Pointwise representation counts for Eisenstein restricted sums

Roy van Rijn

hexagon:2611.00593v1

Abstract

Let A consist of the positive integers supported on primes 1 mod 3, including 1. We count distinct ordered representations $n = a + b$ for $n \equiv 2 \bmod 6$ and $n = a + 3b$ for $n \equiv 4 \bmod 6$, with $a, b \in A$. In either family prescribe an interval of length H centered at x for one actual summand. Put $M = \min(x, n - x)$. For every fixed $0 < \varepsilon < 1$, if $H \le M$ and $H^3 \ge n^{1+\varepsilon} M$, the count has order $HJ(n)/\log n$ for every sufficiently large admissible n. Here $J(n)$ is the product of $(p-1)/(p-2)$ over the odd primes $p \equiv 2 \bmod 3$ dividing n. In particular, central windows of width n^θ are allowed for $2/3 < \theta < 1$, and windows at a prescribed small summand of size comparable to their width are allowed for $1/2 < \theta < 1$. The lower bound combines angular Hecke estimates with a sieve that prescribes small split factors in both summands.

1 The pointwise count

Let $\mathcal{A} = \{a \in \mathbb{Z}_{>0} : p \mid a \Rightarrow p \equiv 1 \bmod 3\}$, where p always denotes a prime. Write $3{\cdot}\mathcal{A} = \{3a : a \in \mathcal{A}\}$. We count ordered pairs (s_1, s_2) of positive integers summing to n, with

$$(s_1, s_2) \in \begin{cases} \mathcal{A} \times \mathcal{A}, & n \equiv 2 \pmod 6, \\ \mathcal{A} \times (3{\cdot}\mathcal{A}) \text{ or } (3{\cdot}\mathcal{A}) \times \mathcal{A}, & n \equiv 4 \pmod 6. \end{cases}$$

In the second line one orientation is prescribed in advance. For $0 < x < n$ let $r(n; x, H)$ count these pairs with $|s_1 - x| \le H/2$. In particular, if the first summand is $3a$, it is $3a$ that lies in the interval.

Theorem 1.1. *Fix $0 < \varepsilon < 1$ and put $M = \min(x, n - x)$. Uniformly for every sufficiently large admissible n and every real x, H with*

$$0 < x < n, \qquad 1 \le H \le M, \qquad H^3 \ge n^{1+\varepsilon} M,$$

one has, in each of the prescribed families,

$$r(n; x, H) \asymp_\varepsilon \frac{HJ(n)}{\log n}, \qquad J(n) = \prod_{\substack{p \mid n,\ p \ge 5 \\ p \equiv 2 \ (3)}} \frac{p-1}{p-2}. \tag{1}$$

The constants in the two bounds and the threshold for n depend only on ε.

The product has a direct interpretation. At $p = 5$, for example, the two conditions $5 \nmid s_1$ and $5 \nmid n - s_1$ forbid two residues when $5 \nmid n$, and one when $5 \mid n$. The ratio of the allowed proportions is $(4/5)/(3/5) = 4/3$. The same calculation explains every factor of $J(n)$ and yields an upper bound by an ordinary sieve on integers.

The lower bound begins with a larger family that can be counted spectrally. Write $N(z) = z\bar{z}$ for the Eisenstein norm on $\mathbb{Z}[\omega]$, with $\omega^2 + \omega + 1 = 0$. The equation $N(z) + N(w) = n$ is a quaternion norm equation. At an inert prime $p \equiv 2 \bmod 3$, $p \mid N(z)$ forces $z \in p\mathbb{Z}[\omega]$. It is therefore possible to remove the large inert primes by a lattice count within the prescribed window.

A separate issue is that many coordinate pairs can give the same two norm values. Sifting out small split primes bounds this multiplicity, with a baseline coordinate count of size $H/(\log n)^2$ before the target factors. To gain a factor of $\log n$ we allow small split primes to occur to exponent one in one summand, or in both summands when they divide the target. For instance, $7 \nmid n$ permits placing 7 in either summand. If $7 \mid n$, its use as a common factor reduces the target to $n/7$. The split-prime local factors for these two situations supply the same logarithmic gain. The prescribed factors can be read off the resulting values, and each pair then has bounded weighted coordinate multiplicity.

The angular estimate costs $\sqrt{M/H}$ in the Hecke remainder. Multiplying by the square-root error from the norm shell gives $\sqrt{nM/H}$. Comparing this with the main-term width H explains $H^3 \geq n^{1+\varepsilon}M$. The proof below treats the finite level and the angular variable together, which lets us prescribe the mixed orientation at any center.

Proof overview. Section 2 estimates the angularly weighted shell with finite congruence tests. Section 3 handles primes dividing the target, with a worked example at 7^2. Section 4 sums over the small split factors to recover the logarithm. Section 5 removes the remaining inert primes, bounds the weight of each distinct pair, and gives the matching integer-sieve upper bound.

Relation to earlier work. Dietmann and Elsholtz [2] prove eventual binary existence for the Gaussian prime restriction $p \equiv 1 \bmod 4$ and obtain $\gg_\delta n^{1-\delta}$ pairs for every $\delta > 0$ without restricting the summand sizes. Howe, Huffman, Kohlmeyer and Kruer [1, Theorem 1.1] prove existence for every positive target 2 mod 4, using quaternionic norm counts and a sieve on the representing vectors. The prime sets used here and in the Gaussian problem are incomparable, as 7 and 17 show. We use the same norm-counting principle for the Eisenstein ring. The new estimates needed here are angular localization with prescribed residue conditions, the densities when a sieving prime divides the target, and a lower bound that counts distinct value pairs at the integer-sieve scale. Ramaré and Viswanadham [4, Introduction and Theorem 1.6] discuss the split-prime Eisenstein set in their sieve framework and prove a ternary additive theorem for primitive Gaussian values.

The Frobenian correlation theorem of Loughran and Matthiesen [9, Theorem 1.9] requires pairwise independent linear parts. Fixing the total gives the one-variable forms $t, n-t$, with proportional linear parts. In the mixed case, restricting to the necessary residue class and dividing one form by 3 leaves the same dependence. Freeing the total gives a two-variable sum, which averages over the slices that our theorem estimates individually.

Iwaniec's half-dimensional sieve [10, Theorem 1] uses a half-dimensional local product and a remainder from counts in residue classes. Sieving both summands directly excludes two residues per inert prime away from the target divisors. As the inert primes have density $1/2$, this gives sieve dimension one. A half-dimensional sieve on one summand with the other already restricted would require progression estimates for that restricted sequence in translated windows, uniformly in the target. Greaves [11, main theorem] obtains a bound of order at least $n/(\log n)^{5/2}$ for prime pairs whose complementary value is a sum of two squares. The cutoff $p, q \leq \sqrt{n}/2$ in that Gaussian input leaves the split of the complementary sum of two squares free. Here the angular Hecke estimate supplies the window-dependent distribution, and the split-factor sum reaches the scale of distinct values.

Corollary 1.2. *The count in every fixed interval of positive length for s_1/n inside $(0,1)$ is of order $nJ(n)/\log n$. In particular the unrestricted count has this order. At any fixed interior share, windows of width n^θ have count of order $n^\theta J(n)/\log n$ for $2/3 < \theta < 1$. For $1/2 < \theta < 1$ and fixed $0 \leq a < b$, the same count holds with $s_1 \in [an^\theta, bn^\theta]$.*

The results give two-sided order bounds. A leading constant and a numerical onset are open here, as are the central and small-summand endpoint exponents $2/3$ and $1/2$.

2 An angular estimate on a quaternion shell

Fix n, x, H as in Theorem 1.1. We first count coordinate representations with an angular weight and prescribed local conditions.

2.1 The norm shell

Let $R = \mathbb{Z}[\omega]$ and $K = \mathbb{Q}(\omega)$. The Eisenstein lattice is norm Euclidean, since every complex number is within squared distance $1/3$ of a lattice point. Write $B = K + Kj$, where $j^2 = -1$ and $jz = \bar{z}j$, and put $\mathcal{O} = R + Rj$. Its reduced norm is $\mathrm{nrd}(z + wj) = N(z) + N(w)$. The trace pairing on $1, \omega, j, \omega j$ has determinant -9, so the order has reduced discriminant 3. The algebra is definite and the number of ramified places is even, so it is ramified at 3 and infinity. Thus $\mathcal{O}$ is maximal.

Rounding both complex coordinates gives a remainder of reduced norm at most $2/3$. In any nonzero integral right ideal, take a least positive norm element α and divide on the left by α. The remainder in that ideal has norm smaller than $\mathrm{nrd}(\alpha)$ unless it vanishes. Every right ideal is therefore principal, as are the fractional ideals by scaling. The unit group U consists of the twelve elements of $R^\times \cup R^\times j$. For $3 \nmid m$, let $\mathcal{Q}_m = \{\alpha \in \mathcal{O} : \mathrm{nrd}(\alpha) = m\}$. At each $\ell^e \| m$, integral right ideals correspond locally to index-ℓ^e sublattices of $\mathbb{Z}_\ell^2$, of which there are $1 + \ell + \cdots + \ell^e$. Each ideal has twelve generators of norm m, giving

$$|\mathcal{Q}_m| = 12\sigma(m), \qquad \sigma(m) = \sum_{d \mid m} d. \tag{2}$$

We use this all-ideal convention throughout [3, Propositions 41.3.1 and 41.3.6].

The number of coordinates of a positive norm a is $6f(a)$, where f is multiplicative. Its local values are $f(p^e) = e + 1$ at split primes $p \equiv 1 \bmod 3$, $f(p^e) = 1$ at 3, and $f(p^e) = \mathbf{1}_{2 \mid e}$ at inert primes $p \equiv 2 \bmod 3$. Indeed a split prime has two conjugate factors in R, and a choice of their exponents gives each possibility up to a unit. The ramified prime in R above 3 is generated by $1 - \omega$ and has norm 3. In particular, $f(a) \le \tau(a)$, where τ is the divisor function. At an inert prime, R/pR is a field, so norm divisibility by p is equivalent to coordinate divisibility by p. For even m, both component norms have the same parity. Both are even precisely on the shell scaled by 2 from $m/4$. The odd-component shell therefore has size

$$R_o(m) = 12\{\sigma(m) - \sigma(m/4)\}, \qquad \frac{R_o(m)}{m} = 18 \prod_{\substack{p^e \| m \\ p \ge 5}} \frac{\sigma(p^e)}{p^e}, \tag{3}$$

where $\sigma(m/4) = 0$ if $4 \nmid m$.

2.2 Finite tests and the Hecke bound

Use the finite group G obtained by multiplying the fixed factor $G_3 = (\mathcal{O}/3\mathcal{O})^\times/\mathbb{F}_3^\times$ and any factors $\mathrm{PGL}_2(\mathbb{Z}/p^a\mathbb{Z})$ at $p \ge 5$, with $a = 1$ or 2. The Hecke index in this subsection is coprime to the level. Write Γ for the image of U in G. The kernel on U is $\{\pm 1\}$, as is seen at 3. Each group has a norm squareclass map, using determinant at split quaternion places. Both squareclasses occur. At 3, for example, the norms of 1 and $1 + j$ give the two classes. They are detected modulo p at every odd level prime.

For $k \ge 0$, let $\rho_k = \mathrm{Sym}^{2k} \mathbb{C}^2$ denote the unitary representation of $\mathrm{SU}(2)$ on that space. For a real quaternion of nonzero norm use $u_\alpha = \alpha/\sqrt{\mathrm{nrd}(\alpha)} \in \mathrm{SU}(2)$, under the usual identification of unit quaternions with $\mathrm{SU}(2)$. The action on order units descends to Γ. Use the space of functions $F : G \to \mathrm{Sym}^{2k} \mathbb{C}^2$ satisfying $F(\gamma g) = \rho_k(\gamma) F(g)$, with squared norm summed once per left coset. The all-ideal Hecke operator is

$$(T_m F)(g) = \frac{1}{12} \sum_{\alpha \in \mathcal{Q}_m} \rho_k(u_\alpha)^{-1} F(\alpha_{\mathrm{fin}} g), \tag{4}$$

where α_{fin} is projective reduction in G. Let $\mathcal{K}$ be the product of the projective order-unit groups at the finite places, and $\mathcal{K}_0$ the kernel of reduction to G. At 3 we use order units, with reduction modulo $3\mathcal{O}_3$. A residue unit lifts to an order unit since its reduced norm is a 3-adic unit. At each $p \geq 5$ in the level, the corresponding reduction of $\mathrm{GL}_2(\mathbb{Z}_p)$ is surjective modulo p^a. Thus $\mathcal{K}/\mathcal{K}_0 = G$.

Class number one gives $PB^\times(\mathbb{A}_f) = PB^\times(\mathbb{Q})\mathcal{K}$, where $\mathbb{A}_f$ denotes the finite adeles. A rational element stabilizing $\mathcal{K}$ has a representative locally equal to a scalar times an order unit. A single rational scalar cancels the valuations of the local scalars, giving an element of U. Consequently the finite adelic quotient is $\Gamma\backslash G$. The projective rational stabilizer at any level coset is trivial. Indeed, $\mathcal{K}_0$ is normal in $\mathcal{K}$ and only the units ± 1 lie in the kernel of reduction. With coefficients, rational left equivariance gives the stated action of Γ [8, Section 2, (4)–(6) and Proposition 2.5]. Each orbit has $|\Gamma|$ elements and hence the same finite measure. At infinity Schur orthogonality for a unit test vector gives the factor $1/(2k+1)$. The resulting automorphic norm differs from the counting norm by a common scalar.

To see the direction and normalization in (4), lift g to $\tilde{g} \in \mathcal{K}$ supported at level primes. A right-ideal representative a in the correspondence of norm m can be chosen supported at primes of m, so $\tilde{g}a = a\tilde{g}$. If the ideal is $\alpha\mathcal{O}$, write $a = \alpha u$ with $u \in \mathcal{K}$ projectively. At level primes u reduces to $\alpha_{\mathrm{fin}}^{-1}$. Hence the summand is $\rho_k(u_\alpha)F(\alpha_{\mathrm{fin}}^{-1}g)$. Changing α by a right order unit cancels by equivariance. Averaging over all twelve generators implements the sum once per ideal. Replacing α by $\bar{\alpha}$ gives (4). Conjugation also proves self-adjointness.

We use the bound

$$\|T_m\| \leq \tau(m)\sqrt{m} \tag{5}$$

on the whole space for $k > 0$, and on the complement of the joint norm-squareclass characters for $k = 0$. Here are the relevant hypotheses for cuspidal transfer. A finite-dimensional smooth irreducible local factor at a split place ℓ is trivial on the norm-one group, since its open normal kernel contains the elementary unipotents by diagonal conjugation. Such a factor cannot occur at positive weight. In fact $\mathcal{O}[1/\ell]^1$ has dense real image in $\mathrm{SU}(2)$. Equation (2) gives infinitely many norm-one elements α/ℓ^a of exact denominator ℓ^a by taking $\mathrm{nrd}(\alpha) = \ell^{2a}$ and omitting $\ell\mathcal{O}$. There are at most $12(2a+1)$ single-component points of that norm, so these elements extend outside the Eisenstein torus normalizer. A proper infinite closed subgroup of $\mathrm{SU}(2)$ normalizes its one-dimensional identity component. It contains the order-three unit ω, which must then lie in that torus and determines it as the Eisenstein torus. This contradicts the points outside its normalizer. For a finite adelic representative g, impose the congruences $g^{-1}\gamma g$ belonging to the level away from ℓ. They cut out a finite-index subgroup of $\mathcal{O}[1/\ell]^1$, still dense by connectedness. At ℓ the discrepancy is absorbed by invariance under the local norm-one group. Rational left invariance then forces the coefficient at g to be fixed by that dense subgroup, which is impossible in the nontrivial irreducible representation.

For $k = 0$, suppose the factor at ℓ is finite-dimensional and let h be a finite adelic norm-one element. Strong approximation for B^1 away from $\{\infty, \ell\}$ lets us choose a rational norm-one element γ approximating ghg^{-1} outside ℓ [3, Main Theorem 28.5.3]. In $gh = \gamma g(g^{-1}\gamma^{-1}gh)$, the final factor can be taken in the right stabilizer of the vector away from ℓ. At ℓ it has norm one and acts trivially. Thus the exceptional constituents are invariant under the entire finite adelic norm-one group. On $\mathcal{K}$ they depend only on the joint norm squareclasses in G. Indeed, at the odd level primes a square norm can be scaled to one, and outside the level the order units already act trivially. Conversely, each product of local signs comes from a quadratic Dirichlet character composed with reduced norm. This is projectively well-defined since scalar norms are squares, and it has trivial real type since real reduced norms are positive. By (4) its eigenvalue is $\sigma(m)$ times its value on the norm class of m. These sign functions span the scalar exceptional space.

The remaining constituents have infinite-dimensional factors at split places. Jacquet–Langlands gives cuspidal GL_2 representations of holomorphic weight $2k+2$ and trivial central character, unramified at every $\ell \mid m$ [5, Theorem 14.4 and Proposition 5.20]. Let α_ℓ, β_ℓ be their

unitary Satake parameters. Their product is one. The classical Hecke roots are $\ell^{k+1/2}\alpha_\ell, \ell^{k+1/2}\beta_\ell$, so Deligne's bound gives $|\alpha_\ell| = |\beta_\ell| = 1$ [6, Theorems 4.9 and 5.1] [7, Theorem 1.6].

For the operator at ℓ^a the all-ideal right cosets are represented by upper triangular matrices with diagonal ℓ^i, ℓ^{a-i} and upper right entry modulo ℓ^i, for $0 \le i \le a$. In normalized unramified induction [5, Section 3], the spherical vector has value $\ell^{a/2-i}\alpha_\ell^i\beta_\ell^{a-i}$ there. Summing the ℓ^i choices of the upper right entry gives the eigenvalue

$$\ell^{a/2}\sum_{i=0}^{a}\alpha_\ell^i\beta_\ell^{a-i}.$$

This includes imprimitive ideals and equals the classical coefficient at ℓ^a divided by ℓ^{ak}. In particular, the recurrence is $T_{\ell^a} = T_\ell T_{\ell^{a-1}} - \ell T_{\ell^{a-2}}$ for $a \ge 2$. The eigenvalue has modulus at most $(a+1)\ell^{a/2}$. Multiplicativity now gives (5) with the same bound at every weight and level.

2.3 A finite test with a prescribed direction

For a test $b : G \to \mathbb{C}$ and a unit vector v in degree k, define

$$F(g) = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\rho_k(\gamma)v\, b(\gamma^{-1}g).$$

This is the orthogonal projection of $b(g)v$ onto equivariant functions in the full counting norm on G. Its coset norm is at most $\|b\|_{\ell^2(G)}/\sqrt{|\Gamma|}$. For another unit vector w, reindexing the shell by the left unit lift of each γ gives

$$12\langle w, (T_mF)(1)\rangle = \sum_{\alpha\in\mathcal{Q}_m} b(\alpha_{\mathrm{fin}})\,\langle w, \rho_k(u_\alpha)^{-1}v\rangle. \tag{6}$$

Here the inner product is linear in its second variable. The averaging factor cancels because for a lift γ_0 the substitution $\alpha = \gamma_0\alpha'$ cancels $\rho_k(\gamma)$ against the archimedean multiplier. This formula allows b to distinguish the two components.

Writing $\alpha = z + yj$, put $t_\alpha = (N(z) - N(y))/m$. For $v = w$ the unit vector proportional to X^kY^k, the matrix coefficient in (6) equals $P_k(t_\alpha)$, where P_k is the degree-k Legendre polynomial with $P_k(1) = 1$. Indeed, the polynomial action gives the binomial formula

$$P_k(t_\alpha) = \sum_{j=0}^{k}(-1)^j\binom{k}{j}^2(N(z)/m)^{k-j}(N(y)/m)^j.$$

Passing to u_α^{-1} leaves the coefficient unchanged.

In degree zero, projecting onto the sign characters replaces b by its average conditioned on the joint norm squareclasses of m. Indeed these characters form an orthogonal basis for functions of the squareclasses, and the eigenvalue signs evaluate them at m. The averaging defining F preserves these means. For a product of local tests the conditional mean is the product of their conditional means. At each positive degree, evaluation at one coset has norm at most one, so (6) is bounded in absolute value by $12\tau(m)\sqrt{m}\|b\|_{\ell^2(G)}$. The same error bound applies to the scalar cuspidal part.

2.4 The cost of a translated window

Choose a fixed smooth $0 \le \phi \le 1$ of compact support in $(-1/2, 1/2)$ and integral $I_\phi > 0$. Put $h = H/n$, $b = M/n$, and $\lambda = x/n$. We use the bump

$$W(t) = \phi\left(\frac{(1+t)/2 - \lambda}{h}\right).$$

As $h \le b$, on its support $1 - t^2 \asymp b$, and the support has length at most $2h$. The constant Legendre coefficient of W is $I_\phi h$.

Lemma 2.1. *The Legendre expansion $W = \sum_{k\ge 0} c_k P_k$ converges uniformly and absolutely, with $\sum_{k\ge 1} |c_k| \ll_\phi \sqrt{b/h}$.*

Proof. We use $|P_k(t)| \ll k^{-1/2}(1-t^2)^{-1/4}$ for $-1 < t < 1$. For a short proof, let $Y(u) = \sqrt{\sin u}\, P_k(\cos u)$ on $0 < u < \pi$. The Legendre equation gives $Y'' + QY = 0$ with $Q = (k+1/2)^2 + 1/(4\sin^2 u)$. The derivative of $Y^2 + (Y')^2/Q$ is $-Q'(Y')^2/Q^2 \ge 0$ up to $\pi/2$. At $\pi/2$ this energy is $O(k^{-1})$, by $P_{2j}(0) = (-1)^j 4^{-j}\binom{2j}{j}$, $P_{2j+1}(0) = 0$ and $P_k'(0) = kP_{k-1}(0)$. Reflection gives the bound on both halves.

Write $\mathcal{L} = -\frac{d}{dt}((1-t^2)\frac{d}{dt})$. In the rescaled coordinate $v = (t - 2\lambda + 1)/(2h)$, the operator is b/h^2 times a differential operator of order two with coefficients and derivatives bounded on the support of ϕ. Indeed its two coefficients in that scale are $-(1-t^2)/(4b)$ and th/b. Integrating by parts twice using $\mathcal{L}P_k = k(k+1)P_k$, and also using the direct integral, gives

$$|c_k| \ll_\phi h\sqrt{k}\, b^{-1/4} \min\left(1, \left(\frac{b}{h^2k^2}\right)^2\right).$$

The factor $\sqrt{k}$ includes the coefficient normalization $(2k+1)/2$. Summing below and above $K = \sqrt{b}/h$ gives $O_\phi(hb^{-1/4}K^{3/2}) = O_\phi(\sqrt{b/h})$. Since $|P_k| \le 1$ on $[-1,1]$, the series converges uniformly. Its Legendre coefficients identify the sum with W by polynomial density. □

Combining this lemma with (6), a finite product test of modulus at most one has weighted shell count

$$12\sigma(m) I_\phi h \prod_p \text{local conditional mean} + O_\phi\Big(\sqrt{|G|}\,\tau(m)\sqrt{m}\sqrt{M/H}\Big). \tag{7}$$

The same W is used when the target is divided by a common factor. Both component norms scale together and t_α is unchanged.

3 Local densities at all target valuations

On a shell at m, put $A_1 = N(z)$ and $A_2 = N(y)$. The bump W restricts both norms to be positive. At a variable prime $p \ge 5$ write $g_m(p)$ for the density of the bad test $p \mid A_1A_2$. For $p \nmid m$ this is the conditional mean in (7). At $p \mid m$ we derive its analogue by reducing to coprime Hecke indices.

3.1 Coprime target and level

At 3 the ordinary family requires no test, since $m \equiv 2 \bmod 3$ forces both norms to be units modulo 3. In the mixed family $m \equiv 1 \bmod 3$, and we require the prescribed component to have 3-adic valuation exactly one. Among the nine elements of $R/3R$ there are six units, two nonzero nonunits, and zero. The nonzero nonunits have norm valuation one, since $1-\omega$ has norm 3 and its square is associated to 3. Norm one modulo 3 requires one unit and one nonunit, giving $2 \cdot 6 \cdot 3 = 36$ raw quaternion residues. Exactly $6 \cdot 2$ have a unit in one prescribed component and a nonzero nonunit in the other. Passing to projective classes preserves the ratio, so either mixed orientation has mean $1/3$.

At an inert $p \nmid m$, by anisotropy a bad point has one component zero modulo pR. Its image in $\mathrm{PGL}_2(\mathbb{F}_p)$ lies in the normalizer of the nonsplit torus $(R/pR)^\times/\mathbb{F}_p^\times$. This is the union of that torus and its translate by j, with $2(p+1)$ elements out of $p(p^2-1)$. The norms of the torus elements cover the squareclasses equally, so $g_m(p) = 2/[p(p-1)]$ in either class.

At a split $p \nmid m$, the two factors of the Eisenstein subalgebra occupy the diagonal of $M_2(\mathbb{F}_p)$. The other Eisenstein component occupies the off-diagonal. Their norms are the products of the respective entries, up to sign. For a fixed nonzero determinant, the first row is uniform on

nonzero rows, each with p completions. Thus a given entry is zero with probability $1/(p+1)$. Two zero entries are possible only when they form an opposite pair. For either such pair there are $p-1$ matrices of the given determinant, giving probability $1/[p(p+1)]$. Inclusion-exclusion gives

$$1 - g_m(p) = B_p := 1 - \frac{4}{p+1} + \frac{2}{p(p+1)} = \frac{(p-1)(p-2)}{p(p+1)}. \tag{8}$$

For the exact condition $v_p(A_i) = 1$ at either one prescribed component, exactly one of its two entries is zero modulo p, and this entry must be nonzero modulo p^2. All matrix lifts of an invertible residue are invertible, and determinant squareclasses are determined modulo p. The conditional probability of the last lift condition is $(p-1)/p$. Therefore the mean of $v_p(A_i) = 1$ at level p^2 is

$$t_p = \frac{2(p-1)^2}{p^2(p+1)}, \qquad a_p := \frac{t_p}{2B_p} = \frac{p-1}{p(p-2)}. \tag{9}$$

These means hold on projective groups as well, since all tests are unchanged by a unit scalar.

3.2 Primes dividing the target

For inert $p \mid m$, divisibility of one norm by p forces the other to be divisible by p as well, so both components are in pR. The bad set is empty if $v_p(m) = 1$. Otherwise it is obtained by multiplying both coordinates by p from the shell at m/p^2. This preserves W and the other prime tests. Hence for $e = v_p(m)$ the scalar density is

$$g_m(p) = 0 \ (e = 1), \qquad g_m(p) = \frac{\sigma(p^{e-2})}{\sigma(p^e)} \ (e \geq 2). \tag{10}$$

Now let $p = \pi\bar{\pi}$ be split in R, and fix r prime to p. At target $p^e r$, let U_e be the weighted count with no restriction at p, and G_e the count with both norms units at p. Carry along W and the other prime tests. At target r, let L_0 count with the additional test

$$\frac{1}{2}\big(\mathbf{1}_{\pi|z} + \mathbf{1}_{\bar{\pi}|z} + \mathbf{1}_{\pi|y} + \mathbf{1}_{\bar{\pi}|y}\big).$$

It has mean $2/(p+1)$ by the single-entry calculation. If one norm has valuation $v > 0$, the $v+1$ allocations of its two prime factors are equally frequent. The average of the test at that pair of norms is $v/(v+1)$. The conditions at other primes are unchanged on reallocating these factors. Indeed, dividing out or inserting factors above p acts by units at every other prime, preserving all the norm valuations and the individual split-prime divisibilities used in the tests.

Classify a pair of norms on the shell $p^e r$ by the minimum j of its two p-adic valuations. If $j < e$, both valuations are j; removing p^j from each norm gives a G_{e-j} pair with allocation multiplier $(j+1)^2$. If $j = e$, the residual target is r. When both residual norms are units the multiplier is $(e+1)^2$; if one has valuation $v > 0$, the ratio of allocation counts is $(e+1)(v+e+1)/(v+1) = (e+1)^2 - e(e+1)v/(v+1)$. In either reduction the normalized norm coordinate stays fixed. This proves

$$U_e = \sum_{j=0}^{e-1} (j+1)^2 G_{e-j} + (e+1)^2 U_0 - e(e+1)L_0 \qquad (e \geq 1). \tag{11}$$

The generating series for $(j+1)^2$ is $A(T) = (1+T)/(1-T)^3$, and that for $e(e+1)$ is $C(T) = 2T/(1-T)^3$. Thus

$$\sum_{e \geq 1} G_e T^e = \frac{\sum_{e \geq 0} U_e T^e}{A(T)} - U_0 + \frac{C(T)}{A(T)} L_0.$$

The coefficients of $1/A(T)$ have absolute value at most eight, and those of $C(T)/A(T)$ at most two. The bad count $U_e - G_e$ is therefore a combination of unrestricted counts at lower p-exponents

and the L_0 count at the unit target, with coefficient absolute sum at most $8e+2$. Applying the same identity to the scalar prediction from (7) uses $U_e = \sigma(p^e)$, $U_0 = 1$, and $L_0 = 2/(p+1)$ after factoring out the other local factors. Substitution gives $\sum_{e\ge 1} G_e T^e = \frac{(p-1)^2}{p+1}\frac{T}{1-pT}$ for those scalar values. In particular

$$1 - g_m(p) = \frac{(p-1)^2 p^{e-1}}{(p+1)\sigma(p^e)} \qquad (e = v_p(m) \ge 1,\ p \text{ split}). \tag{12}$$

Example at a split square. Take $m = 7^2 r$ with $7 \nmid r$. The first two cases of (11) give

$$U_2 - G_2 = 4G_1 + 9U_0 - 6L_0 = 4U_1 - 7U_0 + 2L_0.$$

The term at $7r$ is unrestricted at 7, and the only remaining 7-level test is L_0 at r. For the main term, factor out the other primes and insert $U_2 = 57$, $U_1 = 8$, $U_0 = 1$, $L_0 = 1/4$. The resulting main term for G_2 is $63/2$, giving $1 - g_m(7) = (63/2)/57$. Including the shell factor $\sigma(7^2)/7^2 = 57/49$ gives $9/14$. This is $B_7 \cdot (6/5)$, since $B_7 = 15/28$ at a unit target. In the cofactor sum of Section 4.2 this gives weight $6/5$ without a common factor 7, and $(6/5)/7$ with that common factor, since the residual target $7r$ still has positive valuation at 7. In general (12) gives $E_p = (p-1)/(p-2)$ at every positive valuation.

3.3 The joint estimate

Fix squarefree coprime u, v made of split primes coprime to m. Place the condition $v_p(A_1) = 1$ at $p \mid u$ and $v_p(A_2) = 1$ at $p \mid v$. Give each coordinate pair weight $W(t)/\tau(uv)$. Here and below m is even and prime to 3. Keep the odd-component condition and the prescribed condition at 3. For any squarefree ℓ coprime to $6uv$, let $S_m(\ell)$ be the weighted count additionally bad at every prime dividing ℓ, and put

$$X_m = I_\phi h R_o(m) \beta_m, \qquad \beta_m = \begin{cases} 1, & m \equiv 2 \bmod 6, \\ 1/3, & m \equiv 4 \bmod 6. \end{cases}$$

Extend g_m multiplicatively on squarefree products.

Lemma 3.1. *For $m \le n$ as above and any fixed $\zeta > 0$,*

$$S_m(\ell) = X_m \prod_{p \mid uv} (t_p/2)\, g_m(\ell) + O_{\phi,\zeta}\Big((uv)^3 \ell^{3/2} n^{1/2+\zeta}\sqrt{M/H}\Big). \tag{13}$$

Proof. First omit oddness. If the level is coprime to m, apply (7). A factor at $p \mid uv$ has size $p^3 |\mathrm{PGL}_2(\mathbb{F}_p)| < p^6$ and a factor at $p \mid \ell$ has size less than p^3. Thus the norm cost is $O((uv)^3 \ell^{3/2})$, the fixed factor at 3 being bounded.

For $p \mid (\ell, m)$, eliminate the test by inert scaling or (11). Each time, the remaining test at the eliminated prime is present only at a reduced target coprime to it. The allocation calculation works with any of the other tests still imposed. In particular the test at a split prime produced by an earlier elimination is an average of individual divisibilities, all invariant under changes of allocation at another prime. The coprime conditional means are independent of the nonzero determinant class at those other primes. Extracting split powers and inert squares does not change the target class modulo 3, and the prescribed orientation is preserved. Hence the scalar terms factor, with local factors (10) and (12). The total coefficient variation in the elimination is at most $\tau(m)^4$, because $8e + 2 \le (e+1)^4$. Each resulting target divides m, and the remaining level divides the original level. The product of these losses with the divisor factor in (7) is absorbed by $O_\zeta(n^\zeta)$.

Finally subtract the shell at $m/4$ if it exists. Rescaling its coordinates by 2 preserves the normalized angle, the odd-prime tests and the orientation at 3. The valuations at all odd primes agree with those for m, so the scalar $\sigma(m)$ is replaced by $\sigma(m) - \sigma(m/4)$. This gives (13). □

4 The lower sieve and the split factors

Fix $\kappa, \xi > 0$ with $4\kappa + \frac{5}{2}\xi < \varepsilon/2$. We use a divisor level $D = n^{\xi}$ and prime bounds $Z = n^{\eta}$ and $Y = n^{\lambda_0}$, with $0 < \lambda_0 < \eta$ chosen below. Consider triples of pairwise coprime squarefree integers d, u, v, supported on split primes at most Y, satisfying

$$d \mid n, \qquad (uv, n) = 1, \qquad duv \le n^{\kappa}. \tag{14}$$

On the shell $m = n/d$ use the prescriptions of Lemma 3.1 at u, v, and require $p \nmid A_1 A_2$ at every other prime $5 \le p \le Z$, including the primes of d. Since $d \equiv 1 \bmod 6$, the target m belongs to the same family. The weight on the shell is $W(t) = \phi((dA_1 - x)/H)$, so after rescaling the norm values by d the original window is enforced.

4.1 Finite inclusion-exclusion

We give the sieve weights together with the level they require. Partition the sieving primes into blocks $Z^{2^{-j-1}} < p \le Z^{2^{-j}}$ for $j \ge 0$. For the main-term probabilities $g_m(p)$, the sum in each block is bounded by an absolute C and $v_j = \prod_{p \text{ in block } j}(1 - g_m(p))$ is bounded below by an absolute $c > 0$. In fact the formulas in Section 3 lie uniformly below one and are $O(1/p)$. Prime harmonic Mertens gives a bounded sum of $1/p$ in each block. Omitting primes, including the primes of uv, preserves these bounds. We also use the progression version of Mertens modulo 3, $\sum_{p \le T,\ p \equiv a\ (3)} 1/p = \frac{1}{2}\log\log T + O(1)$ for $a = 1, 2$; see [9, Lemma 2.4].

In block j truncate inclusion-exclusion at consecutive orders $k_j = 2\lceil (K + j)/2 \rceil$ and $k_j - 1$, where K is a fixed large integer. Denote the resulting polynomials in the bad-prime indicators by U_j, L_j. Bonferroni gives $0 \le \mathbf{1}_j \le U_j$ and $L_j \le \mathbf{1}_j$, where $\mathbf{1}_j$ indicates avoidance in the block. Telescoping $\prod_j U_j - \prod_j \mathbf{1}_j$ gives the lower polynomial

$$\prod_j \mathbf{1}_j \ge \prod_j U_j - \sum_j (U_j - L_j) \prod_{i \ne j} U_i. \tag{15}$$

Under independent bad events with probabilities $g_m(p)$,

$$\mathbf{E}U_j \ge v_j, \qquad \mathbf{E}(U_j - L_j) \le \frac{C^{k_j}}{k_j!}.$$

Choose K so that the sum over j of $C^{k_j}/(ck_j!)$ is at most $1/2$. The expectation of the lower polynomial is at least $\frac{1}{2}\prod_j v_j$. Also $0 \le \mathbf{E}U_j - v_j \le \mathbf{E}(U_j - L_j)$, so the expectation of the upper polynomial $\prod_j U_j$ is $O(\prod_j v_j)$. We will use this upper estimate later with integer-sieve probabilities.

Put $S = \sum_{j \ge 0} k_j 2^{-j} < \infty$ and $\eta = \xi/S$. Every divisor in either polynomial is at most $Z^S = D$. The upper coefficients have absolute value at most one, and the lower coefficients at most one plus the number of nonempty blocks, which is $O(\log\log(3n))$. Apply (13) to the lower polynomial with the nonnegative shell weights. For each triple the main contribution is at least

$$\tfrac{1}{2} X_m V_m(Z) \prod_{p \mid uv} a_p, \qquad V_m(Z) = \prod_{5 \le p \le Z} (1 - g_m(p)). \tag{16}$$

Here $a_p = t_p/(2B_p)$ accounts for replacing the ordinary sieve factor at a prime of uv by the exact-valuation factor. Summing the remainders over all divisors uses $\sum_{\ell \le D} \ell^{3/2} \ll D^{5/2}$. There are at most $n^{\kappa + o(1)}$ triples because a fixed product duv has at most $\tau(duv)^2$ decompositions. The total absolute remainder, for any $\zeta > 0$, is

$$O_{\phi,\zeta}\Big(n^{1/2 + 4\kappa + (5/2)\xi + \zeta}\sqrt{M/H}\Big) = o_{\varepsilon}(H/\log n).$$

The equality uses $\sqrt{nM/H} \le Hn^{-\varepsilon/2}$ and the strict choice of κ, ξ, with ζ small enough. All of these estimates are uniform in x, H.

4.2 The logarithm gained from small factors

The target-independent product

$$V_*(Z) = \prod_{\substack{5\le p\le Z\\ p \text{ split}}} B_p \prod_{\substack{5\le p\le Z\\ p \text{ inert}}} b_p, \qquad b_p = 1 - \frac{2}{p(p-1)}$$

satisfies $V_*(Z) \asymp (\log Z)^{-2}$, since $B_p = 1 - 4/p + O(p^{-2})$ and the inert factors have a convergent positive product. To compare this with $V_m(Z)$, include the shell factor $R_o(m)/m$ from (3). For $p^e \| m$ split and $p \le Z$,

$$\frac{\sigma(p^e)}{p^e}(1 - g_m(p)) = \frac{(p-1)^2}{p(p+1)} = B_p E_p, \qquad E_p = \frac{p-1}{p-2}.$$

For $p^e \| m$ inert and $p \le Z$ the combined factor is $1 + 1/p = b_p E_p$, by (10), including $e = 1$. The inert primes dividing m and n are the same. For the inert primes dividing m beyond Z, the shell factor is at least $1 + 1/p = b_p E_p$, and the product of the extra factors b_p is bounded below. All split enhancements are at least one. Using $hm = (H/n)m = H/d$, we get

$$X_m V_m(Z) \gg_\phi \frac{H}{d} J(n) V_*(Z) \prod_{\substack{p\le Y,\ p \text{ split}\\ p\mid m}} E_p. \tag{17}$$

Temporarily drop the product bound in (14). The sum of the cofactor weights in (16) and (17) factors over split $p \le Y$. For $p \nmid n$ the three options of absence, inclusion in u, or inclusion in v have weights $1, a_p, a_p$. If $p^e \| n$, the two options of absence or inclusion in d have weights $E_p, E_p'/p$, where $E_p' = 1$ for $e = 1$ and $E_p' = E_p$ for $e \ge 2$. The compensation at target divisors is the identity

$$E_p + \frac{E_p'}{p} \ge E_p + \frac{1}{p} = 1 + 2a_p.$$

Thus the full cofactor sum is at least $\prod_{p\le Y,\ p \text{ split}}(1 + 2a_p) \asymp \log Y$, since $a_p = 1/p + O(p^{-2})$.

Normalize the local weights to independent probabilities. At $p \nmid n$ the probability of $p \mid duv$ is $2a_p/(1+2a_p) \ll p^{-1}$, and at $p \mid n$ it is at most $1/p$. Hence $\mathbf{E}\log(duv) \le C' \log Y$, uniformly in n, by $\sum_{p\le Y}(\log p)/p \ll \log Y$. Take $0 < \lambda_0 < \min(\eta, \kappa/(3C'))$. Markov's inequality then retains at least half the weight on $duv \le n^\kappa$. Inserting (17) into (16) and subtracting the aggregate remainder proves that the total retained weight is

$$\gg_\varepsilon HJ(n)\frac{\log Y}{(\log Z)^2} \gg_\varepsilon \frac{HJ(n)}{\log n}. \tag{18}$$

5 From coordinates to distinct pairs

For each d fix $\rho_d \in R$ of norm d, obtained by multiplying one factor above each split prime of d. Embed the residual shell at $m = n/d$ in the original shell by $(z, y) \mapsto (\rho_d z, \rho_d y)$. This preserves the fractional norm coordinate, the prescribed orientation at 3, and inert divisibility above Z.

Each original value pair recovers its triple d, u, v. At split primes up to Y, the only possible positive valuation is one, occurring in both norms at the primes of d, only in the first at u, and only in the second at v. The images for distinct triples are consequently disjoint. This makes it possible to bound the remaining losses on the original shell without summing an error over the triples.

5.1 Large inert primes

If an inert prime $p > Z$ divides the first component norm, that component is $p\beta$. The norm of β belongs to $[(x - H/2)/p^2, (x + H/2)/p^2]$. For the other component use $n - x$ in place of x. Each resulting annulus has squared-radius width H/p^2 and outer radius at most $\sqrt{n}/p$. Covering each lattice point by a translated fundamental cell, of fixed area and bounded radius, gives $O(H/p^2 + \sqrt{n}/p + 1)$ possible β. Indeed the cells lie in the annulus obtained by moving the two boundaries by a fixed distance, truncating the inner radius at zero. The complementary positive norm has at most $6 \max_{a \le n} \tau(a) = n^{o(1)}$ coordinate choices.

Since all weights are at most one, summing on the original shell over the two components and $Z < p \le \sqrt{n}$ bounds the lost weight by

$$n^{o(1)} \left(\frac{H}{Z} + \sqrt{n}(1 + \log n) \right) = o_\varepsilon(H/\log n).$$

Here Z is a fixed power of n, and the hypothesis $H^3 \ge n^{1+\varepsilon} M$ with $M \ge H$ gives $H \ge n^{(1+\varepsilon)/2}$. Thus (18) persists after removing every inert prime. Oddness and the condition at 3 now give the required norm values.

5.2 The weight of one value pair

On the residual shell write $A_1 = uk_1$ and $A_2 = vk_2$. All split prime factors of k_1, k_2 exceed $Z = n^\eta$. Each of these two numbers has at most $1/\eta$ split factors counted with multiplicity, and the possible single factor 3 has no effect on coordinate multiplicity. The split primes in uv occur to valuation one. By the multiplicity formula in Section 2, the weighted coordinate multiplicity, after division by $\tau(uv)$, is at most

$$36 f(k_1) f(k_2) \le 36 \cdot 2^{2/\eta}.$$

Each original pair determines its triple and residual pair. Dividing the surviving weight by this constant proves the lower bound of Theorem 1.1.

5.3 The upper bound on integers

For the upper bound, write $s = s_1$ in the interval of length H. At every inert $p \ge 5$ we must exclude the residues $0, n \bmod p$. Let $\nu(p)$ be their number, namely one if $p \mid n$ and two otherwise, and extend ν multiplicatively to squarefree products of these primes. The Chinese remainder theorem and the count in a residue class give $H\nu(\ell)/\ell + O(\nu(\ell))$ integers in all the excluded sets for $p \mid \ell$, uniformly in the interval location and endpoint convention.

Use the upper polynomials of Section 4 with probabilities $\nu(p)/p$, sieving to $Z' = n^{c_1}$ for a sufficiently small fixed $c_1 > 0$. The block probability bounds hold as before. Choose c_1 so that the corresponding divisor level is $D' \le n^{1/4}$. The total error is $O(D' \log(2D')) = o(H/\log n)$, since $\nu(\ell) \le \tau(\ell)$ and $\sum_{\ell \le D'} \tau(\ell) \ll D' \log(2D')$. The upper main term is at most a constant times H times

$$\prod_{\substack{5 \le p \le Z' \\ p \text{ inert}}} (1 - 2/p) \prod_{\substack{5 \le p \le Z', \ p \mid n \\ p \text{ inert}}} \frac{p-1}{p-2} \ll \frac{J(n)}{\log n}.$$

This proves the upper bound and completes Theorem 1.1. The argument for this upper bound in fact works in any interval whose length is at least a fixed positive multiple of $\sqrt{n}$.

Proof of Corollary 1.2. In a fixed interval of shares, take a smaller fixed interval of length at most the distance of its center from the nearest endpoint of $[0, 1]$. This satisfies the hypotheses with $H \asymp n$ for large n, giving the lower bound. Use the upper sieve on the full interval and on $[0, n]$ for the unrestricted count. At $x = \lambda n$ with $0 < \lambda < 1$, a width $H = n^\theta$ satisfies the

condition for any fixed $0 < \varepsilon < 3\theta - 2$. Finally, inside $[an^\theta, bn^\theta]$ take a subinterval of width comparable to n^θ and at most its midpoint. Its distance to the nearer endpoint of $[0, n]$ is comparable to n^θ, so one can use $0 < \varepsilon < 2\theta - 1$. The upper sieve on the full interval gives the matching bound, also for $a = 0$. □

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

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] R. Dietmann and C. Elsholtz, *Sums of two numbers having only prime factors congruent to one modulo four*, Banach Center Publ. 118 (2019), 177–179. https://doi.org/10.4064/bc118-11.

[3] J. Voight, *Quaternion Algebras*, Graduate Texts in Mathematics 288, Springer, 2021, Chapters 28 and 41. https://doi.org/10.1007/978-3-030-56694-4.

[4] O. Ramaré and G. K. Viswanadham, *The trigonometric polynomial on sums of two squares, an additive problem and generalisation*, arXiv:2509.23260v1, 2025. https://arxiv.org/abs/2509.23260v1.

[5] 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.

[6] 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.

[7] 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.

[8] M. Greenberg and J. Voight, *Lattice methods for algebraic modular forms on classical groups*, in Computations with Modular Forms, Contrib. Math. Comput. Sci. 6, Springer, 2014, 147–179. https://jvoight.github.io/articles/orthohecke-240123.pdf.

[9] D. Loughran and L. Matthiesen, *Frobenian multiplicative functions and rational points in fibrations*, J. Eur. Math. Soc. 26 (2024), 4779–4830. https://doi.org/10.4171/jems/1374.

[10] H. Iwaniec, *The half dimensional sieve*, Acta Arith. 29 (1976), 69–95. https://doi.org/10.4064/aa-29-1-69-95.

[11] G. Greaves, *On the representation of a number in the form $x^2 + y^2 + p^2 + q^2$ where p, q are odd primes*, Acta Arith. 29 (1976), 257–274. https://doi.org/10.4064/aa-29-3-257-274.