REPRESENTATIONS BY QUADRATIC FORMS

HAOYUN YAO

ABSTRACT. This is the final paper report for a topic course in 2026 spring at Duke lectured by Lilian Pierce. The topic is on representations by quadratic forms, following and elaborating [IK04, §20.4].

CONTENTS

1. INTRODUCTION

Let $(a_n)n \subseteq \mathbb{C}$ be a sequence, and let $f(z) := \sum_{n\geqslant 0} a_n e^{2\pi i n z}$, $(z \in \mathbb{H})$ be its exponential generating function. By orthogonality, one has the integral representation of each a_n:

$$a_n = \int_{\omega}^{\omega+1} f(x+iy)e^{-2\pi i n(x+iy)}, dx,$$

where $\omega \in \mathbb{H}$, and the implicit path (in $\mathbb{H}$) is arbitrary. Any potentially useful decomposition of the unit interval arising from a suitable choice of ω falls under the umbrella of the circle method.

In [HR18], Hardy and Ramanujan initiated this approach, successfully obtaining an asymptotic expansion for the partition number $p(n)$. Later, in the 1920s, Hardy and Littlewood, in a series of papers, exploited this idea to derive an asymptotic expansion for the size of the set

$$\{(x_1, \dots, x_r) \in \mathbb{Z}^r \mid x_1^k + \cdots + x_r^k = n\}$$

under the assumption that $r > 2^k$. A case of particular interest is $k = 2$, counting the number of ways to write an integer as a sum of squares; the Hardy–Littlewood assumption then becomes $r > 4$. In [Klo27], Kloosterman refined their method to obtain asymptotics when $(r, k) = (4, 2)$. In particular, this result recovers the famous theorem on sums of four squares by Lagrange (for large integers).

In the cases of Hardy-Ramanujan and Kloosterman, the generating function $f(z)$ has strong modular properties. In particular, it admits good asymptotics toward the rational boundary of the upper half plane $\mathbb{H}$. The circle methods aforementioned utilize the Farey sequence, which is a way to sort the reduced fractions of a fixed size of denominators in increasing fashion, providing a nice decomposition of the unit interval. The main term in the expansion often arises from the major arcs, namely those fractions with small denominators, and the error term comes from the minor arcs, their complement. Even in the case when $f(z)$ is not modular, as in the case of Hardy–Littlewood, sufficiently strong estimates for exponential or character sums are sufficient; see [IK04, §20.2] and [PS] for further exposition. We emphasize that the Kloosterman circle method does not distinguish the major and minor arcs. Instead, it relies on strong estimates for complete Kloosterman sums.

The introduction is not intended to be exhaustive. In particular, asymptotics of other sequences (representation numbers of cubic forms or zeros of quadrics) or other refinements are not mentioned. For a concise summary, we refer the interested reader to [HB96].

1.1. **Main.** Following [IK04, §20.4], we discuss the Kloosterman circle method for positive definite integral quadratic forms of variables $\geqslant 4$. To state the result, let $A \in M_r(\mathbb{Z})$ be a positive definite symmetric matrix whose diagonal entries are even, and set $Q(x) = \frac{1}{2}x^t Ax$. Set

$$a_n = r(n, Q) = \#\{x \in \mathbb{Z}^r \mid Q(x) = n\}$$

which is a finite set since Q is positive. The proof of the following theorem is given in §4.2:

Theorem 1.1. For $r \geqslant 4$ and $n > 0$, one has

$$r(n, Q) = \frac{(2\pi)^{\frac{r}{2}} n^{\frac{r}{2}-1}}{\Gamma(\frac{r}{2})|\det A|}\mathfrak{S}(n, Q) + O(n^{\frac{r-1}{4}+\varepsilon})$$

where the implied constant depends on Q and $\varepsilon > 0$. Here $\mathfrak{S}(n, Q)$ is the singular series

$$\mathfrak{S}(n, Q) = \sum_{q=1}^{\infty} q^{-r} \sum_{d \in (\mathbb{Z}/q)^\times} \sum_{h \in (\mathbb{Z}/q)^r} e^{2\pi i \frac{d}{q}(n - Q(h))}$$

and Γ denotes the usual Gamma function. □

Given the potential dependence of the singular series on n, the expansion in Theorem 1.1 is only useful if

(i) $\mathfrak{S}(n, Q)$ is nonvanishing, and
(ii) there exists an upper bound of $\mathfrak{S}(n, Q)$ relatively small with respect to the error term.

We discuss (i) in §5.1, and (ii) briefly in §5.2 with some references indicated.

1.2. **Potential future works.** The argument discussed in the article is purely classical. One can ask if the argument can be replaced by an adelic argument. This is more or less done in [Get18] assuming r is even, however using another (smoothed) form of the circle method introduced by Heath-Brown [HB96]. Strictly speaking, [Get18] only deals with the size of zeros of the quadratic form rather than the representation problem, but [HB96] does two of them in a rather uniform way.

The essential obstruction of an adelic treatment is to find an adelic δ-symbol expansion. When r is even, the unramified computation for the singular series is easier, as in the classical case (see the remark in §5.2). Following the δ-expansion in [Get18] and replicating the argument in loc. cit. and in [HB96], one should be able to present an adelic treatment.

We also note that instead of an asymptotic expansion, in [Get25] a full expansion (again for the size of the zeros) is obtained, still assuming r is even. The assumption is made so that one can work with SL_2 rather than its metaplectic group. One should be able run the argument in loc. cit. for the metaplectic group to obtain a similar result for odd r.

2. PRELIMINARIES

2.1. **Notations.** For a finite dimensional real vector space V, let $V^\vee := \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$ be its linear dual, and let $\mathcal{S}(V)$ denote the space of Schwartz functions. The Fourier transform $\mathcal{F}_{V,V^\vee} : \mathcal{S}(V) \to \mathcal{S}(V^\vee)$ is given by

$$\mathcal{F}_{V,V^\vee} f(v^\vee) := \int_V f(y) e^{2\pi i \langle v, v^\vee \rangle} dv$$

where dv is any Haar measure on V, and $\langle \cdot, \cdot \rangle : V \times V^\vee \to \mathbb{R}$ denotes the canonical pairing. We always choose the Haar measure on $V^\vee$ according to dv so that the Fourier inversion formula holds (upon identifying V with $V^{\vee\vee}$ by the canonical map and $V^\vee$ with the Pontryagin dual of V).

For a measure space (X, μ) and a finite measurable subset $A \subseteq X$, we write $\mathrm{vol}(A, \mu) = \mu(A)$. When the measure is clear from the context, we suppress μ from the notation and simply write $\mathrm{vol}(A)$.

We write $A \ll_? B$ when there exists a constant c depending on the set of parameters ? such that $|A| \leqslant c|B|$. A choice of the constant c will be called an implied constant. We suppress the set ? either when the dependence is clear, or the implied constant can be chosen to be absolute.

For two nonzero integers n, m, we write $\gcd(n, m)$ to denote the largest positive integer d such that $d \mid n$ and $d \mid m$. If $\gcd(n, m) = 1$, we write $n \perp m$. Recall the Bezout lemma: $\gcd(n, m) = \min\{an + bm > 0 \mid n, m \in \mathbb{Z}\}$.

We let M_r and GL_r denote the $\mathbb{Z}$-schemes of $r \times r$ matrices and the invertible ones, respectively. For any ring R, one has

$$\mathrm{GL}_r(R) = \{A \in M_r(R) \mid \det A \in R^\times\}.$$

More generally, for a k-scheme and a k-algebra R, we let $X(R)$ denote the R-points of X:

$$X(R) := \mathrm{Hom}_{\mathbf{Sch}_k}(\mathrm{Spec}\, R, X).$$

When X is cut off by some polynomials $f_1, \ldots, f_\ell \in k[x_1, \ldots, x_r]$ in the affine r-space, one has

$$X(R) = \{x \in R^r \mid f_1(x) = \cdots = f_\ell(x) = 0\}.$$

2.2. **Setting.** Let $r \in \mathbb{Z}_{\geqslant 1}$ and $A \in \mathrm{GL}_r(\mathbb{Q})$ be a positive definite symmetric matrix such that $a_{ii} \in 2\mathbb{Z}$ and $a_{ij} \in \mathbb{Z}$ for $i, j \in [r]$. Let

$$Q(x) := \frac{1}{2} x^t A x = \frac{1}{2} \sum_{i=1}^r a_{ii} x_i^2 + \sum_{i<j} a_{ij} x_i x_j.$$

For $n \in \mathbb{Z}$, let

$$r(n, Q) := \sum_{\substack{x \in \mathbb{Z}^r \\ Q(x) = n}} 1.$$

Let

$$M = M_A := \min \left\{ m \in \mathbb{Z}_{\geqslant 1} \mid mA^{-1} \in M_r(\mathbb{Z}) \right\}. \tag{1}$$

Note that $M \leqslant \det A$, as $A^{-1} = (\det A)^{-1} \mathrm{adj}(A)$. Note that $\det A \in \mathbb{Z}_{\geqslant 1}$ by positivity; nevertheless we will still write $|\det A|$ and $\det A$ interchangeably

2.3. **Theta function.** Form the exponential generating function

$$\theta_Q(\tau) := \sum_{m \in \mathbb{Z}^r} e^{\pi i Q(m)\tau} = \sum_{n=0}^{\infty} r(n,Q) e^{\pi i n \tau}. \tag{2}$$

More generally, form

$$\Theta_Q(\xi \mid \tau) := \sum_{m \in \mathbb{Z}^r} e^{\pi i Q(m)\tau} e^{2\pi i \langle m, \xi \rangle}.$$

For ξ ranging in a fixed compact set, the sum is absolutely convergent. Hence $\Theta_Q : \mathbb{C}^r \times \mathbb{H} \to \mathbb{C}$ is entire, and $\Theta_Q(0 \mid \tau) = \theta_Q(\tau)$.

Lemma 2.1 (Poisson summation)**.** Let V be a finite dimensional real vector space and Γ be a cocompact discrete subgroup of V. Let $\Gamma^\vee$ denote the dual lattice

$$\Gamma^\vee := \{\lambda \in V^\vee \mid \langle \lambda, \Gamma \rangle \subseteq \mathbb{Z}\}.$$

For $f \in \mathcal{S}(V)$, one has

$$\sum_{x \in \Gamma} f(x) = \frac{1}{\mathrm{vol}(V/\Gamma)} \sum_{x \in \Gamma^\vee} \mathcal{F}_{V,V^\vee} f(x)$$

Here $\mathrm{vol}(V/\Gamma)$ is computed the induced quotient measure on V/Γ of dy by the counting measure on Γ.

Proof. See [Ser73, p.107]. □

Lemma 2.2. Let Q^* be the quadratic form on $\mathbb{R}^r$ given by $Q^*(x) := \frac{1}{2}x^t A^{-1} x$. Then

$$\Theta_Q(\xi \mid \tau) = \left(\frac{\tau}{2i}\right)^{-\frac{r}{2}} |\det A|^{-\frac{1}{2}} e^{-4\pi i \tau^{-1} Q^*(\xi)} \Theta_{Q*}\left(\frac{-2A^{-1}\xi}{\tau} \mid \frac{-4}{\tau}\right)$$

Proof. Since A is positive definite, we can find $B \in \mathrm{GL}_r(\mathbb{R})$ such that $B^2 = A$. Then

$$\sum_{m \in \mathbb{Z}^r} e^{\pi i Q(m)\tau} e^{2\pi i m \xi} = \sum_{\gamma \in \Gamma} e^{\pi i \|\gamma\|^2 \tau/2} e^{2\pi i \langle \gamma, B^{-1}\xi \rangle} = \sum_{\gamma \in \Gamma} e^{\pi i \tau/2 (\left\|\gamma + 2B^{-1}\tau^{-1}\xi\right\|^2 - \left\|2B^{-1}\tau^{-1}\xi\right\|^2)}$$

where Γ is the $\mathbb{Z}$-span of the column vectors of B. Let $f \in \mathcal{S}(\mathbb{R}^n)$ be given by

$$f(x) = e^{\pi i \tau/2 \left\|x + 2B^{-1}\tau^{-1}\xi\right\|^2}$$

Assume $\tau = 2it$ with $t > 0$; then $f(x) = e^{-\pi \left\|t^{\frac{1}{2}} x - i t^{-\frac{1}{2}} B^{-1}\xi\right\|^2}$, so that

$$\mathcal{F}f(x) = t^{-\frac{r}{2}} e^{-2\pi i \langle x, -it^{-1}B^{-1}\xi \rangle} e^{-\pi \|x\|^2/t}.$$

By Poisson summation formula, we have

$$\sum_{m \in \mathbb{Z}^r} e^{\pi i Q(m)\tau} e^{2\pi i m \xi} = \frac{e^{-\pi t \left\|2B^{-1}\tau^{-1}\xi\right\|^2}}{\mathrm{vol}(\mathbb{R}^n/\Gamma)} \sum_{\gamma \in \Gamma^\vee} t^{-\frac{r}{2}} e^{-2\pi i \langle \gamma, -it^{-1}B^{-1}\xi \rangle} e^{-\pi \|\gamma\|^2/t}$$

where $\Gamma^\vee$ is the dual lattice

$$\Gamma^\vee := \{\gamma \in \mathbb{R}^n \mid \langle \gamma, \Gamma \rangle \subseteq \mathbb{Z}\}.$$

Note that $\gamma \in \Gamma^\vee$ if and only if $\langle \gamma, Be_i \rangle \in \mathbb{Z}$ for all $i \in [r]$. Since B is symmetric, this is equivalent to saying $\langle B\gamma, e_i \rangle \in \mathbb{Z}$ for all $i \in [r]$. Since $\mathbb{Z}^n$ is self-dual, it follows that $B\Gamma^\vee = \mathbb{Z}^r$. Hence

$$\begin{aligned}
\sum_{\gamma \in \Gamma^\vee} e^{-2\pi i \langle \gamma, -it^{-1}B^{-1}\xi \rangle} e^{-\pi \|\gamma\|^2/t} &= \sum_{m \in \mathbb{Z}^r} e^{-2\pi t^{-1} \langle B^{-1}m, B^{-1}\xi \rangle} e^{-\pi \left\|B^{-1}m\right\|^2/t} \\
&= \sum_{m \in \mathbb{Z}^r} e^{-2\pi t^{-1} \langle m, A^{-1}\xi \rangle} e^{-2\pi Q^*(m)/t} \\
&= \Theta_{Q*}\left(\frac{iA^{-1}\xi}{t} \mid \frac{2i}{t}\right) = \Theta_{Q*}\left(\frac{-2A^{-1}\xi}{\tau} \mid \frac{-4}{\tau}\right)
\end{aligned}$$

so that

$$\Theta_Q(\xi \mid \tau) = \left(\frac{\tau}{2i}\right)^{-\frac{r}{2}} e^{-4\pi i\tau^{-1}Q^*(\xi)} \frac{1}{\mathrm{vol}(\mathbb{R}^n/\Gamma)} \Theta_{Q^*}\left(\frac{-2A^{-1}\xi}{\tau} \mid \frac{-4}{\tau}\right)$$

It remains to notice that $\mathrm{vol}(\mathbb{R}^n/\Gamma) = |\det B| = |\det A|^{\frac{1}{2}}$. ☐

For a later use, we recall the following estimate:

Lemma 2.3. For $\varphi \in \mathcal{S}(\mathbb{R}^r)$ and $a < 1$, one has

$$\sum_{m \in \mathbb{Z}^r - \{0\}} \varphi(am) \ll_{\varphi,r} |a|^{-c}$$

for every $c \geqslant 1$.

Proof. By Poisson summation formula, we have

$$\sum_{m \in \mathbb{Z}^r - \{0\}} \varphi(am) = |a|^{-1} \sum_{m \in \mathbb{Z}^r - \{0\}} \varphi(m/a) + |a|^{-1}\widehat{\varphi}(0) - \varphi(0)$$

Since φ is Schwartz, one has

$$c_\varphi := \sup_{x \in \mathbb{R}^r} \|x\|^{r+1} |\varphi(x)| < \infty$$

so that

$$\sum_{m \in \mathbb{Z}^r - \{0\}} |\varphi(m/a)| \leqslant c_\varphi \sum_{m \in \mathbb{Z}^r - \{0\}} \|m/a\|^{-r-1} \leqslant c_\varphi \sum_{m \in \mathbb{Z}^r - \{0\}} \|m\|^{-r-1} \ll_{\varphi,r} 1$$

Hence

$$\sum_{m \in \mathbb{Z}^r - \{0\}} \varphi(am) \ll_{\varphi,r} |a|^{-1}.$$

Since $a < 1$, we have $|a|^{-1} \leqslant |a|^{-c}$ for all $c \geqslant 1$. ☐

2.4. **Dirichlet series.** For a sequence $(a_n)_n$ we formally form the exponential generating function

$$A(s) := \sum_{n=1}^{\infty} a_n n^{-s}.$$

This is the Dirichlet series attached to $(a_n)_n$. We will need the following fact.

Lemma 2.4. The defining series of $A(s)$ is absolutely convergent whenever

$$\mathrm{Re}(s) > \sigma_a := \limsup_{N \to \infty} \frac{\log \sum_{n \leqslant N} |a_n|}{\log N}.$$

In this case, we have

$$A(s) = s \int_1^\infty \left(\sum_{n \leqslant x} a_n\right) x^{-s-1} dx$$

and

$$\sum_{n \leqslant X} a_n n^{-s} = A(s) + O_\varepsilon(X^{-(\mathrm{Re}(s) - \sigma_a) + \varepsilon})$$

for all $0 < \varepsilon < \mathrm{Re}(s) - \sigma_a$.

Proof. An application of the partial summation; see [MV07, Theorem 1.3, Exercise 1.2.1.4(b)] ☐

Lemma 2.5. For $X \geqslant 0$, one has

$$\sum_{\substack{q \leqslant X \\ q \text{ square-full}}} q^{-\frac{1}{2}} \ll_{\varepsilon} X^{\varepsilon}$$

for every $\varepsilon > 0$.

Proof. Let $a_n = 1$ if n is square-full, and 0 otherwise. Then

$$\sum_{n \leqslant X} a_n = \#\{n \leqslant X \mid n \text{ is square-full}\} \ll X^{\frac{1}{2}}$$

By partial summation, we see

$$\begin{aligned} \sum_{\substack{q \leqslant X \\ q \text{ square-full}}} q^{-s} &= X^{-s} \sum_{n \leqslant X} a_n + s \int_1^X \left(\sum_{n \leqslant t} a_n \right) t^{-s-1} dt \\ &\ll X^{-s+\frac{1}{2}} + s \int_1^X t^{-s-\frac{1}{2}} dt. \end{aligned}$$

When $s = \frac{1}{2}$, this is

$$\sum_{\substack{q \leqslant X \\ q \text{ square-full}}} q^{-\frac{1}{2}} \ll 1 + \log X \ll X^{\varepsilon}.$$

□

3. Exponential sums

3.1. **Gauss sums.** For $a \in \mathbb{Z} - \{0\}$, $q \in \mathbb{Z}_{\geqslant 1}$, $m \in \mathbb{Z}^r$ and $\psi : \mathbb{Z}/q \to \mathbb{C}^{\times}$ a primitive character, define the Gauss sum

$$S_Q(a, m; q, \psi) := \sum_{h \in (\mathbb{Z}/q)^r} \psi(aQ(h) + \langle m, h \rangle)$$

For brevity, we set

$$S_Q(a, m; q) := S_Q(a, m; q, x \mapsto e^{2\pi i \frac{x}{q}}) = \sum_{h \in (\mathbb{Z}/q)^r} e^{2\pi i \frac{aQ(h) + \langle m, h \rangle}{q}}.$$

Lemma 3.1. For $q = q_1 q_2$ with $q_1 \perp q_2$, one has

$$S_Q(a, m; q, \psi) = S_Q(q_2 a, m; q_1, \psi_{q_2}) S_Q(q_1 a, m; q_2, \psi_{q_1})$$

Here ψ_{q_i} denotes the homomorphism $x \mapsto \psi(x q_i)$ which defines a primitive character of $\mathbb{Z}/(q/q_i)$. In particular, for $\gcd(a_1, q_1) = \gcd(a_2, q_2) = 1$, one has

$$S_Q(a_1 q_2 + a_2 q_1, m; q, \psi) = S_Q(a_1, \overline{q_2} m; q_1, \psi_{q_2}) S_Q(a_2, \overline{q_1} m; q_2 \psi_{q_1}).$$

Here $\overline{q_i} q_i \equiv 1 \pmod{q_{i+1}}$.

Proof. By Chinese remainder theorem, one has

$$\begin{aligned} S_Q(a, m; q, \psi) &= \sum_{\substack{h_i \in (\mathbb{Z}/q_i)^r \\ i=1,2}} \psi(aQ(h_1 q_2 + h_2 q_1) + \langle m, h_1 q_2 + h_2 q_1 \rangle) \\ &= \sum_{\substack{h_i \in (\mathbb{Z}/q_i)^r \\ i=1,2}} \psi(aQ(h_1 q_2) + \langle m, h_1 q_2 \rangle) \psi(aQ(h_2 q_1) + \langle m, h_2 q_1 \rangle) \psi\left(a \langle h_1 q_2, A h_2 q_1 \rangle\right) \end{aligned}$$

Since $q \mid a\langle h_1 q_2, A h_2 q_1 \rangle$, the last factor in the summand is trivial. Hence

$$S_Q(a, m; q, \psi) = S_Q(q_2 a, m; q_1, \psi_{q_2}) S_Q(q_1 a, m; q_2, \psi_{q_1})$$

For the last assertion, take $a = a_1q_2 + a_2q_1$ and notice that

$$S_Q(q_2(a_1q_2 + a_2q_1), m; q_1, \psi_{q_2}) = S_Q(a_1q_2^2, m; q_1, \psi_{q_2}) = S_Q(a_1, q_2^{-1}m; q_1, \psi_{q_2})$$

□

We start with a trivial bound:

Lemma 3.2. Let $\gcd(a, q) = 1$. Then

$$|S_Q(a, m; q, \psi)| \leqslant q^{\frac{r}{2}} \gcd(M, q)^{\frac{r}{2}}.$$

Here M is defined in (1). In particular,

$$|S_Q(a, m; q, \psi)| \ll_Q q^{\frac{r}{2}}.$$

Proof. We have

$$\begin{aligned}
|S_Q(a, m; q, \psi)|^2 &= \sum_{h,k\in(\mathbb{Z}/q)^r} \psi\left(aQ(h) + \langle m, h\rangle\right) \overline{\psi}\left(aQ(k) + \langle m, k\rangle\right) \\
(h \mapsto h + k) &= \sum_{h,k\in(\mathbb{Z}/q)^r} \psi\left(a(Q(h + k) - Q(k))\right) \psi(\langle m, h\rangle) \\
&= \sum_{h\in(\mathbb{Z}/q)^r} \psi(aQ(h) + \langle m, h\rangle) \sum_{k\in(\mathbb{Z}/q)^r} \psi(a\langle Ah, k\rangle) \\
&= q^r \sum_{\substack{h\in(\mathbb{Z}/q)^r \\ Ah\equiv_q 0}} \psi(\langle m, h\rangle) \\
&\leqslant q^r \#\{h \in (\mathbb{Z}/q)^r \mid Ah \equiv_q 0\}
\end{aligned}$$

If $Ah \equiv_q 0$, then $Mh = (MA^{-1})Ah \equiv_q 0$ since MA^{-1} is integral. Hence

$$|S_Q(a, m; q, \psi)|^2 \leqslant q^r \#\{h \in (\mathbb{Z}/q)^r \mid Mh \equiv_q 0\} = q^r \gcd(M, q)^r$$

The last assertion is clear as $\gcd(M, q)^{\frac{r}{2}} \leqslant M^{\frac{r}{2}} \ll_Q 1$. □

Lemma 3.3. Let $N \in \mathbb{Z}_{\geqslant 1}$, $1 \leqslant q \leqslant N$ and $\gcd(a, q) = 1$. Then

$$\theta_Q\left(\tau + \frac{2a}{q}\right) = \left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} |\det A|^{-\frac{1}{2}} \sum_{m\in\mathbb{Z}^r} e^{\pi i Q^*(m)\frac{-4}{q^2\tau}} S_Q(a, m; q)$$

and the sum on RHS is absolutely convergent.

Proof. The last assertion follows from Lemma 3.2. For the displayed equality, write

$$\theta_Q\left(\tau + \frac{2a}{q}\right) = \sum_{h\in(\mathbb{Z}/q)^r} \sum_{m\in\mathbb{Z}^r} e^{\pi i Q(h+qm)(\tau+\frac{2a}{q})}.$$

Since

$$Q(h + qm)(\tau + \frac{2a}{q}) \equiv \left(Q(h) + q\langle h, Am\rangle + q^2Q(m)\right)\tau + \frac{2a}{q}Q(h) \pmod{2\mathbb{Z}}$$

we see

$$\begin{aligned}
\theta_Q\left(\tau + \frac{2a}{q}\right) &= \sum_{h\in(\mathbb{Z}/q)^r} e^{\pi i(\tau+\frac{2a}{q})Q(h)} \sum_{m\in\mathbb{Z}^r} e^{\pi i q^2 Q(m)\tau} e^{\pi i q\tau\langle h, Am\rangle} \\
&= \sum_{h\in(\mathbb{Z}/q)^r} e^{\pi i(\tau+\frac{2a}{q})Q(h)} \Theta_Q\left(\frac{q\tau Ah}{2} \mid q^2\tau\right)
\end{aligned}$$

By Lemma 2.2, we have

$$\Theta_Q\left(\frac{q\tau Ah}{2} \mid q^2\tau\right) = \left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} |\det A|^{-\frac{1}{2}} e^{-\pi i\tau Q(h)}\Theta_{Q*}\left(\frac{h}{q} \mid \frac{-4}{q^2\tau}\right).$$

Hence

$$\begin{aligned}
\theta_Q\left(\tau + \frac{2a}{q}\right) &= \left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} |\det A|^{-\frac{1}{2}} \sum_{h\in(\mathbb{Z}/q)^r} e^{2\pi i\frac{a}{q}Q(h)}\Theta_{Q*}\left(\frac{h}{q} \mid \frac{-4}{q^2\tau}\right) \\
&= \left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} |\det A|^{-\frac{1}{2}} \sum_{h\in(\mathbb{Z}/q)^r} e^{2\pi i\frac{a}{q}Q(h)} \sum_{m\in\mathbb{Z}^r} e^{\pi i Q^*(m)\frac{-4}{q^2\tau}} e^{2\pi i\langle m,h/q\rangle} \\
&= \left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} |\det A|^{-\frac{1}{2}} \sum_{m\in\mathbb{Z}^r} e^{\pi i Q^*(m)\frac{-4}{q^2\tau}} \sum_{h\in(\mathbb{Z}/q)^r} e^{2\pi i\frac{a}{q}Q(h)} e^{2\pi i\langle m,h/q\rangle} \\
&= \left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} |\det A|^{-\frac{1}{2}} \sum_{m\in\mathbb{Z}^r} e^{\pi i Q^*(m)\frac{-4}{q^2\tau}} S_Q(a,m;q)
\end{aligned}$$

as we want. ☐

We will need an explicit formula for Gauss sums.

Lemma 3.4. Let $q \in \mathbb{Z}_{\geqslant 1}$ be such that $\gcd(q, 2|\det A|) = 1$. There exist $V \in \mathrm{GL}_r(\mathbb{Z}/q)$ and $D \in T_r(\mathbb{Z}/q)$ such that

$$V^t AV \equiv D \pmod{q}$$

Proof. By Chinese remainder theorem, we have

$$\mathrm{GL}_r(\mathbb{Z}/q) \cong \prod_{p^k \| q} \mathrm{GL}_r(\mathbb{Z}/p^k), \qquad T_r(\mathbb{Z}/q) \cong \prod_{p^k \| q} T_r(\mathbb{Z}/p^k)$$

so it suffices to assume $q = p^k$ is a prime power. The result follows from a Hensel's lemma argument. Although it could be computed directly by solving equations, we provide a reasoning in terms of algebraic geometry.

Consider the algebraic scheme X over $\mathbb{Z}$ whose R-points is given by

$$X(R) := \{(V, D) \in \mathrm{GL}_r(R) \times T_r(R) \mid V^t AV - D = 0\}.$$

Here $T_r \subseteq \mathrm{GL}_r$ denote the subscheme of invertible diagonal matrices. We show X is smooth over $\mathbb{Z}_p$ whenever $p \nmid 2|\det A|$. Let Sym_r be the $\mathbb{Z}$-scheme of $r \times r$ symmetric matrices

$$\mathrm{Sym}_r(R) := \{A \in M_r(R) \mid A = A^t\}.$$

Consider the map

$$f : X \to \mathrm{Sym}_r$$

which is given on R-points by the formula $f(V, D) = V^t AV - D$. Then

$$df_{(V,D)}(x, y) = x^t AV + V^t Ax - y$$

Since the map $X \mapsto X + X^t$ defines a surjection $M_r(R) \to \mathrm{Sym}_r(R)$ for any ring where 2 acts as an invertible operator, it follows that from that fact that AV is invertible that $df_{(V,D)}$ is surjective for all $(V, D) \in X(R)$. Since

$$X = f^{-1}(0)$$

by Jacobian criterion[1] X is smooth over $\mathbb{Z}_p$.

Our goal is to show $X(\mathbb{Z}/q)$ is nonempty. It is sufficient to show $X(\mathbb{Z}_p) \neq \varnothing$, as there is a canonical projection $X(\mathbb{Z}_p) \to X(\mathbb{Z}/q)$. By Hensel's lemma (c.f. [GH24, Lemma 17.7.5]), it suffices to show $X(\mathbb{Z}/p) \neq \varnothing$. But this follows from the standard linear algebra fact (c.f. [Lam05, Corollary 2.4]). ☐

---

[1] Here X being smooth over $\mathbb{Z}_p$ actually means that the structural morphism $X \to \operatorname{Spec} \mathbb{Z}_p$ is smooth. FILL IN

Lemma 3.5. For $\gcd(q, 2a) = 1$, one has

$$\sum_{x\in\mathbb{Z}/q}\psi(x^2)=\frac{1+i^q}{1+i}\left(\frac{a_\psi}{q}\right)\sqrt{q}$$

Here $\left(\frac{\cdot}{q}\right)$ is the Jacobi symbol and $a_\psi \in (\mathbb{Z}/q)^\times$ satisfies $\psi(x) = e^{2\pi i\frac{a_\psi x}{q}}$.

Proof. See [IK04, Theorem 3.4] and [Lan94, IV, §3]. □

Lemma 3.6. Let $(a, q) = 1$ and $m \in \mathbb{Z}^r$. Suppose in addition that $(q, 2|\det A|) = 1$. Then

$$S_Q(a,m;q,\psi)=\left(\frac{1+i^q}{1+i}\left(\frac{2a a_\psi}{q}\right)\sqrt{q}\right)^r\left(\frac{|\det A|}{q}\right)\psi\left(-\bar{a}Q^*(m)\right)$$

where $\bar{a}a \equiv 1 \pmod{q}$.

Proof. By Lemma 3.4 we can find $V \in \mathrm{GL}_r(\mathbb{Z}/q)$ and diagonal $D \in T(\mathbb{Z}/q)$ such that $V^tAV \equiv D \pmod{q}$. Then we can write

$$\sum_{h\in(\mathbb{Z}/q)^r}\psi(aQ(h)+\langle m,h\rangle)\overset{h\mapsto Vh}{=}\sum_{h\in(\mathbb{Z}/q)^r}\psi(a\langle h,Dh\rangle/2+\langle V^tm,h\rangle)$$

Write $V^tm = (m_1, \ldots , m_r) \bmod q$, and $D = \mathrm{diag}(d_1, \ldots , d_n)$. Then the sum above is

$$\prod_{j\in[r]}\sum_{h\in\mathbb{Z}/q}\psi(\frac{1}{2}ad_jh^2+hm_j)=\prod_{j\in[r]}\sum_{h\in\mathbb{Z}/q}\psi\left(\frac{1}{2}ad_j(h+\overline{ad_j}m_j)^2\right)\psi\left(-\frac{\overline{ad_j}m_j^2}{2}\right)$$

Firstly we note that

$$\prod_{j\in[r]}\psi\left(-\frac{\overline{ad_j}m_j^2}{2}\right)=\psi\left(\frac{-\bar{a}}{2}\sum_{j\in[r]}\overline{d_j}m_j^2\right)=\psi\left(\frac{-\bar{a}}{2}\langle V^tm,D^{-1}V^tm\rangle\right)=\psi\left(-\bar{a}Q^*(m)\right)$$

Secondly, by a change of variables and Lemma 3.5, we deduce

$$\prod_{j\in[r]}\sum_{h\in\mathbb{Z}/q}\psi\left(\frac{1}{2}ad_j(h+\overline{ad_j}m_j)^2\right)=\prod_{j\in[r]}\sum_{h\in\mathbb{Z}/q}\psi\left(\frac{1}{2}ad_jh^2\right)=\left(\frac{1+i^q}{1+i}\left(\frac{2aa_\psi}{q}\right)\sqrt{q}\right)^r\left(\frac{|\det A|}{q}\right)$$

Here throughout the proof $\frac{1}{2}$ in the additive character ψ should be computed in $(\mathbb{Z}/q)^\times$.

□

3.2. **Kloosterman-Salié sums.** For $(\chi,\psi,\varphi)\in\widehat{(\mathbb{Z}/q)^\times}\times\widehat{(\mathbb{Z}/q)}^2$, consider the complete character sum

$$S(\chi;\psi,\varphi):=\sum_{x\in(\mathbb{Z}/q)^\times}\chi(x)\psi(x)\varphi(x^{-1}).$$

We will be considering the a special case:

$$S(a,b,r;q):=S\left(\left(\frac{\cdot}{q}\right)^r,e^{\frac{2\pi ia(\cdot)}{q}},e^{\frac{2\pi ib(\cdot)}{q}}\right)=\sum_{x\in(\mathbb{Z}/q)^\times}\left(\frac{x}{q}\right)^r\exp\left(2\pi i\frac{ax+b\bar{x}}{q}\right)$$

Here $\left(\frac{\cdot}{q}\right)$ is the Jacobi symbol. When r is even, this is the Kloosterman sum. When r is odd, this is the Salié sum.

Lemma 3.7. For $a, b \in \mathbb{Z}$, $q \in \mathbb{Z}_{\geqslant 1}$ and r even, one has

$$|S(a,b,r;q)|\leqslant(a,b,q)^{\frac{1}{2}}q^{\frac{1}{2}}d_2(q)$$

where $d_2(q)$ is the divisor function.

Proof. See [IK04, Corollary 11.12].

□

Lemma 3.8. For $a, b \in \mathbb{Z}$, $q \in 1 + 2\mathbb{Z}_{\geqslant 0}$ and r odd, one has

$$|S(a, b, r; q)| \leqslant (a, b, q)^{\frac{1}{2}} q^{\frac{1}{2}} d_2(q)$$

where $d_2(q)$ is the divisor function.

Proof. See [Edna Luo Jones' thesis, Lemma 4.19]. ☐

3.3. **A complete sum.** For $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^r$ and $\psi : \mathbb{Z}/q \to \mathbb{C}^\times$ a primitive character consider the complete sum

$$K(a, b, m; q, \psi) := \sum_{d \in (\mathbb{Z}/q)^\times} \psi(ad + b\overline{d}) S_Q(-\overline{d}, m; q, \psi)$$

Lemma 3.9. If $q = q_1 q_2$ with $q_1 \perp q_2$, then

$$K(a, b, m; q, \psi) = K(a, b, m; q_1, \psi_{q_2\overline{q_2}}) K(a, b, m; q_2, \psi_{q_1\overline{q_1}})$$

Here $\overline{q_i}$ is the inverse of q_i in $(\mathbb{Z}/q_{i+1})^\times$.

Proof. By Chinese remainder theorem, we see

$$\begin{aligned} &K(a, b, m; q, \psi) \\ &\qquad = \sum_{\substack{d_i \in (\mathbb{Z}/q_i)^\times \\ i=1,2}} \psi \left(a(d_1 q_2 \overline{q_2} + d_2 q_1 \overline{q_1}) + b(\overline{d_1} q_2 \overline{q_2} + \overline{d_2} q_1 \overline{q_1}\right) S_Q(-\overline{d_1} q_2 \overline{q_2} - \overline{d_2} q_1 \overline{q_1}, m; q, \psi) \\ &\qquad = \sum_{\substack{d_i \in (\mathbb{Z}/q_i)^\times \\ i=1,2}} \psi_{q_2\overline{q_2}} \left(a d_1 + b\overline{d_1}\right) \psi_{q_1\overline{q_1}} \left(a d_2 + b\overline{d_2}\right) S_Q(-\overline{d_1} q_2 \overline{q_2} - \overline{d_2} q_1 \overline{q_1}, m; q, \psi) \end{aligned}$$

By Lemma 3.1, we have

$$S_Q(-\overline{d_1} q_2 \overline{q_2} - \overline{d_2} q_1 \overline{q_1}, m; q, \psi) = S_Q(-\overline{d_1}\,\overline{q_2}, \overline{q_2} m; q_1, \psi_{q_2}) S_Q(-\overline{d_2}\,\overline{q_1}, \overline{q_1} m; q_2, \psi_{q_1}).$$

The result now follows upon noticing

$$S_Q(-\overline{d_1}\,\overline{q_2}, \overline{q_2} m; q_1, \psi_{q_2}) = S_Q(-\overline{d_1}, m; q_1, \psi_{q_2\overline{q_2}})$$

☐

Now write $q = q_1 q_2$ with $q_1 \perp q_2 \perp 2|\det A|$. On one hand, by triangle inequality and Lemma 3.2, one has

$$|K(a, b, m; q_1, \psi_{q_2\overline{q_2}})| \leqslant \gcd(M, q_1)^{\frac{r}{2}} q_1^{1+\frac{r}{2}}$$

On the other hand, by Lemma 3.6 one has

$$\begin{aligned} K(a, b, m; q_2, \psi_{q_1\overline{q_1}}) &= \sum_{d \in (\mathbb{Z}/q_2)^\times} \psi_{q_1\overline{q_1}}(ad + b\overline{d}) \left(\frac{1+i^q}{1+i} \left(\frac{-2\overline{d} a_{\psi_{q_1\overline{q_1}}}}{q_2}\right) \sqrt{q_2}\right)^r \left(\frac{|\det A|}{q_2}\right) \psi_{q_1\overline{q_1}} \left(d Q^*(m)\right) \\ &= \sum_{d \in (\mathbb{Z}/q_2)^\times} \psi_{q_1\overline{q_1}}(ad + b\overline{d}) \left(\frac{1+i^q}{1+i} \left(\frac{-2d a_{\psi}}{q_2}\right) \sqrt{q_2}\right)^r \left(\frac{|\det A|}{q_2}\right) \psi_{q_1\overline{q_1}} \left(d Q^*(m)\right) \\ &= \left(\frac{1+i^q}{1+i} \left(\frac{-2 a_{\psi}}{q_2}\right) \sqrt{q_2}\right)^r \left(\frac{|\det A|}{q_2}\right) \sum_{d \in (\mathbb{Z}/q_2)^\times} \left(\frac{d}{q_2}\right)^r \psi_{q_1\overline{q_1}} \left((a + Q^*(m))d + b\overline{d}\right) \\ &= \left(\frac{1+i^q}{1+i} \left(\frac{-2 a_{\psi}}{q_2}\right) \sqrt{q_2}\right)^r \left(\frac{|\det A|}{q_2}\right) \sum_{d \in (\mathbb{Z}/q_2)^\times} \left(\frac{d}{q_2}\right)^r \psi_{q_1\overline{q_1}} \left((a + Q^*(m))d + b\overline{d}\right) \end{aligned}$$

By the bound in §3.2, one has

$$\begin{aligned}\left|\sum_{d\in(\mathbb{Z}/q_2)^\times}\left(\frac{d}{q_2}\right)^r\psi_{q_1\overline{q_1}}\left((a+Q^*(m))d+b\overline{d}\right)\right| &\leqslant \mathrm{gcd}(a_\psi q_1\overline{q_1}(a+Q^*(m)),a_\psi q_1\overline{q_1}b,q_2)^{\frac{1}{2}}q_2^{\frac{1}{2}}d_2(q_2)\\ &= \mathrm{gcd}(a+Q^*(m),b,q_2)^{\frac{1}{2}}q_2^{\frac{1}{2}}d_2(q_2)\\ &\leqslant \mathrm{gcd}(a+Q^*(m),b,q_2)^{\frac{1}{2}}q_2^{\frac{1}{2}}d_2(q)\end{aligned}$$

so that

$$|K(a,b,q_1m;q_2,\psi_{q_1\overline{q_1}})|\leqslant \mathrm{gcd}(a+Q^*(m),b,q_2)^{\frac{1}{2}}q_2^{\frac{r+1}{2}}d_2(q)$$

In summary,

Lemma 3.10. Write $q=q_1q_2$ with $q_1\perp q_2\perp 2|\det A|$. Then

$$|K(a,b,m;q,\psi)|\leqslant \mathrm{gcd}(M,q_1)^{\frac{r}{2}}\,\mathrm{gcd}(a+Q^*(m),b,q_2)^{\frac{1}{2}}q_1^{\frac{1}{2}}q^{\frac{r+1}{2}}d_2(q_2)$$

□

4. KLOOSTERMAN CIRCLE METHOD

4.1. **Feray sequence.** Let $N\in\mathbb{Z}_{\geqslant 1}$. The **Feray sequence of order** N is the strictly increasing

$$0=\frac{0}{1}<\cdots<\frac{a'}{q'}<\frac{a}{q}<\frac{a''}{q''}<\cdots<\frac{1}{1}=1$$

with $1\leqslant q\leqslant N$ and $\mathrm{gcd}(a,q)=1$.

Lemma 4.1. The adjacent points $\frac{a'}{q'}$ and $\frac{a''}{q''}$ to $\frac{a}{q}$ are characterized by the conditions

$$\begin{aligned} q'\leqslant N<q+q', &\qquad aq'\equiv 1 \pmod{q}\\ q''\leqslant N<q+q'', &\qquad aq''\equiv -1 \pmod{q}\end{aligned}$$

Proof. There exist $x_0,y_0\in\mathbb{Z}_{\geqslant 1}$ such that $ax_0-qy_0=1$, and the general solution to $ax-qy=1$ is given by $(x,y)=(x_0,y_0)+t(q,a)$. Choose $t\in\mathbb{Z}$ so that $(t+1)q>N-x_0\geqslant tq$; then the resulting (x,y) satisfies

$$x\leqslant N<x+q$$

Then $\frac{y}{x}$ is a reduced fraction of order C. We claim (as a pair) that

$$(x,y)=(q',a').$$

Let $d:=aq'-qa'\in\mathbb{Z}_{\geqslant 1}$. One has then $(q',a')=d(x,y)+s(q,a)$ for some $s\in\mathbb{Z}$. Since $x+q>N\geqslant q'$, it follows that $s\in\mathbb{Z}_{\leqslant 0}$ and hence

$$\frac{a'}{q'}=\frac{dy+sa}{dx+sq}\leqslant\frac{y}{x}<\frac{a}{q}.$$

By definition of $\frac{a'}{q'}$, this proves the equality $(x,y)=(q',a')$. The characterization of $\frac{a''}{q''}$ is proved in a similar way. □

For $0<\frac{a}{q}<1$, set

$$M\left(\frac{a}{q}\right):=\left(\frac{a'+a}{q'+q},\frac{a+a''}{q+q''}\right]=\frac{a}{q}+\left(\frac{-1}{q(q'+q)},\frac{1}{q(q+q'')}\right]$$

Set also

$$M(0) = \left(0, \frac{1}{N+1}\right] \cup \left(\frac{N}{N+1}, 1\right] = 0 + \left(-\frac{1}{N+1}, \frac{1}{N+1}\right] \text{ mod } 1$$

Then one has

$$(0,1] = \bigsqcup_{\substack{0\leqslant a<q\leqslant N\\ \gcd(a,q)=1}} M\left(\frac{a}{q}\right) \tag{3}$$

Lemma 4.2. Let $N \in \mathbb{R}_{\geqslant 1}$. Let $f : \mathbb{R} \to \mathbb{C}$ a periodic continuous function with period 1 such that $f(-x) = \overline{f(x)}$. Then

$$\int_0^1 f(x)dx = 2\mathrm{Re} \sum_{q\leqslant N} \int_0^{\frac{1}{qN}} \sum_{\substack{N<d\leqslant q+N\\ qdx<1\\ \gcd(q,d)=1}} f\left(x - \frac{\overline{d}}{q}\right) dx$$

Here $\overline{d}$ is any integer such that $d\overline{d} \equiv 1 \pmod q$.

Proof. Replacing N by $\lfloor N\rfloor$, we may assume $N \in \mathbb{Z}_{\geqslant 1}$. By (3) and the periodicity of f, we have

$$\int_0^1 f(x)dx = \sum_{\substack{0\leqslant a<q\leqslant N\\ \gcd(a,q)=1}} \int_{M(\frac{a}{q})} f(x)dx = \sum_{\substack{0\leqslant a<q\leqslant N\\ \gcd(a,c)=1}} \int_{-\frac{1}{q(q+q')}}^{\frac{1}{q(q+q'')}} f\left(\frac{a}{q} + x\right) dx$$

By Lemma 4.1, the numerator a is inverse to $q + q' \equiv q'$ mod q, and inverse to $-(q + q'') \equiv -q''$ mod q. Hence the last sum equals

$$\sum_{\substack{q\leqslant N<d\leqslant q+N\\ \gcd(q,d)=1}} \left(\int_{-\frac{1}{qd}}^{0} f\left(\frac{\overline{d}}{q} + x\right) dx + \int_0^{\frac{1}{qd}} f\left(-\frac{\overline{d}}{q} + x\right) dx\right)$$

Since $f(-x) = \overline{f(x)}$, the above expression is simplified to

$$\int_0^1 f(x)dx = \sum_{\substack{q\leqslant N<d\leqslant q+N\\ \gcd(q,d)=1}} 2\mathrm{Re} \int_0^{\frac{1}{qd}} f\left(x - \frac{\overline{d}}{q}\right) dx = 2\mathrm{Re} \sum_{q\leqslant N} \int_0^{\frac{1}{qN}} \sum_{\substack{N<d\leqslant q+N\\ qdx<1\\ \gcd(c,d)=1}} f\left(x - \frac{\overline{d}}{q}\right) dx$$

□

4.2. **Performing the circle method.** The proof of Theorem 1.1 will occupy this subsection. Upon applying Lemma 4.2 to the function $f(x) = \theta_Q(2x + iy)e^{-\pi i n(2x+iy)}$, from (2) we see

$$r(n,Q) = 2\mathrm{Re} \sum_{q\leqslant N} \int_0^{\frac{1}{qN}} \sum_{\substack{N<d\leqslant q+N\\ qdx<1\\ \gcd(q,d)=1}} \theta_Q(2(x - \frac{\overline{d}}{q}) + iy)e^{-\pi i n(2(x-\frac{\overline{d}}{q})+iy)}dx$$

Set

$$T_Q(n,q;x) := \sum_{\substack{N<d\leqslant q+N\\ qdx<1\\ \gcd(q,d)=1}} \theta_Q(2(x - \frac{\overline{d}}{q}) + iy)e^{2\pi i n\frac{\overline{d}}{q}}$$

so that

$$r(n,Q) = 2\mathrm{Re} \sum_{q\leqslant N} \int_0^{\frac{1}{qN}} T_Q(n,q;x)e^{-\pi i n(2x+iy)}dx$$

By Lemma 3.3 with $\tau = 2x + iy$, we have

$$\theta_Q(2(x - \frac{\overline{d}}{q}) + iy) = \left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} |\det A|^{-\frac{1}{2}} \sum_{m\in\mathbb{Z}^r} e^{\pi i Q^*(m)\frac{-4}{q^2\tau}} S_Q(-\overline{d}, m; q)$$

so that

$$T_Q(n, q; x) = \left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} |\det A|^{-\frac{1}{2}} \sum_{m\in\mathbb{Z}^r} e^{\pi i Q^*(m)\frac{-4}{q^2\tau}} \left(\sum_{\substack{N<d\leqslant q+N \\ qdx<1 \\ \gcd(q,d)=1}} e^{2\pi i n\frac{\overline{d}}{q}} S_Q(-\overline{d}, m; q) \right)$$

Set

$$T_m(n, q; x) := \sum_{\substack{N<d\leqslant q+N \\ qdx<1 \\ \gcd(q,d)=1}} e^{2\pi i n\frac{\overline{d}}{q}} S_Q(-\overline{d}, m; q)$$

so that

$$T_Q(n, q; x) = \left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} |\det A|^{-\frac{1}{2}} \sum_{m\in\mathbb{Z}^r} e^{\pi i Q^*(m)\frac{-4}{q^2\tau}} T_m(n, q; x)$$

Lemma 4.3. Write $q = q_1 q_2$ with $q_1 \perp q_2 \perp 2|\det A|$. Then

$$|T_m(n, q; x)| \leqslant 2\log(2q) \gcd(M, q_1)^{\frac{r}{2}} \gcd(n, q_2)^{\frac{1}{2}} q_1^{\frac{1}{2}} q^{\frac{r+1}{2}} d_2(q_2)$$

Proof. Note that by orthogonality one has

$$\sum_{\substack{N<d\leqslant q+N \\ qdx<1 \\ \gcd(q,d)=1}} f(d) = \sum_{\ell\in\mathbb{Z}/q} \left(\frac{1}{q} \sum_{\substack{N<b\leqslant q+N \\ qbx<1}} e^{2\pi i\frac{-b\ell}{q}} \right) \sum_{d\in(\mathbb{Z}/q)^\times} e^{2\pi i\frac{d\ell}{q}} f(d).$$

Hence

$$\begin{aligned} T_m(n, q; x) &= \sum_{\ell\in\mathbb{Z}/q} \left(\frac{1}{q} \sum_{\substack{N<b\leqslant q+N \\ qbx<1}} e^{2\pi i\frac{-b\ell}{q}} \right) \sum_{d\in(\mathbb{Z}/q)^\times} e^{2\pi i\frac{d\ell}{q}} e^{2\pi i n\frac{\overline{d}}{q}} S_Q(-\overline{d}, m; q) \\ &= \sum_{\ell\in\mathbb{Z}/q} \left(\frac{1}{q} \sum_{\substack{N<b\leqslant q+N \\ qbx<1}} e^{2\pi i\frac{-b\ell}{q}} \right) K(\ell, n, m; q) \end{aligned}$$

One has

$$\left| \frac{1}{q} \sum_{\substack{N<b\leqslant q+N \\ qbx<1}} e^{2\pi i\frac{-b\ell}{q}} \right| \leqslant \frac{1}{q} \min\left\{ q, \frac{1}{2\,\|\ell/q\|} \right\}$$

for $\|\cdot\|$ denote the distance to $\mathbb{Z}$. Let us assume the sum over ℓ varies over a complete set of residue classes mod q within the interval $[-q/2, q/2]$. For such ℓ one has $\|\ell/q\| = |\ell|/q$, so that

$$\left| \frac{1}{q} \sum_{\substack{N<b\leqslant q+N \\ qbx<1}} e^{2\pi i\frac{-b\ell}{q}} \right| \leqslant \min\{1, \frac{1}{2|\ell|}\} \leqslant \frac{1}{1+|\ell|}$$

Here note either $\ell = 0$ or $|\ell| \geqslant 1$. Insert this bound and use Lemma 3.10 to conclude that

$$\begin{aligned}
|T_m(n,q;x)| &\leqslant \sum_{|\ell|\leqslant q/2} \frac{1}{1+|\ell|} \operatorname{gcd}(M,q_1)^{\frac{r}{2}} \operatorname{gcd}(\ell+Q^*(m),n,q_2)^{\frac{1}{2}} q_1^{\frac{1}{2}} q^{\frac{r+1}{2}} d_2(q_2) \\
&\leqslant \left(\sum_{|\ell|\leqslant q/2} \frac{1}{1+|\ell|}\right) \operatorname{gcd}(M,q_1)^{\frac{r}{2}} \operatorname{gcd}(n,q_2)^{\frac{1}{2}} q_1^{\frac{1}{2}} q^{\frac{r+1}{2}} d_2(q_2) \\
&\leqslant \left(1+2\log(1+\frac{q}{2})\right) \operatorname{gcd}(M,q_1)^{\frac{r}{2}} \operatorname{gcd}(n,q_2)^{\frac{1}{2}} q_1^{\frac{1}{2}} q^{\frac{r+1}{2}} d_2(q_2) \\
&\leqslant 2\log(2q) \operatorname{gcd}(M,q_1)^{\frac{r}{2}} \operatorname{gcd}(n,q_2)^{\frac{1}{2}} q_1^{\frac{1}{2}} q^{\frac{r+1}{2}} d_2(q_2)
\end{aligned}$$

□

Let us write the decomposition

$$\begin{aligned}
r(n,Q) &= 2\mathrm{Re} \sum_{q\leqslant N} \left(\int_0^{\frac{1}{q(q+N)}} + \int_{\frac{1}{q(q+N)}}^{\frac{1}{qN}} \right) T_Q(n,q;x) e^{-\pi i n(2x+iy)} dx \\
&= 2|\det A|^{-\frac{1}{2}} \mathrm{Re} \sum_{q\leqslant N} \int_0^{\frac{1}{q(q+N)}} \left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} T_0(n,q;x) e^{-2\pi i n(2x+iy)} dx \qquad (4) \\
&\quad + 2|\det A|^{-\frac{1}{2}} e^{\pi n y} \mathrm{Re} \sum_{q\leqslant N} \int_{\frac{1}{q(q+N)}}^{\frac{1}{qN}} \left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} T_0(n,q;x) e^{-2\pi i n x} dx \qquad (5) \\
&\quad + 2|\det A|^{-\frac{1}{2}} e^{\pi n y} \mathrm{Re} \sum_{q\leqslant N} \int_0^{\frac{1}{qN}} \left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} \sum_{m\in\mathbb{Z}^r-\{0\}} e^{\pi i Q^*(m)\frac{-4}{q^2\tau}} T_m(n,q;x) e^{-2\pi i n x} dx \qquad (6)
\end{aligned}$$

For a fixed n and q, notice that the value $T_m(n,q;x)$ is constant in $0 < x < \frac{1}{q(q+N)}$ (as $qbx < q(q+N)x < 1$ holds in this range).

4.2.1. *Main term.* Note if $0 < x < \frac{1}{q(q+N)}$, then $qdx < q(q+N)x < 1$ holds automatically. Hence

$$\begin{aligned}
(4) &= 2|\det A|^{-\frac{1}{2}} \mathrm{Re} \sum_{q\leqslant N} \int_0^{\frac{1}{q(q+N)}} \left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} e^{-\pi i n(2x+iy)} \sum_{\substack{N<d\leqslant q+N \\ \gcd(q,d)=1}} e^{2\pi i n\frac{\bar{d}}{q}} \sum_{h\in(\mathbb{Z}/q)^r} e^{-2\pi i \frac{\bar{d}Q(h)}{q}} dx \\
&= 2|\det A|^{-\frac{1}{2}} \mathrm{Re} \sum_{q\leqslant N} \left(q^{-r} \mathfrak{g}_Q(n,q) \int_0^{\frac{1}{q(q+N)}} \left(\frac{\tau}{2i}\right)^{-\frac{r}{2}} e^{-\pi i n(2x+iy)} dx \right)
\end{aligned}$$

where we've put

$$\begin{aligned}
\mathfrak{g}_Q(n,q) := T_0(n,q;0) &:= \sum_{\substack{N<d\leqslant q+N \\ \gcd(q,d)=1}} e^{2\pi i n\frac{\bar{d}}{q}} \sum_{h\in(\mathbb{Z}/q)^r} e^{-2\pi i \frac{\bar{d}Q(h)}{q}} \\
&= \sum_{d\in(\mathbb{Z}/q)^\times} e^{2\pi i n\frac{d}{q}} \sum_{h\in(\mathbb{Z}/q)^r} e^{-2\pi i \frac{dQ(h)}{q}} \\
&= \sum_{d\in(\mathbb{Z}/q)^\times} \sum_{h\in(\mathbb{Z}/q)^r} e^{2\pi i \frac{d}{q}(n-Q(h))}.
\end{aligned}$$

From this expression it is clear that $\mathfrak{g}_Q(n,q) \in \mathbb{R}$. Hence

$$\begin{aligned}
(4) &= 2|\det A|^{-\frac{1}{2}} \sum_{q\leqslant N} q^{-r} \mathfrak{g}_Q(n,q) \mathrm{Re} \int_0^{\frac{1}{q(q+N)}} \left(\frac{\tau}{2i}\right)^{-\frac{r}{2}} e^{-\pi i n(2x+iy)} dx \\
&= |\det A|^{-\frac{1}{2}} \sum_{q\leqslant N} q^{-r} \mathfrak{g}_Q(n,q) \int_{-\frac{1}{q(q+N)}}^{\frac{1}{q(q+N)}} \left(\frac{\tau}{2i}\right)^{-\frac{r}{2}} e^{-\pi i n(2x+iy)} dx
\end{aligned}$$

Lemma 4.4. One has

$$\int_{-\frac{1}{q(q+N)}}^{\frac{1}{q(q+N)}} \left(\frac{\tau}{2i}\right)^{-\frac{r}{2}} e^{-\pi i n(2x+iy)} dx = \frac{(2\pi)^{\frac{r}{2}} n^{\frac{r}{2}-1}}{\Gamma\left(\frac{r}{2}\right)} + O((qN)^{\frac{r}{2}-1})$$

Proof. Write

$$\text{LHS} = \int_{\mathbb{R}} \left(\frac{2x+iy}{2i}\right)^{-\frac{r}{2}} e^{-\pi i n(2x+iy)} dx - \int_{|x|>\frac{1}{q(q+N)}} \left(\frac{2x+iy}{2i}\right)^{-\frac{r}{2}} e^{-\pi i n(2x+iy)} dx$$

We've seen in class (c.f. [PS, §2.6.9]) that

$$\int_{\mathbb{R}} (y-ix)^{-s} e^{-2\pi i n(x+iy)} dx = \frac{(2\pi)^s n^{s-1}}{\Gamma(s)}$$

for $y > 0$ and $n \geqslant 1$. Replacing y by $y/2$ and $s = \frac{r}{2}$ in the above identity shows that

$$\int_{\mathbb{R}} \left(\frac{2x+iy}{2i}\right)^{-\frac{r}{2}} e^{-\pi i n(2x+iy)} dx = \frac{(2\pi)^{\frac{r}{2}} n^{\frac{r}{2}-1}}{\Gamma\left(\frac{r}{2}\right)}.$$

It remains to bound

$$\int_{|x|>\frac{1}{q(q+N)}} \left(\frac{2x+iy}{2i}\right)^{-\frac{r}{2}} e^{-\pi i n(2x+iy)} dx \ll \int_{|x|>\frac{1}{q(q+N)}} x^{-\frac{r}{2}} dx \ll (qN)^{\frac{r}{2}-1}.$$

□

So far we've arrived at

$$(4) = \frac{(2\pi)^{\frac{r}{2}} n^{\frac{r}{2}-1}}{|\det A|\Gamma(\frac{r}{2})} \sum_{q\leqslant N} q^{-r} \mathfrak{g}_Q(n,q) + O\left(N^{\frac{r}{2}-1} \sum_{q\leqslant N} q^{-\frac{r}{2}-1} T_Q(n,q)\right).$$

By Lemma 5.2 and a partial summation to the error term, one deduces that

$$(4) = \frac{(2\pi)^{\frac{r}{2}} n^{\frac{r}{2}-1}}{|\det A|\Gamma(\frac{r}{2})} \mathfrak{S}(n,Q) + O_{Q,\varepsilon}\left(n^{\frac{r}{2}-1} N^{\frac{3-r}{2}+\varepsilon} + N^{\frac{r-1}{2}} n^{\varepsilon}\right), \tag{7}$$

where

$$\mathfrak{S}(n,Q) := \sum_{q=1}^{\infty} q^{-r} \mathfrak{g}_Q(n,q).$$

We postpone the discussion of $\mathfrak{S}(n,Q)$ to §5.

4.2.2. *Error term.* Let $\lambda > 0$ be the least eigenvalue of $\frac{1}{2}A^{-1}$; then $|Q^*(m)| \geqslant \lambda \|m\|$ for all $m \in \mathbb{Z}^r$. Then

$$\left|e^{\pi i Q^*(m)\frac{-4}{q^2\tau}}\right| \leqslant \exp\left(\frac{-4\pi\lambda y \|m\|}{q^2|\tau|^2}\right)$$

For $\tau = 2x + iy$ with $0 < x < (qN)^{-1}$, we have

$$\frac{q^2|\tau|^2}{y} = \frac{q^2(4x^2+y^2)}{y} \leqslant \frac{4N^{-2}+q^2y^2}{y}.$$

Here we need to take

$$y = N^{-2} \tag{♠}$$

so that

$$\frac{q^2|\tau|^2}{y} \leqslant 4 + q^2 y \leqslant 5$$

By Lemma 2.3 we have

$$\left|\sum_{m\in\mathbb{Z}^r-\{0\}} e^{\pi i Q^*(m)\frac{-4}{q^2\tau}}\right| \ll_Q \left(\frac{q^2|\tau|^2}{y}\right)^c$$

for every $c \geqslant 1$. By Lemma 4.3, we see that

$$\begin{aligned}\left|\left(\frac{q^2\tau}{2i}\right)^{-\frac{r}{2}} \sum_{m\in\mathbb{Z}^r-\{0\}} e^{\pi i Q^*(m)\frac{-4}{q^2\tau}} T_m(n,q;x)e^{-2\pi i n x}\right| \\ &\ll_Q |q^2\tau|^{-\frac{r}{2}} \left(\frac{q^2|\tau|^2}{y}\right)^c \left(2\log(2q)\operatorname{gcd}(M,q_1)^{\frac{r}{2}}\operatorname{gcd}(n,q_2)^{\frac{1}{2}} q_1^{\frac{1}{2}} q^{\frac{r+1}{2}} d_2(q_2)\right) \\ &\ll_{\varepsilon,Q} y^{-\frac{r}{2}+c}\operatorname{gcd}(n,q_2)^{\frac{1}{2}} q_1^{\frac{1}{2}} q^{\frac{-r+1}{2}+\varepsilon}\end{aligned}$$

and hence

$$|(6)| \ll_{Q,\varepsilon} e^{\pi n y} y^{-\frac{r}{2}+c} \sum_{q\leqslant N} q^{\frac{-r+3}{2}+\varepsilon}(qN)^{-1} \ll e^{\pi n y} y^{-\frac{r}{2}+c} N^{-\frac{3}{2}+\varepsilon} \tag{8}$$

To leverage the error terms in (7) and (8), we choose

$$N = n^{\frac{1}{2}}, \qquad c = \frac{r}{4} \geqslant 1. \tag{$\clubsuit$}$$

Then

$$n^{\frac{r}{2}-1}N^{\frac{3-r}{2}+\varepsilon} + N^{\frac{r-1}{2}}n^{\varepsilon} + e^{\pi n y}y^{-\frac{r}{2}+c}N^{-\frac{3}{2}+\varepsilon} \ll n^{\frac{r-1}{4}+\varepsilon} + n^{\frac{r-1}{4}+\varepsilon} + n^{\frac{r-3}{4}+\varepsilon} \ll n^{\frac{r-1}{4}+\varepsilon}$$

Finally, for $(q(q+N))^{-1} < x < (qN)^{-1}$, one has

$$q^2|\tau| \geqslant \frac{2q^2}{q(q+N)} = \frac{2q}{q+N} \geqslant 1$$

so by Lemma 4.3 we see

$$|(5)| \ll_{Q,\varepsilon} e^{\pi n y} \sum_{q\leqslant N}\left(\frac{1}{qN} - \frac{1}{q(q+N)}\right) q^{\frac{r+2}{2}+\varepsilon} \ll N^{-2}\sum_{q\leqslant N} q^{\frac{r}{2}+\varepsilon} \ll_{\varepsilon} N^{\frac{r-2}{2}+\varepsilon} = n^{\frac{r-2}{4}+\varepsilon} \ll n^{\frac{r-1}{4}+\varepsilon}$$

This completes the proof of Theorem 1.1.

5. SINGULAR SERIES

In this section we discuss the analytic and arithmetic properties of the **singular series**

$$\mathfrak{S}(n,Q) := \sum_{q=1}^{\infty} q^{-r}\mathfrak{g}_Q(n,q).$$

We emphasize that this is (at least formally for now) a Dirichlet series.

5.1. Absolute convergence.

Recall that

$$\mathfrak{g}_Q(n,q) = T_0(n,q;0) = \sum_{d\in(\mathbb{Z}/q)^\times} e^{2\pi i n\frac{d}{q}} S_Q(-d,0;q) = \sum_{d\in(\mathbb{Z}/q)^\times}\sum_{h\in(\mathbb{Z}/q)^r} e^{2\pi i\frac{d(n-Q(h))}{q}}.$$

Lemma 5.1. $q \mapsto \mathfrak{g}_Q(n,q)$ is multiplicative.

Proof. Say $q = q_1q_2$ with $q_1 \perp q_2$. By Chinese remainder theorem, we have

$$\mathfrak{g}_Q(n,q) = \sum_{\substack{d_i\in(\mathbb{Z}/q_i)^\times \\ i=1,2}} e^{2\pi i n\frac{d_1q_2+d_2q_1}{q_1q_2}} S_Q(-d_1q_2-d_2q_2,0;q_1q_2).$$

By Lemma 3.1, this equals

$$\sum_{\substack{d_i\in(\mathbb{Z}/q_i)^\times\\ i=1,2}} e^{2\pi i n\left(\frac{d_1}{q_1}+\frac{d_2}{q_2}\right)} S_Q(-d_1,0;q_1)S_Q(-d_2,0;q_2)=\mathfrak{g}_Q(n,q_1)\mathfrak{g}_Q(n,q_2).$$

□

Lemma 5.2. The singular series

$$\mathfrak{S}(n,Q):=\sum_{q=1}^{\infty} q^{-r}\mathfrak{g}_Q(n,q)$$

is absolutely convergent for $n>0$ and $r\geqslant 4$. One has

$$\mathfrak{S}(n,q)\ll_{Q,\varepsilon}\begin{cases}1 & \text{, if } r\geqslant 5\\ n^{\varepsilon} & \text{, if } r=4\end{cases}$$

for every $\varepsilon>0$. One has

$$\sum_{q\leqslant N} q^{-r}\mathfrak{g}_Q(n,q)=\mathfrak{S}(n,Q)+O_\varepsilon(N^{\frac{3-r}{2}+\varepsilon})$$

for $0<\varepsilon<\dfrac{r-3}{2}$.

Proof. For readers' convenience, we replicate the argument in [HB96, §11]. Write $q=q'q''$ with q' square-free, q'' square-full and $q'\perp q''$. By Lemma 5.1 and Lemma 3.2 , we see

$$\mathfrak{g}_Q(n,q)=\mathfrak{g}_Q(n,q')\mathfrak{g}_Q(n,q'')\ll_Q|\mathfrak{g}_Q(n,q')|q''^{1+\frac{r}{2}}$$

By Lemma 4.3 and the fact that $(q')_1\leqslant \text{rad}(2|\det A|):=\prod_{p|2|\det A|}p$, we see

$$\begin{aligned}|\mathfrak{g}_Q(n,q')|&\leqslant 2\log(2q')\gcd(M,(q')_1)^{\frac{r}{2}}\gcd(n,(q')_2)^{\frac12}(q')_1^{\frac12}q'^{\frac{r+1}{2}}d_2((q')_2)\\ &\ll_{\varepsilon,Q} q'^{\frac{r+1}{2}+\varepsilon}\gcd(n,q')^{\frac12}\end{aligned}$$

Hence

$$\begin{aligned}\sum_{q\leqslant N}|\mathfrak{g}_Q(n,q)|&\ll\sum_{q\leqslant N}q''^{1+\frac{r}{2}}q'^{\frac{r+1}{2}+\varepsilon}\gcd(n,q')^{\frac12}\\ &\leqslant N^{\frac{r+1}{2}+\varepsilon}\sum_{q\leqslant N}q''^{\frac12}\gcd(n,q')=N^{\frac{r+1}{2}+\varepsilon}\sum_{q''\leqslant N}q''^{\frac12}\sum_{q'\leqslant N/q''}\gcd(n,q')\end{aligned}$$

Now

$$\sum_{\substack{k\leqslant X\\ k\text{ square free}}}\gcd(n,k)=\sum_{p|n}p\sum_{\substack{k\leqslant X\\ p|k}}1\leqslant\sum_{p|n}p\frac{X}{p}\leqslant Xd_2(n)$$

so that

$$\sum_{q\leqslant N}|\mathfrak{g}_Q(n,q)|\ll N^{\frac{r+1}{2}+\varepsilon}\sum_{q''\leqslant N}q''^{\frac12}\frac{N}{q''}d_2(n)\leqslant N^{\frac{r+3}{2}+\varepsilon}d_2(n)\sum_{\substack{q''\leqslant N\\ q''\text{ square-full}}}q''^{-\frac12}\ll_{\varepsilon,Q}N^{\frac{r+3}{2}+2\varepsilon}d_2(n)$$

Here we've used Lemma 2.5. By Lemma 2.4 the series is absolutely convergent as long as

$$r>\limsup_{N\to\infty}\frac{\sum_{q\leqslant N}|\mathfrak{g}_Q(n,q)|}{\log N}=\frac{r+3}{2}+2\varepsilon$$

or $r>3+4\varepsilon$. In addition, by the identity in the lemma, we see

$$\mathfrak{S}(n,Q)\ll_Q d_2(n)\ll n^{\varepsilon}.$$

For $r \geqslant 5$, simply notice that by the trivial bound we have

$$\sum_{q=1}^{\infty} q^{-r}\mathfrak{g}_Q(n,q) \ll \sum_{q\geqslant 1} q^{-r+1+\frac{r}{2}} = \sum_{q\geqslant 1} q^{-\frac{r}{2}+1} \leqslant \sum_{q\geqslant 1} q^{-\frac{3}{2}} \ll 1.$$

The last assertion follows from the same lemma. ☐

5.2. **Local densities.** By the lemmas above there is an Eulerian product expansion:

$$\mathfrak{S}(n,Q) = \prod_{p<\infty}\sum_{k=0}^{\infty} p^{-kr}\mathfrak{g}_Q(n,p^k) = \prod_{p<\infty}\left(1+\sum_{k=1}^{\infty} p^{-kr}\mathfrak{g}_Q(n,p^k)\right)$$

Following the discussion in class (c.f. [PS, §2.6.7]), we see

$$\delta_p(n) := \sum_{k=0}^{\infty} p^{-kr}\mathfrak{g}_Q(n,p^k) = \lim_{E\to\infty}\sum_{k=0}^{E} p^{-kr}\mathfrak{g}_Q(n,p^k) = \lim_{k\to\infty}\frac{\#\{x\in(\mathbb{Z}/p^k)^r \mid Q(x)=n\}}{p^{k(r-1)}}$$

In fact, the limit stabilizes:

Lemma 5.3. For $n>0$, one has

$$\delta_p(n) = \frac{\#\{x\in(\mathbb{Z}/p^k)^r \mid Q(x)=n\}}{p^{k(r-1)}}$$

for $k > \max\{2\operatorname{ord}_p 8\det A, \operatorname{ord}_p n\}$.[2]

Proof. Let X be the zero locus of $Q-n$, viewed as a $\mathbb{Z}$-scheme. Note $0 \notin X(\mathbb{Z}/p^m)$ for all $m \geqslant \operatorname{ord}_p n + 1$, as $n \not\equiv 0 \pmod{p^m}$. For simplicity, we assume $p \perp 2\det A$ to demonstrate the technique, and leave the case $p \mid 2\det A$ for the readers.

Suppose $p \perp 2\det A$. We claim that $X(\mathbb{Z}/p^{m+1}) \to X(\mathbb{Z}/p^m)$ is surjective[3] for all $m \geqslant \operatorname{ord}_p n + 1$, and each fibre has size p^{r-1}. Let $x \in X(\mathbb{Z}/p^m)$, and let $y = x + p^m a \in (\mathbb{Z}/p^{m+1})^r$ for some $a \in (\mathbb{Z}/p)^r$. Then

$$Q(y) = Q(x) + p^{2m}Q(a) + 2p^m\langle a, Ax\rangle \equiv Q(x) + 2p^m\langle a, Ax\rangle \pmod{p^{m+1}}.$$

Write $Q(x) = p^m b$ for some $b \in \mathbb{Z}_p$; then

$$0 \equiv p^m b + 2p^m\langle a, Ax\rangle \pmod{p^{m+1}}$$

is equivalent to $b \equiv -2\langle a, Ax\rangle \pmod p$. Since $-2Ax \neq 0 \bmod p$, there are exactly p^{r-1} such a solving the congruence. Hence

$$\frac{\#X(\mathbb{Z}/p^{m+1})}{p^{(m+1)(r-1)}} = \frac{p^{r-1}\#X(\mathbb{Z}/p^m)}{p^{(m+1)(r-1)}} = \frac{\#X(\mathbb{Z}/p^m)}{p^{m(r-1)}}.$$

☐

Corollary 5.3.1. One has $\delta_p(n) \neq 0$ for $p \perp 2|\det A|$.

Proof. This follows from Lemma 5.3 and the fact that $Q(x) = n$ is always solvable in $\mathbb{Z}_p^r$ when $r \geqslant 4$ (c.f. [Ser73, p.37 Corollary]). ☐

Remark 5.4. In [IK04, p.479] it is claimed that $\delta_p(n) \neq 0$ for all $p \mid 2|\det A|$ if and only if the congruence $Q(x) \equiv n \pmod{2^7|\det A|^3}$ is solvable. I cannot work out a proof nor find a precise reference.

Remark 5.5. Corollary 5.3.1 can also be proved by an explicit computation, at least when r is even. See [IK04, p.479].

---

[2] In [Iwa97, p.184] the limit is claimed to stabilize for $k > 2\operatorname{ord}_p 8\det A$, while in [Igu78, p.78 (79)] (in a purely local setting) the stable range depends on n. The argument provided below can be viewed as a very special case of the one given in [Igu78].

[3] The surjectivity statement follows from Hensel's lemma (c.f. [Ser73, Theorem 2.2.1]). We replicate the proof to compute the size of the fibre.

REFERENCES

[Get18] Jayce R. Getz. Secondary terms in asymptotics for the number of zeros of quadratic forms over number fields. *J. Lond. Math. Soc. (2)*, 98(2):275–305, 2018.

[Get25] Jayce R. Getz. Summation formulae for quadrics. *Selecta Math. (N.S.)*, 31(2):Paper No. 41, 42, 2025.

[GH24] Jayce R. Getz and Heekyoung Hahn. *An introduction to automorphic representations—with a view toward trace formulae*, volume 300 of *Graduate Texts in Mathematics*. Springer, Cham, [2024] ©2024.

[HB96] D. R. Heath-Brown. A new form of the circle method, and its application to quadratic forms. *J. Reine Angew. Math.*, 481:149–206, 1996.

[HR18] Godfrey H Hardy and Srinivasa Ramanujan. Asymptotic formulaæ in combinatory analysis. *Proceedings of the London Mathematical Society*, 2(1):75–115, 1918.

[Igu78] Jun-ichi Igusa. *Forms of higher degree*, volume 59 of *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*. Tata Institute of Fundamental Research, Bombay; Narosa Publishing House, New Delhi, 1978.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[Iwa97] Henryk Iwaniec. *Topics in classical automorphic forms*, volume 17 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1997.

[Klo27] Hendrik Douwe Kloosterman. On the representation of numbers in the form $ax^2+by^2+cz^2+dt^2$. *Acta mathematica*, 49(3):407–464, 1927.

[Lam05] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[MV07] Hugh L. Montgomery and Robert C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[PS] Lillian Pierce and Elias M. Stein. *In preparation*.

[Ser73] J.-P. Serre. *A course in arithmetic*, volume No. 7 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French.