Twenty-four rational points on a genus-29 curve from order-five bimagic squares

Akram Younso
Project direction and correspondence

November 2026

hexagon:2611.01372v1

Abstract

We determine the rational points on a degree-28 residual curve in the centrally antisymmetric order-five bimagic equations. A pencil of quadrics on this curve gives a degree-16 map to the line. Two simultaneous square conditions on its image reduce the arithmetic to four covers. Descent over quadratic fields, the Mordell–Weil sieve and two elliptic Chabauty computations restrict the rational image to four exceptional parameters. Three fibres contribute eight rational points each. The fourth splits into four conjugate pairs over $\mathbb{Q}(\sqrt{10})$. All 24 rational points give arrays with exactly three distinct entries.

1 The curve and its rational locus

An order-five bimagic array has equal sums on its five rows, five columns and two main diagonals, and likewise after squaring each entry. For an associative array, opposite cells have constant sum. Subtracting the middle entry makes opposite cells negatives and makes all first moments zero. Common translation and scaling preserve the moment equations. This leads to projective coordinates on the linear space of centered arrays. The historical distinct-entry problem provides the motivation [1].

We study one residual curve $C \subset \mathbb{P}^7_{\mathbb{Q}}$ in this space. Here is an intrinsic recipe in the chosen coordinates, also fixing precisely which branch is meant. In $\mathbb{Q}[z_0, \dots, z_7]$ take the nine quadratic forms $q_1, \dots, q_6, c_1, c_2, c_3$ of Appendix A; saturate their ideal by the irrelevant ideal and by the product of the sixteen linear forms listed there. Let C be the resulting projective scheme. Saturation takes the closure after removing components contained in the collision hyperplanes. Individual points of the residual curve can therefore lie on these hyperplanes.

Theorem 1. *The curve C is smooth and geometrically integral of degree 28 and genus 29. Its rational locus consists exactly of the 24 points in Appendix B. In the centered array coordinates each has exactly three distinct cell values.*

The result excludes distinct-entry arrays on this branch. The full moment variety has other components. We give the arithmetic argument below and supply the equations, scripts and machine certificates for its computational steps in the accompanying supplement.

2 A pencil and two square conditions

The saturated ideal has Hilbert series $(1 + 6t + 12t^2 + 10t^3 - t^4)/(1 - t)^2$, giving Hilbert polynomial $28n - 28$. We recall how the geometric checks enter. At 101 the reduction of a characteristic-zero

basis generates the independently saturated ideal. A generic pencil section gives a field of degree 28 over $\mathbb{F}_{101}(t)$; equality with the equidimensional primary hull excludes lower-dimensional associated primes. Generic length one then makes the special ideal prime. The saturated Jacobian has rank at least six on the projective charts, including the locus where the original quadrics lose rank. Thus its curve is smooth. A rational smooth point on this integral special curve forces its constant field to be $\mathbb{F}_{101}$, giving geometric integrality. The identical Hilbert series in both characteristics implies that each homogeneous part over $\mathbb{Z}_{(101)}$ is free. Flatness and properness transfer smoothness and geometric integrality to the generic projective fibre. The corresponding ideal and chart calculations are included in the supplement.

Let $f = F_0/Q_{33}$ for the two quadrics of Appendix A. On C each cuts a divisor of degree 56. Matching the zero-dimensional multiplication algebras of the two sections gives a common divisor of degree 40, so $\deg f = 16$. The quarter-turn and an axial reflection induce a Klein four-group on C (the half-turn acts by scalar multiplication). The three nonidentity elements have fixed-point counts $8, 0, 0$; Riemann–Hurwitz gives genus seven for $D = C/V_4$. Both quadrics are invariant. The induced function f has degree four on D.

For clarity, the arithmetic input from the quotient has a short form. In $\mathbb{Q}(D)$ both of the following are squares:

$$-3f(f^2+2), \qquad 3(f+1)(f+2)(f^2+2f+6)(3f^2+2f+4). \tag{1}$$

Here is how the equations are certified. A primitive invariant Y is a ratio of quadrics with denominator Q_{33}. Its quartic over $\mathbb{Q}(f)$ is given in the supplementary file `br28_tetragonal_exact_v4_certificate.md`. Clearing denominators and reducing modulo the saturated ideal gives zero over $\mathbb{Q}$. For primitivity, the good fibre $f = 2$ at 101 exhibits four distinct values of the integral ratio Y, each with multiplicity four. A relation of smaller Y-degree, made primitive at 101 and stripped of any common power of $f - 2$ after reduction, would contradict this fibre. For the monic quartic $Y^4 + bY^3 + cY^2 + dY + e$ the cubic resolvent $Z^3 - cZ^2 + (bd - 4e)Z + 4ce - b^2e - d^2$ splits into three distinct linear factors. The transitive quartic group therefore equals the Klein four-group. At each resolvent root z, the squared difference between the sums of the two paired roots is $b^2 - 4c + 4z$. Two of the resulting squareclasses are represented by (1). Their odd branch orders distinguish the two classes and their product. In particular a rational point of C with nonexceptional rational f satisfies the two square conditions simultaneously.

3 The four covers

Write $f = a/b$ in lowest terms. Set

$$A = (a+b)(a+2b), \quad B = (a+b)^2 + 5b^2, \quad C_1 = 3a^2 + 2ab + 4b^2.$$

For finite $f \neq -1, -2$, squarehood of $3ABC_1$ forces $A, B, C_1 > 0$. The pairwise resultants of the dehomogenized forms are $30, 60, 180$; they have no common projective zero outside $2, 3, 5$. Thus their squarefree parts d_A, d_B, d_C divide 30 and $3d_Ad_Bd_C$ is a square. If a is even and b odd, $C_1/4 = 3(a/2)^2 + (a/2)b + b^2$ is odd; for odd a, C_1 is odd. Hence d_C is odd. There are 32 formal triples.

Lemma 2. *Only* $(1,1,3), (2,6,1), (3,5,5), (6,6,3)$ *can occur.*

Proof. For $q = 16, 9$, write p for the prime dividing q. Test $(a,b) = (u,1)$ for all $u \bmod q$ and $(1,v)$ for $p \mid v$. These charts cover primitive pairs up to unit scaling, which preserves all four square tests

by homogeneity. Require A, B, C_1 to be d_i times squares and $-3ab(a^2+2b^2)$ to be a square. At 16 the four displayed triples and $(10,6,5),(30,6,15)$ remain. Modulo 9 the latter two fail. The complete enumeration is also checked by the Lean kernel. □

Put $s=(f+1)/(f+2)$, $B_0=6s^2-10s+5$, $C_0=12s^2-14s+5$. The three conditions become squarehood of $s/d_A, B_0/d_B, C_0/d_C$. We treat exceptional values projectively.

The rational rank-zero quotient. On $(3,5,5)$ write $t=f+1$ and $y^2=15t(t+1)(t^2+5)$. Taking $X=75/t+75$, $Y=75y/t^2$ gives $Y^2=X^3-150X^2+6750X$. PARI/GP returns rank bounds $[0,0]$ and torsion generated by $(0,0)$ of order two. The inverse $f=75/(X-75)-1$ sends the two points to $-1,-2$.

Descent for the other three covers. For the first two work over $K=\mathbb{Q}(w)$, $w^2=-5$, with $\beta=(5+w)/6$ and $B_0=6(s-\beta)(s-\bar{\beta})$. Away from $2,3,5$ a pole of s has even valuation since s/d_A is square. At a zero of $s-\beta$ the conjugate factor is a unit, so this valuation too is even. The S-class group is trivial and the squareclasses of the S-units are generated by $-1, 2, 1-w, -1-w, -w$. Taking norms leaves the possibilities

$$\gamma = h(1-w) \quad (1,1,3), \qquad \gamma = h \quad (2,6,1), \qquad h \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

with $\gamma(s-\beta)$ square. Indeed $\mathrm{Norm}(s-\beta)=B_0/6$ has class 6 and 1 respectively. For $(6,6,3)$ use $v^2=-11$, $\alpha=(7+v)/12$ and $C_0=12(s-\alpha)(s-\bar{\alpha})$. The class group is trivial; support above $2,3,11$ and the square norm $C_0/12$ give the same eight h, this time with $h(s-\alpha)$ square. The supplement certifies both ordinary class groups with PARI/GP and verifies triviality of the two localized class groups.

The following table gives a good prime at which each discarded class has empty intersection with the reductions of the global elliptic groups. A dash marks the class to be treated globally.

	-1	1	-2	2	-3	3	-6	6
$(1,1,3)$	23	7	23	7	7	43	7	–
$(2,6,1)$	23	7	23	7	7	–	7	29
$(6,6,3)$	23	59	23	53	23	53	23	–

For each prime the sieve reduces the base elliptic curve $Y^2=X^3+18X$ ($X=-3f$) and the three quotients given by products of two of the three square roots. It enumerates the reductions of the global groups, using the *same* roots to compute all three quotient images and the same s for the number-field square test. An empty intersection excludes the class at every height. Both base torsion cosets are accounted for; the opposite coset in each of the three rows is already excluded at 13. The quotient maps, reductions and local tests are provided as executable rational and finite-field arithmetic. Primitivity is essential here. We use Cremona's published generators for 2304p1, 9600bn1, 28800bn1, 660b1, 31680cj1, 52800do1, 79200en2 and 158400jl1 [5]. In particular the generator for the last quotient has raw coordinates $(1,79)$.

4 The surviving elliptic curves

The class $h=6$ on $(1,1,3)$. Use $W^2=6(1-w)(s-\beta)$ and $\eta^2=((1+w)/2)(s-\bar{\beta})C_0$. Their product is $3B_0C_0$, a square on the cover. With $X=6(1+w)s-(10+4w)$ and $Y=6(1+w)\eta$ the equations become

$$Y^2=X^3+(13+w)X^2+(30+12w)X, \qquad s=\{6(5-w)+(1-w)X\}/36.$$

Over K the rank bounds are $[1,1]$, with torsion generated by $T=(0,0)$. Put $P=(-4+2w,-12+6w)$. Elliptic Chabauty on $\langle P,T\rangle$ returns $O,P,-P$ with rational s and index integer 120. For $\ell=2,3,5$ the division checks on P and its torsion translate certify saturation at ℓ. Thus the subgroup index is coprime to 120, the condition for completeness in Magma's Chabauty algorithm [2, 6]. The images are $\infty,1,1$. The leading coefficient 6 of B_0 excludes a rational lift of $s=\infty$ on this cover; $s=1$ gives $f=\infty$.

The class $h=3$ on $(2,6,1)$. The auxiliary quartic $z^2=6sC_0(s-\beta)$ gives

$$Y^2=X^3+(10+14w)X^2+180wX, \qquad s=-5(5+w)/(X-30).$$

The two-isogeny descent gives Kummer image sizes four and two. On the dual side the remaining classes $w,-11w$ fail at the dyadic prime: both local charts are empty at precision eight in its uniformizer. On the original side $P=(-20-10w,100-40w)$ and $T=(0,0)$ have independent classes $-1,-w$. The rank is one and $\langle P,T\rangle$ has odd index. Elliptic Chabauty with this explicit group map returns index integer 8; coprimality now follows without finding an odd saturation index. The rational images are $0,1/2,1/2$. At zero, $3(s-\beta)$ has nonsquare norm $15/2$; $s=1/2$ gives $f=0$.

The class $h=6$ on $(6,6,3)$. Write $W^2=6(s-\alpha)$ and $y^2=2B_0C_0$. The substitution $X=6(s-\bar{\alpha})$, $Y=3y/W$ gives

$$Y^2=X^3+(-3-v)X^2+(9+3v)X/2, \qquad s=(7-v)/12+X/6.$$

Here $W=0$ would give the irrational $s=\alpha$. The rank bounds over $\mathbb{Q}(v)$ are $[0,0]$ and the torsion has order two. Its nonidentity point maps to $(7-v)/12$, leaving only $s=\infty$ over $\mathbb{Q}$, or $f=-2$. This finishes the restriction to $f\in\{0,-2,-1,\infty\}$.

5 Recovering points on the original curve

The pencil has base points in all three rational fibres, so the value of the map there must be read after cancellation in the local ring. At the eight points listed over ∞ the orders of (F_0,Q_{33}) are $(1,3)$; at the eight over zero they are $(3,1)$. The multiplication matrices for the two sections give these orders on the smooth curve. At the remaining eight listed points the orders are $(1,1)$ and the local jets of F_0+2Q_{33} vanish to order at least three. Each list therefore contributes at least $8\cdot 2=16$ to its own fibre. Since the map has degree 16, all three lists are exhaustive.

Over -1 the shared section has four quadratic factors in a separating coordinate. Their discriminants are $10u^2$ for $u=124,526,478,924$. At each of the eight conjugate points the local jet computation gives ramification index at least two. This accounts for the entire fibre and excludes rational lifts. Finally the linear map to the 25 cells evaluated on the table gives twelve zero first moments, twelve equal second moments and three distinct entries in every case. This proves Theorem 1.

Verification and credits. The electronic supplement is available from the immutable BR28 verification release v1.0.0. The reviewed source is in the verification repository `Aky-lab/br28-genus29` at revision `5ad9006`. It includes the three Magma V2.29-10 inputs and fresh outputs, the Singular and PARI/GP calculations, and the point-table and sieve code. Lean 4.30 checks normalization and distinctness, vanishing on 33 explicit generators, all cell and line-moment checks, and the finite squareclass sieve. The identification of those generators with the saturated ideal uses Singular;

the global exhaustion uses the descents and computer algebra above. Standard background on covering and the Mordell–Weil sieve is given in [3, 4]. Akram Younso directed the project. AI agents developed the mathematical argument, computation, formal checks and manuscript.

A Defining equations and pencil

To recover the array, let M have as its rows the following coefficients, in row-major cell order up to the central cell:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 & 1 & -1 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 1 & 2 & -1 & -1 & 1 & -2 \\ -1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

The first twelve cells are Mz, the middle cell is zero and the last twelve are the negatives of the first twelve in reverse order.

Each column ij gives the coefficient of $z_i z_j$, counted once. The two blocks continue the same rows.

	00	01	02	03	04	05	06	07	11	12	13	14	15	16	17	22	23	24
q_1	2	-2	2	2	0	0	0	0	2	-2	-2	0	0	0	0	2	2	0
q_2	4	-4	0	8	-8	-4	0	-8	2	-4	-8	4	4	-4	8	4	8	0
q_3	2	-4	4	6	-2	-2	2	-4	2	-4	-6	2	2	-2	4	2	6	-2
q_4	2	0	-2	0	-2	0	-2	0	0	0	0	0	0	0	0	2	0	2
q_5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0
q_6	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
c_1	0	-2	2	2	1	0	0	0	2	-2	-3	0	0	0	0	0	2	-1
c_2	-1	0	1	-1	2	0	0	1	-1	0	1	-1	1	1	0	1	1	1
c_3	-1	4	-4	-4	0	1	0	1	-2	3	4	-1	-1	-1	-1	-1	-4	1
F_0	0	1	-2	0	0	1	-2	2	0	1	0	-1	-1	1	-2	0	0	2
Q_{33}	0	2	-4	-3	-2	0	-2	0	0	2	3	0	0	0	0	0	-3	2

	25	26	27	33	34	35	36	37	44	45	46	47	55	56	57	66	67	77
q_1	0	0	0	2	0	0	0	0	-2	-2	2	-2	-2	2	-2	-2	2	-2
q_2	-4	8	-8	8	-8	-8	8	-16	2	2	2	6	0	-2	6	2	-6	6
q_3	-2	2	-4	6	-4	-4	4	-8	0	2	-2	4	0	-2	4	0	-4	4
q_4	0	2	0	0	0	0	0	0	0	-2	4	-2	-2	2	-2	0	2	-2
q_5	0	0	0	0	0	0	0	0	-2	-2	2	-2	-2	2	-2	-2	2	0
q_6	0	0	0	0	0	0	0	0	0	2	-2	2	0	-2	2	0	-2	0
c_1	0	0	0	3	-1	-1	1	-2	-1	-1	0	0	0	0	0	0	0	0
c_2	-1	-1	-1	-1	4	0	0	2	0	0	0	-2	0	0	0	0	0	0
c_3	1	1	1	-4	0	2	0	2	0	0	0	0	0	0	-1	0	0	0
F_0	1	0	2	0	2	2	-2	4	0	-1	0	-2	-1	1	-2	0	2	-2
Q_{33}	0	2	0	-3	0	0	0	0	0	0	3	0	0	0	0	0	0	0

The sixteen linear factors for the saturation are $z_0, \dots, z_7$ and

$$z_5 + z_7, \quad z_4 + z_5 - z_6 + z_7, \quad z_0 - z_1 + z_2 + z_3, \quad z_0 - z_2 - z_4 - z_6,$$
$$z_0 - z_1 + z_2 + 2z_3 - z_4 - z_5 + z_6 - 2z_7, \quad z_6 - z_7, \quad z_6 + z_7, \quad z_5 - z_6.$$

B Rational points in primitive projective coordinates

The first nonzero entry is positive. The fibre labels give the value after resolving the pencil.

f	z_0	z_1	z_2	z_3	z_4	z_5	z_6	z_7
∞	1	1	1	-1	-1	-1	0	1
∞	1	-1	-1	-1	1	-1	0	-1
∞	1	1	1	0	0	-1	1	1
∞	1	1	-1	0	0	1	1	-1
∞	1	1	1	0	0	1	-1	-1
∞	1	-1	-1	0	0	1	1	1
∞	1	1	1	-1	1	1	0	-1
∞	1	1	-1	1	1	-1	0	1
0	1	-1	-1	-1	0	-1	1	1
0	1	1	-1	0	1	1	0	-1
0	1	1	1	-1	0	1	1	-1
0	1	1	1	0	1	-1	0	1
0	1	1	1	0	-1	1	0	1
0	1	1	-1	1	0	-1	1	1
0	1	1	1	-1	0	-1	-1	-1
0	1	-1	-1	0	1	1	0	-1
-2	0	1	1	0	0	0	-1	0
-2	1	1	0	0	1	0	0	-1
-2	0	1	1	0	-1	0	0	0
-2	0	0	1	0	0	1	0	0
-2	1	1	0	0	0	0	1	1
-2	1	0	0	0	0	-1	0	1
-2	0	0	1	-1	0	-1	0	0
-2	1	0	0	-1	0	1	0	-1

References

[1] C. Boyer, Some notes on the magic squares of squares problem, *Math. Intelligencer* (2005), doi:10.1007/BF02985794.

[2] N. Bruin, Chabauty methods using elliptic curves, *J. reine angew. Math.* 562 (2003), 27–49.

[3] N. Bruin and M. Stoll, Two-cover descent on hyperelliptic curves, arXiv:0803.2052.

[4] N. Bruin and M. Stoll, The Mordell–Weil sieve: proving non-existence of rational points on curves, arXiv:0906.1934.

[5] J. Cremona, *Elliptic curve data*, generator tables and documentation, `https://johncremona.github.io/ecdata/`.

[6] Computational Algebra Group, University of Sydney, *Magma Handbook*, elliptic Chabauty over number fields, `https://magma.maths.usyd.edu.au/magma/handbook/text/1568`.