (Appendix A.3). The input file of the rank-five family stores these residue classes under `reference_character_states`. The input file of the rank-six family stores them under `states`, and the congruences that define the progression under `moduli`. The program for the rank-seven family computes them itself.

### A.3 What the programs check

We list the checks in Table A.1. The programs compute the local data at a representative pair. In the rank-five family, this pair is  $(M_0, -1)$ , which lies in the congruence class. In the rank-six family, it is  $(19, 11)$ , which is congruent to  $(M_0, N_0)$  modulo 64, 81, and 7; the cofactors are also checked at  $(M_0, N_0)$ . In the rank-seven family, it is  $(18, 11)$ , which is congruent to  $(M_0, N_0)$  modulo 512, 81, 7, and 13.

In terms of the subsections of Sections 6 to 8, the programs check the coefficients and the identity  $A^2F + 4BH = CJ$  of the datum; the rational points and their classes; the values  $W$ ,  $M_0$ , and  $N_0$ , the cofactors, and the residues of the  $p_i$  that enter the rows; the residues used in the fixed-place lemma, at the representative pair; the characters at the moving primes; and the matrices, their ranks, and their kernels. The arguments in these subsections that apply to every pair of the congruence class are not checked by the programs. We now comment on some of the entries of Table A.1.

**Polynomial identities.** The coordinates of each rational point are homogeneous in  $(M, N)$ , of degree 4 for  $x$  and 6 for  $y$ , and the coefficients of  $x^2$  and  $x$  in the equations have degrees 4 and 8. After we clear the constant denominators, the differ-

| Check                                                                                                                     | Rank five | Rank six   | Rank seven   |
|---------------------------------------------------------------------------------------------------------------------------|-----------|------------|--------------|
| $(a_i, b_i)$ primitive; all 66 values $\Delta_{ij}$ nonzero and factored over $S$ ; $b_i$ ( $i \geq 1$ ) supported on $S$ | yes       | yes        | yes          |
| The identity $A^2F + 4BH = CJ$                                                                                            | yes       | yes        | yes          |
| The rational points on $E$ and $E'$                                                                                       | 5         | 6          | 7            |
| The images under $\hat{\phi}$ of the points of $E'$ lie on $E$                                                            | yes       | yes        | yes          |
| Class of each point equal to its stated class                                                                             | table     | table      | yes          |
| The values $W, M_0, N_0$ from the stated congruences                                                                      | yes       | yes        | yes          |
| Cofactors $c_i$ equal to the exact $\{2, 3\}$ -parts of $L_i$ at the representative                                       | yes       | yes        | yes          |
| $q \mid W/c_i$ and $q \nmid L_i(M_0, N_0)/c_i$ for the primes $q \mid W$                                                  | yes       | yes        | yes          |
| $d_q$ at the primes of $S$ not dividing $W$                                                                               | yes       | yes        | no           |
| Some point of $\mathbb{F}_q^2$ avoids all zero sets, for $q \leq 11$                                                      | —         | —          | yes          |
| Positivity of the $L_i$ on the cone                                                                                       | endpoints | no         | at one ratio |
| Residues and valuations used in the fixed-place lemma, at the representative                                              | yes       | yes        | yes          |
| Congruence tests for the local images at the fixed places                                                                 | at 2      | at 2, 3, 7 | no           |
| Rows independent of the characters of the primes of $S$ not dividing $W$                                                  | yes       | yes        | yes          |
| Reciprocity consistency for all 66 pairs                                                                                  | yes       | yes        | yes          |
| The four matrices, rebuilt and compared with the stored codes                                                             | yes       | yes        | yes          |
| Ranks, reduced row bases, kernels spanned by the point classes                                                            | yes       | yes        | yes          |

Table A.1. The checks made by the three programs. “Table” means that the class codes are computed from a table of supports, not from the coordinates of the points. A dash means that the check is not needed, because every prime  $q \leq 11$  divides  $W$ .

ence  $y^2 - x^3 - \alpha x^2 - \beta x$  is therefore a homogeneous polynomial  $P(M, N)$  of degree 12. The polynomial  $P(M, 1)$  has degree at most 12. If it vanishes at the thirteen values  $M = 0, 1, \dots, 12$ , then all its coefficients vanish, and we have  $P = 0$ , including at  $N = 0$ . The programs for the rank-five and rank-six families evaluate  $P(M, 1)$  at these thirteen values in exact rational arithmetic, and the program for the rank-seven family compares the exact rational coefficients of  $P(M, 1)$ . For the identity  $A^2F + 4BH = CJ$ , the rank-five program compares the coefficients of the two sides at  $N = 1$ . The rank-six program checks it at the same thirteen values; five would suffice, since its degree is four. The rank-seven program compares the coefficients of  $(AF)^2 + 4BFH$  and  $CFJ$ , which are  $F$  times the two sides. For the images under  $\hat{\phi}$ , the programs compute  $\hat{\phi}(x, y) = (y^2/(4x^2), y(x^2 - \beta')/(8x^2))$  at the points of  $E'$  and check that the results lie on  $E$ . The rank-five and rank-six programs also compare them with explicit formulas, at the values of  $M$  with  $x \neq 0$ . In the rank-five family, these images are the points of Section 6 that give five independent points on  $E$ ; in the other two families, the text does not use them.

**Local data.** The programs check the residues and valuations used in the fixed-place lemmas at the representative pair. That these residues and valuations are the same at every pair of the congruence class is proved in Sections 6 to 8, and the programs do not check it.

**Congruence tests for local images.** Several programs test which classes of  $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$  pass a necessary condition modulo a power of  $p$  for containing the  $x$ -coordinate of a point. Let  $y^2 = x^3 + \alpha x^2 + \beta x$  with  $\alpha, \beta \in \mathbb{Z}_p$ , and let  $d \in \mathbb{Z}_p \setminus \{0\}$  with  $\beta/d \in \mathbb{Z}_p$ . A point  $(x, y)$  with  $x \neq 0$  in the class of  $d$  can be written as  $x = d(v/s)^2$  with  $v, s \in \mathbb{Z}_p$  not both divisible by  $p$ . Then  $w = ys^3/(dv)$  satisfies

$$w^2 = dv^4 + \alpha v^2 s^2 + (\beta/d)s^4,$$

and  $w \in \mathbb{Z}_p$ . Either  $s$  is a unit, and we may take  $s = 1$ , or  $p \mid s$  and  $v$  is a unit, and we may take  $v = 1$ . If neither case has a solution modulo  $p^k$ , then no point with  $x \neq 0$  has  $x$  in the class of  $d$ . When  $\beta$  is a unit and  $d$  has odd valuation, the class is excluded by valuations instead. A class that passes the test need not lie in the local image, so these tests confirm the upper bounds of the fixed-place lemmas but do not prove them. The rank-five program performs the test at  $p = 2$  modulo  $2^6$ . It does so at each of the sixteen pairs  $(54 + 64r, -1 + 64s)$  with  $0 \leq r, s \leq 3$ , which represent the classes modulo 256 of the pairs congruent to  $(54, -1)$  modulo 64. The passing classes are  $\{1, 2\}$  on  $E$  and  $\{1, -1, 2, -2\}$  on  $E'$ , which are the subgroups of Lemma 6.5. The rank-six program performs the test modulo  $2^9, 3^5$ , and  $7^3$  at the single pair  $(19, 11)$ , and it builds its fixed rows from the passing classes, which are the subgroups of Lemma 7.5. The rank-seven program does not perform this test. Instead, it checks the finite computations in the proof

of Lemma 8.6 at 2: which odd residues modulo 8 solve the two congruences of that proof, and which classes the integers  $s^2 + 2r^2$  with  $s$  or  $r$  odd represent.

**Characters and reciprocity.** Each entry of a moving row is a sum in  $\mathbb{F}_2$  of characters  $\lambda_i(z)$  of fixed integers  $z$ , of cross symbols, and of  $\eta$  (Lemmas 4.11 and 4.12). It is therefore an affine function over  $\mathbb{F}_2$  of the characters  $\lambda_i(q)$  of the primes  $q$  of  $S$  that do not divide  $W$ . The rank-five and rank-six programs change one of these characters at a time and check that no row changes, on both sides and for both values of  $\eta$ . They do so for the  $6 \cdot 12 = 72$  characters with  $q \in \{13, 41, 131, 257, 409, 2089\}$  in the rank-five family, and for the  $3 \cdot 12 = 36$  characters with  $q \in \{13, 19, 41\}$  in the rank-six family. Since each entry is affine in these characters, we conclude that the rows do not depend on any joint choice of them. The rank-seven program checks instead that every prime that occurs to an odd power in some  $b_i$ , in the products of cofactors, or in one of the 54 determinants  $\Delta_{ij}$  that enter the rows divides  $W$ . These are the pairs  $\{i, j\}$  not contained in  $I_H$  or in  $I_J$ . All three programs also check the relation  $\lambda_i(p_j) + \lambda_j(p_i) = \lambda_i(-1)\lambda_j(-1)$  of quadratic reciprocity for all 66 pairs, with the cross symbols given by the formulas of Lemma 4.12 and the characters chosen above. This checks the signs in these formulas for one choice of characters; it does not replace the proof of Lemma 4.12.

**Matrices.** Each program builds the rows of  $\mathbf{M}_E(\eta)$  and  $\mathbf{M}_{E'}(\eta)$  for  $\eta = 0, 1$  from the fixed rows and the formulas of Lemma 4.11, and compares them with the codes stored in its input file, which are those of Tables A.2 to A.4. It then computes, by Gaussian elimination over  $\mathbb{F}_2$ , the rank, the reduced row basis, and the kernel of each matrix. It checks that the codes of the classes of the rational points lie in the kernel, are linearly independent, and span the kernel.

## A.4 What the programs do not check

We now list the statements that the programs do not check. All of them are proved in the text.

- The results of Sections 3 and 4: the descent maps, the local images at the moving primes, the rows at the moving primes, the reciprocity formulas, and Proposition 4.18.
- The fixed-place lemmas for all valuations of  $x$ , and the constancy of the residues they use on the congruence class.
- The positivity of the twelve forms on the cones (the rank-five program checks it at the endpoints of the interval of slopes, and the rank-seven program at one interior ratio).
- The results of Section 5, and hence the infinitude of the prime specializations.
- The formula for the  $j$ -invariant and the degree of the  $j$ -map (Lemma 4.3).

- The constructions of Appendix B, except that the rank-seven program checks the equation of the conic and the point of  $E$  that it gives.

The programs do not read the  $\text{\TeX}$  source of this paper, and some fields of the input files are descriptive and are not used. For example, the rank-six program uses its own table of the  $a_i$  and  $b_i$ , not the copy in its input file. A change in the text must therefore be compared with the programs by hand.

## A.5 The row codes

Tables A.2 to A.4 list the rows of the matrices  $\mathbf{M}_E(\eta)$  and  $\mathbf{M}_{E'}(\eta)$  of Sections 6 to 8 as row codes, in the column order of Appendix A.2. The rows appear in the order of the text and carry the names used there: first the fixed rows  $f_k^*$ , then the moving rows  $r_i^*$  at  $p_0, \dots, p_3$ , then the moving rows  $r_i^*$  at the primes  $p_i$  with  $i \in O_*$ . The column  $\eta$  gives the code of the corresponding row of  $\mathbf{M}_*(\eta)$ . The fixed rows do not depend on  $\eta$ , and every moving row at  $\eta = 1$  is the moving row at  $\eta = 0$  plus  $u_*$ ; in terms of codes, the two moving codes differ by a bitwise exclusive or with 4080 or 8160. Table A.5 lists the codes of the classes of the rational points, in the order of the text, and the reduced row bases printed by the programs. The reduced row bases are the same for  $\eta = 0$  and  $\eta = 1$ . For row reduction, the programs use the highest nonzero bit of a code as its pivot and print the basis in decreasing order of pivots; thus they eliminate columns from right to left in the column order above. The pivots of each printed basis are distinct, which shows that the ranks are as stated.

| $E$        |            |            | $E'$       |            |            |
|------------|------------|------------|------------|------------|------------|
| Row        | $\eta = 0$ | $\eta = 1$ | Row        | $\eta = 0$ | $\eta = 1$ |
| $f_1^E$    | 1669       | 1669       | $f_1^{E'}$ | 108        | 108        |
| $f_2^E$    | 3948       | 3948       | $f_2^{E'}$ | 3206       | 3206       |
| $f_3^E$    | 267        | 267        | $f_3^{E'}$ | 1          | 1          |
| $f_4^E$    | 4          | 4          | $r_0^{E'}$ | 1424       | 2656       |
| $f_5^E$    | 3718       | 3718       | $r_1^{E'}$ | 898        | 3186       |
| $r_0^E$    | 1424       | 2656       | $r_2^{E'}$ | 66         | 4018       |
| $r_1^E$    | 642        | 3442       | $r_3^{E'}$ | 1597       | 2509       |
| $r_2^E$    | 322        | 3762       | $r_4^{E'}$ | 1494       | 2598       |
| $r_3^E$    | 4029       | 77         | $r_5^{E'}$ | 3887       | 223        |
| $r_8^E$    | 3888       | 192        | $r_6^{E'}$ | 799        | 3311       |
| $r_9^E$    | 37         | 4053       | $r_7^{E'}$ | 2442       | 1658       |
| $r_{10}^E$ | 924        | 3180       |            |            |            |
| $r_{11}^E$ | 2572       | 1532       |            |            |            |

Table A.2. Row codes of  $\mathbf{M}_E(\eta)$  and  $\mathbf{M}_{E'}(\eta)$  for the rank-five family (Section 6), with columns  $-1, 2, 3, 5, p_0, \dots, p_7$  for  $E$  and  $-1, 2, 3, 5, p_0, \dots, p_3, p_8, \dots, p_{11}$  for  $E'$ ; input keys E0, E1, Ep0, Ep1.

| $E$        |            |            | $E'$       |            |            |
|------------|------------|------------|------------|------------|------------|
| Row        | $\eta = 0$ | $\eta = 1$ | Row        | $\eta = 0$ | $\eta = 1$ |
| $f_1^E$    | 2          | 2          | $f_1^{E'}$ | 1981       | 1981       |
| $f_2^E$    | 3875       | 3875       | $f_2^{E'}$ | 2          | 2          |
| $f_3^E$    | 4          | 4          | $f_3^{E'}$ | 3613       | 3613       |
| $f_4^E$    | 1557       | 1557       | $f_4^{E'}$ | 1          | 1          |
| $r_0^E$    | 839        | 3255       | $r_0^{E'}$ | 3927       | 167        |
| $r_1^E$    | 2139       | 1963       | $r_1^{E'}$ | 1147       | 2955       |
| $r_2^E$    | 1586       | 2498       | $r_2^{E'}$ | 2610       | 1474       |
| $r_3^E$    | 2879       | 1231       | $r_3^{E'}$ | 2239       | 1871       |
| $r_8^E$    | 1961       | 2137       | $r_4^{E'}$ | 1430       | 2662       |
| $r_9^E$    | 1765       | 2325       | $r_5^{E'}$ | 3036       | 1068       |
| $r_{10}^E$ | 1409       | 2673       | $r_6^{E'}$ | 241        | 3841       |
| $r_{11}^E$ | 734        | 3374       | $r_7^{E'}$ | 164        | 3924       |

Table A.3. Row codes of  $\mathbf{M}_E(\eta)$  and  $\mathbf{M}_{E'}(\eta)$  for the rank-six family (Section 7), with columns  $-1, 2, 3, 7, p_0, \dots, p_7$  for  $E$  and  $-1, 2, 3, 7, p_0, \dots, p_3, p_8, \dots, p_{11}$  for  $E'$ ; input keys E0, E1, Ep0, Ep1.

| $E$        |            |            | $E'$       |            |            |
|------------|------------|------------|------------|------------|------------|
| Row        | $\eta = 0$ | $\eta = 1$ | Row        | $\eta = 0$ | $\eta = 1$ |
| $f_1^E$    | 4943       | 4943       | $f_1^{E'}$ | 7705       | 7705       |
| $f_2^E$    | 8020       | 8020       | $f_2^{E'}$ | 4117       | 4117       |
| $f_3^E$    | 195        | 195        | $f_3^{E'}$ | 8          | 8          |
| $f_4^E$    | 4          | 4          | $f_4^{E'}$ | 7626       | 7626       |
| $r_0^E$    | 4896       | 3264       | $f_5^{E'}$ | 16         | 16         |
| $r_1^E$    | 219        | 7995       | $f_6^{E'}$ | 1          | 1          |
| $r_2^E$    | 340        | 7860       | $r_0^{E'}$ | 5408       | 2752       |
| $r_3^E$    | 3583       | 4639       | $r_1^{E'}$ | 6811       | 1403       |
| $r_8^E$    | 7945       | 233        | $r_2^{E'}$ | 2388       | 5812       |
| $r_9^E$    | 7734       | 470        | $r_3^{E'}$ | 6399       | 1823       |
| $r_{10}^E$ | 466        | 7730       | $r_4^{E'}$ | 5503       | 2719       |
| $r_{11}^E$ | 3121       | 5073       | $r_5^{E'}$ | 5914       | 2298       |
|            |            |            | $r_6^{E'}$ | 5914       | 2298       |
|            |            |            | $r_7^{E'}$ | 5479       | 2695       |

Table A.4. Row codes of  $\mathbf{M}_E(\eta)$  and  $\mathbf{M}_{E'}(\eta)$  for the rank-seven family (Section 8), with columns  $-1, 2, 3, 7, 13, p_0, \dots, p_7$  for  $E$  and  $-1, 2, 3, 7, 13, p_0, \dots, p_3, p_8, \dots, p_{11}$  for  $E'$ ; input keys  $E0, E1, Ep0, Ep1$ .

| Family           | Classes of the rational points | Reduced row basis                        | Rank |
|------------------|--------------------------------|------------------------------------------|------|
| Rank five, $E$   | 4081, 243, 3274                | 2051, 1027, 523, 267, 137, 73, 33, 17, 4 | 9    |
| Rank five, $E'$  | 4082, 3840, 824, 1378          | 2322, 1288, 794, 152, 66, 42, 4, 1       | 8    |
| Rank six, $E$    | 4081, 3848, 865, 1449          | 2137, 1048, 521, 328, 209, 33, 4, 2      | 8    |
| Rank six, $E'$   | 4080, 248, 3220, 2384          | 2072, 1068, 552, 284, 164, 84, 2, 1      | 8    |
| Rank seven, $E$  | 8163, 483, 6306, 3291, 6554    | 4611, 3075, 265, 130, 65, 42, 24, 4      | 8    |
| Rank seven, $E'$ | 8164, 482, 1696, 2848          | 4100, 2212, 1154, 546, 422, 70, 16, 8, 1 | 9    |

Table A.5. Codes of the classes of the rational points, including the class of  $T$  first, and the reduced row bases of the matrices, for  $\eta = 0$  and  $\eta = 1$ . The number of classes plus the rank equals the number of columns.

## Origin of the three families

This appendix explains how the three families were found; nothing in it is used in the proofs of Theorems 6.7, 7.8, and 8.9. In each case, we start from a pair of 2-isogenous curves over  $\mathbb{Q}(t)$  whose coefficients are, up to constants, products of the linear factors  $t - t_0$ , where  $t_0$  runs over the six rational parameters of the bad fibers, and we pull the pair back along a rational parametrization of a conic that has rational points above each of these six parameters. The six linear factors then pull back to quadratic forms that split into the twelve linear forms  $L_i$ , and points that are defined only over the function field of the conic become rational points of the new curves. Appendices B.1 and B.2 start from the rank-four pair of Zywna [55, §6.5], and Appendix B.3 starts from another pair of the same form.

### B.1 The rank-five family

The datum  $\mathfrak{D}_5$  of Section 6 arises from a pair of curves of Zywna by a base change along a conic. Every identity below is an identity between polynomials or rational functions, which can be checked by expansion; we keep the notation of Section 6.

**Zywna's pair.** In [55, §6.5], Zywna considers the curves

$$\begin{aligned} E_Z : y^2 &= x^3 - 70(t^2 - 25^2)x^2 + 2^4 \cdot 7^2(t^2 - 11^2)(t^2 - 25^2)x, \\ E'_Z : y^2 &= x^3 + 140(t^2 - 25^2)x^2 + 2^2 \cdot 3^2 \cdot 7^2(t^2 - 25^2)(t^2 - 39^2)x \end{aligned} \tag{B.1}$$

over  $\mathbb{Q}(t)$ , where we write  $t$  for his parameter  $T$ , and he uses them to obtain infinitely many elliptic curves of rank four over every number field. The coefficients of  $E'_Z$  are  $-2\alpha$  and  $\alpha^2 - 4\beta$  for the coefficients  $\alpha, \beta$  of  $E_Z$ , since  $70^2(t^2 - 625)^2 - 4 \cdot 784(t^2 - 121)(t^2 - 625) = 1764(t^2 - 625)(t^2 - 1521)$ . The discriminants of both models vanish exactly at the six parameters  $t = \pm 11, \pm 25, \pm 39$ . Zywna lists the points

$$\begin{aligned} P_1^Z &= (14(t^2 - 11^2), 1176(t^2 - 11^2)), \\ P_2^Z &= (2(t - 11)(t - 25), (36t + 780)(t - 11)(t - 25)) \end{aligned}$$

of  $E_Z$ , and the points

$$\begin{aligned} Q_1^Z &= (2(t - 25)(t - 39), (64t + 1760)(t - 25)(t - 39)), \\ Q_2^Z &= (-14(t^2 - 25^2), 4704(t^2 - 25^2)) \end{aligned}$$

of  $E'_Z$ .

**A quadratic condition.** For  $k \in \mathbb{Q}^\times$ , we consider the abscissa  $x = k(t - 25)(t - 39)$  on  $E'_Z$ ; for  $k = 2$ , it is the abscissa of  $Q_1^Z$ . Since  $(t^2 - 25^2)(t^2 - 39^2)$  is divisible by  $(t - 25)(t - 39)$ , the right side of the equation of  $E'_Z$  at this abscissa equals  $x^2 q_k(t)$ , where

$$\begin{aligned} q_k(t) &= k(t - 25)(t - 39) + 140(t^2 - 625) + \frac{1764}{k}(t + 25)(t + 39) \\ &= \left(k + 140 + \frac{1764}{k}\right)t^2 + 64\left(\frac{1764}{k} - k\right)t + 975\left(k + \frac{1764}{k}\right) - 87500. \end{aligned} \quad (\text{B.2})$$

The point  $(x, x\sqrt{q_k(t)})$  is then defined over the extension  $\mathbb{Q}(t)(\sqrt{q_k(t)})$ , which is  $\mathbb{Q}(t)$  itself when  $q_k(t)$  is a square in  $\mathbb{Q}(t)$  (as for  $k = 2$ , where  $q_2(t) = 256(2t + 55)^2$ ). For the value of  $k$  chosen below,  $q_k$  is not a square, and this extension is the function field of the conic  $z^2 = q_k(t)$ . Above a parameter  $t_0$ , this conic has two rational points if and only if  $q_k(t_0)$  is a nonzero square. For  $k = 2s^2$  with  $s \in \mathbb{Q}^\times$ , the values of  $q_k$  at the six bad parameters are given in Table B.1.

Table B.1. The values  $q_{2s^2}(t_0)$  at the bad parameters  $t_0$ .

| $t_0$ | $q_{2s^2}(t_0)$ | $t_0$ | $q_{2s^2}(t_0)$       | $t_0$ | $q_{2s^2}(t_0)$          |
|-------|-----------------|-------|-----------------------|-------|--------------------------|
| -25   | $(80s)^2$       | -11   | $(12(5s^2 - 49)/s)^2$ | -39   | $16^2(39s^2 + 490)$      |
| 25    | $(1680/s)^2$    | 11    | $(28(s^2 - 45)/s)^2$  | 39    | $(112/s)^2(10s^2 + 351)$ |

Four of these values are nonzero squares for every  $s \in \mathbb{Q}^\times$ , since  $49/5$  and  $45$  are not squares in  $\mathbb{Q}$ . The other two are squares if and only if  $10s^2 + 351$  and  $39s^2 + 490$  are squares. For  $s = 41$ , we have

$$10 \cdot 41^2 + 351 = 17161 = 131^2, \quad 39 \cdot 41^2 + 490 = 66049 = 257^2,$$

and all six values are nonzero. With  $k = 2 \cdot 41^2 = 3362$ , comparing coefficients in (B.2), we find

$$q_{3362}(t) = \left(\frac{16}{41}\right)^2 C(t), \quad C(t) = 22999t^2 - 1412660t + 20953150.$$

**The conic.** The conic  $z^2 = C(t)$  has the rational point  $(t, z) = (25, 105)$ . Since  $C(25 + h) = 105^2 - 262710h + 22999h^2$ , the line  $z = 105 + m(t - 25)$  meets the conic again at

$$t = \frac{25m^2 - 210m - 837685}{m^2 - 22999}, \quad z = -\frac{105(m^2 + 2502m + 22999)}{m^2 - 22999}.$$

We use the coordinate  $m = 113 - 62N/M$  on the line of slopes. Substituting it and multiplying the numerators and denominators by  $M^2$ , we obtain

$$t = \frac{D_1}{D}, \quad z = \frac{Z}{D}, \quad Z = -105(5137M^2 - 2728MN + 62N^2), \quad (\text{B.3})$$

where  $D$  and  $D_1$  are the quadratic forms (6.9); indeed, the numerator and denominator of  $t$  become  $62D_1$  and  $62D$ . The form  $D$  has no rational zero other than  $(0, 0)$ , because its discriminant  $4 \cdot 22999 = 4 \cdot 109 \cdot 211$  is not a square. The six parameters  $\pm 11, \pm 25, \pm 39$  pull back to products of the linear forms of Table 6.1:

$$\begin{aligned} D_1 - 25D &= -210L_0L_1, & D_1 + 25D &= -10L_2L_3, \\ D_1 - 39D &= 14L_4L_5, & D_1 + 39D &= -2L_6L_7, \\ D_1 - 11D &= -14L_8L_9, & D_1 + 11D &= -6L_{10}L_{11}. \end{aligned} \quad (\text{B.4})$$

Each line of (B.4) is an identity between binary quadratic forms. Multiplying the two identities in each line, we obtain

$$t^2 - 25^2 = \frac{2100F}{D^2}, \quad t^2 - 39^2 = -\frac{28H}{D^2}, \quad t^2 - 11^2 = \frac{84J}{D^2}. \quad (\text{B.5})$$

The identity (6.1) is the pullback of the linear relation  $25(t^2 - 25^2) - 9(t^2 - 39^2) = 16(t^2 - 11^2)$ : inserting (B.5) and dividing by 84, we find  $625F + 3H = 16J$ .

**The scaling.** We substitute  $t = D_1/D$  in (B.1). For  $E'_Z$ , the change of coordinates  $x = (14/D)^2 x_1, y = (14/D)^3 y_1$  gives

$$y_1^2 = x_1^3 + \frac{140 \cdot 2100F}{14^2} x_1^2 + \frac{1764 \cdot 2100F \cdot (-28H)}{14^4} x_1 = x_1^3 + 1500F x_1^2 - 2700FH x_1,$$

which is the curve  $E$  of (6.3). For  $E_Z$ , the same change of coordinates gives  $y_1^2 = x_1^3 - 750F x_1^2 + 3600FJ x_1$ , which is not the curve  $E'$  but is isomorphic to it by  $(x_1, y_1) \mapsto (4x_1, 8y_1)$ . Equivalently, the change of coordinates  $x = (7/D)^2 x_1, y = (7/D)^3 y_1$  takes  $E_Z$  to

$$y_1^2 = x_1^3 - \frac{70 \cdot 2100F}{7^2} x_1^2 + \frac{784 \cdot 2100F \cdot 84J}{7^4} x_1 = x_1^3 - 3000F x_1^2 + 57600FJ x_1,$$

which is  $E'$ . In other words, the scale  $14/D$  takes  $E'_Z$  to  $E$ , and it takes the curve  $y^2 = x^3 - 280(t^2 - 25^2)x^2 + 12544(t^2 - 25^2)(t^2 - 11^2)x$ , which is 2-isogenous to  $E'_Z$  in the normalization of Section 3 and isomorphic to  $E_Z$  by  $(x, y) \mapsto (x/4, y/8)$ , to  $E'$ . Zywin's model  $E_Z$  itself requires the scale  $7/D$ .

**The points.** Under these changes of coordinates, three of the five points of Table 6.3 are images of Zywin's points. The point  $Q_2^Z$  of  $E'_Z$  goes to  $P_1$ ; the points  $P_1^Z$  and  $P_2^Z$  of  $E_Z$  (with the scale  $7/D$ ) go to  $Q_1$  and  $Q_2$ . The point  $P_2$  is the image of  $(2(t+25)(t+39), (64t-1760)(t+25)(t+39))$ , which is the point of  $E'_Z$  obtained from  $Q_1^Z$  by replacing  $t$  with  $-t$  and changing the sign of the ordinate; it lies on  $E'_Z$  because the coefficients of  $E'_Z$  are even in  $t$ . Finally, the point of  $E'_Z$  over the conic with abscissa  $3362(t-25)(t-39)$  becomes the point of  $E$  with

$$x = -50430 L_0 L_1 L_4 L_5, \quad \frac{y}{x} = \frac{8}{287} Z.$$

At a prime specialization, its class is  $[-10 p_0 p_1 p_4 p_5] = \mathbf{v}_1 + \mathbf{v}_3$  in the notation of (6.11), and it does not increase the lower bound of Lemma 6.2.

**The point  $Q_3$ .** Let  $C$  be the point of  $E$  over the conic that we have just described. The point  $Q_3$  of Table 6.3 comes from  $C$  through the dual isogeny. We set

$$\Xi = -627M^2 + 719MN + 20N^2, \quad R = (2400 L_1 L_2 L_9 L_{11}, 28800 \Xi L_1 L_2 L_9 L_{11}).$$

Then  $R$  lies on  $E'$ , and the group laws of  $E$  and  $E'$  and the formula (3.8) for  $\hat{\phi}$  give the identities

$$\hat{\phi}(R) = C - P_2 - T, \quad R = Q_1 + Q_3, \quad (\text{B.6})$$

which hold at every  $(M, N)$  with  $FHJ \neq 0$ , with the ordinates of Table 6.3. For the first identity, one computes that

$$C - P_2 - T = (36 \Xi^2, 36 \Xi (100 L_1 L_2 L_9 L_{11} - L_0 L_3 L_8 L_{10})),$$

whose abscissa is a square, as it must be, since  $\delta_E(C) = \delta_E(P_2)\delta_E(T)$  and  $\ker \delta_E = \hat{\phi}(E'(Q))$ . In words,  $Q_3 = R - Q_1$ , where  $R$  is a preimage of  $C - P_2 - T$  under  $\hat{\phi}$ . Equivalently,  $C = T + P_2 + \hat{\phi}(Q_1 + Q_3)$ .

## B.2 The rank-six family

The datum  $\mathfrak{D}_6$  of Section 7 arises from a rank-four surface of Zywinia [55, §6.5]. We use the quadratic forms  $D_0, D_1$  of Sections 7.1 and 7.2.

**Zywinia's pair.** Let  $U = t^2 - 25^2$ ,  $V = t^2 - 11^2$  and  $W_t = t^2 - 39^2$ . In [55, §6.5], Zywinia considers the elliptic curve

$$E_Z: y^2 = x^3 - 70U x^2 + 2^4 7^2 UV x \quad (\text{B.7})$$

over  $\mathbb{Q}(t)$ , and the 2-isogenous curve  $E'_Z: y^2 = x^3 + 140U x^2 + 2^2 3^2 7^2 UW_t x$ . In the notation of Section 3, these are  $E_{\alpha_Z, \beta_Z}$  and  $E_{\alpha'_Z, \beta'_Z}$  with  $\alpha_Z = -70U$  and  $\beta_Z = 784UV$ ; indeed  $\alpha_Z^2 - 4\beta_Z = 196U(25U - 16V) = 1764UW_t$ , since  $25U - 16V = 9W_t$ . Zywinia shows that the images of the descent maps of  $E_Z$  and  $E'_Z$  over  $\mathbb{Q}(t)$  have dimension at least three, using the points  $(0, 0)$ ,

$$(14(t^2 - 11^2), 1176(t^2 - 11^2)), \quad (2(t - 11)(t - 25), (36t + 780)(t - 11)(t - 25))$$

on  $E_Z$ , and the points  $(0, 0)$ ,

$$(2(t - 25)(t - 39), (64t + 1760)(t - 25)(t - 39)), \quad (-14(t^2 - 25^2), 4704(t^2 - 25^2))$$

on  $E'_Z$ , and he deduces from his Theorem 4.1 that, over every number field, there are infinitely many elliptic curves of rank four. The discriminants of  $E_Z$  and  $E'_Z$  vanish at the six parameters  $t = \pm 11, \pm 25, \pm 39$ .

**A conic over which both curves gain a point.** Let  $s, u \in \mathbb{Q}$  with  $s^2 + u^2 = 5$ ,  $s \neq 0$  and  $s \neq u$ . Substituting  $x = 14s^2U$  into the equation of  $E_Z$  and dividing by  $x^2$ , we find  $y^2/x^2 = q(t)$ , where

$$q(t) = x - 70U + \frac{784UV}{x} = (14s^2 - 70)U + \frac{56}{s^2}V.$$

On  $E'_Z$ , the substitution  $x = -14(s - u)^2U$  gives  $y^2/x^2 = (2s/(s - u))^2q(t)$ ; this is where the condition  $s^2 + u^2 = 5$  is used, since the difference of the two sides is a rational function whose numerator is divisible by  $s^2 + u^2 - 5$ . For  $(s, u) = (22/13, 19/13)$ , we find

$$q(t) = \left(\frac{84}{143}\right)^2(47311 - 30t^2), \quad \frac{2s}{s - u} = \frac{44}{3}.$$

Then both curves acquire a point over the function field of the conic

$$\mathcal{C}: z^2 = 47311 - 30t^2. \quad (\text{B.8})$$

The conic has the rational point  $(t, z) = (25, 169)$ , since  $47311 - 30 \cdot 25^2 = 169^2$ . We also have  $47311 - 30 \cdot 11^2 = 209^2$  and  $47311 - 30 \cdot 39^2 = 41^2$ . In other words, each of the six bad parameters  $\pm 11, \pm 25, \pm 39$  lifts to two rational points of  $\mathcal{C}$ . The line  $z = 169 + m(t - 25)$  meets  $\mathcal{C}$  where  $h = t - 25$  satisfies  $h((m^2 + 30)h + 338m + 1500) = 0$ . Its second intersection with  $\mathcal{C}$  is, for  $m = M/N$ ,

$$t = \frac{D_1}{D_0}, \quad z = \frac{Z}{D_0}, \quad Z = -169M^2 - 1500MN + 5070N^2,$$

and  $Z^2 + 30D_1^2 = 47311D_0^2$ . Since  $D_0 = M^2 + 30N^2 > 0$  for  $(M, N) \neq (0, 0)$ , this parametrization has no poles at rational parameters.

**The pullbacks.** The six linear factors of  $U, V, W_t$  pull back to products of two of the forms  $L_i$  of Table 7.1:

$$\begin{aligned} D_1 - 25D_0 &= -2L_1L_2, & D_1 + 25D_0 &= 2L_0L_3, \\ D_1 - 11D_0 &= 2L_4L_5, & D_1 + 11D_0 &= 2L_6L_7, \\ D_1 - 39D_0 &= -2L_8L_9, & D_1 + 39D_0 &= 2L_{10}L_{11}. \end{aligned} \quad (\text{B.9})$$

Multiplying these identities in pairs, we obtain, at  $t = D_1/D_0$ ,

$$U = -\frac{4F}{D_0^2}, \quad V = \frac{4H}{D_0^2}, \quad W_t = -\frac{4J}{D_0^2},$$

and the identity  $25U - 16V = 9W_t$  becomes (7.3). The change of variables  $x_Z = (2/D_0)^2x$ ,  $y_Z = (2/D_0)^3y$  transforms  $E_Z$  and  $E'_Z$  at  $t = D_1/D_0$  into the curves  $E$  and  $E'$  of (7.5). For example, the coefficients of  $E_Z$  become  $-70U(D_0/2)^2 = 70F$  and  $784UV(D_0/2)^4 = -784FH$ . We conclude that  $E_{M,N}$  is the pullback of  $E_Z$  along the parametrization of  $\mathcal{C}$ , written in the parameter  $m = M/N$ , and  $E'_{M,N}$  is the pullback of  $E'_Z$ ; no quadratic twist occurs. The cofactors  $c_i$  and the congruence class of Section 7.3 are not part of this construction.

**The points.** Under this change of variables, three of the four points of Zywinia displayed above, and the image of the fourth under  $t \mapsto -t$ , become, up to sign, points of Table 7.2. The two points of  $E_Z$  become  $P_1$  and  $P_2$ . The point  $(-14(t^2 - 25^2), 4704(t^2 - 25^2))$  of  $E'_Z$  becomes  $Q_1$ , and the point  $(2(t + 25)(t + 39), (1760 - 64t)(t + 25)(t + 39))$ , which is the image of  $(2(t - 25)(t - 39), (64t + 1760)(t - 25)(t - 39))$  under  $t \mapsto -t$ , becomes  $-Q_2$ . The conic supplies the further points

$$C = \left(-\frac{6776}{169}F, -\frac{25872}{2197}FZ\right) \in E(\mathbb{Q}(m)), \quad C' = \left(\frac{126}{169}F, \frac{7056}{2197}FZ\right) \in E'(\mathbb{Q}(m)),$$

which come from the substitutions  $x = 14s^2U$  and  $x = -14(s - u)^2U$ ; note that  $6776/169 = 14(22/13)^2$  and  $126/169 = 14(3/13)^2$ . Their classes  $[-14F] = \delta_E(T)\delta_E(P_1)$  and  $[14F] = \delta_{E'}(Q_1)$  lie in the span of the classes of the pulled-back points, and  $C$  and  $C'$  do not enlarge the images of the descent maps directly. The remaining points  $P_3$  and  $Q_3$  are related to them through the isogenies  $\phi$  and  $\hat{\phi}$  of (3.8). Using the group law, one checks that

$$\phi(P_3) = C' - Q_1, \quad \hat{\phi}(Q_1 + Q_3) = C + P_1 + T. \quad (\text{B.10})$$

These identities are consistent with Proposition 3.4: since  $\delta_{E'}(C') = \delta_{E'}(Q_1)$  and  $\delta_E(C) = \delta_E(T)\delta_E(P_1)$ , the points  $C' - Q_1$  and  $C + P_1 + T$  lie in the kernels  $\phi(E(\mathbb{Q}(m)))$  and  $\hat{\phi}(E'(\mathbb{Q}(m)))$  of the descent maps. The classes of the preimages  $P_3$  and  $Q_1 + Q_3$  are not in the span of the classes of the pulled-back points. They account for the increase of the rank from four to six: by Lemma 7.2, the classes of  $T, P_1, P_2, P_3$  and of  $T', Q_1, Q_2, Q_3$  are independent at every prime specialization of  $\mathfrak{D}_6$ .

### B.3 The rank-seven family

We explain how the datum  $\mathfrak{D}_7$  of Section 8 arises from a 2-isogeny pair over  $\mathbb{Q}(t)$  by a base change along a conic, and how the conic is related to the point  $P_4$  of Table 8.3. Every identity below is an identity between polynomials or rational functions, which can be checked by expansion; we keep the notation of Section 8. A base change along a conic, over which a multisection of degree two becomes a section, is a classical device for producing new sections [30, §2.2], [13, Lecture III, p. 2003]; see also the general multisection argument in [36, Corollary 4.3] and its conic-bundle application in [27, §1.2 and Theorem 2.4]. An explicit construction of the same kind is given in [11, §4].

**The starting pair.** For  $\rho, v, w \in \mathbb{Q}$  with  $\rho \neq 0, \pm 1$  and

$$(1 - \rho^2)^2 w^2 = (1 + \rho^2)^2 - 4\rho^2 v^2, \quad (\text{B.11})$$

we consider the curves

$$\begin{aligned} \mathcal{E} : y^2 &= x^3 - (1 + \rho^2)(t^2 - 1)x^2 + \rho^2(t^2 - 1)(t^2 - v^2)x, \\ \mathcal{E}' : y^2 &= x^3 + 2(1 + \rho^2)(t^2 - 1)x^2 + (1 - \rho^2)^2(t^2 - 1)(t^2 - w^2)x \end{aligned} \quad (\text{B.12})$$

over  $\mathbb{Q}(t)$ . Writing  $\alpha_t$  and  $\beta_t$  for the coefficients of  $\mathcal{E}$ , we have

$$\alpha_t^2 - 4\beta_t = (t^2 - 1)((1 - \rho^2)^2 t^2 - (1 + \rho^2)^2 + 4\rho^2 v^2) = (1 - \rho^2)^2 (t^2 - 1)(t^2 - w^2),$$

where we used (B.11) in the last step. In other words,  $\mathcal{E}'$  is the curve 2-isogenous to  $\mathcal{E}$  in the sense of Section 3. Both curves have a split form: their coefficients are products of the factors  $t \mp 1$ ,  $t \mp v$  and  $t \mp w$ , and their finite bad fibers lie over the set  $\{\pm 1, \pm v, \pm w\}$ . For the parameters used below, these are six distinct points.

The rank-four pair of Zywinia [55, §6.5] has this form. Indeed, if we substitute  $25t$  for his parameter and write his coordinates as  $(625x, 15625y)$ , his two curves become

$$y^2 = x^3 + 14\alpha_t x^2 + 14^2\beta_t x$$

and its companion, where  $\alpha_t, \beta_t$  are the coefficients of  $\mathcal{E}$  for  $(\rho, v, w) = (2, 11/25, 39/25)$ ; that is, they are the quadratic twists by 14 of the curves (B.12) with these parameters. The rank-seven family starts instead from

$$\rho = \frac{182}{241}, \quad v = -\frac{209}{241}, \quad w = \frac{16769}{8319}. \quad (\text{B.13})$$

The starting pair is therefore not Zywinia's pair of [55, §6.5]; it is a 2-isogeny pair of the same split-factor form. For the values (B.13), we have  $\rho^2 = 33124/58081$ ,  $v^2 = 43681/58081$ ,  $1 + \rho^2 = 91205/241^2$  and  $1 - \rho^2 = 24957/241^2 = 3 \cdot 8319/241^2$ , and (B.11) reduces to the integer identity

$$91205^2 - 4 \cdot 33124 \cdot 43681 = 2530794249 = 9 \cdot 16769^2.$$

**The conic.** We look for points of  $\mathcal{E}$  with abscissa  $x = \rho^2 t^2$ . At this abscissa, we have

$$x + \alpha_t + \frac{\beta_t}{x} = \rho^2 t^2 - (1 + \rho^2)(t^2 - 1) + \frac{(t^2 - 1)(t^2 - v^2)}{t^2} = \frac{v^2 + (\rho^2 - v^2)t^2}{t^2}.$$

For the parameters (B.13), this equals  $(43681 - 10557t^2)/(241^2 t^2)$ . By (8.8), a point  $(\rho^2 t^2, \rho^2 t^2 r)$  lies on  $\mathcal{E}$  exactly when  $r^2 = (43681 - 10557t^2)/(241t)^2$ . The curve  $\mathcal{E}$  therefore acquires the point

$$\left(\rho^2 t^2, \frac{\rho^2 t z}{241}\right) \quad (\text{B.14})$$

over the function field of the conic

$$z^2 = 43681 - 10557t^2. \quad (\text{B.15})$$

The conic has the rational point  $(t, z) = (1, 182)$ , since  $43681 - 10557 = 33124 = 182^2$ . For  $m = M/N$ , the line  $z = 182 + m(t - 1)$  meets the conic in the points with  $(t - 1)((m^2 + 10557)t - m^2 + 364m + 10557) = 0$ . The second intersection is  $(t, z) = (\Theta/D_0, Z/D_0)$ , where  $D_0 = M^2 + 10557N^2$  is the form of (8.7) and

$$\Theta = M^2 - 364MN - 10557N^2, \quad Z = -182M^2 - 21114MN + 1921374N^2. \quad (\text{B.16})$$

These forms satisfy  $Z^2 + 10557\Theta^2 = 43681D_0^2$ . Since  $D_0 > 0$  for  $(M, N) \neq (0, 0)$ , every nonzero pair  $(M, N)$  gives a rational point  $(\Theta/D_0, Z/D_0)$  of the conic.

**Splitting of the bad fibers.** Above each of the six bad parameters  $t_0 \in \{\pm 1, \pm v, \pm w\}$ , the conic (B.15) has rational points, because  $43681 - 10557t_0^2$  is a nonzero square: it equals  $182^2$ ,  $(45562/241)^2$  and  $(77714/2773)^2$  for  $t_0 = \pm 1$ ,  $\pm v$  and  $\pm w$ , respectively. Correspondingly, each quadratic form  $\Theta - t_0 D_0$ , scaled to have integer coefficients, factors over  $\mathbb{Q}$  into two of the linear forms  $L_i$  of Table 8.1:

$$\begin{aligned} \Theta - D_0 &= -2L_1L_3, & \Theta + D_0 &= 2L_0L_2, \\ 241\Theta - 209D_0 &= 2L_6L_7, & 241\Theta + 209D_0 &= 2L_4L_5, \\ 8319\Theta - 16769D_0 &= -2L_8L_9, & 8319\Theta + 16769D_0 &= 2L_{10}L_{11}. \end{aligned} \quad (\text{B.17})$$

Multiplying the identities in each row gives, at  $t = \Theta/D_0$ ,

$$t^2 - 1 = -\frac{4F}{D_0^2}, \quad t^2 - v^2 = \frac{4H}{241^2 D_0^2}, \quad t^2 - w^2 = -\frac{4J}{8319^2 D_0^2}. \quad (\text{B.18})$$

This is where the parameters (B.13) matter: each of the six bad parameters pulls back to a product of two linear forms, so that the base change keeps twelve linear factors.

**The curves of the family.** Inserting (B.18) into (B.12), we find that at  $t = \Theta/D_0$  the coefficients of  $x^2$  and  $x$  are

$$\frac{4 \cdot 91205 F}{241^2 D_0^2} \quad \text{and} \quad -\frac{16 \cdot 33124 FH}{241^4 D_0^4} \quad \text{for } \mathcal{E}, \quad -\frac{8 \cdot 91205 F}{241^2 D_0^2} \quad \text{and} \quad \frac{144 FJ}{241^4 D_0^4} \quad \text{for } \mathcal{E}'.$$

With  $\mu = 2/(241D_0)$ , we write the coordinates of  $\mathcal{E}$  and  $\mathcal{E}'$  as  $(\mu^2 x, \mu^3 y)$ . This divides the coefficients of  $x^2$  and  $x$  by  $\mu^2$  and  $\mu^4$ . It transforms  $\mathcal{E}$  into  $y^2 = x^3 + 91205Fx^2 - 33124FHx$  and  $\mathcal{E}'$  into  $y^2 = x^3 - 182410Fx^2 + 9FJx$ , which are the curves (8.3). No quadratic twist occurs in this step.

**The conic point.** Under these substitutions, the point (B.14) becomes the point

$$C = \left( 8281 \Theta^2, \frac{8281}{2} D_0 \Theta Z \right) \in E_{M,N}(\mathbb{Q}),$$

where  $8281 = 91^2$ . Its class in  $\delta_E(E(\mathbb{Q}))$  is trivial. Indeed, if  $\Theta \neq 0$ , the abscissa  $(91\Theta)^2$  is a nonzero square. Since  $\Theta = (M - 391N)(M + 27N)$ , the case  $\Theta = 0$  occurs for  $M/N = 391$  and  $M/N = -27$ . Then  $C = (0, 0) = T$ , whose class is  $[\beta]$ , and  $t = 0$ , so that the coefficient  $\rho^2(t^2 - 1)(t^2 - v^2) = (\rho v)^2$  of  $\mathcal{E}$  is a square; after the change of coordinates, this gives  $\beta = (19019 D_0^2/2)^2$ , and the class is trivial in this case as well. On the cone  $\mathcal{K}_7$ , both factors of  $\Theta$  are positive, and only the first case occurs. In either case,  $C$  supplies no nontrivial class in  $\delta_E(E(\mathbb{Q}))$ . This does not mean that  $C$  is a torsion point, and the conic base change may well raise the Mordell–Weil rank through  $C$ ; but the class used in Section 8 is that of  $P_4$ , through the relation proved below.

**The point  $P_4$ .** At every prime specialization of  $\mathfrak{D}_7$ , the class of  $P_4$  in Table 8.5 is not trivial, by Lemma 8.3, and  $P_4$  is related to  $C$  as follows. The identities

$$L_0L_3L_8L_{10} = \alpha + 16562\Theta^2 - 91D_0Z, \quad 9L_1L_2L_9L_{11} = \alpha + 16562\Theta^2 + 91D_0Z, \quad (\text{B.19})$$

with  $\alpha = 91205F$  and  $16562 = 2 \cdot 91^2$ , can be checked by expansion. Their product is  $(\alpha + 16562\Theta^2)^2 - 8281D_0^2Z^2 = 9FJ = \alpha^2 - 4\beta$ . We set

$$R = (L_0L_3L_8L_{10}, -182\Theta L_0L_3L_8L_{10}).$$

Writing  $x_R = L_0L_3L_8L_{10}$ , the equation of  $E'$  at  $R$  reads  $(x_R - \alpha)^2 - 4\beta = 182^2\Theta^2x_R$ , after division by  $x_R$ . By (B.19), we have  $x_R - \alpha = 16562\Theta^2 - 91D_0Z$ . Inserting this and  $-4\beta = 2 \cdot 16562\alpha\Theta^2 + 16562^2\Theta^4 - 8281D_0^2Z^2$ , which is the product identity above, we find that the left side equals  $2 \cdot 16562^2\Theta^4 - 33124 \cdot 91\Theta^2D_0Z + 33124\alpha\Theta^2 = 33124\Theta^2x_R = 182^2\Theta^2x_R$ . Hence  $R \in E'_{M,N}(\mathbb{Q})$ . We use the isogenies  $\phi: E \rightarrow E'$  and  $\hat{\phi}: E' \rightarrow E$  of (3.8), writing  $(x', y')$  for the coordinates on  $E'$ :

$$\phi(x, y) = \left( \frac{x^2 + \alpha x + \beta}{x}, \frac{y(x^2 - \beta)}{x^2} \right), \quad \hat{\phi}(x', y') = \left( \frac{y'^2}{4x'^2}, \frac{y'(x'^2 - \beta')}{8x'^2} \right).$$

At  $R$ , we have  $y'^2/(4x'^2) = 182^2\Theta^2/4 = 8281\Theta^2$  and

$$\frac{y'(x'^2 - \beta')}{8x'^2} = -\frac{91\Theta}{4} \left( x_R - \frac{\beta'}{x_R} \right) = -\frac{91\Theta}{4} (L_0L_3L_8L_{10} - 9L_1L_2L_9L_{11}) = \frac{8281}{2} D_0\Theta Z,$$

where we used  $\beta' = 9FJ = L_0L_3L_8L_{10} \cdot 9L_1L_2L_9L_{11}$  and (B.19). We conclude that  $\hat{\phi}(R) = C$ .

The point  $Q_3$  of Table 8.3 has abscissa  $(16/225)L_0L_3L_8L_{10}$ , which differs from  $x_R$  since  $L_0L_3L_8L_{10} \neq 0$ . The chord through  $R$  and  $-Q_3$  therefore defines  $R - Q_3$ , and expanding the chord formulas, one finds

$$x(R - Q_3) = \frac{D_3^2}{361} = x(\phi(P_4)), \quad y(R - Q_3) = -y(\phi(P_4)),$$

where  $x(\phi(P_4)) = (y/x)^2 = (D_3/19)^2$  by Table 8.3. This shows that  $R - Q_3 = -\phi(P_4)$ . Applying  $\hat{\phi}$  and using  $\hat{\phi} \circ \phi = [2]$  (Proposition 3.4(a)), we obtain

$$C = \hat{\phi}(Q_3) - [2]P_4.$$

In words,  $P_4$  is a half of  $\hat{\phi}(Q_3) - C$ . The class of  $C$  is trivial, as shown above, and so is the class of  $\hat{\phi}(Q_3)$ , by Proposition 3.4(b); at every prime specialization, the class of  $P_4$  is not. This is how the conic produces the new class of  $P_4$ . Its independence from the other classes is proved directly in Lemma 8.3.

## References

- [1] A. O. Bender and Peter Swinnerton-Dyer. Solubility of certain pencils of curves of genus 1, and of the intersection of two quadrics in  $\mathbb{P}^4$ . *Proceedings of the London Mathematical Society*, 83(2):299–329, 2001. doi: 10.1112/plms/83.2.299.
- [2] Manjul Bhargava and Christopher Skinner. A positive proportion of elliptic curves over  $\mathbb{Q}$  have rank one. *Journal of the Ramanujan Mathematical Society*, 29(2):221–242, 2014.
- [3] Tim D. Browning, Lilian Matthiesen, and Alexei N. Skorobogatov. Rational points on pencils of conics and quadrics with many degenerate fibres. *Annals of Mathematics*, 180(1):381–402, 2014. doi: 10.4007/annals.2014.180.1.8.
- [4] Dongho Byeon and Keunyoung Jeong. Infinitely many elliptic curves of rank exactly two. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 92(5):64–66, 2016. doi: 10.3792/pjaa.92.64.
- [5] J. W. S. Cassels. *Lectures on Elliptic Curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991. doi: 10.1017/CBO9781139172530.
- [6] Jean-Louis Colliot-Thélène. Hasse principle for pencils of curves of genus one whose Jacobians have a rational 2-division point: close variation on a paper of Bender and Swinnerton-Dyer. In Emmanuel Peyre and Yuri Tschinkel, editors, *Rational Points on Algebraic Varieties*, volume 199 of *Progress in Mathematics*, pages 117–161. Birkhäuser, Basel, 2001. doi: 10.1007/978-3-0348-8368-9\_5.
- [7] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc. Sur le principe de Hasse et l’approximation faible, et sur une hypothèse de Schinzel. *Acta Arithmetica*, 41(1): 33–53, 1982. doi: 10.4064/aa-41-1-33-53.
- [8] Jean-Louis Colliot-Thélène and Peter Swinnerton-Dyer. Hasse principle and weak approximation for pencils of Severi–Brauer and similar varieties. *Journal für die reine und angewandte Mathematik*, 453:49–112, 1994. doi: 10.1515/crll.1994.453.49.
- [9] Jean-Louis Colliot-Thélène, Alexei N. Skorobogatov, and Peter Swinnerton-Dyer. Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points. *Inventiones Mathematicae*, 134(3):579–650, 1998. doi: 10.1007/s00220050274.
- [10] Andrej Dujella and Juan Carlos Peral. High rank elliptic curves induced by rational Diophantine triples. *Glasnik Matematički. Series III*, 55(2):237–252, 2020. doi: 10.3336/

gm.55.2.05.

- [11] Andrej Dujella and Juan Carlos Peral. An elliptic curve over  $\mathbb{Q}(u)$  with torsion  $\mathbb{Z}/4\mathbb{Z}$  and rank 6. *Rad Hrvatske akademije znanosti i umjetnosti. Matematičke znanosti*, 28:185–192, 2024. doi: 10.21857/y54jof4o2m. Mathematical-series volume 28, academy volume 558.
- [12] Andrej Dujella, Matija Kazalicki, and Juan Carlos Peral. Elliptic curves with torsion groups  $\mathbb{Z}/8\mathbb{Z}$  and  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ . *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas*, 115, 2021. doi: 10.1007/s13398-021-01112-5. Article 169.
- [13] Noam D. Elkies. Elliptic curves and surfaces of high rank, I, II, III. In *Explicit Methods in Number Theory*, volume 4 of *Oberwolfach Reports*, pages 1992–2006. European Mathematical Society, 2007. doi: 10.4171/OWR/2007/34. Contribution to the workshop report, whose DOI is given here; preprint entitled Three lectures on elliptic surfaces and curves of high rank.
- [14] Noam D. Elkies. An elliptic K3 surface  $X/\mathbb{Q}(t)$  with Mordell–Weil rank 17, I: Formulas for  $X$  and base changes of rank 18 and 19. Preprint, arXiv:2608.25406v1, 2026.
- [15] Keqin Feng. Non-congruent numbers, odd graphs and the Birch–Swinnerton-Dyer conjecture. *Acta Arithmetica*, 75(1):71–83, 1996. doi: 10.4064/aa-75-1-71-83.
- [16] Ben Green and Terence Tao. The Möbius function is strongly orthogonal to nilsequences. *Annals of Mathematics*, 175(2):541–566, 2012. doi: 10.4007/annals.2012.175.2.3.
- [17] Ben Green, Terence Tao, and Tamar Ziegler. An inverse theorem for the Gowers  $U^{s+1}[N]$ -norm. *Annals of Mathematics*, 176(2):1231–1372, 2012. doi: 10.4007/annals.2012.176.2.11. See also the authors’ 2024 erratum and the corrected preprint arXiv:1009.3998v5 (2026).
- [18] Benjamin Green and Terence Tao. Linear equations in primes. *Annals of Mathematics*, 171(3):1753–1850, 2010. doi: 10.4007/annals.2010.171.1753.
- [19] Yonatan Harpaz, Alexei N. Skorobogatov, and Olivier Wittenberg. The Hardy–Littlewood conjecture and rational points. *Compositio Mathematica*, 150(12):2095–2111, 2014. doi: 10.1112/S0010437X14007568.
- [20] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem, II. *Inventiones Mathematicae*, 118:331–370, 1994. doi: 10.1007/BF01231536. With an appendix by P. Monsky, pp. 365–370.
- [21] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990. doi: 10.1007/978-1-4757-2103-4.

- [22] Keunyoung Jeong. Infinitely many elliptic curves of rank exactly two II. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 95(6):53–57, 2019. doi: 10.3792/pjaa.95.53.
- [23] Wataru Kai. Linear patterns of prime elements in number fields. Preprint, arXiv:2306.16983v5, 2023. Revised 12 March 2026.
- [24] Daniel Kane and Zev Klagsbrun. On the joint distribution of  $\text{Sel}_\phi(E/\mathbb{Q})$  and  $\text{Sel}_{\hat{\phi}}(E'/\mathbb{Q})$  in quadratic twist families. Preprint, arXiv:1702.02687v1, 2017.
- [25] Anthony Kling and Ben Savoie. A graph-theoretic approach to computing Selmer groups of elliptic curves  $y^2 = x^3 + bx$  over  $\mathbb{Q}(i)$ . arXiv:2410.22714v2, 2024. Version 2, 21 June 2025. Published online in *Journal of Number Theory*, 25 September 2026, doi:10.1016/j.jnt.2026.08.014.
- [26] Peter Koymans and Carlo Pagano. Elliptic curves of rank one over number fields. Preprint, arXiv:2505.16910v1, 2025.
- [27] Daniel Loughran and Cecília Salgado. Rank jumps on elliptic surfaces and the Hilbert property. *Annales de l'Institut Fourier*, 72(2):617–638, 2022. doi: 10.5802/aif.3457.
- [28] Junyu Lu. Prescribed ideal classes and elliptic points in Ennola cubic fields. Preprint, arXiv:2610.04254v1, 2026.
- [29] Barry Mazur and Karl Rubin. Ranks of twists of elliptic curves and Hilbert’s tenth problem. *Inventiones Mathematicae*, 181(3):541–575, 2010. doi: 10.1007/s00222-010-0252-0.
- [30] Jean-François Mestre. Courbes elliptiques de rang  $\geq 12$  sur  $\mathbb{Q}(t)$ . *Comptes Rendus de l'Académie des Sciences. Série I. Mathématique*, 313:171–174, 1991.
- [31] Louis J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proceedings of the Cambridge Philosophical Society*, 21:179–192, 1922.
- [32] Keiji Oguiso and Tetsuji Shioda. The Mordell–Weil lattice of a rational elliptic surface. *Commentarii Mathematici Universitatis Sancti Pauli*, 40(1):83–99, 1991.
- [33] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood. A heuristic for boundedness of ranks of elliptic curves. *Journal of the European Mathematical Society*, 21(9):2859–2903, 2019. doi: 10.4171/JEMS/893.
- [34] László Rédei. Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *Journal für die reine und angewandte Mathematik*, 171:55–60, 1934. doi: 10.1515/crll.1934.171.55.
- [35] László Rédei and Hans Reichardt. Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers. *Journal für die reine und angewandte Mathematik*, 170:69–74, 1934. doi: 10.1515/crll.1934.170.69.

- [36] Cecília Salgado. On the rank of the fibers of rational elliptic surfaces. *Algebra & Number Theory*, 6(7):1289–1313, 2012. doi: 10.2140/ant.2012.6.1289.
- [37] Ben Savoie. Infinitely many elliptic curves over  $\mathbb{Q}(i)$  with rank 2 and  $j$ -invariant 1728. Preprint, arXiv:2506.17605v2, 2025.
- [38] Ben Savoie. Infinitely many elliptic curves over  $\mathbb{Q}(i)$  of exact ranks 4 and 6 with  $j$ -invariant 1728. Preprint, arXiv:2608.13202v1, 2026.
- [39] Andrzej Schinzel and Waław Sierpiński. Sur certaines hypothèses concernant les nombres premiers. *Acta Arithmetica*, 4(3):185–208, 1958. doi: 10.4064/aa-4-3-185-208. Correction: *Acta Arithmetica* 5 (1959), no. 2, 259, doi:10.4064/aa-5-2-259.
- [40] Matthias Schütt and Tetsuji Shioda. Elliptic surfaces. *Advanced Studies in Pure Mathematics*, 60:51–160, 2010.
- [41] Tetsuji Shioda. Some remarks on elliptic curves over function fields. *Astérisque*, 209:99–114, 1992. URL [https://www.numdam.org/item/AST\\_1992\\_\\_209\\_\\_99\\_0/](https://www.numdam.org/item/AST_1992__209__99_0/). Journées Arithmétiques, 1991 (Geneva).
- [42] Joseph H. Silverman. Heights and the specialization map for families of abelian varieties. *Journal für die reine und angewandte Mathematik*, 342:197–211, 1983. doi: 10.1515/crll.1983.342.197.
- [43] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. doi: 10.1007/978-0-387-09494-6.
- [44] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015. doi: 10.1007/978-3-319-18588-0.
- [45] Alexei Skorobogatov and Peter Swinnerton-Dyer. 2-descent on elliptic curves and rational points on certain Kummer surfaces. *Advances in Mathematics*, 198(2):448–483, 2005. doi: 10.1016/j.aim.2005.06.005.
- [46] Peter Swinnerton-Dyer. Rational points on certain intersections of two quadrics. In Wolf Barth, Klaus Hulek, and Herbert Lange, editors, *Abelian Varieties*, pages 273–292. Walter de Gruyter, Berlin, 1995. doi: 10.1515/9783110889437.273.
- [47] Terence Tao and Tamar Ziegler. The primes contain arbitrarily long polynomial progressions. *Acta Mathematica*, 201(2):213–305, 2008. doi: 10.1007/s11511-008-0032-5. See the 2013 erratum.
- [48] Terence Tao and Tamar Ziegler. Erratum to “The primes contain arbitrarily long polynomial progressions”. *Acta Mathematica*, 210(2):403–404, 2013. doi: 10.1007/s11511-013-0097-7.
- [49] John Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In Bryan J. Birch and Willem Kuyk, editors, *Modular Functions of One Variable IV*,

- volume 476 of *Lecture Notes in Mathematics*, pages 33–52. Springer, Berlin, Heidelberg, 1975. doi: 10.1007/BFb0097582.
- [50] André Weil. L’arithmétique sur les courbes algébriques. *Acta Mathematica*, 52:281–315, 1929. doi: 10.1007/BF02592688.
- [51] Maosheng Xiong and Alexandru Zaharescu. Selmer groups and Tate–Shafarevich groups for the congruent number problem. *Commentarii Mathematici Helvetici*, 84(1): 21–56, 2009. doi: 10.4171/CMH/151.
- [52] David Zywina. There are infinitely many elliptic curves over the rationals of rank 2. Preprint, arXiv:2502.01957v1, 2025.
- [53] David Zywina. An elliptic surface with infinitely many fibers for which the rank does not jump. Preprint, arXiv:2502.01026, 2025.
- [54] David Zywina. Rank one elliptic curves and rank stability. Preprint, arXiv:2505.16960v1, 2025.
- [55] David Zywina. On the infinitude of elliptic curves over a number field with prescribed small rank. Preprint, arXiv:2602.10865v1, 2026.