Exact Sumsets of Primitive Quadratic Norms

Roy van Rijn

Abstract

We determine the exact binary sumsets of primitive quadratic norm values at discriminants $-3, -7, -8, -11$. The local congruence conditions are sufficient in three cases; at discriminant -7 the complete additional exception set is $\{7, 77, 203\}$. Stronger split-prime core identities separate the ramified dilations. The proofs combine quaternionic norm shells, precisely normalized classical Hecke bounds, and dyadic and ramified local filters. Explicit infinite estimates, rational interval certificates, complete finite sumset scans and multiplicative descent cover every positive target. We supply standalone verification code and explain the finite reductions that make the certificates complete. All sumsets concern numerical values, without coordinate multiplicities.

hexagon:2611.00673v1

1 Exact binary sumsets

Which integers are sums of two primitive values of a quadratic norm? We determine the complete sumsets in four class-number-one cases, including every small exception and a proof covering every remaining target.

The companion paper [9] develops broader pointwise correlation asymptotics. The exact classifications here have their own classical proof route and do not depend on that paper.

For a negative discriminant d, put

$$P_d = \{Q_d(x,y) > 0 : x, y \in \mathbb{Z},\ \gcd(x,y) = 1\},$$

d	$Q_d(x,y)$
-3	$x^2 - xy + y^2$
-7	$x^2 + xy + 2y^2$
-8	$x^2 + 2y^2$
-11	$x^2 + xy + 3y^2$.

Zero coordinates and both signs are allowed. Each summand is a positive numerical value; different coordinate representations do not create new summands.

Theorem 1.1. *The exact binary sumsets are*

d	$P_d + P_d$
-3	$\{N \geq 2 : N \text{ even},\ N \not\equiv 0, 12 \pmod{18}\}$,
-7	$\{N \geq 2 : 49 \nmid N\} \setminus \{7, 77, 203\}$,
-8	$\{N \geq 2 : 16 \nmid N\}$,
-11	$\{N \geq 2 : N \text{ even},\ 121 \nmid N\}$.

For the Eisenstein row, let

$$\mathcal{A} = \{n \geq 1 : p \mid n \Longrightarrow p \equiv 1 \pmod{3}\}.$$

Here $1 \in \mathcal{A}$. Proposition 3.1 proves

$$P_{-3} = \mathcal{A} \sqcup (3 \cdot \mathcal{A}).$$

An inert prime cannot divide a primitive norm, while the ramified prime occurs at most once; conversely the split-prime core and its ramified dilation have primitive witnesses. The same

reduction in the other three rings explains why we prove stronger core sumset identities before restoring ramified factors.

Our method adapts the quaternionic norm-shell and torus-normalizer argument used for the Gaussian restricted-prime theorem of Howe, Huffman, Kohlmeyer and Kruer [1, Theorem 1.1]. A quaternion shell produces many candidate pairs of binary norms. The Hecke spectrum bounds the fraction spoiled by each forbidden prime. Exact dyadic and ramified filters keep the total fraction below one. The spectral input is classical Jacquet–Langlands and the weight-two Ramanujan bound; Section 2 states its normalization. The applications require different local quotients, including all ideal classes and inverse-unit mass at discriminant eleven.

Explicit estimates settle an infinite range; rational interval certificates meet complete finite scans, and multiplicative descent exhausts the targets. Appendix A explains the exact programs and completeness arguments. Table 1 records these joins. Here C_d is the core defined in its section, n is a reduced target, and m at -8 is an odd inert-supported core. Each interval certificate covers every target of the indicated reduced families in its interval.

Table 1: Coverage of the exact classifications. All finite scans include only the locally eligible targets of the indicated families.

d	Complete finite scan	Rational interval bridge	Infinite estimate	Descent and dilation
-3	$N < 10^8$: $\mathcal{A}+\mathcal{A}$ and $\mathcal{A}+3\cdot\mathcal{A}$.	No interval bridge needed.	Reduced $n \geq 10^8$, in both admissible classes modulo six.	Remove all split-prime factors, then scale back; use $P_{-3} = \mathcal{A} \sqcup 3\cdot\mathcal{A}$.
-7	$N \leq 2^{24}$: $C_7 + C_7$ and $P_7 + P_7$, with their listed exceptions.	257 intervals on $[2^{24}, 2^{37})$; 17 on $[2^{37}, 2^{54})$, for inert-supported targets and split primes.	The same reduced families for $n \geq 2^{54}$.	Remove split factors; patch quotients $11, 29$. Ramified dilation by seven gives the primitive exceptions.
-8	$N \leq 2^{27}$: $C_8 + C_8$ and $C_8 + 2C_8$.	107 intervals: $m \in [2^{27}, 2^{60})$ for mixed sums, $[2^{26}, 2^{60})$ at $2m$, and $[2^{20}, 2^{60})$ at $4m$.	Inert cores $m \geq 2^{60}$; the mixed prime boundary holds for primes $N \geq 2^{22}$.	Remove split factors; the remaining targets are $m, 2m, 4m$. Use $P_{-8} = C_8 \sqcup 2C_8$.
-11	$N \leq 2^{25}$: $C_{11} + C_{11}$.	35 intervals on $[2^{25}, 2^{60})$, for even inert-supported targets prime to eleven.	The same reduced family for $n \geq 2^{60}$.	Remove split factors; ramified dilation by eleven gives $P_{-11} + P_{-11}$.

Section 3 proves the two Eisenstein core identities; Sections 4–6 treat the other discriminants.

2 The quaternionic Hecke estimate

The large-target arguments below use the same classical spectral input. We state it once, allowing the fixed dyadic level needed for discriminant -8. The arithmetic sections identify their finite quotients, their character components and their shell normalizations separately.

Let B be a definite quaternion algebra over $\mathbb{Q}$, and write $H = PB^\times$. Let $U \subset H(\mathbb{A}_f)$ be an open compact subgroup obtained from order units and congruence kernels. Equip the finite space

$$X = H(\mathbb{Q})\backslash H(\mathbb{A}_f)/U$$

with its invariant probability measure. Before imposing a fine level, the mass of a locally principal ideal class is proportional to the reciprocal of the size of its projective unit group. If the fine stabilizers are trivial, this is uniform counting measure on fine points, whose pushforward is the stated class measure. It is essential to retain every ideal class.

For an integer m prime to the discriminant of B and to the nonmaximal or auxiliary level primes, let T_m be the all-integral-ideal Hecke operator, with maximal local level at every prime

dividing m. This includes imprimitive ideals. Its constant eigenvalue is $\sigma(m)$, and its local recurrence is

$$T_{\ell^{a+2}} = T_\ell T_{\ell^{a+1}} - \ell T_{\ell^a}.$$

These conventions are those of [2, Propositions 41.3.1 and 41.3.6].

Lemma 2.1. *The operators T_m are commuting and self-adjoint for the invariant measure. On the orthogonal complement of all global reduced-norm characters occurring in $L^2(X)$,*

$$\|T_m\| \le \tau(m)\sqrt{m}.$$

More precisely, every simultaneous eigenvector in that complement has unramified roots $\sqrt{\ell}\,u_\ell, \sqrt{\ell}\,v_\ell$ with $|u_\ell| = |v_\ell| = 1$ and $u_\ell v_\ell = 1$. Fixed operators at level primes are not covered by this unramified assertion.

Proof. First, reversing an ideal flag gives the adjoint. If $J \subset I$ has relative reduced norm m, elementary divisors at its split index primes give $mI \subset J$. The reversal

$$(J \subset I) \longmapsto (mI \subset J)$$

is an involution up to central scaling. At auxiliary primes m is a unit and the local ideals are equal, so their markings transfer through that equality; identifying mI with I changes the marking only by a projectively trivial scalar. Thus the reverse marked correspondence has the same kernel. On fine quotients it is symmetric, and on coarse quotients its pushforward is symmetric for inverse-unit mass. The usual relatively prime ideal composition gives commutativity and the displayed recurrence.

We specify the automorphic input and its hypotheses. Decompose the automorphic functions on this definite quotient, with trivial infinite type, into irreducible constituents. A finite-dimensional irreducible smooth representation of $\mathrm{GL}_2(\mathbb{Q}_\ell)$ is a determinant character. Indeed its kernel is open, after intersecting the open stabilizers of a basis; conjugation of elementary unipotents by diagonal matrices and normality show that this kernel contains $\mathrm{SL}_2(\mathbb{Q}_\ell)$.

If a constituent is a character at one split finite place ℓ, strong approximation for B^1, away from $\{\infty, \ell\}$, shows that it is a global norm character. To make the implication explicit, for an automorphic function f, a finite adele x and $h \in B^1(\mathbb{A}_f)$, approximate xhx^{-1} outside ℓ by $\gamma \in B^1(\mathbb{Q})$, sufficiently closely for the right stabilizers of f. Outside ℓ, the points xh and γx then have the same value; at ℓ the discrepancy lies in the local norm-one group, which acts trivially. Left rational invariance gives $f(xh) = f(x)$. Thus the constituent factors through reduced norm. The strong approximation hypothesis is satisfied because B^1 is split and noncompact at ℓ [2, Main Theorem 28.5.3].

After removing the global norm characters, every split local factor is infinite dimensional. Global Jacquet–Langlands therefore transfers each remaining constituent to a cuspidal representation of GL_2 [3, Theorem 14.4]. Its trivial infinite type transfers to weight two [3, Section 5, Proposition 5.20]. At each $\ell \mid m$ the quaternion algebra is split and the level is maximal, so transfer preserves the unramified eigenvalues. Fixed levels elsewhere, including a nonmaximal dyadic level, do not change this assertion.

The weight-two roots have absolute value $\sqrt{\ell}$: combine the Frobenius–Hecke relation and purity in [4, Theorems 4.9 and 5.1] with [5, Theorem 1.6]. The central character is trivial, so the normalized roots have product one. The all-ideal eigenvalue at ℓ^a is

$$\ell^{a/2} \sum_{j=0}^{a} u_\ell^j v_\ell^{a-j},$$

whose absolute value is at most $(a+1)\ell^{a/2}$. Multiplicativity and simultaneous self-adjointness give the claimed operator norm. □

3 The Eisenstein proof

3.1 Arithmetic preliminaries and split-prime cores

Let $Q(x,y) = x^2 - xy + y^2$, $\omega^2 + \omega + 1 = 0$ and $R = \mathbb{Z}[\omega]$. Thus $Q(x,y) = N(x + y\omega)$. We use the semigroup $\mathcal{A}$ defined above and write $\mathcal{N} = P_{-3}$. Every member of $\mathcal{A}$ is 1 mod 6. The ramified dilation $3{\cdot}\mathcal{A} = \{3a : a \in \mathcal{A}\}$ has residue 3 mod 6.

The elementary norm-value identity separates the two binary problems. Its proof uses only prime splitting and unique factorization.

Proposition 3.1. *The primitive Eisenstein norms are exactly*

$$\mathcal{N} = \mathcal{A} \sqcup (3{\cdot}\mathcal{A}).$$

Proof. If an inert prime p divides $Q(x,y)$, it divides both coordinates, since R/pR is a field, including when $p = 2$. Also $9 \mid Q(x,y)$ forces $3 \mid x, y$. Indeed, $3 \mid Q(x,y)$ gives $x + y \equiv 0 \pmod 3$; writing $y = -x + 3t$ gives

$$Q(x,y) = 3(x^2 - 3xt + 3t^2).$$

Divisibility by 9 now forces $3 \mid x$, and hence $3 \mid y$. Thus a primitive norm has no inert prime factor and contains at most one factor 3. It belongs to the stated union.

Conversely, the triangular Eisenstein lattice has covering radius $1/\sqrt{3}$, so rounding gives a remainder of norm at most $1/3 < 1$. Thus $R = \mathbb{Z}[\omega]$ is norm Euclidean and is a unique factorization domain. For a rational prime $q \equiv 1 \pmod 3$, choose a nontrivial cube root $t \in \mathbb{F}_q^\times$. The ideal $(q, \omega - t)$ has quotient $\mathbb{F}_q$; its principal generator π_q therefore has norm q. The two distinct roots t, t^{-1} yield conjugate, nonassociate factors. Thus $q = \pi_q \bar{\pi}_q$, up to a unit. For $a = \prod q^{e_q} \in \mathcal{A}$, choose one factor π_q at each q and put $z = \prod \pi_q^{e_q}$. Then $N(z) = a$. The element $(1 - \omega)z$ has norm $3a$. Neither element is divisible by a rational prime: a split rational prime would require both conjugate factors, an inert prime cannot divide its norm, and 3 is associated to $(1 - \omega)^2$, whereas at most one factor $1 - \omega$ was used. Their coordinates in the integral basis $1, \omega$ are therefore coprime. Finally, the two sets are disjoint, since elements of $\mathcal{A}$ are prime to 3. □

Theorem 3.2. *One has*

$$\mathcal{A} + \mathcal{A} = \{n > 0 : n \equiv 2 \pmod 6\}, \qquad \mathcal{A} + (3{\cdot}\mathcal{A}) = \{n > 0 : n \equiv 4 \pmod 6\}.$$

A reduction that helps both problems. Put $\mathcal{P} = \{p \text{ prime} : p \equiv 2 \pmod 3\}$. For either admissible residue class, write $n = gn_0$, where $g \in \mathcal{A}$ contains every prime-power factor of n with prime 1 modulo 3. Since $g \equiv 1 \pmod 6$, the target n_0 has the same residue as n. A decomposition of either type for n_0 scales by g to the corresponding decomposition of n. We can therefore concentrate on

$$n \equiv 2 \text{ or } 4 \pmod 6, \qquad p \mid n \Longrightarrow p \in \mathcal{P}. \tag{1}$$

This reduction will matter in the divisor estimates and in the exact calculation at 3. The finite certificates cover all targets in their respective ranges, so they need no reduction.

3.2 Counting with Eisenstein norms

We begin by finding plenty of candidate pairs. A quaternion packages two Eisenstein norms into one multiplicative norm, which lets us count the representations exactly. This count is the supply of pairs from which we will remove the bad ones.

For positive integers, write $\sigma(n) = \sum_{d|n} d$ and $\tau(n) = \sum_{d|n} 1$. A term $\sigma(n/4)$ is interpreted as zero when $4 \nmid n$. Let $\omega^2 + \omega + 1 = 0$, $R = \mathbb{Z}[\omega]$, and

$$Q(x, y) = x^2 - xy + y^2 = N_{\mathbb{Q}(\omega)/\mathbb{Q}}(x + y\omega).$$

For instance, $Q(3, 1) = 7$ and $Q(4, 1) = 13$, so 20 is represented by $Q(x, y) + Q(u, v)$ with both norms already in $\mathcal{A}$.

Consider the definite quaternion algebra and order

$$B = \mathbb{Q}(\omega) \oplus \mathbb{Q}(\omega)j, \qquad j^2 = -1, \quad jz = \bar{z}j, \qquad \mathcal{O} = R \oplus Rj.$$

Its reduced norm is

$$\mathrm{nrd}(z + wj) = N(z) + N(w).$$

In the basis $1, \omega, j, \omega j$, the trace pairing has determinant -9. Consequently $\mathcal{O}$ has reduced discriminant 3. Definiteness and the parity of the ramification set imply that the algebra discriminant is 3, so $\mathcal{O}$ is maximal.

Every complex number is within squared distance $1/3$ of an Eisenstein integer: the equilateral triangles in the lattice have circumradius $1/\sqrt{3}$. Rounding the two complex coordinates independently gives

$$\forall x \in B \otimes \mathbb{R} \quad \exists q \in \mathcal{O} : \quad \mathrm{nrd}(x - q) \le 2/3 < 1.$$

The one-coordinate rounding bound also makes R norm Euclidean, hence a unique factorization domain. The two-coordinate bound makes $\mathcal{O}$ norm Euclidean on either side. In a nonzero integral right ideal, choose α of least positive norm and divide each β by α on the left. A nonzero remainder would have smaller norm, so the ideal is $\alpha\mathcal{O}$. Fractional ideals reduce to this case by scaling; the right ideal class number is one.

The units are precisely $R^\times \cup R^\times j$, and there are twelve. For $3 \nmid n$ let

$$\mathcal{Q}_n = \{\alpha \in \mathcal{O} : \mathrm{nrd}(\alpha) = n\}, \qquad r(n) = |\mathcal{Q}_n|.$$

At a prime $\ell \mid n$ the order is locally $M_2(\mathbb{Z}_\ell)$. There are $1 + \ell + \cdots + \ell^e$ integral right ideals of reduced norm ℓ^e, by the index-ℓ^e sublattice count in $\mathbb{Z}_\ell^2$. Multiplication of the local counts and principality give $\sigma(n)$ right ideals of norm n, each with twelve generators of that norm. Hence

$$r(n) = 12\sigma(n) \qquad (3 \nmid n). \tag{2}$$

This is the usual all-integral-ideal normalization of a Brandt operator; see [2, Proposition 41.3.1].

For $n \equiv 2 \pmod 3$, both component norms in every representation $n = Q(x, y) + Q(u, v)$ are $1 \pmod 3$, because $Q(x, y) \equiv (x + y)^2 \pmod 3$ is either 0 or 1. In particular both summands are positive and neither is divisible by 3.

3.3 Keeping the unwanted primes out

A norm representation is only a candidate. A prime $p \equiv 2 \pmod 3$ can occur to even exponent in an Eisenstein norm, and that already keeps the value out of $\mathcal{A}$. The useful feature is that divisibility of the norm forces divisibility of both coordinates.

For $p \in \mathcal{P}$, the quotient R/pR is a field, including when $p = 2$. Therefore

$$p \mid Q(x, y) \quad \Longleftrightarrow \quad p \mid x \text{ and } p \mid y. \tag{3}$$

We first establish the unfiltered Hecke estimate. Section 3.4 will impose oddness and derive the local bounds used in the sieve.

3.3.1 The finite quotient and its Hecke operator

Fix an odd $p \in \mathcal{P}$, so $p \geq 5$, and first suppose $p \nmid n$. Reduction gives $\mathcal{O}/p\mathcal{O} \simeq M_2(\mathbb{F}_p)$, with norm equal to determinant. Write

$$G_p = \mathrm{PGL}_2(\mathbb{F}_p), \quad \Gamma_p = \rho_p(\mathcal{O}^\times), \quad Y_p = \Gamma_p \backslash G_p.$$

Only ± 1 among the units reduce to scalars, so $|\Gamma_p| = 6$ and $|Y_p| = p(p^2-1)/6$. Equip $\mathbb{C}[Y_p]$ with counting measure and define

$$(T_n f)(\Gamma_p g) = \frac{1}{12} \sum_{\alpha \in \mathcal{Q}_n} f(\Gamma_p \rho_p(\alpha) g). \tag{4}$$

Right multiplication by a unit permutes $\mathcal{Q}_n$, proving that this is well-defined. It commutes with the right G_p action. Conjugation preserves $\mathcal{Q}_n$ and is projective inversion, so T_n is self-adjoint. Also $T_n 1 = \sigma(n) 1$.

The determinant character $\chi_p(\Gamma_p g) = (\det(g)/p)$ is well-defined, because the units have norm one and scalar matrices have square determinant. Directly, $T_n \chi_p = (n/p)\sigma(n)\chi_p$.

3.3.2 The spectral bound

This is the main imported ingredient. It turns the large supply of norm representations into control of their distribution modulo a prime. The normalization matters, so we identify the concrete operator before using Jacquet–Langlands and the weight-two Ramanujan bound.

There are three things to check: the finite operator must be the stated Hecke correspondence, the two large character components must be removed, and the remaining spectrum must transfer to weight two. The proof below checks these points in that order. Readers following the arithmetic first can use the bound and continue with the normalizer average in the next subsubsection.

Lemma 3.3. *On $\{1, \chi_p\}^\perp \subset \mathbb{C}[Y_p]$, the operator T_n has norm at most $\tau(n)\sqrt{n}$, provided $(n, 3p) = 1$.*

Proof. Class number one identifies the adelic quotient at the reduction kernel with $\Gamma_p \backslash G_p$. Indeed an adelic ideal principalizes; and a rational projective element in all local order-unit groups can be rescaled by a rational scalar to an order unit, since the local valuations of its norm are even. Its invariant measure is counting measure up to normalization.

The all-integral-ideal correspondence divides the principal shell by twelve units. Principalization acts by $\rho_p(\alpha^{-1})$; projectively this equals $\rho_p(\bar{\alpha})$, and conjugation permutes the shell. Thus its operator is exactly (4), including the prime-power normalization. Every global norm character restricts to a character of G_p. A character of $\mathrm{GL}_2(\mathbb{F}_p)$ kills elementary unipotents and hence factors through determinant; descent to PGL_2 leaves only the trivial and quadratic determinant characters. Both have been identified above. Removing them, Lemma 2.1 therefore applies for $(n, 3p) = 1$ and gives the asserted bound. □

3.3.3 Torus-normalizer averaging

The image $C_p = (R/pR)^\times / \mathbb{F}_p^\times$ is a nonsplit torus. Its normalizer is $K_p = C_p \cup C_p \rho_p(j)$, of order $2(p+1)$. All twelve order units lie in $R^\times \cup R^\times j$, so $\Gamma_p \subset K_p$. Put

$$O_p = \Gamma_p \backslash K_p \subset Y_p, \qquad f_p = 1_{O_p}, \qquad \mu_p = \frac{|O_p|}{|Y_p|} = \frac{2}{p(p-1)}.$$

An invertible quaternion has one of its two Eisenstein components zero modulo p exactly when its projective reduction lies in K_p. Let $b_p(n)$ count the unfiltered representations spoiled by p. Consequently

$$b_p(n) = 12(T_n f_p)(\Gamma_p).$$

Both f_p and $T_n f_p$ are right-K_p invariant. Therefore

$$(T_n f_p)(\Gamma_p) = \frac{\langle f_p, T_n f_p \rangle}{|O_p|}.$$

The norm map $\mathbb{F}_{p^2}^\times \to \mathbb{F}_p^\times$ is onto, so O_p has equally many determinant-square and determinant-nonsquare points. Thus $f_p - \mu_p 1$ is orthogonal to both 1 and χ_p, and has squared norm $|O_p|(1-\mu_p)$. The spectral lemma gives

$$\frac{b_p(n)}{r(n)} \le \frac{2}{p(p-1)} + \frac{\tau(n)\sqrt{n}}{\sigma(n)} \left(1 - \frac{2}{p(p-1)}\right). \tag{5}$$

3.4 An odd-component filter and the mixed case

The prime 2 need not take a share of the error budget. We can remove its obstruction exactly by keeping only odd norm components. This helps both binary problems and leaves room for the extra condition at 3 in the mixed case.

Throughout this subsection, n is even and $3 \nmid n$. Write $n = 2^e m$ with $e \ge 1$ and m odd, and put

$$S(n) = \sigma(n) - \sigma(n/4),$$

where a term with nonintegral argument is zero. Let $\mathcal{Q}_n^o$ consist of the representations in $\mathcal{Q}_n$ for which both Eisenstein component norms are odd.

3.4.1 Selecting odd components

Since 2 is inert in $\mathbb{Z}[\omega]$, an even component norm has both coordinates even. The two component norms of an even target have the same parity. Thus the representations excluded from $\mathcal{Q}_n^o$ are exactly the scalar multiples 2α, with $\alpha \in \mathcal{Q}_{n/4}$. Consequently

$$R_o(n) := |\mathcal{Q}_n^o| = 12S(n), \qquad S(n) = 3 \cdot 2^{e-1}\sigma(m) \ge \frac{3}{2}n. \tag{6}$$

Both retained norms are positive, since zero is even.

For an odd inert prime p, let $b_p^o(n)$ count the retained representations in which p divides either component norm. When $p \mid n$, all four coordinates are divisible by p whenever one component norm is. Scaling by p preserves oddness. Therefore

$$b_p^o(n) = 0 \quad (p^2 \nmid n), \qquad b_p^o(n) = 12S(n/p^2) \quad (p^2 \mid n),$$

and the usual local divisor-sum calculation gives

$$\frac{b_p^o(n)}{R_o(n)} < \frac{1}{p^2}. \tag{7}$$

3.4.2 The odd-component spectral estimate

Fix an odd inert prime $p \nmid n$, and use the quotient Y_p and operators T_u of Section 3.3. At this odd prime, the scalar 2 reduces projectively to the identity. Thus

$$D_n := T_n - T_{n/4}$$

is exactly the operator obtained by retaining only $\mathcal{Q}_n^o$; again the second term is zero when $4 \nmid n$. Its constant eigenvalue is $S(n)$, and its determinant-character eigenvalue is $(n/p)S(n)$, since 4 is a square modulo p.

On the orthogonal complement of these two characters, consider a simultaneous cuspidal eigenvector. At 2, write the normalized Satake roots as u, v, with $|u| = |v| = 1$ and $uv = 1$. The

last identity follows from the trivial central character of the projective quotient. The all-ideal eigenvalue at 2^e, minus the eigenvalue at 2^{e-2}, is

$$2^{e/2}\left(u^e+v^e+\frac{1}{2}\sum_{s=1}^{e-1}u^s v^{e-s}\right).$$

For $e=1$ the sum is empty. To obtain this expression, use $uv=1$ to identify the terms from 2^{e-2} with the interior terms from 2^e; the former have an additional factor $1/2$. Its absolute value is at most $((e+3)/2)2^{e/2}$. Multiplicativity and Lemma 3.3 at the odd factors of m now give

$$\|D_n\|_{\{1,\chi_p\}^\perp}\le\frac{e+3}{2}\tau(m)\sqrt{n}. \tag{8}$$

This estimate uses cancellation before taking absolute values.

Suppose further that n is reduced, so every prime factor lies in $\mathcal{P}$. The ratio of the right side of (8) to $S(n)$ is

$$n^{-3/10}H(e)\prod_{q^a\|m}F_q(a),\qquad H(e)=\frac{e+3}{3\,2^{e/5}},\qquad F_q(a)=\frac{(a+1)q^{4a/5}}{1+q+\cdots+q^a}.$$

The ratio $H(e+1)/H(e)$ decreases with e, and exact fifth-power comparisons show that $H(e)$ attains its maximum for $e\ge1$ at $e=4$. For $q\ge32$, one has $F_q(a)\le(a+1)q^{-a/5}\le1$. For the remaining odd inert primes, successive ratios are bounded by $((a+2)/(a+1))q^{-1/5}$. Once this upper bound is at most one it remains so. Checking the preceding exponents gives

q	5	11	17	23	29
maximizing exponent	2	1	1	1	0.

The product of the fifth powers of these maxima, including $H(4)^5$, is

$$\frac{22466116414662801589843 75}{52336356030243694706688}<\frac{59049}{1024}=\left(\frac{9}{4}\right)^5.$$

Thus the ratio in question is less than $(9/4)n^{-3/10}$.

The normalizer-orbit averaging argument of Section 3.3 applies to D_n with degree $S(n)$. Its orbit indicator has the same orthogonality to both character constituents. Therefore

$$\frac{b_p^o(n)}{R_o(n)}\le\frac{2}{p(p-1)}+\frac{9}{4}n^{-3/10}. \tag{9}$$

When $p\mid n$, (7) is already smaller than the first term, so (9) holds for every odd inert prime.

3.4.3 A six-point quotient at the ramified prime

For $\mathcal{A}+\mathcal{A}$, a target 2 modulo 3 forces both component norms to be 1 modulo 3. The mixed target is 1 modulo 3, so exactly one component norm is divisible by 3. To make it $3b$ with $b\in\mathcal{A}$, we must keep its exponent of 3 equal to one. We are left with a concrete task: count the representations with a component norm divisible by 9. A six-point quotient gives that count exactly, without another spectral estimate. Put

$$\overline{R}=R/3R,\qquad G_3=(\mathcal{O}/3\mathcal{O})^\times/\mathbb{F}_3^\times,\qquad \Gamma_3=\mathrm{image}(\mathcal{O}^\times),\qquad Y_3=\Gamma_3\backslash G_3.$$

For $z=x+y\omega$ one has $N(z)\equiv(x+y)^2 \pmod 3$. Among the 81 residue quaternions $z+wj$, exactly nine have norm zero: both of the corresponding coordinate sums vanish. The other 72

are units, since quaternionic conjugation supplies their inverses after dividing by norm. Hence $|G_3| = 36$. Only ± 1 of the twelve order units become scalars, so $|\Gamma_3| = 6$ and $|Y_3| = 6$.

The norm modulo 3 is well-defined projectively and is one on Γ_3. Each norm class Y_3^+ and Y_3^- has three points. Indeed, norm one occurs when exactly one of the two coordinate sums is nonzero, and norm two when both are nonzero; each condition describes 36 unit quaternions before projectivizing.

The six units of $\overline{R}$ are exactly the reductions of $\pm 1, \pm\omega, \pm\omega^2$. Every point of Y_3^- may therefore be represented by $1 + tj$, with $t \in \overline{R}^\times$: first normalize its first component by a left Eisenstein unit. Left multiplication by j, followed by the same normalization, sends t to $-t$, because $t\bar{t} = 1$. Left multiplication by an Eisenstein unit leaves the normalized ratio unchanged. These exhaust all order units, so the three left cosets are exactly

$$\Gamma_3(1 + j), \qquad \Gamma_3(1 + \omega j), \qquad \Gamma_3(1 + \omega^2 j).$$

Right multiplication by ω, followed by left normalization, sends t to $t\omega$ and cycles these three points. Thus the right Γ_3-action is transitive on Y_3^-.

The same ideal-class argument as in Lemma 3.3 realizes Y_3 as an adelic quotient, now taking the kernel of reduction $\mathcal{O}_3^\times \to G_3$ at 3 and maximal-order units elsewhere. For $3 \nmid u$, its all-ideal Hecke operator is still

$$(T_u f)(\Gamma_3 g) = \frac{1}{12} \sum_{\alpha \in \mathcal{Q}_u} f(\Gamma_3 \rho_3(\alpha) g),$$

with degree $\sigma(u)$, counting measure, self-adjointness and the prime-power recurrence already established.

For an inert prime ℓ, T_ℓ interchanges the two norm classes. Its value on the base-point indicator is constant on the opposite three-point class, by the transitive right Γ_3-action just proved. Self-adjointness and degree $\ell + 1$ make that value $(\ell + 1)/3$. Equivariance under G_3 transports this conclusion to every point. Thus, with the two norm classes ordered first,

$$T_\ell = \frac{\ell + 1}{3} \begin{pmatrix} 0 & J_3 \\ J_3 & 0 \end{pmatrix},$$

where J_3 is the 3 by 3 all-ones matrix. It has eigenvalues $\ell + 1$ and $-(\ell + 1)$ on the constant and norm-sign characters, and acts as zero on the four-dimensional space W of functions with sum zero on each norm class.

The all-ideal recurrence shows that the scalar on W at ℓ^a is zero for odd a and $(-\ell)^{a/2}$ for even a. For a reduced target n, multiplicativity gives

$$\lambda_n = \begin{cases} 0, & n \text{ is not a square,} \\ (-1)^{\Omega(n)/2}\sqrt{n}, & n \text{ is a square,} \end{cases}$$

where Ω counts prime factors with multiplicity.

3.4.4 The exact count and its odd-component bound

For the unfiltered identity, allow any positive reduced target $n \equiv 1 \pmod 3$, without an evenness requirement. If $9 \mid Q(x, y)$, then $y = -x + 3t$ for some integer t, and $Q(x, y) \equiv 3x^2 \pmod 9$. Thus $3 \mid x, y$; the converse is immediate. A component norm is divisible by 9 exactly when that component is zero modulo $3R$. Since $3 \nmid n$, the other component is a unit of $\overline{R}$. Its reduction is an Eisenstein unit, so the projective reduction of the quaternion lies in Γ_3. The converse also holds.

Let δ be the indicator of the base point $\Gamma_3 \in Y_3^+$, and let $B_3(n)$ count the unfiltered representations with a component norm divisible by 9. Then

$$B_3(n) = 12(T_n \delta)(\Gamma_3).$$

The projection of δ onto the constant and norm-sign characters has diagonal value $1/3$, and the projection onto W has diagonal value $2/3$. Since $n \equiv 1 \pmod 3$, both characters have eigenvalue $\sigma(n)$. It follows that

$$B_3(n) = 4\sigma(n) + 8\lambda_n. \tag{10}$$

Return now to even $n = 2^e m$. Let $B_3^o(n)$ count the same obstruction among the retained odd-component representations. Scaling by 2 preserves divisibility of either norm by 9, so $B_3^o(n) = B_3(n) - B_3(n/4)$, with the second term omitted when $4 \nmid n$. The unfiltered formula applies even when $n/4$ is odd. If n is not a square, both λ terms vanish. If n is a square, then $e \geq 2$ and $\lambda_{n/4} = -\lambda_n/2$. Therefore

$$B_3^o(n) = 4S(n) + 12\lambda_n,$$

with the last term interpreted as zero for nonsquares. Dividing by (6) gives

$$\frac{B_3^o(n)}{R_o(n)} = \frac{1}{3} + \frac{\lambda_n}{S(n)} \leq \frac{1}{3} + \frac{2}{3\sqrt{n}}. \tag{11}$$

3.5 Putting numbers on the estimates

Norm multiplicities bound the large-prime losses; residue counts bound the small-prime losses.

Define

$$M(n) = \max_{1 \leq u \leq n} \prod_{\substack{q^e \| u \\ q \equiv 1 \pmod 3}} (e+1).$$

Unique factorization in R shows that a positive integer u has either no Eisenstein norm representations or exactly $6 \prod_{q \equiv 1 \pmod 3} (e_q + 1)$ of them. Inert prime exponents must be even, and the ramified prime contributes no choice. In particular the count is at most $6M(n)$ for $u \leq n$.

Lemma 3.4. *For every positive integer n, one has $M(n) \leq (15/8)n^{1/5}$.*

Proof. The relevant local factors are $G_q(a) = (a+1)q^{-a/5}$ for split primes $q \equiv 1 \pmod 3$. For $q \geq 32$, the inequality $a + 1 \leq 2^a$ gives $G_q(a) \leq 1$. The successive ratio $(a+2)/((a+1)q^{1/5})$ decreases with a, so each maximum is found by checking up to the first E with $(E+2)^5 \leq q(E+1)^5$. For $q = 7, 13, 19, 31$, the maximizing exponents are $2, 1, 1, 1$. The product of the fifth powers of these maxima is

$$\frac{7962624}{375193} < \left(\frac{15}{8}\right)^5.$$

Multiplication over prime factors of each $u \leq n$ proves the bound. □

Lemma 3.5. *The number of nonzero Eisenstein integers of norm at most t is at most $6\lfloor t \rfloor \leq 6t$ for $t \geq 0$.*

Proof. Each orbit of the six units has a unique representative $x + y\omega$ with $x \geq 1$ and $0 \leq y < x$. Give this representative the label $L = x(x-1)/2 + y + 1$. Labels are distinct positive integers. For $x \geq 2$,

$$L \leq x(x+1)/2 \leq 3x^2/4 \leq Q(x, y),$$

and $x = 1$ is immediate. Thus at most $\lfloor t \rfloor$ orbits occur. □

For an odd inert prime p, divisibility of a component norm by p allows that component to be divided by p. Among the retained odd components it is nonzero. Lemma 3.5 gives at most $6n/p^2$ choices, and the other component has at most $6M(n)$ choices for each norm value. Counting either spoiled component and dividing by $R_o(n) = 12S(n) \geq 18n$ gives

$$\frac{b_p^o(n)}{R_o(n)} \leq \frac{4M(n)}{p^2} \leq \frac{15}{2}\frac{n^{1/5}}{p^2}. \tag{12}$$

Let $\mathcal{P}_o = \mathcal{P} \setminus \{2\}$. For $P \geq 5$, we need

$$\#\{p \in \mathcal{P}_o : p \leq P\} \leq \frac{2P}{15} + \frac{17}{15}, \tag{13}$$

$$\sum_{\substack{p \in \mathcal{P}_o \\ p > P}} p^{-2} \leq \frac{2}{15P} + \frac{8}{5P^2}, \tag{14}$$

$$\sum_{p \in \mathcal{P}_o} \frac{2}{p(p-1)} < \frac{3}{20}. \tag{15}$$

Here are elementary proofs. Apart from 5, these primes occupy the residues $11, 17, 23, 29 \pmod{30}$. If $A(t)$ counts positive integers in these four residues, the discrepancy $A(t) - 2t/15$ is 30-periodic, decreases linearly between jumps at $11, 17, 23, 29$, and has endpoint and left-limit bounds

$$-\frac{22}{15} \leq A(t) - \frac{2t}{15} \leq \frac{2}{15}.$$

This proves (13), and also $A(t) - A(P) \leq 2(t-P)/15 + 8/5$ for $t \geq P$. Partial summation gives the all-real bound

$$\sum_{\substack{p \in \mathcal{P}_o \\ p > P}} p^{-2} \leq 2 \int_P^\infty \frac{A(t) - A(P)}{t^3}\, dt \leq \frac{2}{15P} + \frac{8}{5P^2}.$$

Prime 5 contributes the extra 1 in the counting estimate and is absent from this tail because $P \geq 5$. Finally all odd inert primes are among $6k-1$, $k \geq 1$. Bounding the tail after $k = 3$ by an integral yields

$$\sum_{p \in \mathcal{P}_o} \frac{2}{p(p-1)} \leq \frac{1}{10} + \frac{1}{55} + \frac{1}{136} + \int_3^\infty \frac{2\,dx}{(6x-2)^2} = \frac{6569}{44880} < \frac{3}{20}.$$

3.6 Leaving a decomposition unspoiled

Combine the small-prime spectral and large-prime lattice bounds, including the condition at 3 in the mixed case.

Assume (1), put $X = n^{1/4}$ and $P = 2X$, and suppose $X \geq 100$. For the odd inert primes up to P, equations (9), (13) and (15) give

$$\sum_{\substack{p \in \mathcal{P}_o \\ p \leq P}} \frac{b_p^o(n)}{R_o(n)} < \frac{3}{20} + \frac{9}{4} X^{-6/5} \left(\frac{4X}{15} + \frac{17}{15} \right).$$

For the larger primes, equations (12) and (14) give

$$\sum_{\substack{p \in \mathcal{P}_o \\ p > P}} \frac{b_p^o(n)}{R_o(n)} \leq \frac{15}{2} X^{4/5} \left(\frac{1}{15X} + \frac{2}{5X^2} \right).$$

The mixed case also excludes the ramified obstruction (11). Its total spoiled fraction is therefore less than

$$\frac{29}{60} + \frac{11}{10} X^{-1/5} + \frac{111}{20} X^{-6/5} + \frac{2}{3X^2}. \tag{16}$$

Since $(5/2)^5 < 100$, one has $X^{-1/5} < 2/5$ and $X^{-6/5} < 1/250$, while $X^{-2} \leq 1/10000$. Thus (16) is strictly smaller than

$$\frac{29}{60} + \frac{11}{10}\frac{2}{5} + \frac{111}{20}\frac{1}{250} + \frac{2}{30000} = \frac{591}{625} < 1.$$

At least one odd-component representation survives.

If $n \equiv 4 \pmod 6$, exactly one component norm is 0 modulo 3, since an Eisenstein norm is 0 or 1 modulo 3. Neither norm contains an inert prime, and neither is divisible by 9. The component divisible by 3 is therefore $3b$ with $b \in \mathcal{A}$, and the other is in $\mathcal{A}$. This proves the mixed statement for reduced $n \geq 10^8$.

If $n \equiv 2 \pmod 6$, both component norms are 1 modulo 3. The ramified obstruction is absent, so the same strict bound applies after omitting its contribution. A surviving representation gives two members of $\mathcal{A}$. This proves the other binary statement in the same infinite range. Both values admit primitive coordinate representations by Proposition 3.1; the surviving quaternion coordinates themselves need not be primitive.

3.7 Finishing the finite ranges

The infinite estimates start at 10^8; below it we use the exact membership sieve and complete target scans.

For $c \in \{2, 4\}$ put

$$H_c = \left\lfloor \frac{10^8 - c - 1}{6} \right\rfloor .$$

Index the possible summands by $6j+1$, $0 \leq j \leq H_c$, and set $\varepsilon_j = 1$ unless a prime $p \equiv 5 \pmod 6$, $p \leq 9999$, divides $6j+1$. For such a divisor set $\varepsilon_j = 0$; negative indices also have value zero.

This is an exact membership test for $\mathcal{A}$. Each indexed integer is odd and prime to 3. If it contains an inert prime factor, the total number of inert factors counted with multiplicity is even, since the integer is 1 modulo 3. At least one of these factors is at most the square root, which is less than 10000. For a prime $p \equiv 5 \pmod 6$, precisely the indices $(5p-1)/6 + rp$, $r \geq 0$, are removed.

Proposition 3.6. *For every target $n = 6k+2 < 10^8$, there is an $i \leq 35$ with $2i \leq k$ and $\varepsilon_i \varepsilon_{k-i} = 1$. For every target $n = 6k+4 < 10^8$, there is a $j \leq 33$ with $3j \leq k$ and $\varepsilon_j \varepsilon_{k-3j} = 1$.*

Computer-assisted proof. The standard-library program described in Appendix A constructs the exact membership sieve, checks the small candidates by direct divisor tests, and requires a witness at every target index. Its two complete scans give the following results:

family	targets	largest target	small summand bound
$\mathcal{A} + \mathcal{A}$	16,666,667	99,999,998	$6i+1 \leq 211$
$\mathcal{A} + 3{\cdot}\mathcal{A}$	16,666,666	99,999,994	$6j+1 \leq 199$

Neither scan has an uncovered target. The witnesses give, respectively,

$$6k+2 = (6i+1) + (6(k-i)+1), \qquad 6k+4 = (6(k-3j)+1) + 3(6j+1).$$

All terms are positive members of the required sets. Separate NumPy implementations reproduce every membership flag and witness; their normalized digests agree with the standalone verifier. The integer arithmetic and receipt conventions are specified in Appendix A and the supplement. □

Proposition 3.6, the infinite-range argument in Section 3.6, and the initial multiplicative reduction prove Theorem 3.2.

The finite witness menu cannot work for every target:

Proposition 3.7. *For either $c = 1$ or $c = 3$, and every finite $F \subset \mathcal{A}$, there are infinitely many positive $n \equiv c+1 \pmod 6$ with $n \notin \mathcal{A} + (c{\cdot}F)$.*

Proof. The case $F = \varnothing$ is immediate. Otherwise choose distinct odd inert primes q_f, one for each $f \in F$. There are arbitrarily many such primes: for any finite collection including 2, the integer three times their product minus one has an inert prime factor outside the collection. The Chinese remainder theorem gives an arithmetic progression of solutions to

$$n \equiv c+1 \pmod 6, \qquad n \equiv cf \pmod{q_f} \quad (f \in F).$$

Choose its positive terms larger than $c \max F$. Then $n - cf > 0$ is divisible by the forbidden prime q_f, so it is not in $\mathcal{A}$, for every $f \in F$. □

Thus the finite witness bounds 211 and 199 cannot be replaced by fixed global bounds of the same kind.

3.8 Primitive and higher sumsets

With both binary identities proved, Proposition 3.1 identifies their union with the primitive norm values $\mathcal{N} = P_{-3} = \mathcal{A} \sqcup (3{\cdot}\mathcal{A})$. For a set $S \subset \mathbb{Z}_{>0}$, let kS denote the sum of exactly k members of S, with repetitions allowed. We distinguish this from a dilation, writing $3{\cdot}S = \{3s : s \in S\}$.

We can now use the two binary answers in their simplest form:

$$\mathcal{A} + \mathcal{A} = \{n > 0 : n \equiv 2 \pmod 6\}, \qquad \mathcal{A} + (3{\cdot}\mathcal{A}) = \{n > 0 : n \equiv 4 \pmod 6\}. \tag{17}$$

The mixed identity fills the second family of residue classes. Together with the first identity, it gives the complete two-summand answer below.

Proposition 3.8. *One has*

$$\mathcal{N} + \mathcal{N} = \{n \in \mathbb{Z}_{>0} : n \text{ is even},\ n \not\equiv 0, 12 \pmod{18}\}.$$

Proof. Expand the sum using Proposition 3.1. The three possibilities and their exact positive residue classes are

summands	residue classes modulo 18
$a + b \quad (a, b \in \mathcal{A})$	$2, 8, 14$
$a + 3b \quad (a, b \in \mathcal{A})$	$4, 10, 16$
$3a + 3b \quad (a, b \in \mathcal{A})$	$6.$

The first two rows follow from (17); the last is three times its first identity. Their union is the stated set. □

The missing classes also have a direct local explanation. Every primitive norm is odd. If their sum is divisible by 3, both summands belong to $3{\cdot}\mathcal{A}$; each is 3 modulo 18, so their sum is 6 modulo 18. This excludes 0 and 12 modulo 18.

Two summands are the hard part. For more summands, the presence of 1 does most of the work: subtract some ones, use a binary decomposition, and put the ones back.

Proposition 3.9. *For every $k \geq 2$, one has*

$$k\mathcal{A} = \{n \in \mathbb{Z} : n \geq k,\ n \equiv k \pmod 6\}.$$

Consequently every positive integer is a sum of at most seven elements of $\mathcal{A}$, and seven is necessary. For every $k \geq 3$, one has

$$k\mathcal{N} = \{n \in \mathbb{Z} : n \geq k,\ n \equiv k \pmod 2\}.$$

Every positive integer is then a sum of at most four primitive norms, and four is necessary.

Proof. For $k\mathcal{A}$, positivity and congruence are necessary. Conversely, subtract $k-2$ copies of 1 from an integer on the right. The remainder is at least 2 and congruent to 2 modulo 6, so it is a sum of two members of $\mathcal{A}$. For $n \geq 7$, choose the unique $k \in \{2,3,4,5,6,7\}$ congruent to n modulo 6; the formula applies. For $n < 7$, use ones. A sum of r elements of $\mathcal{A}$ equal to 25 has $r \equiv 1 \pmod 6$. Since $25 = 5^2 \notin \mathcal{A}$, it cannot have fewer than seven terms, and

$$25 = 13 + 7 + 1 + 1 + 1 + 1 + 1.$$

Every primitive norm is odd. To prove the converse for three summands, let $n \geq 3$ be odd. If $n \equiv 3 \pmod 6$, use the formula for $3\mathcal{A}$. If $n \equiv 5 \pmod 6$, write $n = 3 + (a+b)$ using the first binary identity. If $n \equiv 1 \pmod 6$, then $n \geq 7$ and the mixed identity writes $n = 3 + (a+3b)$. All three summands in each case are primitive norms. For $k > 3$, subtract $k-3$ ones and apply the three-summand result. Thus odd integers at least 3 use three terms and even integers at least 4 use four; 1 and 2 use one and two ones. The integer 12 is not a sum of two primitive norms by Proposition 3.8, and parity excludes one or three terms. Since $12 = 3+3+3+3$, four is sharp. □

The two sharp examples mark the end of this chain: the binary identities give all the higher sumsets, and 12 and 25 show exactly where the universal bounds stop.

4 Discriminant -7

Put

$$Q_7(x,y) = x^2 + xy + 2y^2, \qquad P_7 = \{Q_7(x,y) > 0 : \gcd(x,y) = 1\},$$

and let C_7 contain 1 and the positive integers supported on primes congruent to $1, 2, 4 \pmod 7$. In particular, 2 is allowed.

Theorem 4.1. *The exact sumsets are*

$$C_7 + C_7 = \{n \geq 2 : 7 \nmid n\} \setminus \{11, 29\}, \qquad P_7 + P_7 = \{N \geq 2 : 49 \nmid N\} \setminus \{7, 77, 203\}.$$

For every $N \geq 2^{69}$ with $49 \nmid N$,

$$\#\{(a,b) \in P_7^2 : a + b = N\} \geq N^{2/3}/20000.$$

Pairs are ordered and summands are numerical values.

We write Q, P, C for these objects within this section. The proof first produces a uniform sieve inequality on a quaternion norm shell. Exact interval certificates connect its infinite range to a complete finite sumset computation. A final descent removes split prime factors, including the exceptional quotients $11, 29$.

4.1 The value criterion and the ramified prime

Let $R = \mathbb{Z}[\omega]$, where $\omega = (1 + \sqrt{-7})/2$. The Minkowski ideal-class bound is $(2/\pi)\sqrt{7} < 2$, so every ideal class has a representative of norm one. Thus R has class number one. At an inert prime, divisibility of a norm forces divisibility of both coordinates. At a split prime, a primitive element can use only one of the two conjugate prime ideals. At the ramified prime, its exponent as an ideal divisor is at most one: the square of that prime ideal is (7). Conversely, assigning each entire split prime power to one of its principal prime ideals, and choosing a ramified exponent zero or one, gives a primitive generator. Therefore

$$P = C \,\dot\cup\, 7C. \tag{18}$$

This is a statement about values; individual coordinate witnesses used for the shell sieve need not be primitive at split primes.

Multiplication by $\pi = \sqrt{-7}$ has matrix

$$M = \begin{pmatrix} -1 & -4 \\ 2 & 1 \end{pmatrix}, \qquad M^2 = -7I, \quad \det M = 7, \quad Q(Mv) = 7Q(v).$$

For a primitive vector of norm coprime to 7, the image is still primitive. Indeed the determinant treats all other primes, while both output coordinates vanish modulo 7 precisely when $2x + y \equiv 0 \pmod 7$, which would imply $7 \mid Q(x, y)$.

Modulo 7, $Q(x, y) = (x + 4y)^2$. Since -1 is not a square, two nonzero squares cannot sum to zero. Every element of C is a nonzero square modulo 7, and (18) gives

$$7m \in P + P \quad \Longleftrightarrow \quad m \in C + C. \tag{19}$$

In particular $49 \mid N$ is impossible for $N \in P + P$. Every split prime preserves C under multiplication.

4.2 The shell and its finite quotients

Consider

$$B = (-7, -1)_{\mathbb{Q}}, \qquad O = R \oplus Rj, \qquad j^2 = -1, \quad ja = \bar{a}j.$$

Its reduced norm is $Q \oplus Q$. The algebra has discriminant 7, and this order is maximal [2, Theorem 15.5.5 and Example 15.5.7]. Its units are $\{\pm 1, \pm j\}$: the two nonnegative component norms sum to one, and the units of R are ± 1. The projective unit group Γ consequently has order two. The projective mass formula gives total ideal-class mass $(7 - 1)/12 = 1/2$ [2, Theorem 25.1.1]. The principal class already contributes $1/|\Gamma| = 1/2$. There is therefore one right-ideal class.

For $7 \nmid n$, every integral right ideal of norm n is principal and has four generators. The all-ideal degree formula [2, Propositions 41.3.1 and 41.3.6] gives

$$r_O(n) := \#\{\alpha \in O : \mathrm{nrd}(\alpha) = n\} = 4\sigma(n). \tag{20}$$

Likewise ideal factorization in R gives

$$r_Q(t) = 2 \sum_{d \mid t} \chi_{-7}(d) \le 2M(X) \quad (1 \le t \le X), \qquad M(X) = \max_{1 \le t \le X} \prod_{\substack{\ell \mid t \\ \chi_{-7}(\ell) = 1}} (v_\ell(t) + 1). \tag{21}$$

For an odd inert prime q, reduction gives $G_q = \mathrm{PGL}_2(\mathbb{F}_q)$. At 7, reduction modulo the radical gives

$$G_7 = \mathbb{F}_{49}^*/\mathbb{F}_7^*,$$

a cyclic group of order eight. Use the quotient $\Gamma \backslash \prod G_\ell$, for auxiliary levels 7, q, or $q, 7$, with uniform probability measure. The image of Γ injects at every such level. At odd q, j cannot be scalar: its trace is zero and its norm is one. At 7, $j \notin \mathbb{F}_7$. This argument includes $q = 3$.

For index n coprime to 7 and the added levels, the all-ideal Hecke operator has degree $\sigma(n)$ and satisfies

$$(T_n h)(x_0) = \frac{1}{4} \sum_{\mathrm{nrd}\, \alpha = n} h(\rho(\alpha)). \tag{22}$$

Principalization initially gives inverse generators. Projectively $\alpha^{-1} = \bar{\alpha}$, and conjugation permutes the shell, which proves the displayed orientation and normalization. The operator is self-adjoint and commutes with the right finite group action.

The global norm characters at level 7 are $1, \chi_7$, where χ_7 is the quadratic residue-field norm character. At joint level $q, 7$ they are precisely

$$1, \ \chi_7, \ \chi_q, \ \chi_7\chi_q, \tag{23}$$

with χ_q the determinant square character. To check completeness, the maximal local unit norm maps are onto away from the auxiliary levels. Reduction kernels and projective central scalars leave only the two square classes at each auxiliary prime. Globally, reduced norms are all positive rationals by the Hasse–Schilling norm theorem [2, Main Theorem 14.7.4]; rational square classes give exactly (23). The strong-approximation step in Lemma 2.1 excludes other constituents having a finite-dimensional full smooth local factor at a split place. It is the full local factor, rather than a space of level-fixed vectors, to which that argument applies.

Consequently Lemma 2.1 gives, on the orthogonal complement of the characters (23),

$$\|T_n\| \le \tau(n)\sqrt{n}. \tag{24}$$

At every prime dividing n, including 2, the quaternion algebra is split and the local order is maximal. The all-ideal prime-power eigenvalue is a sum of $a+1$ monomials in two roots of absolute value $\sqrt{\ell}$, so the constant in (24) is one.

One must not remove every character of a finite right action. For example $\Gamma\backslash G_7 \simeq C_4$ has two quartic characters. The norm-two shell has eight pure-component points reducing to Γ and four mixed points $\pm 1 \pm j$ reducing to $h = [1+j]$. Here $h \neq 1$ and $h^2 = 1$, because $(1+j)^2 = 2j$. Thus $T_2 = 2I + R_h$, with spectrum $3, 3, 1, 1$. The global norm characters have eigenvalue 3, whereas the quartic characters have eigenvalue 1 and remain in the complement in (24).

4.3 A simultaneous ramified and inert filter

For $7 \nmid n$, put

$$E(n) = \frac{\tau(n)\sqrt{n}}{\sigma(n)}, \qquad \gamma(n) = \frac{3 - \chi_{-7}(n)}{4}.$$

Let $G(n)$ count shell points for which both field norms are 7-units. These norms are necessarily positive. The two component axes reduce to the single base point of $\Gamma\backslash G_7$. Its indicator δ has mean $1/4$, coefficient $1/4$ on χ_7, and complementary squared norm $1/8$. Apply (22) to the correlation of δ with itself, and use (24). The resulting lower bound is

$$\frac{G(n)}{4\sigma(n)} \ge \gamma(n) - \tfrac{1}{2}E(n). \tag{25}$$

If $\chi_{-7}(n) = -1$, an axis is impossible already modulo 7; then $G(n) = 4\sigma(n)$ exactly.

For inert $q \nmid n$, the invertible residues with one field component zero form the normalizer H_q of a nonsplit torus. It contains the unit image and has order $2(q+1)$, hence fraction

$$\mu_q = \frac{2}{q(q-1)}$$

in G_q. The determinant character has mean zero on H_q, because the torus norm is onto $\mathbb{F}_q^*$.

Retain the ramified filter on the joint quotient. Let u require the q-coordinate in H_q and the 7-coordinate in $\Gamma_7 = \{1, j\}$. Let v require the same q-condition and the complementary 7-condition. Both are right-invariant under $H_q \times \Gamma_7$, and the base orbit is the support of u. Consequently

$$(T_n v)(x_0) = \frac{\langle u, T_n v\rangle}{\mathbb{E}u}.$$

This identity does not require $v(x_0) = 1$. Writing $a = \mu_q/4$, the coefficients on the four characters in (23) are respectively

$$(a, a, 0, 0) \quad \text{and} \quad (3a, -a, 0, 0).$$

The complementary squared norms are $a - 2a^2$ and $3a - 10a^2$. If $b_q(n)$ counts points bad at q inside the 7-unit shell, Cauchy's inequality and (24) therefore give

$$\begin{aligned} \frac{b_q(n)}{4\sigma(n)} &\le \gamma(n)\mu_q + \sqrt{(1 - \mu_q/2)(3 - 5\mu_q/2)}\, E(n) \\ &\le \gamma(n)\mu_q + \tfrac{7}{4}E(n). \end{aligned} \tag{26}$$

For $\chi_{-7}(n) = -1$, omit level 7. The ordinary H_q indicator has complementary squared norm $\mu_q(1-\mu_q)$; the error in (26) improves to $E(n)$.

If $q \mid n$, anisotropy forces both coordinate blocks to be divisible by q as soon as either is. The spoiled count is zero when $v_q(n) = 1$, and otherwise is exactly $G(n/q^2)$. Thus

$$\frac{b_q(n)}{4\sigma(n)} \le \frac{\sigma(n/q^2)}{\sigma(n)} < q^{-2} \le \gamma(n)\mu_q. \tag{27}$$

No level-q operator is applied to an index divisible by q.

For large primes use geometry instead. Row integration gives

$$S_Q(X) := \#\{(x,y) : 0 < Q(x,y) \le X\} \le \frac{2\pi}{\sqrt{7}}X + (2 + 4/\sqrt{7})\sqrt{X} \le 3X.$$

For integers $X \ge 36$, the last inequality follows from $\pi < 22/7$, $\sqrt{7} > 66/25$, and $50/21+58/99 < 3$. The finite certificate checks $1 \le X \le 35$; flooring extends the result to real X. A nonzero q-divisible block is q times a nonzero vector. Choose its orientation, count it by $3n/q^2$, and use (21) for the other block. Hence

$$b_q(n) \le 12M(n)n/q^2. \tag{28}$$

Only $q \le \sqrt{n}$ can occur.

Let $\mathcal{I}$ be the inert primes and put

$$B = \sum_{q\in\mathcal{I}} \mu_q, \quad \Pi(z) = \#\{q \in \mathcal{I} : q \le z\}, \quad T(z) = \sum_{\substack{q\in\mathcal{I}\\ q>z}} q^{-2}.$$

A union bound using (25)–(28) leaves a shell proportion at least

$$\gamma(n)(1-B) - E(n)\{\tfrac{1}{2} + \tfrac{7}{4}\Pi(z)\} - 3M(n)T(z). \tag{29}$$

In the negative-character case the sharper sufficient inequality is

$$E(n)\Pi(z) + 3M(n)T(z) < 1 - B. \tag{30}$$

A surviving pair has positive norms in C, so proves $n \in C + C$.

4.4 Complete arithmetic envelopes

The inert primes belong to $3, 5, 13 \pmod{14}$. Counting those progressions, then bounding each decreasing tail by its first term and integral, gives

$$\Pi(z) \le 3z/14 + 13/14, \qquad T(z) \le 3/(14z) + 3/z^2. \tag{31}$$

For the count, $13/14$ is the largest discrepancy within one period; this is checked over the fourteen residue positions.

Here and below, numerical certificate statements use exact integers or rational numbers. Set $R_0 = 2^{19}$, $D_0 = 2^{64}$. Let a_r be the least integer greater than R_0 in residue $r \pmod{14}$, for $r = 3, 5, 13$, and put

$$\overline{B} = \frac{1}{D_0}\sum_{\substack{q\in\mathcal{I}\\ q\le R_0}} \left\lceil \frac{2D_0}{q(q-1)} \right\rceil + \frac{2(R_0+1)}{R_0} \sum_{r=3,5,13} \left(\frac{1}{a_r^2} + \frac{1}{14a_r}\right).$$

Since $\mu_q \le 2(R_0+1)/(R_0q^2)$ above R_0, this is an upper bound for B. Exact evaluation gives

$$B \le \overline{B} < 47/100. \tag{32}$$

The finite Euler calculations also give

$$M(X) \le 8X^{1/6}, \qquad E(n) < \frac{91}{20} n^{-1/3} \quad (n \text{ inert-supported}), \qquad E(n) \le 15 n^{-1/3} \quad (7 \nmid n). \tag{33}$$

We give the completeness bounds for these computations. For $M(X)^6/X$, each split prime contributes $(a+1)^6/\ell^a$. For $\ell \ge 64$ it is at most one, using $a+1 \le 2^a$. Below 64, exponents through 8 suffice: the subsequent ratios are at most $(10/9)^6/2 < 1$. The exact product of the finite maxima is below 8^6.

For $E(n)^6 n^2$, the prime-power factor is

$$W_\ell(a) = \frac{(a+1)^6 \ell^{5a}}{\sigma(\ell^a)^6}. \tag{34}$$

Its next/current ratio is strictly less than $((a+2)/(a+1))^6/\ell$. At inert primes below 64, caps 4 at 3, 3 at 5, and 1 at $13, 17, 19, 31, 41, 47, 59, 61$ therefore suffice. All larger primes have factor at most one. Their exact product is less than $(91/20)^6$. For all primes other than 7, use caps $8, 4, 3, 2$ at $2, 3, 5, 11$, and 1 at the other primes below 64. Their product is less than 15^6. This proves every bound in (33) without an upper bound on n.

For smaller ranges we use exact envelopes. A maximizer defining $M(U)$ uses nonincreasing exponents on an initial segment of the smallest split primes: interchanging out-of-order exponents lowers the integer cost and preserves the divisor product. A recursion through $U = 2^{54}$, recording every initial prefix and nonincreasing exponent profile of cost at most U, has 2556 states. Its completeness follows because the next prime-prefix product exceeds U, and no exponent exceeds $\lfloor \log_2 U \rfloor$.

For E, enumerate the 5120 tuples within the inert caps above, retaining integer cost and the product of (34). Partition them by

$$(v_3(n), v_5(n)) \in \{0, 1, \ge 2\}^2.$$

Deleting primes at least 64 and capping the other exponents increases the normalized factor and reduces the cost, preserving this category. Thus the cost-restricted maxima dominate all inert-supported $n \le U$. Take their upward sixth roots with denominator 10^6, verified by sixth powers, and call the result $c_{a,b}(U)$. On $L \le n \le U$ in category (a, b),

$$E(n) \le \frac{c_{a,b}(U)}{\lfloor L^{1/3} \rfloor}. \tag{35}$$

The global frontier is defined in the same way without categories.

4.5 The finite interval certificate

A sharper large-prime count is used when $\chi_{-7}(n) = 1$. The ordered nonzero square residues summing to $n \pmod 7$ are uniquely $n/2, n/2$. Define

$$S_r(X) = \#\{(x, y) : 0 < Q(x, y) \le X,\ Q(x, y) \equiv r \pmod 7\}, \quad F(X) = \max_{r=1,2,4} S_r(X).$$

If one block is $q\alpha$, then $Q(\alpha) \equiv n/(2q^2) \pmod 7$. The complete ordinary point table is computed through $X_0 = 2^{18}$. For $0 \le y \le \lfloor \sqrt{4X_0/7} \rfloor$, set $h = \lfloor \sqrt{4X_0 - 7y^2} \rfloor$ and enumerate

$$-\lfloor (h+y)/2 \rfloor \le x \le \lfloor (h-y)/2 \rfloor.$$

Weight a row by two when $y > 0$ and by one at $y = 0$; simultaneous sign reversal supplies the omitted rows. This lists every signed vector. The individual coefficients are also checked against $2 \sum_{d \mid t} \chi_{-7}(d)$. The first seven positive F-values are $2, 4, 4, 6, 6, 6, 6$.

Fix an interval $[L,U]$ and include the first j inert primes as small primes, always including $3,5$. Every omitted $q \le \sqrt{U}$ is required to satisfy $\lfloor U/q^2 \rfloor \le X_0$. For category $(a,b) \in \{0,1,2\}^2$, where 2 denotes valuation at least two, put

$$D_{a,b} = \frac{3^a}{\sigma(3^a)} \frac{5^b}{\sigma(5^b)}, \qquad d = \#\{p \in \{3,5\} : p \mid n\}.$$

Since $p^a/\sigma(p^a)$ decreases with a, $n/\sigma(n) \le D_{a,b}$. For $\chi_{-7}(n) = 1$, the large-prime error is at most

$$\frac{M(U) D_{a,b}}{L} \sum_{\substack{q \in \mathcal{I} \text{ omitted} \\ q \le \sqrt{U}}} F(\lfloor U/q^2 \rfloor). \tag{36}$$

The factor is M, because the two orientations and the bound $2M(U)$ for the other block are divided by $4\sigma(n)$.

A known divisor $p = 3$ or 5 needs no spectral error. In (27) its cost is $\delta_p = 0$ at valuation one and p^{-2} above it. Its baseline refund is $\gamma\mu_p - \delta_p$. For e given by (35), a sufficient positive-character test is consequently

$$e\{\tfrac{1}{2} + \tfrac{7}{4}(j-d)\} + \text{the term in (36)} < \tfrac{1}{2}(1-\overline{B}) + \sum_{\substack{p=3,5 \\ p \mid n}} (\mu_p/2 - \delta_p). \tag{37}$$

For the negative character use small error $e(j-d)$, large error $3M(U)D_{a,b} \sum_{q \text{ omitted}, q \le \sqrt{U}} q^{-2}$, and baseline $1 - \overline{B} + \sum(\mu_p - \delta_p)$. Reciprocal squares are rounded upward with denominator D_0.

Lemma 4.2 (Exact interval certificate)**.** *Every inert-supported $n \ge 2^{24}$, and every split prime $n \ge 2^{24}$, belongs to $C + C$.*

Proof. Here is the complete finite part of the certificate. Partition $[2^{24}, 2^{37})$ at all points $2^k + j2^{k-4}$, $24 \le k \le 36$, $0 \le j \le 16$, and at every jump in the M- or category E-frontiers. The resulting 257 adjacent integer intervals are checked to have no gap. On each interval test both character signs and all nine valuation categories by (37) and its negative-character version. Also test the positive-character boundary $\tau(n) \le 4$, with $e = 4/\lfloor \sqrt{L} \rfloor$ and no category discounts. There are $257 \cdot 19 = 4883$ cases. For each case choose the allowed prime cut minimizing its rational error. This can be found by comparing the cost of one more spectral term with the decrease of the large-prime tail; those decreases are nonincreasing. Direct enumeration of every allowable cut gives the same finite test.

Every case has margin greater than $1/64$, with all point-table queries at most X_0 and required primes below R_0. The exact worst-case parameters and error are recorded under `fine_interval_certificates.worst_case` in the supplement's -7 receipt.

For $37 \le k \le 53$, put $L = 2^k$, $U = 2^{k+1} - 1$, $d_k = M(U)$, and let e_k come from the global E-frontier. The seventeen exact tests are

$$e_k\{\tfrac{1}{2} + \tfrac{7}{4}\Pi(z_k)\} + 3d_k T(z_k) < (1-\overline{B})/2 - 1/64. \tag{38}$$

The prime sum through R_0 and the three progression integrals define the rational tail. The cut again minimizes the displayed error. All seventeen cases pass. The certificate additionally checks $4\lfloor L^{1/3} \rfloor \le \lfloor \sqrt{L} \rfloor$. Since its global normalized E-constant is at least one, $4/\sqrt{n} \le e_k$; these tests cover split primes as well.

For the infinite tail $n \ge 2^{54}$, take $z = (7/4)n^{1/4}$ in (29). For inert-supported n, (33) bounds the error by

$$\frac{185799}{31360} n^{-1/12} + \left(\frac{17}{8} \frac{91}{20} + \frac{1152}{49} \right) n^{-1/3}.$$

Using $(45/2)^{12} < 2^{54}$, $n^{1/3} \ge 2^{18}$, this is less than $53/200$, with margin $9574319/6165626880 > 1/1024$. The baseline is greater than $53/200$ by (32). For $\tau(n) \le 4$, $E(n) \le 4n^{-1/2} \le (91/20)n^{-1/3}$, so the same infinite tail applies. The three consecutive ranges cover the asserted families. All finite tables and integer roundings are reproduced by the submitted certificate program. □

4.6 Finite coverage and exceptional descent

For $B_0 = 2^{24}$, the submitted computation constructs every P-membership flag in two ways: complete primitive coordinate enumeration and the factorization criterion (18). The full bytearrays agree. Deleting multiples of 7 gives the complete C-flags. There are respectively 2490663 and 2161776 flagged values.

For completeness, the coordinate enumeration may restrict to $y \geq 0$ and $x \geq -y/2$, since simultaneous negation and conjugation preserve norm and gcd. The inequality $(2x+y)^2 + 7y^2 \leq 4B_0$ then gives finite exact bounds. For each value flag array A, form its binary integer $B_A = \sum_{j \leq B_0} A(j)2^j$ and the truncated union

$$U_A = \bigvee_{\substack{1 \leq a \leq 5000 \\ A(a)=1}} (B_A \ll a).$$

Here $\vee$ is bitwise union and $\ll$ is an exact integer shift. Every set bit has actual positive summands. The 1050 primitive anchors and 903 core anchors cover every locally eligible target through B_0, except respectively $\{7, 77, 203\}$ and $\{11, 29\}$. Every omitted bit is tested by a complete positive-pair search through half the target; none has a representation. The union also has no locally forbidden bit. No summand above B_0 can contribute to a target in this range. Membership arrays are compared before hashing; the stored hashes are identifiers of these exact finite objects, not substitutes for reconstructing and comparing them.

Suppose there were a least exception n to the asserted $C + C$ identity outside $11, 29$. Finite coverage makes $n > B_0$. If a split prime $q \mid n$, multiplicative closure and leastness imply $n/q \in \{1, 11, 29\}$. The first case makes n a split prime and is covered by Lemma 4.2. In the other cases, $n = 11q$ or $29q$. Division by 11 or 29, which are themselves split primes, shows that q must be 11 or 29; otherwise a smaller represented target lifts. The only products left are already represented:

$$121 = 8 + 113, \qquad 319 = 2 + 317, \qquad 841 = 32 + 809.$$

All summands lie in C. With no split prime factor, n is inert-supported, again contradicting Lemma 4.2. This proves the core identity. The exclusions modulo 7 were proved earlier, and

$$C \cap [1, 29] = \{1, 2, 4, 8, 11, 16, 22, 23, 29\}$$

checks the two exceptional nonrepresentations directly.

For $7 \nmid N$, the core identity supplies primitive values except at $11, 29$; the patches $11 = 4 + 7$ and $29 = 1 + 28$ use values in P. If $7 \mid N$, (19) shows that failure occurs exactly at quotient $1, 11, 29$, hence at $7, 77, 203$. Multiples of 49 are impossible. This proves the two exact identities in Theorem 4.1.

4.7 The explicit lower bound

For arbitrary $7 \nmid n$, use the last bound in (33), put $z = n^{1/4}$, and use the weaker $\Pi(z) \leq 3z/14 + 3/2$. The error in (29) is at most

$$\frac{603}{56} n^{-1/12} + \frac{951}{8} n^{-1/3}.$$

For $n \geq 2^{66}$, $n^{1/12} > 45$, $n^{1/3} \geq 2^{22}$; the error is at most $281051653/1174405120$. Its distance below $53/200$ is $150828519/5872025600 > 1/40$. Since $4\sigma(n) \geq 4n$, at least $n/10$ coordinate points survive. Each ordered value pair has at most $(2M(n))^2 \leq 256n^{1/3}$ coordinate witnesses by (21). Thus it yields at least $n^{2/3}/2560$ ordered C-pairs.

For $N \geq 2^{69}$, $49 \nmid N$, write $N = 7^e n$ with $e = 0$ or 1. Then $n > 2^{66}$. Multiply both core values by 7^e, using (18). This injects the value pairs into P^2. As $7^{2/3} < 4$, the resulting lower bound is stronger than $N^{2/3}/20000$, as required.

5 Discriminant -8

Put

$$Q_8(x,y) = x^2 + 2y^2, \qquad P_8 = \{Q_8(x,y) > 0 : \gcd(x,y) = 1\},$$

and let C_8 contain 1 and the positive integers whose prime factors are 1 or 3 (mod 8).

Theorem 5.1. *There are no exceptional admissible targets:*

$$\begin{aligned} C_8 + C_8 &= \{N \geq 2 : N \text{ even},\ 8 \nmid N\}, \\ C_8 + 2C_8 &= \{N \geq 3 : N \text{ odd}\}, \\ P_8 + P_8 &= \{N \geq 2 : 16 \nmid N\}. \end{aligned}$$

For every $N \geq 2^{78}$ with $16 \nmid N$,

$$\#\{(a,b) \in P_8^2 : a + b = N\} \geq N^{2/3}/4800.$$

Write Q, P, C for these objects in this section. The exact dyadic shell formulas will supply both a large-core theorem and an analytic prime boundary. Sharper selected-shell bounds then reduce the remaining work to 107 rational interval tests and complete finite core coverage.

5.1 Primitive values and dyadic reduction

The ring $R = \mathbb{Z}[\sqrt{-2}]$ is norm Euclidean: rounding both coordinates leaves error norm at most $1/4 + 2/4 = 3/4 < 1$. Thus it is principal. An inert prime, congruent to $5, 7$ (mod 8), dividing a norm divides both coordinates. Primitivity permits the ramified prime ideal of norm two to exponent at most one. For split primes, orient each full prime power to one of the two conjugate principal prime ideals. These observations prove

$$P = C \,\dot\cup\, 2C. \tag{39}$$

Every C-value is 1 or 3 (mod 8). Consequently

$$P + P = (C + C) \cup 2(C + C) \cup (C + 2C). \tag{40}$$

The first two terms have residues respectively $2, 4, 6$ (mod 8) and $4, 8, 12$ (mod 16), whereas the last has odd targets at least three. This proves every local exclusion in the theorem; the two core identities imply the full identity.

Multiplication by $\varpi = \sqrt{-2}$ acts by

$$(x, y) \longmapsto (-2y, x).$$

It bijects primitive odd-norm vectors with primitive even-norm vectors; the latter have even first coordinate and odd second coordinate, and the inverse is $(X, Y) \mapsto (Y, -X/2)$. At odd primes the determinant is a unit. Thus every division or multiplication by two below is justified on the indicated parity class; no general closure of primitive vectors under doubling is being assumed.

5.2 Exact dyadic shell formulas

Let $r(N)$ count the full signed ordered $Q \oplus Q$ shell, let $s(N)$ count $Q \oplus 4Q$, and let $G_2(N)$ count shell points for which neither binary coordinate pair is divisible by two. Only dyadic primitivity is imposed in G_2. With $\sigma(t) = 0$ for nonpositive or nonintegral t, define

$$f_{32}(\tau) = \eta(4\tau)^2\eta(8\tau)^2 = \sum_{N \geq 1} a_N q^N = q \prod_{j \geq 1} (1 - q^{4j})^2 (1 - q^{8j})^2.$$

Then

$$\begin{aligned} r(N) &= 4\sigma(N) - 4\sigma(N/2) + 8\sigma(N/4) - 32\sigma(N/8), \\ s(N) &= \sigma(N) - \sigma(N/2) + 8\sigma(N/16) - 32\sigma(N/32) + a_N, \\ G_2(N) &= r(N) - 2s(N) + r(N/4). \end{aligned} \tag{41}$$

We include the modular verification, so these formulas do not depend on extrapolating a finite list of shell counts.

The even Gram matrices of $Q \oplus Q$ and $Q \oplus 4Q$ have levels $8, 32$ and square determinants $64, 1024$. Their theta series therefore belong respectively to $M_2(\Gamma_0(8))$ and $M_2(\Gamma_0(32))$, with trivial character. Put $E_2(\tau) = 1 - 24\sum_{n\geq 1}\sigma(n)q^n$. The proposed Eisenstein series are

$$\begin{aligned} E_r &= -\tfrac{1}{24}\{4E_2(\tau) - 4E_2(2\tau) + 8E_2(4\tau) - 32E_2(8\tau)\}, \\ E_s &= -\tfrac{1}{24}\{E_2(\tau) - E_2(2\tau) + 8E_2(16\tau) - 32E_2(32\tau)\}. \end{aligned}$$

To verify holomorphy at all cusps, write

$$D_d(\tau) = dE_2(d\tau) - E_2(\tau) = \frac{1}{2\pi i}\frac{d}{d\tau}\log\frac{\Delta(d\tau)}{\Delta(\tau)}.$$

The quotient is a modular function, nonzero in the upper half-plane and meromorphic at cusps. If at a cusp of width h it is $q_c^{\nu}U(q_c)$, $U(0) \neq 0$, its logarithmic derivative has expansion

$$\frac{1}{h}\left(\nu + q_c\frac{U'(q_c)}{U(q_c)}\right).$$

There is no cusp pole. Hence D_d is holomorphic of weight two, and

$$E_r = D_2/12 - D_4/12 + D_8/6, \qquad E_s = D_2/48 - D_{16}/48 + D_{32}/24$$

have the required levels. Both have constant term one.

Martin–Ono [6, Theorem 1, level-32 row] identify f_{32} as a normalized weight-two newform. The Sturm bounds are 2 at level 8 and 8 at level 32 [7, Theorem 1]. The necessary coefficient lists are

N	0	1	2	3	4	5	6	7	8
$[q^N]\Theta_{Q\oplus Q}$	1	4	8						
$[q^N]E_r$	1	4	8						
$[q^N]\Theta_{Q\oplus 4Q}$	1	2	2	4	4	4	8	8	8
$[q^N](E_s + f_{32})$	1	2	2	4	4	4	8	8	8

They follow by direct lattice enumeration, divisor sums, and truncated multiplication of the displayed eta product. All coefficients are integers. Apply Sturm's congruence theorem modulo every rational prime: each coefficient of the difference is divisible by every prime, so is zero. This proves the first two formulas in (41); the last is inclusion-exclusion.

The CM formula in [6, Theorems 2 and 3] gives $|a_p| \leq 2\sqrt{p}$ at every odd prime, with $a_p = 0$ for $p \equiv 3 \pmod 4$. Its unramified Hecke roots have modulus $\sqrt{p}$; the Euler recurrence and multiplicativity imply $|a_N| \leq \tau(N)\sqrt{N}$ for odd N. The eta product is supported on $N \equiv 1 \pmod 4$, so its even coefficients vanish.

Write $N = 2^e m$, m odd. For $0 \leq e \leq 3$,

$$r(N) = 4c_e\sigma(m), \qquad (c_0, c_1, c_2, c_3) = (1, 2, 6, 6),$$

and

$$(G_2(m), G_2(2m), G_2(4m), G_2(8m)) = (2\sigma(m) - 2a_m,\ 4\sigma(m),\ 20\sigma(m),\ 16\sigma(m)). \tag{42}$$

For $e \geq 4$, $G_2(N) = 0$.

5.3 The nonmaximal dyadic order and Hecke bound

Let H be the Hurwitz order in Hamilton's quaternion algebra, with generators I, J, K. Put $\iota = I + J$, $j = K$, and

$$O = \mathbb{Z}[\iota] \oplus \mathbb{Z}[\iota]j = \{a + bI + cJ + dK : a, b, c, d \in \mathbb{Z},\ b \equiv c \pmod 2\}.$$

Here $\iota^2 = -2$, $j^2 = -1$, $j\iota = -\iota j$, and the norm is $Q \oplus Q$. This order has index four in H; it is not maximal at two.

We verify its locally principal right-ideal class number directly. The Hurwitz order is norm Euclidean. After rounding a real quaternion to an integer vector, let its coordinate errors be $|r_i| \le 1/2$, and put $s = \sum r_i^2$. The squared distance to an appropriate half-integer vector is $s - \sum |r_i| + 1$. Since $s \le \frac{1}{2}\sum |r_i|$, one of the two distances is at most $1/2$. Thus all Hurwitz right ideals are principal.

Away from two, $O_\ell = H_\ell$. Normalize the additive volume of H_2 to one. Its half-integer coset consists of odd-norm elements, as does half its integer coset; hence $\mathrm{vol}(H_2^\times) = 3/4$. The additive volume of O_2 is $1/4$, and half its elements have odd norm, so $\mathrm{vol}(O_2^\times) = 1/8$. The unit index is six. The 24 Hurwitz units have stabilizer

$$O^\times = \{\pm 1, \pm K\}$$

of size four on these cosets, so act transitively. Principalization in H, followed by this unit transitivity at two, principalizes every locally principal O-ideal.

The dyadic unit norm map is onto $\mathbb{Z}_2^\times$. Indeed 1, $1 + \iota$, $1 + \iota + \iota j$, $1 + \iota + 2j$ have norms $1, 3, 5, 7$. Their inverses belong to O_2. Every 2-adic unit is one of these four norms times a unit square, supplied by a rational 2-adic scalar.

For odd inert p, reduction gives $O/pO = M_2(\mathbb{F}_p)$. The projective unit image Γ_p has order two, and the fine quotient is $Y_p = \Gamma_p \backslash \mathrm{PGL}_2(\mathbb{F}_p)$, with uniform measure. Class number one identifies this quotient with the adelic congruence quotient: its stabilizer is precisely the projective unit image. To check this, local scalar corrections have even norm valuations and combine into one rational scalar, leaving an O-unit. For $p \nmid n$, define concretely

$$(T_n h)(\Gamma_p g) = \frac{1}{4} \sum_{\mathrm{nrd}\,\alpha = n} h(\Gamma_p \rho_p(\alpha) g). \tag{43}$$

For odd m, this is the all-integral-ideal operator, of degree $\sigma(m)$. Inverse principal generators give the displayed orientation by quaternion conjugation. The global norm characters on Y_p are exactly 1 and the determinant square character χ_p. The norm surjectivity just proved prevents an additional dyadic character. At p, central scalars and the reduction kernel leave only determinant square classes. Lemma 2.1, including its strong-approximation exclusion of finite-dimensional split-place factors, therefore yields

$$\|T_m\|_{\{1,\chi_p\}^\perp} \le \tau(m)\sqrt{m} \quad (m \text{ odd},\ p \nmid m). \tag{44}$$

All primes dividing m have maximal split local level. No unramified theorem at two has been used.

For $0 \le e \le 3$, let $A_e = T_{2^e}$ be given by (43). It is self-adjoint with nonnegative entries, row sum c_e, and norm at most c_e. It has χ_p-eigenvalue $(2/p)^e c_e$. Coprime local factorization gives

$$T_{2^e m} = A_e T_m = T_m A_e. \tag{45}$$

For example, for $\alpha \in O$ of norm $2^e m$, the right superideal with localization O_2 at two and αO_ℓ at odd primes is integral, locally principal, and of norm m. Write it as βO, $\mathrm{nrd}\,\beta = m$; then $\alpha = \beta\gamma$, $\mathrm{nrd}\,\gamma = 2^e$. Exactly four choices differ by an O-unit. Reversing the coprime local factors gives commutation. Thus the complementary norm of T_N is at most $c_e \tau(m)\sqrt{m}$.

5.4 The uniform sieve and its infinite ranges

Put

$$\begin{aligned}\mathcal{I} &= \{p \text{ prime} : p \equiv 5, 7 \pmod 8\},\\ E(m) &= \frac{\tau(m)\sqrt{m}}{\sigma(m)},\\ M(X) &= \max_{1\le t\le X} \prod_{\substack{\ell\mid t\\ \ell\equiv 1,3(8)}} (v_\ell(t)+1).\end{aligned}$$

Let $b_p(N)$ count full-shell points with at least one binary coordinate pair divisible by p. For $p \nmid N$, that condition is the nonsplit-torus normalizer H_p, of order $2(p+1)$. Its fraction in $\mathrm{PGL}_2(\mathbb{F}_p)$ is $\mu_p = 2/(p(p-1))$. Its indicator u has mean μ_p, zero coefficient on χ_p, and $\|u-\mu_p\|^2 = \mu_p(1-\mu_p)$, since the torus norm is onto. The operator commutes with the right action and is constant on the support of u. Thus $\langle u, T_N u\rangle = \mu_p b_p(N)/4$. Equations (44)–(45) give

$$\frac{b_p(N)}{r(N)} \le \mu_p + (1-\mu_p)E(m) \le \mu_p + E(m). \tag{46}$$

If $p \mid N$, anisotropy forces both blocks divisible by p. The spoiled count is zero at valuation one; otherwise its ratio is $\sigma(m/p^2)/\sigma(m) < p^{-2} \le \mu_p$. This treats every target valuation without applying a level-p estimate to an index divisible by p.

For a first bound on large primes,

$$\#\{(x,y) : 0 < x^2 + 2y^2 \le X\} \le \pi X/\sqrt{2} + (2+\sqrt{2})\sqrt{X} \le 4X.$$

The last inequality holds for $X \ge 4$; the three smaller integer bounds give $2, 4, 8$ points. Flooring gives real X. In the G_2-shell both blocks are nonzero, and $r_Q(t) \le 2M(N)$. Choose the divisible block, count its quotient vector, and use this bound for the other block. The large-p spoiled proportion is at most

$$L_e M(N) p^{-2}, \qquad L_e = \frac{4\cdot 2^e}{c_e} \le \frac{16}{3}. \tag{47}$$

Also

$$\begin{aligned}B &:= \sum_{p\in\mathcal{I}} \mu_p < 3/16,\\ \Pi(P) &:= \#\{p \in \mathcal{I} : p \le P\} \le P/4 + 1,\\ &\qquad \sum_{\substack{p\in\mathcal{I}\\ p>P}} p^{-2} \le 1/(4P) + 2/P^2.\end{aligned} \tag{48}$$

The last two statements follow from the progressions $5, 7 \pmod 8$. For the first, sum inert primes below 64 exactly and bound the rest by

$$\frac{5}{2}\left(\frac{1}{69^2} + \frac{1}{8\cdot 69} + \frac{1}{71^2} + \frac{1}{8\cdot 71}\right).$$

The resulting bound is $B < 3/16$; its exact rational value is in the supplement.

By (42), $G_2(N)/r(N) \ge 1/2 - E(m)/2$. A sufficient condition for a positive surviving shell is

$$B + E(m)(P/4 + 3/2) + L_e M(N)\{1/(4P) + 2/P^2\} < 1/2. \tag{49}$$

Surviving norms are positive, have no inert factor, and satisfy the dyadic condition in (39); their values lie in P.

The complete finite Euler products give

$$\begin{aligned}&M(X) \le 6X^{1/6}, && M(X) \le 2X^{1/4},\\ &\tau(m) \le 7m^{1/6} \quad (m \text{ inert}-\text{supported}), && \tau(m) \le 42m^{1/6} \quad (m \text{ odd}).\end{aligned} \tag{50}$$

For the sixth-power bounds, maximize $(a+1)^6/p^a$ at each odd prime below 64, over $0 \le a \le 6$. The factors decrease afterwards, and factors at primes at least 64 are at most one by $a+1 \le 2^a$. The split and inert products are respectively below $6^6, 7^6$; their product gives 42^6. For the fourth-power split bound only primes $3, 11$ contribute, and their product is $4096/297 < 2^4$. These calculations establish (50) for all X, m.

Since $N \le 8m$, $M(N) \le 9m^{1/6}$. For arbitrary odd m, use $P = m^{1/4}$ in (49). The terms after B are at most

$$\frac{45}{2}m^{-1/12} + 159m^{-1/3}.$$

If $m \ge 2^{75}$, use $m^{1/12} > 224/3$ to obtain

$$\frac{3}{16} + \frac{135}{448} + \frac{159}{2^{25}} < \frac{1}{2}. \tag{51}$$

This proves the stated global onset $N \ge 2^{78}$. The margin is $2620327/234881024 > 1/100$. In every eligible stratum $r(N) \ge 3N$, and each ordered value pair has at most $(2M(N))^2 \le 144N^{1/3}$ witnesses. The count is therefore at least $N^{2/3}/4800$.

Two additional uniform families follow from the same inequality. For inert-supported m, use $P = 2m^{1/4}$ and $\tau(m) \le 7m^{1/6}$. The error after B is at most

$$\frac{19}{2}m^{-1/12} + \frac{69}{2}m^{-1/3}.$$

For $m \ge 2^{60}$, its total with B is bounded by

$$\frac{3}{16} + \frac{19}{64} + \frac{69}{2^{21}} < \frac{1}{2}. \tag{52}$$

Thus all $2^e m$, $0 \le e \le 3$, in this family lie in $P + P$. At m the two values must be in different parity classes; at $2m$ both are in C; at $8m$ both are in $2C$, and division by two gives $4m \in C + C$. This proves the three core conclusions above the onset.

For an odd prime n, use $E(n) \le 2n^{-1/2}$, $M(n) \le 2n^{1/4}$, $L_0 = 4$, and $P = 2n^{3/8}$. The error after B is at most $2n^{-1/8} + 7n^{-1/2}$. For $n \ge 2^{22}$, it is dominated by $3/10 + 7/2048$, and

$$3/16 + 3/10 + 7/2048 < 1/2. \tag{53}$$

Every such prime lies in $P + P$; since it is odd, it lies in $C + 2C$. The finite mixed-core coverage below will supply all smaller odd primes, so no separate prime-family search is required.

5.5 Sharper selected shells

The improved lattice bounds are

$$\begin{aligned} S_Q(X) &:= \#\{(x,y) : 0 < Q(x,y) \le X\} \le \tfrac{8}{3}X, \\ S_o(X) &:= \#\{(x,y) : Q(x,y) \le X,\ Q(x,y) \text{ odd}\} \le 2X. \end{aligned} \tag{54}$$

For the first, use the preceding row bound and $\pi < 22/7$, $7/5 < \sqrt{2} < 10/7$. At integer $X \ge 81$ the ratio is at most $110/49 + 8/21 = 386/147 < 8/3$. The complete point table checks $1 \le X \le 80$. For odd norm the first coordinate is odd; row integration gives

$$S_o(X) \le \frac{\pi X}{2\sqrt{2}} + (1+\sqrt{2})\sqrt{X} + 1.$$

At $X \ge 25$, divide by X and use $55/49 + 17/35 + 1/25 < 2$. The point table checks $1 \le X \le 24$. Both counts vanish below one, and flooring proves the real bounds.

For odd m, sieve the following selected subsets:

N	selected subset	proportion at least	$\mathcal{L}$	δ
m	$G_2(m)$	$1/2 - E(m)/2$	$8/3$	$1/2$
$2m$	both field norms odd	$1/2$	2	0
$4m$	both field norms odd	$2/3$	$4/3$	0

(55)

The even subset sizes are exact. Multiplication of both components by ϖ bijects the full shell of norm $N/2$ with the part of the norm-N shell having both norms even. The odd-odd complement has size $r(N) - r(N/2)$, namely $4\sigma(m)$ at $2m$ and $16\sigma(m)$ at $4m$. All selected components are nonzero.

For the first row, (54) and $r_Q(t) \le 2M(N)$ bound the large-prime count by $(32/3)M(N)N/p^2$, giving normalized coefficient $\mathcal{L} = 8/3$. For the other rows use $S_o(N/p^2) \le 2N/p^2$. The numerator is $8M(N)N/p^2$; division by the respective full shells $8\sigma(m)$ and $24\sigma(m)$ gives 2 and 4/3. The small-prime bound (46) is applied in the full shell, not in the selected subset. Consequently, with λ the third-column constant $1/2, 1/2, 2/3$, a sufficient condition in each row is

$$B + E(m)(\Pi(P) + \delta) + \mathcal{L}M(N)T(P) < \lambda, \quad T(P) = \sum_{\substack{p \in \mathcal{I} \\ p > P}} p^{-2}. \tag{56}$$

This follows by subtracting the union of all bad events from the selected subset; no Hecke stability of that subset is needed. After sieving the rows give respectively $C + 2C, C + C, C + C$.

5.6 The complete interval and finite certificates

For inert-supported odd m, a sharper bound is

$$E(m) < \frac{18}{5} m^{-1/3}. \tag{57}$$

Raise the normalized prime-power factors to the sixth power: they are $(a+1)^6 p^{5a}/\sigma(p^a)^6$. Primes at least 64 contribute at most one. For each smaller inert prime, exponents through three suffice: the subsequent ratio is strictly less than $(5/4)^6/p \le (5/4)^6/5 < 1$. The exact product of the finite maxima is below $(18/5)^6$. Thus (57) is an unrestricted bound.

For the bounded M-envelope, enumerate nonincreasing exponents on initial segments of the smallest split primes. Swapping exponents $a < b$ at $p < q$ lowers the integer cost by $(p/q)^{b-a}$, preserving the divisor product, so no maximizer is lost. The recursion through 2^{63} has 2970 states. The product of the first thirteen split primes exceeds 2^{63}, and $3^{40} > 2^{63}$; these bound both its depth and exponent range.

Set $R_0 = 65536$, $D_0 = 2^{64}$. For $P < R_0$, define

$$V(P) = \frac{1}{D_0} \sum_{\substack{p \in \mathcal{I} \\ P < p \le R_0}} \lceil D_0/p^2 \rceil + \frac{1}{4R_0} + \frac{2}{R_0^2} \ge T(P). \tag{58}$$

The prime list is a complete Eratosthenes sieve; the final two terms majorize all larger primes by the two progressions. Thus $\Pi(P)$ is exact and $V(P)$ is an upward rational bound.

For $N = fm$, $f = 1, 2, 4$, and $2^k \le m < 2^{k+1}$, put

$$d_{f,k} = M(f(2^{k+1} - 1)), \qquad e_k = \frac{18}{5\lfloor (2^k)^{1/3} \rfloor}, \qquad P = \min\left(R_0 - 1, \left\lfloor \sqrt{\mathcal{L} d_{f,k}/e_k} \right\rfloor\right).$$

All of these quantities are obtained by integer and rational operations, using squared comparisons for square roots. The certificate verifies

$$\frac{3}{16} + e_k(\Pi(P) + \delta) + \mathcal{L} d_{f,k} V(P) < \lambda - \frac{1}{256} \tag{59}$$

on every interval in the following table:

f	core family	k-range	number
1	$C + 2C$	$27 \le k \le 59$	33
2	$C + C$ at $2m$	$26 \le k \le 59$	34
4	$C + C$ at $4m$	$20 \le k \le 59$	40

There are 107 tests, with all exact inputs and fractions in the supplement's certificate. Each row has minimum margin greater than $1/256$, with the exact minima recorded there. Together with (52), these tests cover all inert cores above the finite ranges below.

It remains to describe that finite coverage independently of any asymptotic statement. Put $B_0 = 2^{27}$. A complete prime sieve constructs the membership flags of $C \cap [1, B_0]$ by removing multiples of 2 and every prime $5, 7 \pmod 8$. No larger prime can divide a value in this interval. These complete flags are also authenticated by primitive coordinate enumeration: $x \ge 1$ odd, $y \ge 0$, $x^2+2y^2 \le B_0$, $\gcd(x, y) = 1$. Independent sign changes justify those coordinate restrictions. The two full bytearrays are compared, rather than merely their hashes.

Pack the flags as $B_C = \sum_{n\in C, n\le B_0} 2^n$, and form B_{2C} by doubling their positions. The exact truncated unions

$$U_e = \bigvee_{\substack{a\le 5000\\ a\in C}} (B_C \ll a),$$

$$U_o = \bigvee_{\substack{a\le 5000\\ a\in C}} (B_{2C} \ll a) \ \vee \bigvee_{\substack{b\le 5000\\ b\in 2C}} (B_C \ll b)$$

have only genuine sums. There are 699 core anchors and 365 doubled anchors. After truncation at B_0, U_e equals exactly the periodic mask $2, 4, 6 \pmod 8$; U_o equals exactly the odd mask with position one removed. Thus every one of 50331648 even strong targets and 67108863 mixed odd targets is covered, with no locally forbidden position covered. A short anchor has not been postulated: the union actually covers every required bit. The certificate programs reconstruct these arrays and compare the complete target masks.

5.7 Completion by descent

Suppose that a least eligible exception to $C + C$ exists. Its dyadic valuation is one or two. A split prime factor q can be removed: the quotient is a smaller eligible even target at least two, and multiplication by q lifts a representation. Thus the least exception is $2m$ or $4m$ with odd inert-supported m. The finite coverage, the corresponding interval row in (59), and (52) cover every such m, a contradiction.

For $C + 2C$, a least missing odd $N \ge 3$ with a split prime factor either is a single split prime, or descends to a smaller odd target at least three. The prime boundary is covered by (53) above 2^{22} and by the finite mixed coverage below that bound. With no split factor, N is inert-supported and is covered by the finite computation, its 33 interval tests, and the infinite tail. This proves both strong core identities. Their local exclusions and (40) prove the full primitive identity. The explicit count was already obtained from (51), completing Theorem 5.1.

6 The exact sumset at discriminant -11

Put $Q(x, y) = x^2 + xy + 3y^2$, and let C contain one and the positive integers supported on primes with $(p/11) = 1$. Write P for the positive primitive values of Q.

Theorem 6.1. *One has the exact identities*

$$C + C = \{n \ge 2 : 2 \mid n,\ 11 \nmid n\}, \qquad P + P = \{N \ge 2 : 2 \mid N,\ 121 \nmid N\}.$$

The field ring $R = \mathbb{Z}[\omega]$, $\omega = (1 + \sqrt{-11})/2$, has class number one. Indeed the Minkowski bound $(2/\pi)\sqrt{11} < 3$ leaves only norms one and two, while two is inert; see [8, Theorem 4.3]. Primitive ideal factorization therefore gives

$$P = C \,\dot\cup\, 11C. \tag{60}$$

An inert prime dividing a norm divides both coordinates; at the ramified prime a primitive norm has valuation at most one. Conversely, orienting an entire split prime power to a single principal prime ideal, and optionally multiplying by $\sqrt{-11}$, produces every value in (60). In particular all these values are odd. Modulo eleven, $4Q = (2x + y)^2$, and -1 is a nonsquare. Thus a sum of two primitive values divisible by eleven uses two ramified values; it is not divisible by 121. Multiplication by $\sqrt{-11}$ has coordinate matrix

$$\begin{pmatrix} -1 & -6 \\ 2 & 1 \end{pmatrix}, \qquad M^2 = -11I, \qquad Q(Mv) = 11Q(v).$$

It carries primitive eleven-unit values to primitive values of eleven times their norm. Consequently the first identity in the theorem implies the second, by writing $N = 11^e n$, $e \in \{0, 1\}$.

6.1 Shells and the filtered Hecke quotient

Take $B = (-11, -1)_{\mathbb{Q}}$ and $O = R \oplus Rj$, with $j^2 = -1$ and $ja = \bar a j$. The algebra has discriminant eleven, and this is a maximal order [2, Theorem 15.5.5 and Example 15.5.7]. Its norm is $F = Q \oplus Q$, and its units are $\{1, -1, j, -j\}$. Write $\sigma(t) = 0$ and $T_t = 0$ for nonintegral positive indices. The exact shell formula is

$$r_F(m) = \frac{12}{5}\{\sigma(m) - 11\sigma(m/11)\} + \frac{8}{5}a_m, \qquad \sum_{m\ge 1} a_m q^m = \eta(\tau)^2\eta(11\tau)^2. \tag{61}$$

For completeness, the rank-four theta series has weight two, level eleven and trivial character. The Eisenstein series $(11E_2(11\tau) - E_2(\tau))/10$ is holomorphic at every cusp: it is one tenth of the logarithmic derivative of the modular function $\Delta(11\tau)/\Delta(\tau)$, whose cusp expansion is $q_c^v U(q_c)$ with $U(0) \neq 0$. The eta-product is the normalized weight-two newform of level eleven [6, Theorem 1, level-eleven row]. After multiplying the claimed identity by five, both sides have integral coefficients. Their coefficients through degree two agree: the theta coefficients are $(1, 4, 4)$ and the cusp coefficients $(0, 1, -2)$. The Sturm bound is $2[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(11)]/12 = 2$. Sturm's theorem applied modulo every prime proves equality [7, Theorem 1]. Independent lattice enumeration and eta-product multiplication verify this complete coefficient list.

For an even $n = 2^t m$ with m odd and $11 \nmid n$, let $G(n)$ count shell points with both field norms odd. Since $R/2R = \mathbb{F}_4$, an even field norm has both coordinates even; hence

$$G(n) = r_F(n) - r_F(n/4), \qquad S(n) = \sigma(n) - \sigma(n/4) = 3 \cdot 2^{t-1}\sigma(m) \ge \tfrac{3}{2}n.$$

Put

$$\mathcal{D}(n) = \tau(m)\sqrt{m}\, 2^{t/2}\frac{t+3}{2}, \qquad E = \frac{2\mathcal{D}(n)}{3S(n)}. \tag{62}$$

The filtered cusp coefficient satisfies $|a_n - a_{n/4}| \le \mathcal{D}(n)$. Indeed the normalized roots at two have product one, and

$$a_{2^t} - a_{2^{t-2}} = 2^{t/2}\left(u^t + v^t + \frac{1}{2}\sum_{j=1}^{t-1} u^j v^{t-j}\right), \qquad |u| = |v| = 1.$$

For $t = 1$ the interior sum is empty. Multiplicativity proves

$$G(n) \ge \frac{12}{5}S(n)(1 - E). \tag{63}$$

Moreover $\sigma(m) \geq \tau(m)\sqrt{m}$ by the arithmetic–geometric mean inequality at each prime power. Therefore $E \leq 2(t+3)/(9\,2^{t/2}) \leq 4\sqrt{2}/9 < 1$. All estimates in this subsection require the reduced target $11 \nmid n$; the ramified factor is restored only after obtaining value pairs.

For clarity, we retain all quaternionic ideal classes. Their projective unit mass is $(11-1)/12 = 5/6$ [2, Theorem 25.1.1]. The principal class has projective stabilizer size two, so its probability is

$$w = \frac{1/2}{5/6} = \frac{3}{5}. \tag{64}$$

At an odd inert prime $p \geq 7$, impose the projective reduction kernel with quotient $G_p = \mathrm{PGL}_2(\mathbb{F}_p)$. At eleven use the radical quotient $G_{11} = \mathbb{F}_{121}^{\times}/\mathbb{F}_{11}^{\times}$, of order twelve. Every projective unit stabilizer injects into these groups: a noncentral norm-one unit has integral trace $-1, 0, 1$, whereas scalar reduction would force p to divide its trace discriminant -3 or -4. Thus the fine quotients have uniform point measure, principal fiber probability w, and, at eleven, ten points with six in the principal fiber.

For a function h supported on that fiber, the all-ideal correspondence at its base point x_0 has the normalization

$$(T_m h)(x_0) = \frac{1}{4} \sum_{\substack{\alpha \in O \\ \mathrm{nrd}\,\alpha = m}} h(\rho_p(\alpha)). \tag{65}$$

Each principal-return ideal has four generators. Principalization initially uses α^{-1}, but projectively this is $\bar{\alpha}$, and conjugation permutes the shell.

There are exactly two global norm characters at these fine levels: 1 and the quadratic residue character ψ_p. Away from the auxiliary prime the maximal units have all unit norms; at that prime the kernel has square residue norms, central scalars have square norms, and rational reduced norms give all positive rationals [2, Main Theorem 14.7.4]. The resulting norm quotient has order two. Lemma 2.1 therefore bounds the complementary spectrum. For $D_n = T_n - T_{n/4}$, the constant and character eigenvalues are $S(n)$ and $(n/p)S(n)$, and its complementary norm is at most $\mathcal{D}(n)$, by the same cancellation of roots used above. No operator is used at an auxiliary level prime dividing its index.

6.2 The local sieve and its positive margin

Let $\mathcal{I} = \{p \text{ odd prime} : (p/11) = -1\}$, and write $b_p(n)$ for the odd-shell points with at least one field component norm divisible by p. If $p \nmid n$, the nonsplit torus normalizer $H_p \subset G_p$ has order $2(p+1)$, contains the principal projective unit group, and describes exactly the invertible quaternions having one zero field component. Put $\mu_p = 2/(p(p-1))$ and $h = \mathbf{1}_{\Gamma_0 \backslash H_p}$. Its mean is $\nu = w\mu_p$; its quadratic-character mean is zero because the torus norm is onto. Right-H_p invariance gives $(D_n h)(x_0) = \langle h, D_n h \rangle_\pi / \nu$, where π is the all-ideal invariant probability measure. This is the orbit identity of Proposition B.1, with orbit measure $\nu = w\mu_p$. Its nonconstant squared norm is $\nu(1-\nu)$, so

$$\frac{b_p(n)}{G(n)} \leq \frac{\mu_p + (5/2)E}{1-E}. \tag{66}$$

If $p \mid n$, anisotropy forces both components divisible by p as soon as one is. The count is zero unless $p^2 \mid n$, and otherwise is $G(n/p^2)$. Since $S(n/p^2) \leq S(n)/p^2$ and $\mathcal{D}(n/p^2) \leq \mathcal{D}(n)/p$, its ratio is at most $(p^{-2} + E/p)/(1-E)$, which is bounded by (66). This covers arbitrary target valuations.

At eleven the two field-component axes project to the single base point in the principal fiber. Its indicator has mean $1/10$ and projection coefficient $1/10$ on both 1 and ψ_{11}; the complementary squared norm is $2/25$. Evaluation at a point of probability $1/10$ gives

$$\frac{b_{11}(n)}{G(n)} \leq \frac{1/3 + 2E}{1-E}. \tag{67}$$

Set

$$M(X)=\max_{1\le v\le X}\prod_{\substack{q\mid v\\(q/11)=1}}(v_q(v)+1),\qquad B_0=\sum_{p\in\mathcal{I}}\mu_p,$$

$$\Pi(P_0)=\#\{p\in\mathcal{I}:p\le P_0\},\qquad T(P_0)=\sum_{\substack{p\in\mathcal{I}\\p>P_0}}p^{-2}.$$

Ideal factorization gives $r_Q(v)\le 2M(X)$ for $1\le v\le X$. We also need the lattice bound

$$\#\{(x,y)\in\mathbb{Z}^2:0<Q(x,y)\le X\}\le\frac{12}{5}X. \tag{68}$$

For $g(y)=\sqrt{\max(X-11y^2/4,0)}$, each integer row contains at most $2g(y)+1$ points. Integrating the decreasing rows and removing the origin gives

$$S_Q(X)\le\frac{2\pi}{\sqrt{11}}X+(2+4/\sqrt{11})\sqrt{X}.$$

For integers $X\ge 49$, use $\pi<22/7$, $\sqrt{11}>33/10$ and $\sqrt{X}\ge 7$; the resulting ratio is at most $440/231+106/231=26/11<12/5$. Exact lattice enumeration checks $5S_Q(j)\le 12j$ for $1\le j\le 48$; for real X apply the integer bound at $\lfloor X\rfloor$.

Both odd-shell components are nonzero. Divisibility of one of their norms by an inert p forces that component to be p times a nonzero vector. Bound its choices by (68), the other component's choices by $2M(n)$, and count both orientations. This gives $b_p(n)\le(48/5)M(n)n/p^2$. Combining this large-prime estimate with (63), (66) and (67), a sufficient condition for a point whose two norms lie in C is

$$B_0+\frac{8}{3}M(n)T(P_0)+E\left(3+\frac{5}{2}\Pi(P_0)\right)<\frac{2}{3}. \tag{69}$$

Indeed the number remaining is at least $(12/5)S(n)$ times the positive difference. This counts values in C; their initial coordinate witnesses need not be primitive at split primes, because (60) supplies primitive witnesses of the same values.

Odd inert primes occupy the five classes $7,13,17,19,21 \pmod{22}$. Counting these progressions and integrating x^{-2} gives

$$\Pi(P_0)\le\frac{5}{22}P_0+\frac{3}{2},\qquad T(P_0)\le\frac{5}{22P_0}+\frac{5}{P_0^2},\qquad B_0<\frac{9}{100}. \tag{70}$$

For the last bound sum the actual inert primes through sixty-four, and majorize each remaining progression starting at $65,73,79,83,85$ by $a^{-2}+(22a)^{-1}$, using $\mu_p\le(7/3)p^{-2}$ for $p\ge 7$. These are rational inequalities.

For every $X\ge 1$ one has $M(X)\le 7X^{1/6}$. To certify this unrestricted bound, maximize $(a+1)^6/p^a$ over the split primes $p<64$ and $0\le a\le 10$. Their rational product is less than 7^6. Larger exponents cannot improve it, since $12^6<2\cdot 11^6$ and successive ratios decrease. For $p\ge 64$, $a+1\le 2^a$ makes every factor at most one.

For an even integer $n=2^tm$ supported on inert primes, the sharper bound

$$E<\frac{11}{4}n^{-1/3} \tag{71}$$

is also an exact Euler certificate. In fact

$$En^{1/3}=\frac{2(t+3)}{9}\,2^{-t/6}\prod_{p^a\parallel m}\frac{(a+1)p^{5a/6}}{\sigma(p^a)}.$$

The dyadic factor is at most one, with maximum at $t=6$: $9^6>2\cdot 8^6$ and $10^6<2\cdot 9^6$ bracket the change of the successive ratios. For odd inert $p\ge 64$ the sixth power is at most $(a+1)^6/p^a\le 1$.

For $p < 64$ the successive sixth-power ratio for $a \geq 2$ is less than $(4/3)^6/p < 1$. Thus only exponents zero, one and two at $7, 13, 17, 19, 29, 41, 43, 61$ occur in the finite maximum. Its exact product, recorded under `sharp_core_bounds` in the supplement's -11 receipt, is less than $(11/4)^6$. Taking $P_0 = n^{1/4}$ in (69) and using (70), the left side is bounded by

$$\frac{9}{100} + \frac{3065}{528} n^{-1/12} + \frac{5371}{48} n^{-1/3}.$$

For $n \geq 2^{60}$ this is less than $9/100 + 3065/(528 \cdot 32) + 5371/(48 \cdot 2^{20}) < 2/3$. Thus every such inert core belongs to $C + C$.

6.3 Thirty-five intervals and the finite certificate

The remaining analytic range is covered without enumerating its individual targets. The function $M(X)$ is exactly computable: remove nonsplit factors, then assign nonincreasing positive exponents to the smallest split primes. Swapping exponents $a < b$ at $p < q$ preserves the divisor product and reduces the integer by $(p/q)^{b-a}$. Hence enumerating initial split-prime prefixes with nonincreasing exponents exhausts the maxima. The first twelve split primes have product greater than 2^{61}, and $3^{41} > 2^{61}$; these inequalities certify the finite prime and exponent limits.

For $k = 25, \ldots, 59$ put

$$L_k = 2^k, \quad U_k = 2^{k+1} - 1, \quad d_k = M(U_k), \quad e_k = \frac{11}{4\lfloor \sqrt[3]{L_k} \rfloor}, \qquad P_k = \left\lfloor \sqrt{\frac{16 d_k}{15 e_k}} \right\rfloor.$$

For an inert core in this interval, $M(n) \leq d_k$ and $E \leq e_k$. Sieve the primes through $R_0 = 65536$ exactly and set $D_0 = 2^{64}$,

$$A_k = \#\{p \in \mathcal{I} : p \leq P_k\}, \quad V_k = \frac{1}{D_0} \sum_{\substack{p \in \mathcal{I} \\ P_k < p \leq R_0}} \left\lceil \frac{D_0}{p^2} \right\rceil + \frac{5}{22 R_0} + \frac{5}{R_0^2}.$$

All $P_k < R_0$, so $A_k = \Pi(P_k)$ and $V_k \geq T(P_k)$. The supplied integer/rational certificate checks all thirty-five inequalities

$$\frac{9}{100} + \frac{8}{3} d_k V_k + e_k \left(3 + \frac{5}{2} A_k \right) < \frac{2}{3} - \frac{1}{1024}. \tag{72}$$

Thus (69) covers every inert core in $[2^{25}, 2^{60})$, and the infinite estimate covers the rest.

Finally construct the exact flags of $C \cap [1, 2^{25}]$ by removing multiples of every forbidden prime, including two and eleven. Let B_C be the packed integer whose bit j is this membership flag. The finite certificate computes

$$\bigvee_{\substack{a \leq 5000 \\ a \in C}} (B_C \ll a),$$

using 774 short summands, and verifies that after truncation through 2^{25} it contains every eligible even eleven-unit target bit. There are exactly $2^{24} - \lfloor 2^{25}/22 \rfloor = 15252015$ such bits. Every set bit has genuine positive summands. Complete independent coordinate/gcd enumeration authenticates all membership flags through 2^{25}: simultaneous sign reversal permits $y \geq 0$, reflection $x \mapsto -x - y$ permits $2x + y \geq 0$, and $4Q = (2x + y)^2 + 11y^2$ gives exhaustive integer bounds. Only positive odd values with $11 \nmid Q(x, y)$ are retained after the gcd test; this excludes the ramified part $11C$ of P. The full bytearrays are compared before hashing.

A least even eleven-unit exception to $C + C$, if it existed, would exceed 2^{25}. A split prime factor q would leave the smaller eligible even target $n/q \geq 2$, whose representation lifts on multiplication by q. The least exception is therefore supported on inert primes, a case excluded by (72) and the infinite bound. Conversely $C + C$ has only even targets, and no multiple of eleven because -1 is nonsquare. This proves the first identity in Theorem 6.1; the ramified reduction proves the second.

AI assistance and review. ChatGPT (OpenAI) assisted with mathematical arguments, literature checks, exposition, proof review and verification code.

A Finite certificates and their verification

The verification programs, exact rational certificates and replay instructions are in the frozen certificate supplement (GitHub commit `b854dddcda88`), under `certificates/`. The archive also retains the sources of that edition; its certificate files apply to this article. The separate TeX sources compile without executing verification code. Table 1 gives the complete finite domains and the interval and descent arguments joining them to the infinite ranges.

Membership and coverage. The prime sieve deletes every multiple of a forbidden prime. For the Eisenstein indexing $6j+1$, any inert factor has another inert factor counted with multiplicity, so one is below the square root; primes below 10000 suffice in the stated domain. The other three discriminants use the complete prime sieves specified in their sections.

If B_C is the packed membership array, the unions of shifts $B_C \ll a$, with the indicated ramified dilation in a mixed family, contain only genuine positive sums. Comparing the full truncated union with the predicted target mask proves coverage of every eligible integer and exclusion of every forbidden one. For a listed exception, testing every possible summand up to half the target proves nonrepresentation. The exact programs reconstruct these arrays and target comparisons, not merely their hashes.

Independent coordinate enumeration authenticates the full membership arrays at the certificate bounds. At $-7, -11$, use $4Q = (2x+y)^2 + |d|y^2$, sign reversal and $x \mapsto -x-y$ to restrict to $y \geq 0,\ 2x+y \geq 0$, with integer square-root limits. At -8, independent sign changes restrict to the first quadrant. Apply the coordinate gcd test throughout. At -11, retain only positive odd norms with $11 \nmid Q(x,y)$, thereby authenticating C, rather than $P = C \dot\cup 11C$. The full bytearrays are compared; deleting a unit, inserting a forbidden prime power or corrupting a target mask must be rejected.

Exact arithmetic and completeness. Divisor maxima are exhausted by nonincreasing exponents on the smallest eligible primes, with the explicit prime and exponent limits proved in each section. Omitted Euler factors are at most one. Rational rounding and arithmetic-progression tails bound the prime sums. Integer comparisons after clearing positive denominators then certify every target in each interval. The interval endpoints meet the finite scans and infinite estimates; descent exhausts the remaining targets. In particular the three rows of (59) have minimum margin greater than $1/256$. Their exact minima are recorded in `primitive_norm_minus8_checks.json`, under `interval_certificate`, together with all 107 inequalities.

Receipt conventions. The supplement's four sumset verifiers and coordinate authenticator produce the corresponding JSON receipts; the theta, Euler and local checks are included there too. Membership arrays are ordered zero-one bytes indexed by the integer, or by j for $6j+1$. Packed bit n is the coefficient of 2^n. Eisenstein witness digests use the least short index at increasing target indices, encoded as signed little-endian 32-bit integers. The ordinary and mixed arrays have their respective domain lengths. The expected membership and witness digests are in `binary_certificates_receipt.json`; the other families' digests and rational margins are in their named JSON receipts. The standalone verifiers use integer arithmetic and Python's standard library; their assertions reject optimized execution. Hashes identify the supplied bytes; the membership, interval and descent arguments above establish their mathematical role.

B Orbit averaging and a sieve criterion

The two elementary estimates below isolate the averaging and small/large-prime split used in the local sieves.

Proposition B.1. *Let a finite group G act on the right on a finite set Y equipped with a G-invariant probability measure π. Let $K \le G$, and let $\Omega = y_0K$ be a K-orbit of positive measure. On $L^2(Y,\pi)$ put $f = 1_\Omega$ and $\mu = \pi(\Omega)$. Suppose T is self-adjoint, commutes with the G-action, and satisfies $T1 = d1$ with $d > 0$. Let $E \subset L^2(Y,\pi)$ be a subspace such that*

$$\|Tv\| \le \Lambda\|v\| \quad (v \in E^\perp), \qquad f - \mu 1 \in E^\perp,$$

where $\Lambda \ge 0$. Then

$$\left|\frac{(Tf)(y_0)}{d} - \mu\right| \le \frac{\Lambda}{d}(1-\mu).$$

In particular, the same right side bounds the upper deviation.

Proof. Right-K invariance makes Tf constant on Ω. Writing $f = \mu 1 + h$, one has $h \perp 1$, $\|h\|_\pi^2 = \mu(1-\mu)$, and

$$(Tf)(y_0) = \frac{\langle f, Tf\rangle_\pi}{\mu} = d\mu + \frac{\langle h, Th\rangle_\pi}{\mu}.$$

Self-adjointness and $T1 = d1$ remove the cross terms; the spectral hypothesis bounds the last numerator in absolute value by $\Lambda\mu(1-\mu)$. □

Only transitivity on Ω is used. At -11, its measure is $\mu = (3/5)\mu_p$; Section 6 checks the norm-character orthogonality and the separate ramified contribution.

Proposition B.2. *For each admissible positive integer $n \ge n_0$, let $\mathcal{R}_n$ be a finite set of $R(n) > 0$ candidate representations. Let E_n be an exceptional bad subset, and $B_{p,n}$ bad subsets indexed by a fixed set $\mathcal{S}$ of primes. Every representation outside $E_n \cup \bigcup_{p\in\mathcal{S}} B_{p,n}$ is assumed to be good. Suppose, uniformly in the admissible targets and primes, that*

$$\frac{|E_n|}{R(n)} \le \rho + \eta(n), \qquad \frac{|B_{p,n}|}{R(n)} \le \mu_p + C_1 n^{\delta-1/2}, \qquad \frac{|B_{p,n}|}{R(n)} \le C_2 n^\delta p^{-2},$$

where $C_1, C_2, \rho, \mu_p, \eta(n) \ge 0$, $\delta < 1/4$, $\eta(n) \to 0$, and

$$\sum_{p\in\mathcal{S}} \mu_p \le M < \infty, \qquad \rho + M < 1.$$

Assume also, for every real $P \ge P_0 > 0$, that

$$\#\{p \in \mathcal{S} : p \le P\} \le \alpha P + \beta, \qquad \sum_{\substack{p\in\mathcal{S}\\ p>P}} p^{-2} \le \frac{\gamma}{P} + \frac{\zeta}{P^2},$$

with nonnegative constants. For fixed $t > 0$, put

$$L_1 = \alpha t C_1 + \frac{\gamma C_2}{t}, \qquad L_2 = \beta C_1 + \frac{\zeta C_2}{t^2}.$$

Every admissible $n \ge \max\{n_0, (P_0/t)^4\}$ satisfying

$$\eta(n) + L_1 n^{\delta-1/4} + L_2 n^{\delta-1/2} < 1 - \rho - M$$

has a good representation. In particular, every sufficiently large admissible target does.

If the constants are effectively known and η has an effective modulus $N_\eta(u)$, meaning $\eta(n) \le u$ for all admissible $n \ge N_\eta(u)$, put $\Delta = 1 - \rho - M$, $a = 1/4 - \delta$ and $b = 1/2 - \delta$. An explicit sufficient cutoff is

$$\max\left\{n_0, (P_0/t)^4, N_\eta(\Delta/4), (4L_1/\Delta)^{1/a}, (4L_2/\Delta)^{1/b}\right\}.$$

Proof. Split at $P = tn^{1/4}$, using the first local bound below P and the second above it. The convergent union bound is

$$\frac{|E_n| + \sum_p |B_{p,n}|}{R(n)} \le \rho + M + \eta(n) + L_1 n^{\delta - 1/4} + L_2 n^{\delta - 1/2}.$$

A value below one gives a good representation. Both powers tend to zero, and at the effective cutoff each of the three error terms is at most $\Delta/4$. □

The prime-count hypotheses always admit the crude choices $\alpha = \gamma = \zeta = 1$, $\beta = 0$, $P_0 = 1$, by comparison with integers and a decreasing integral. Arithmetic residue information improves these constants. When $\alpha C_1, \gamma C_2 > 0$, the choice $t = \sqrt{\gamma C_2/(\alpha C_1)}$ minimizes L_1, though not necessarily the complete cutoff. The mixed Eisenstein application uses $\delta = 1/5$, $\rho = 1/3$, $\eta(n) = 2/(3\sqrt{n})$, $C_1 = 9/4$, $C_2 = 15/2$, $M = 3/20$ and $(\alpha, \beta, \gamma, \zeta) = (2/15, 17/15, 2/15, 8/5)$. Section 3.6 uses $t = 2$ and the sharper direct inequality there to obtain 10^8.

C The remaining balanced exception question

The complete Eisenstein finite scan also tests $n/3 \le a, b \le 2n/3$ in the ordinary family $\mathcal{A} + \mathcal{A}$. For $2 \le n < 10^8$, $n \equiv 2 \pmod 6$, its only failures are 8 and 44. This suggests the exact classification

$$\{n \ge 2 : \exists a, b \in \mathcal{A},\ n = a + b,\ n/3 \le a, b \le 2n/3\} = \{n > 0 : n \equiv 2 \pmod 6\} \setminus \{8, 44\},$$

where the left side is interpreted target by target. The finite scan alone does not prove that these are the only failures. Even an eventual balanced theorem needs an effective onset and a complete certificate meeting that onset to settle this exact question.

References

[1] W. Howe, G. Huffman, J. Kohlmeyer, and L. Kruer, *Euler's 1747 conjecture on sums of integers with restricted prime factors*, Hexagon 2611.00370v1, 12 November 2026. https://hexagonmath.org/2611.00370v1.

[2] J. Voight, *Quaternion Algebras*, Graduate Texts in Mathematics 288, Springer, 2021. Theorem numbering follows the author edition 1.0.7u, 5 August 2026, Chapters 14, 15, 25, 28 and 41. https://jvoight.github.io/quat-book.pdf. https://doi.org/10.1007/978-3-030-56694-4.

[3] H. Jacquet and R. P. Langlands, *Automorphic Forms on* GL(2), Lecture Notes in Mathematics 114, Springer, 1970, Theorem 14.4 and Section 5. https://publications.ias.edu/sites/default/files/automorphic-forms-on-gl2_rpl_9.pdf.

[4] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Séminaire Bourbaki, exposé 355 (1968/69), published 1971, 139–172. https://www.numdam.org/item/SB_1968-1969__11__139_0.pdf.

[5] P. Deligne, *La conjecture de Weil. I*, Publications Mathématiques de l'IHÉS 43 (1974), 273–307. https://www.numdam.org/item/PMIHES_1974__43__273_0.pdf.

[6] Y. Martin and K. Ono, *Eta-quotients and elliptic curves*, Proceedings of the American Mathematical Society **125** (1997), 3169–3176. Author edition, 6 May 1996: https://uva.theopenscholar.com/files/ken-ono/files/026_8.pdf.

[7] J. Sturm, *On the congruence of modular forms*, in Number Theory (New York, 1984–1985), Lecture Notes in Mathematics 1240, Springer, Berlin, 1987, 275–280. https://doi.org/10.1007/BFb0072985.

[8] J. S. Milne, *Algebraic Number Theory*, version 3.08, 19 July 2020, Theorem 4.3. https://www.jmilne.org/math/CourseNotes/ANT.pdf.

[9] R. van Rijn, *Pointwise Correlations of Quadratic Form Values and Splitting Semigroups*, version 1, Zenodo, 2026. https://doi.org/10.5281/zenodo.24371355.