

# EQUIDISTRIBUTION OF BOUNDED TORSION CM POINTS

By

BOB HOUGH \*

**Abstract.** Averaging over imaginary quadratic fields, we prove, quantitatively, the equidistribution of CM points associated to 3-torsion classes in the class group. We conjecture that this equidistribution holds for points associated to ideals of any fixed odd order. We prove a partial equidistribution result in this direction and present empirical evidence.

## 1 Introduction

Let  $-D$ ,  $D > 0$  be a fundamental discriminant, and write  $H_k(-D)$  for the order  $k$  elements in the class group  $H(-D)$ . Probably the easiest-to-state consequence of the Cohen–Lenstra Heuristics [5] for imaginary quadratic fields is the prediction that when fields are ordered by increasing size of discriminant, for any odd  $k > 1$  the average of  $|H_k|$  is asymptotically 1,<sup>1</sup>

$$(1) \quad \sum_{0 < D < X}^{\flat} |H_k(-D)| \sim \sum_{0 < D < X}^{\flat} 1, \quad X \rightarrow \infty.$$

At any rate, in the special case  $k = 3$  this is the only evidence for the Heuristics which is actually known, thanks to a theorem of Davenport and Heilbronn [6]. We wish to broaden the prediction (1) to the assertion that the shapes of lattices of any given odd torsion appear with a common uniform intensity among the shapes of all two-dimensional lattices, as the discriminant grows. We will see that this broader interpretation helps to explain the discrepancy between (1) and tabulated data.

---

\*This material is based upon work supported by the National Science Foundation under agreement No. DMS-1128155. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

The author acknowledges the support of a Ric Weiland Fellowship during his graduate studies at Stanford University.

<sup>1</sup>We use  $\flat$  to restrict sums to fundamental discriminants.

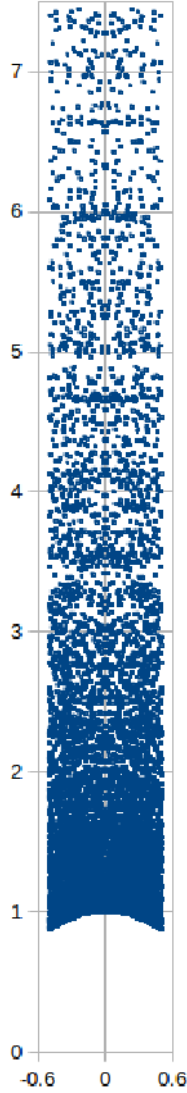


Figure 1. Heegner points associated to 101-torsion classes in imaginary quadratic fields of discriminant  $\approx -4 \cdot 10^6$ .

To elaborate, an ideal  $\mathfrak{a}$  in the imaginary quadratic field  $\mathbb{Q}(\sqrt{-D})$  is a two-dimensional lattice in  $\mathbb{C}$ . To this lattice attach a complex number  $z_{\mathfrak{a}}$ , which is the ratio of any pair of generators; this number characterizes the shape of the ideal up to homothety. After possibly exchanging the role of the generators,  $z_{\mathfrak{a}}$  is in the

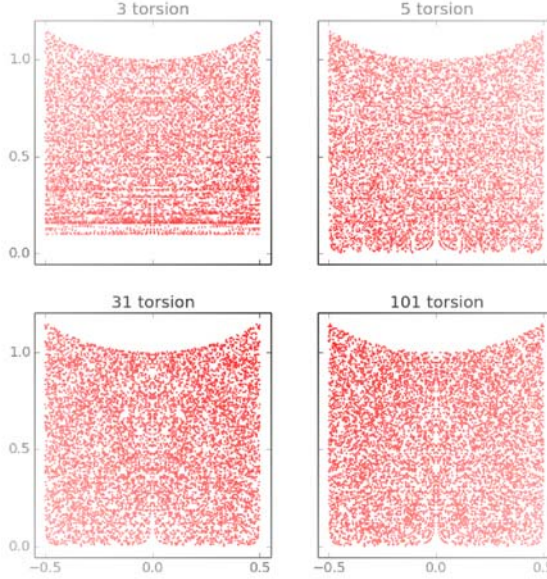


Figure 2. Heegner points associated to torsion classes of fixed order in imaginary quadratic fields of discriminant  $\approx -4 \cdot 10^6$ . The transformation  $y \mapsto \frac{1}{y}$  has been made, so that the ambient measure is Lebesgue.

upper half plane  $\mathbb{H}$ , and making a linear change of basis, it lies on the modular surface  $\mathcal{F} = \mathrm{PSL}_2(\mathbb{Z}) \backslash \mathbb{H}$ . This point is common to all ideals of the same shape (ideal class), and is the CM point of the class. Now a famous theorem of Linnik [12] and Duke [7] asserts that the CM points of classes in  $H(-D)$  equidistribute with respect to the translation-invariant hyperbolic probability measure

$$d\mu(z) = \frac{3}{\pi} \frac{dx dy}{y^2}$$

on  $\mathcal{F}$ , as  $D \rightarrow \infty$ . Motivated by the Linnik–Duke theorem, we make our conjecture.

**Conjecture 1.** *Let  $K$  be a continuous function of compact support on  $\mathcal{F}$ . For each odd  $k > 1$  we have*

$$\lim_{X \rightarrow \infty} \frac{\sum_{0 < D < X}^b \sum_{[\mathfrak{a}] \in H_k(-D)} K(z_{[\mathfrak{a}]})}{\sum_{0 < D < X}^b 1} = \int_{\mathcal{F}} K(z) d\mu(z).$$

The conjecture is well-supported by visual evidence; see Figures 1 and 2. In fact, notice that the equidistribution already suggests itself in ranges of discriminants at which the convergence in the Cohen–Lenstra Heuristics (1) is unconvincing; see Table 1.

Range	# Disc.	3	5	7	11	31
–1024	53	28	40	36	10	0
–2048	104	80	64	78	60	0
–4096	206	142	172	162	150	0
–8192	415	316	364	336	240	0
–16384	831	632	752	738	650	270
–32768	1660	1338	1544	1578	1330	690
–65536	3320	2730	3192	2850	2770	1890
–131072	6638	5532	6200	6276	5800	4860
–262144	13286	11480	12844	12348	12110	10830
–524288	26558	23254	25072	25614	25840	21210
–1048576	53114	47144	51328	51960	50540	45210
–2097152	106251	95716	102340	104724	103170	96960
–4194304	212485	193416	208288	210108	207290	195570
–8388608	424972	391050	417516	418248	415590	398550
–16777216	849944	789452	836176	838776	832600	815790
–33554432	1699872	1592438	1675940	1683882	1675150	1645380
–67108864	3399779	3208270	3363532	3383604	3361140	3324120
–134217728	6799584	6459970	6736896	6761478	6765140	6685350
–268435456	13599079	12988450	13484300	13582980	13555960	13422870
–536870912	27198220	26116790	27013804	27078228	27113010	26934720

Table 1. Discriminants of the form  $4d$ ,  $d \equiv 2 \pmod{4}$  are counted in each specified diadic range, between  $2R$  and  $R$ . The counts appearing below each prime  $p$  are the corresponding counts of order  $p$  class group elements.

Our main result is a quantitative proof of Conjecture 1 for the case  $k = 3$ . We also have a partial result toward the conjecture for larger  $k$ , which asserts that the CM points are equidistributing ‘in the cusp’. It is a confounding fact that, at least on the basis of visible evidence, the cusp appears to be the last place where the CM points equidistribute.

**Notation and conventions.** All limiting statements are taken with respect to a growing parameter  $X$ , which is a bound for the size of discriminants considered. For positive functions  $A(X), B(X)$ ,  $A \sim B$  means  $\lim \frac{A}{B} = 1$ . We use the Vinogradov notation  $A \ll B$  with the same meaning as  $A = O(B)$ .  $A \asymp B$  means  $A \ll B$  and  $B \ll A$ ;  $\epsilon$  is reserved for a fixed positive parameter which may be taken arbitrarily small.

Given integrable function  $f$  on  $\mathbb{R}^+$ , its Mellin transform is defined, where absolutely convergent, by

$$\tilde{f}(s) = \int_0^\infty f(x)x^{s-1}dx, \quad s \in \mathbb{C}$$

and possibly extended elsewhere by analytic continuation.

## 2 Precise statement of results

Recall that the ring of integers in an imaginary quadratic field takes one of three forms depending on the behavior of the discriminant  $-D$  at the prime 2. Since we perform calculations in the ring of integers, for the remainder of this article we restrict to fundamental discriminants of the form  $-D = -4d$  where  $d > 0$ ,  $d \equiv 2 \pmod{4}$  is square-free; all of our arguments carry over to the other two cases with minor modifications. In this case, the ring of integers is given by  $\mathcal{O} = \mathbb{Z}[\sqrt{-d}]$  within the field  $\mathbb{Q}(\sqrt{-d})$ .

We build on the earlier work of Soundararajan [13], and much earlier, Ankeny and Chowla [1], who studied the divisibility problem for the class group through a parameterization of **primitive ideals**; see also [4] in the real quadratic setting, and [8] for the best result on divisibility by 3. A primitive ideal  $\mathfrak{a} \subset \mathcal{O}$  is an ideal that does not admit a factorization  $\mathfrak{a} = (p\mathcal{O}) \cdot \mathfrak{b}$ , where  $p$  is a prime of  $\mathbb{Z}$  and  $\mathfrak{b}$  is another ideal of  $\mathcal{O}$ . At the level of lattices, this says that  $\mathfrak{a}$  is not an integer dilation of another ideal. A useful characterization of the primitive ideals is that they are exactly those ideals  $\mathfrak{a}$  for which  $\{0, 1, \dots, N\mathfrak{a} - 1\}$  forms a complete set of residues for  $\mathcal{O}/\mathfrak{a}$ .<sup>2</sup> In particular, this means that there is a canonical choice of generators for the lattice  $\mathfrak{a}$  given by  $\mathfrak{a} = [N\mathfrak{a}, b + \sqrt{-d}]$ , where  $b$  is uniquely determined by the conditions

$$-\frac{N\mathfrak{a}}{2} < b \leq \frac{N\mathfrak{a}}{2}, \quad b \equiv -\sqrt{-d} \pmod{\mathfrak{a}}.$$

To  $\mathfrak{a}$  is then associated the ‘Heegner point’

$$(2) \quad z_{\mathfrak{a}} = \frac{b + \sqrt{-d}}{N\mathfrak{a}}.$$

Note that this point lies in the strip  $(-\frac{1}{2}, \frac{1}{2}] \times \mathbb{R}^+ = \Gamma_{\infty} \backslash \mathbb{H}$ , where  $\Gamma_{\infty}$  is the subgroup of  $\Gamma$  stabilizing the cusp  $\infty$ . It is a pretty geometric fact that, fixing an ideal class  $[\mathfrak{a}]$  in the class group  $H(-D)$ , the collection of Heegner points of primitive ideals of class  $[\mathfrak{a}]$  are exactly the images of the CM point  $z_{[\mathfrak{a}]}$  in the various fundamental domains for  $\Gamma \backslash \mathbb{H}$  within the strip  $\Gamma_{\infty} \backslash \mathbb{H}$  (see [11], Chapter 22). Therefore, the equidistribution of CM points within the fundamental domain  $\mathcal{F}$  is equivalent to the equidistribution of the corresponding Heegner points in the strip  $\Gamma_{\infty} \backslash \mathbb{H}$ , and this is the point of view that we shall adopt. We also introduce the notation  $P_k(-D)$  to denote the primitive ideals with classes in  $H_k(-D)$ . Throughout we count discriminants using a smooth test function  $\phi : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$  of compact support, satisfying  $\phi(0) = 1$ .

Our first result establishes the equidistribution for 3-torsion Heegner points.

---

<sup>2</sup>For another characterization in terms of the prime factorization, see Section 4.

**Theorem 2.1.** *Let  $K(x, y)$  be a continuous function, compactly supported in the strip  $\Gamma_\infty \setminus \mathbb{H}$ . Let  $T = T(X)$  be a parameter satisfying  $1 \leq T \leq X^{\frac{1}{6}-\epsilon}$ . Then, as  $X \rightarrow \infty$ ,*

$$\sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \sum_{\alpha \in P_3(-4d)} K\left(\Re z_\alpha, \frac{\Im z_\alpha}{T}\right) \sim \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \int_{\Gamma_\infty \setminus \mathbb{H}} K\left(x, \frac{y}{T}\right) \frac{3}{\pi} \frac{dx dy}{y^2}.$$

Notice that this Theorem gives more than just the equidistribution in  $\mathcal{F}$ , which follows from the case  $T = 1$ , since it also holds effectively into the cusp, for  $T < X^{\frac{1}{6}-\epsilon}$ . Actually the result is stronger still, since we have given only a qualitative statement, whereas we can actually give quantitative estimates with power saving error terms; see the discussion before Theorem 3.1 in the next section. For instance, with discriminants counted with a smooth weight as above, our method may be used to yield the Davenport–Heilbronn Theorem ((1),  $k = 3$ ) with a negative secondary main term of size  $X^{\frac{5}{6}}$ , giving an alternative proof of a recent result of Taniguchi–Thorne [14] and Bhargava, Shankar and Tsimerman [3]. As the proof of this result requires some further technical difficulties it has not been included here; see the author’s thesis [9]. Previously, Terr [15] has considered a related equidistribution problem for orders in cubic fields, by a different method, but his work yields only the qualitative equidistribution. Since the completion of this work, Terr’s result has been further generalized by Bhargava and Harron to give an analogous result for the shapes of orders in quartic and quintic fields [2].

For  $k > 3$  we cannot prove the full equidistribution, but we can prove that Heegner points equidistribute ‘in the cusp’.

**Theorem 2.2.** *Let  $K$  be as in the previous theorem, and now assume that  $k$  is odd,  $k > 3$ . Let  $T = T(X)$  be a parameter growing with  $X$  in such a way that  $X^{\frac{1}{2}-\frac{1}{k-2}+\epsilon} < T < X^{\frac{1}{2}-\frac{1}{k}-\epsilon}$ . Then, as  $X \rightarrow \infty$ ,*

$$\begin{aligned} \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \sum_{\alpha \in P_k(-4d)} K\left(\Re z_\alpha, \frac{\Im z_\alpha}{T}\right) \\ \sim \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \int_{\mathcal{F}} K\left(x, \frac{y}{T}\right) \frac{3}{\pi} \frac{dx dy}{y^2}. \end{aligned}$$

**Corollary 2.3.** *For any odd  $k \geq 5$ , as  $X \rightarrow \infty$*

$$\sum_{D < X}^b |H_k(-D)| \gg X^{\frac{1}{2}+\frac{1}{k-2}-\epsilon}.$$

In the case  $k = 5$  this improves the bound  $\sum_{D < X}^b |H_5(-D)| \gg X^{\frac{4}{5}}$  from [13].

The reader will no doubt have noticed that in both theorems we no longer claim that the equidistribution of  $k$ -torsion Heegner points in the cusp once  $\Im(z) > X^{\frac{1}{2}-\frac{1}{k}}$ . There is a good reason for this—see Figure 2. If  $\mathfrak{a} \neq (1)$  is a primitive  $k$ -torsion ideal in  $\mathbb{Z}[\sqrt{-d}]$ , then  $\mathfrak{a}^k = (x+y\sqrt{-d})$  is principal, and  $y \neq 0$ , since  $\mathfrak{a}$  is primitive. Hence  $N\mathfrak{a}^k = x^2 + dy^2 \geq d$  so that we have the upper bound

$$\Im(z_{\mathfrak{a}}) = \frac{\sqrt{d}}{N\mathfrak{a}} \leq d^{\frac{1}{2}-\frac{1}{k}}.$$

Since the set  $\{z \in \Gamma_{\infty} \backslash \mathbb{H} : \Im(z) > X^{\frac{1}{2}-\frac{1}{k}}\}$  has hyperbolic volume  $\asymp X^{-\frac{1}{2}+\frac{1}{k}}$ , the absence of Heegner points in this set suggests a negative secondary term in (1) of size  $X^{\frac{1}{2}+\frac{1}{k}}$ . After a fashion, we are able to determine this quantity of missing torsion points as the negative secondary main term in the following theorem.

**Theorem 2.4.** *Let  $k > 3$  be odd. Let  $\psi$  be a  $C^{\infty}$  function on  $\mathbb{R}^+$  supported in  $[1, \infty)$ , with  $\psi \equiv 1$  on a neighborhood of  $\infty$ . Denote  $\tilde{\phi}, \tilde{\psi}$  the Mellin transforms. There exists a  $\delta = \delta_k > 0$  such that for  $T$  in the range*

$$X^{\frac{1}{2}-\frac{1}{k}-\delta_k} \leq T \ll X^{\frac{1}{2}-\frac{1}{k}}$$

*we have the asymptotic with two main terms:*

$$\begin{aligned} \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \sum_{\mathfrak{a} \in P_k(-4d)} \psi\left(\frac{\Im z_{[\mathfrak{a}]}}{T}\right) \\ = \frac{6}{\pi^3} \tilde{\phi}(1) \tilde{\psi}(-1) \frac{X}{T} + c_k \tilde{\phi}\left(\frac{1}{2} + \frac{1}{k}\right) X^{\frac{1}{2}+\frac{1}{k}} + o(X^{\frac{1}{2}+\frac{1}{k}}); \\ c_k = \frac{\Gamma(\frac{1}{2} - \frac{1}{k}) \zeta(1 - \frac{2}{k})}{k \pi^{\frac{3}{2}} \Gamma(1 - \frac{1}{k})} \\ \times [1 - 2^{\frac{1}{k}} + 2^{1-\frac{1}{k}}] \prod_{p \text{ odd}} \left[1 + \frac{1}{p+1} \left(\frac{1}{p^{\frac{1}{k}}} - \frac{1}{p^{1-\frac{2}{k}}} - \frac{1}{p^{1-\frac{1}{k}}} - \frac{1}{p}\right)\right]. \end{aligned}$$

*The secondary term of size  $X^{\frac{1}{2}+\frac{1}{k}}$  is negative, since  $\zeta(1 - \frac{2}{k}) < 0$ .*

**Remark.** Our proof will show that we may take any  $\delta_k < \frac{2}{k^2}$ .

When  $k = 3$ , the term  $c_3 \tilde{\phi}(\frac{5}{6}) X^{\frac{5}{6}}$  is the actual negative secondary term in the Davenport–Heilbronn Theorem when discriminants are counted with smooth weight  $\phi$ . For  $k = 5, 7$ , inclusion of this secondary term in the right side of (1) brings this prediction into good agreement with tabulated data for relatively small discriminants; see Table 2. For  $k \geq 9$ , the agreement is not as good in the region in which we have numerical data.

X	$\sum_{d < X} h_5(-4d)$	Cohen-Lenstra	CL- $\Sigma$	$\text{CL} + c_5 X^{\frac{7}{10}}$	$\text{CL} + c_5 X^{\frac{7}{10}} - \Sigma$
1000000	194464	202642	8178	194510	46
2000000	392996	405285	12289	392074	-922
4000000	791328	810569	19241	789108	-2220
8000000	1588520	1621139	32619	1586275	-2245
16000000	3186224	3242278	56054	3185641	-583
32000000	6393960	6484556	90596	6392548	-1412
64000000	12818136	12969112	150976	12819645	1509
128000000	25673816	25938223	264407	25695414	21598

X	$\sum_{d < X} h_7(-4d)$	Cohen-Lenstra	CL- $\Sigma$	$\text{CL} + c_7 X^{\frac{9}{14}}$	$\text{CL} + c_7 X^{\frac{9}{14}} - \Sigma$
1000000	197094	202642	5548	196900	-194
2000000	397902	405285	7383	396318	-1584
4000000	796266	810569	14303	796568	302
8000000	1595088	1621139	26051	1599277	4189
16000000	3201048	3242278	41230	3208143	7095
32000000	6427098	6484556	57458	6431257	4159
64000000	12870768	12969112	98344	12885890	15122
128000000	25832964	25938223	105259	25808279	-24685

Table 2. Aggregate order 5 and 7 elements in the class group of quadratic fields of discriminant  $-4d$ ,  $d < X$  are tabulated. Conjectural secondary main terms of size  $X^{\frac{7}{10}}$  and  $X^{\frac{9}{14}}$  respectively improve the numerical fit of the Cohen-Lenstra heuristics.

### 3 Discussion of method

One description of the divisibility argument in [13] is that the norm equation

$$N\alpha^k = m^k = x^2 + dy^2$$

is used to parametrize and count some  $k$ -torsion primitive ideals of  $\mathbb{Z}[\sqrt{-d}]$  whose Heegner point lies within a band in the cusp of  $\mathcal{F}$ . We refine the parameterization used so as to give the exact location of the counted points. A precise statement of the parameterization along with a local version is at the beginning of the next section.

Our proofs of equidistribution are by Weyl's criterion, that is, we use that the linear span of functions of the form

$$e(fx)\psi(y), \quad f \in \mathbb{Z}, \quad \psi \in C_c^\infty(\mathbb{R}^+)$$

is dense in the space of continuous functions of compact support on the strip  $\mathbb{R}/\mathbb{Z} \times \mathbb{R}^+$ . This reduces the proofs of Theorems 2.1 and 2.2 to the estimates (here  $\psi_T(y) = \psi(\frac{y}{T})$ , and  $\tilde{\phi}$  and  $\tilde{\psi}$  denote the Mellin transforms)

$$(3) \quad \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \sum_{\alpha \in P_k(-4d)} e(f\Re z_\alpha) \psi_T(\Im z_\alpha) = \delta_{f=0} \tilde{\phi}(1) \tilde{\psi}(-1) \frac{X}{T} + o\left(\frac{X}{T}\right),$$

for any  $\phi, \psi \in C_c^\infty(\mathbb{R}^+)$ ,  $f \in \mathbb{Z}$  and for  $T$  in the stated ranges of the theorems. Strictly speaking, to obtain quantitative equidistribution one requires estimates of



the type (3) with error terms that make explicit the dependence on the frequency  $f$  and function space norms of the test function  $\psi$ . In the quantitative theorems that we state below we have tracked the frequency dependence but omit the dependence on  $\psi$ .

**Theorem 3.1.** *Let  $\psi \in C_c^\infty(\mathbb{R}^+)$ . Let  $f \in \mathbb{Z}$  and  $T = T(X)$  be a parameter that satisfies  $1 \leq T \leq X^{\frac{1}{6}-\epsilon}$ . Define  $\psi_T(y) = \psi\left(\frac{y}{T}\right)$ . We have*

$$\begin{aligned} & \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \sum_{\alpha \in P_3(-4d)} e(f\Re z_\alpha) \psi_T(\Im z_\alpha) \Big/ \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \\ &= \delta_{f=0} \cdot \left[ \frac{3}{\pi T} \int_0^\infty \psi(y) \frac{dy}{y^2} \right] + O\left((1+|f|)^{\frac{1}{2}} \frac{X^{-\frac{1}{8}+\epsilon}}{T^{\frac{5}{4}}}\right) + O(X^{-\frac{1}{6}+\epsilon}). \end{aligned}$$

To obtain Theorem 2.1, approximate the function  $K(x, y)$  as a linear combination of functions  $\psi(y)e(fx)$  and apply the above theorem term-by-term.

For  $k$ -torsion with  $k > 3$  the estimate that we prove is as follows.

**Theorem 3.2.** *Let  $k > 3$  be odd, and  $\psi \in C^\infty(\mathbb{R}^+)$  supported in  $[1, \infty)$  with  $\psi \equiv 1$  on a neighborhood of  $\infty$ . Let  $f \in \mathbb{Z}$  and let  $T = T(X)$  be a parameter, with  $\psi_T(y) = \psi\left(\frac{y}{T}\right)$  as before. If  $f = 0$ , then for  $T$  in the range  $X^{\frac{1}{2}-\frac{1}{k-2}+\epsilon} < T < X^{\frac{1}{2}-\frac{1}{k}-\epsilon}$  we have the asymptotic*

$$\begin{aligned} (4) \quad & \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \sum_{\alpha \in P_k(-4d)} \psi_T(\Im z_\alpha) \Big/ \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \\ &= \frac{3}{\pi T} \int_0^\infty \psi(y) \frac{dy}{y^2} + \frac{\pi^2}{2} c_k \frac{\tilde{\phi}(\frac{1}{2} + \frac{1}{k})}{\tilde{\phi}(1)} X^{\frac{1}{k}-\frac{1}{2}} + O\left(\frac{X^{\frac{k}{4}-1+\epsilon}}{T^{\frac{k}{2}}}\right) + O(X^{\frac{1}{2k-2}-\frac{1}{2}+\epsilon}) \end{aligned}$$

with  $c_k$  the constant of Theorem 2.4.

If  $f \neq 0$  then for  $T$  in the range  $X^{\frac{1}{2}-\frac{1}{k-2}+\epsilon} < T < X^{\frac{1}{2}-\frac{1}{k}-\epsilon}$  we have the bound

$$\begin{aligned} & \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \sum_{\alpha \in P_k(-4d)} e(f\Re z_\alpha) \psi_T(\Im z_\alpha) \Big/ \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \\ &= O\left(\frac{X^{\frac{k}{4}-1+\epsilon}}{T^{\frac{k}{2}}}\right) + O\left(\frac{|f|^{\frac{1}{2}} X^{\frac{k}{8}-\frac{1}{2}+\epsilon}}{T^{\frac{k}{4}+\frac{1}{2}}}\right) + O(X^{\frac{1}{k}-\frac{1}{2}+\epsilon}). \end{aligned}$$

In the range  $T > X^{\frac{1}{2}-\frac{1}{k}-\frac{2}{k^2}+\epsilon}$ , the expression (4) is an asymptotic formula with two main terms, and so we obtain Theorem 2.4. Notice that the terms with fixed  $f \neq 0$  are dominated by the main term with  $f = 0$  once  $T > X^{\frac{1}{2}-\frac{1}{k-2}+\epsilon}$ . Although we have stated this Theorem for  $\psi$  with  $\lim_{t \rightarrow \infty} \psi(t) = 1$ , any function  $\psi_0$  with compact support on  $\mathbb{R}^+$  is the difference of two such functions. Thus we may

obtain the stated result for any  $\psi$  having compact support, but there will be no secondary main term. In particular, Theorem 2.2 follows from this Theorem by approximating  $K(x, y)$  in the space of functions of form  $\psi(y)e(fx)$ .

The remainder of the paper is concerned with proving Theorems 3.1 and 3.2.

## 4 Parameterization

The starting point is the following parameterization of ideals in  $k$ -torsion classes of the class group of  $\mathbb{Q}(\sqrt{-d})$ .

**Proposition 4.1.** *Let  $d \equiv 2 \pmod{4}$  be square-free and  $k \geq 3$  be odd. The set*

$$\{(\ell, m, n, t) \in (\mathbb{Z}^+)^4 : \ell m^k = \ell^2 n^2 + t^2 d, (\ell mn, t) = 1\}$$

*is in bijection with primitive ideal pairs  $\{\mathfrak{a}, \bar{\mathfrak{a}}\}$  with  $\mathfrak{a} \neq (1)$  and  $\mathfrak{a}^k$  principal in  $\mathbb{Q}(\sqrt{-d})$ . Explicitly, the ideals  $\mathfrak{a}, \bar{\mathfrak{a}}$  are given as  $\mathbb{Z}$ -modules by*

$$\mathfrak{a} = [\ell m, \ell n t^{-1} + \sqrt{-d}], \quad \bar{\mathfrak{a}} = [\ell m, -\ell n t^{-1} + \sqrt{-d}],$$

*where  $N\mathfrak{a} = \ell m$  and  $t^{-1}$  is the inverse of  $t$  modulo  $m$ . In particular,*

$$z_{\mathfrak{a}} = \frac{nt^{-1}}{m} + i \frac{\sqrt{d}}{\ell m}, \quad z_{\bar{\mathfrak{a}}} = \frac{-nt^{-1}}{m} + i \frac{\sqrt{d}}{\ell m}.$$

In our statement of results we have already mentioned two characterizations of the primitive ideals of  $\mathcal{O}$ , but for the proof of Proposition 4.1 it is convenient to have a third. Recall that ideals of  $\mathcal{O}$  have unique factorization, with the behavior in  $\mathcal{O}$  of the primes  $p\mathcal{O}$  of  $\mathbb{Z}$  described by the quadratic character<sup>3</sup> of  $-d \pmod{p}$

$$p\mathcal{O} = \begin{cases} \mathfrak{p}^2 & p|d, \\ \mathfrak{p}\bar{\mathfrak{p}} & \left(\frac{-d}{p}\right) = 1, \\ p\mathcal{O} & \left(\frac{-d}{p}\right) = -1. \end{cases}$$

We say that  $p$  either ramifies, splits, or remains inert. The different is the product of primes containing  $(d)$ ,

$$\mathfrak{d} = \prod_{\mathfrak{p} | (d)} \mathfrak{p}.$$

In this description, an ideal  $\mathfrak{a}$  of  $\mathcal{O}$  is primitive if and only if it factors as  $\mathfrak{a} = \mathfrak{h}\mathfrak{b}$  with  $\mathfrak{h}|\mathfrak{d}$ ,  $(\mathfrak{b}, \mathfrak{d}) = (1)$  and  $(\mathfrak{b}, \bar{\mathfrak{b}}) = (1)$ . In particular,  $\mathfrak{b}$  contains only primes  $\mathfrak{p}$  dividing split primes, with at most one of  $\mathfrak{p}, \bar{\mathfrak{p}}$  appearing.

---

<sup>3</sup> $\left(\frac{-d}{p}\right)$  is the Legendre symbol.

**Proof of Proposition 4.1.** Take  $\mathfrak{a} \neq (1)$  primitive with  $\mathfrak{a}^k$  principal and write  $\mathfrak{a} = \mathfrak{h}\mathfrak{b}$ , where  $\mathfrak{h}|\mathfrak{d}$  and  $(\mathfrak{b}, \mathfrak{d}) = (1)$ . We have  $\mathfrak{b} \neq (1)$ , since otherwise  $\mathfrak{a} = \mathfrak{h} \Rightarrow [\mathfrak{h}]^k = [\mathfrak{h}] = [(1)]$ , which forces  $\mathfrak{h} = (1)$ . Now

$$(5) \quad \mathfrak{a}^k \mathfrak{h}^{-(k-1)} = (x + t\sqrt{-d})$$

is principal. It is also primitive since  $(x+t\sqrt{-d}) = \mathfrak{h}\mathfrak{b}^k$  and  $(\mathfrak{b}, \overline{\mathfrak{b}}) = (1)$ ,  $(\mathfrak{b}, \mathfrak{d}) = (1)$ . Let  $m = N\mathfrak{b}$ ,  $\ell = N\mathfrak{h}$  and take norms in eqn. (5) to obtain  $\ell m^k = x^2 + t^2 d$ . Here  $\ell|x$  so writing  $x = \ell n$ ,  $m^k = \ell n^2 + t^2 \ell$  where  $\ell \overline{\ell} = d$ . Now primitivity of the ideal  $(\ell n + t\sqrt{-d})$  implies  $(t, \ell n) = 1$ . Also  $(m, t) = 1$ , since if  $p|(m, t)$  then  $p^2|\ell n^2$  so  $p|(n, t)$ , which is false. Finally, primitivity of  $(\ell n + t\sqrt{-d})$  implies  $n, t \neq 0$ . We may fix  $t > 0$  by multiplying by  $\pm 1$ ; the choice of sign for  $n$  is determined by a choice between the ideals  $\mathfrak{a}$  and  $\overline{\mathfrak{a}}$ .

Now suppose we begin with a solution  $(\ell, m, n, t)$  to  $\ell m^k = \ell^2 n^2 + t^2 d$  with  $(\ell m n, t) = 1$  and  $\ell, m, n, t > 0$ . Observe that  $\ell|d$ , so  $\ell$  is square-free. We claim that also  $(m, n) = 1$ , which implies  $(m, d) = 1$ . Indeed,  $(m, n) = 1$  follows from the fact that  $d$  is square-free, since if  $p|(m, n)$  then  $p \nmid t$  so that  $p^2|d = \frac{\ell m^k - \ell^2 n^2}{t^2}$ , a contradiction.

Write  $(\ell n + t\sqrt{-d}) = \mathfrak{h}\mathfrak{c}$  where  $\mathfrak{h}|\mathfrak{d}$  and  $(\mathfrak{c}, \mathfrak{d}) = (1)$ . Then  $(\ell)(m^k) = \mathfrak{h}^2 \mathfrak{c}\overline{\mathfrak{c}}$  and  $(m, d) = 1$  implies  $\mathfrak{h}^2 = (\ell)$  and  $\mathfrak{c}\overline{\mathfrak{c}} = (m^k)$ . Moreover,  $\mathfrak{c}$  is primitive since it divides  $(\ell n + t\sqrt{-d})$ , and  $\mathfrak{c}$  is prime to  $\mathfrak{d}$  so  $(\mathfrak{c}, \overline{\mathfrak{c}}) = (1)$ , and hence there exists  $\mathfrak{b}$  with  $\mathfrak{c} = \mathfrak{b}^k$ ,  $\overline{\mathfrak{c}} = \overline{\mathfrak{b}}^k$ . Note that  $(\mathfrak{b}, \mathfrak{d}) = (1)$  and  $\mathfrak{b}$  is primitive. Then letting  $\mathfrak{a} = \mathfrak{h}\mathfrak{b}$ ,  $\overline{\mathfrak{a}} = \mathfrak{h}\overline{\mathfrak{b}}$  we get that  $\{\mathfrak{a}, \overline{\mathfrak{a}}\} \neq \{(1), (1)\}$  is a pair of primitive ideals satisfying  $\mathfrak{a}^k = (\ell)^{\frac{k-1}{2}}(\ell n + t\sqrt{-d})$  is principal. Since there were no choices in determining the pair  $(\mathfrak{a}, \overline{\mathfrak{a}})$ , this completes the bijection.

Taking  $\mathfrak{a}$  to be the ideal in the pair  $(\mathfrak{a}, \overline{\mathfrak{a}})$  that corresponds to  $n, t > 0$ , we now specify  $\mathfrak{a}$  in terms of  $\ell, m, n, t$ . Since  $\mathfrak{a}$  is primitive,  $\mathfrak{a} = [N\mathfrak{a}, b + \sqrt{-d}]$  as a  $\mathbb{Z}$ -module, where  $b$  is determined modulo  $N\mathfrak{a}$ . From the above bijection,  $N\mathfrak{a} = \ell m$ , so it remains to determine  $b \bmod \ell m$ . Writing  $\mathfrak{a} = [\ell m, b + \sqrt{-d}]$  and multiplying,

$$\mathfrak{a}^2 = (\ell)\mathfrak{b}^2 = [\ell^2 m^2, \ell m b + \ell m \sqrt{-d}, b^2 - d + 2b\sqrt{-d}].$$

For the right side to be divisible by  $\ell$ , we must have  $\ell|b^2 - d$  so  $\ell|b^2 \Rightarrow \ell|b$  so write  $b = \ell b'$ . Since  $\mathfrak{a}$  contains the element  $\ell m$ , and  $\mathfrak{b}^2$  contains both the elements  $\ell m^2$  and  $\ell m b' + m\sqrt{-d}$ , the ideal

$$\mathfrak{a}(\mathfrak{b}^2)^{\frac{k-3}{2}} \mathfrak{b}^2 = (\ell)^{-\frac{k-1}{2}} \mathfrak{a}^k = (\ell n + t\sqrt{-d})$$

contains the element  $(\ell m)(\ell m^2)^{\frac{k-3}{2}}(\ell m b' + m\sqrt{-d})$ . Hence for some integers  $x, y$ ,

$$\ell^{\frac{k+1}{2}} m^{k-1} b' + \ell^{\frac{k-1}{2}} m^{k-1} \sqrt{-d} = (\ell n + t\sqrt{-d})(x + y\sqrt{-d})$$

and, therefore,

$$\ell^{\frac{k+1}{2}} m^k b' + \ell^{\frac{k-1}{2}} m^k \sqrt{-d} = (\ell n + t\sqrt{-d})(mx + my\sqrt{-d}).$$

Now factor  $\ell m^k = (\ell n + t\sqrt{-d})(\ell n - t\sqrt{-d})$  and cancel  $(\ell n + t\sqrt{-d})$  from both sides of the above equation to find

$$\begin{aligned} & (\ell n - t\sqrt{-d})(\ell^{\frac{k-1}{2}} b' + \ell^{\frac{k-3}{2}} \sqrt{-d}) \\ &= (\ell^{\frac{k+1}{2}} n b' + \ell^{\frac{k-3}{2}} t d) + (\ell^{\frac{k-1}{2}} n - \ell^{\frac{k-1}{2}} t b') \sqrt{-d} = mx + my\sqrt{-d}. \end{aligned}$$

Hence

$$\ell^{\frac{k-1}{2}} n \equiv \ell^{\frac{k-1}{2}} t b' \pmod{m} \quad \Rightarrow \quad b' \equiv t^{-1} n \pmod{m}$$

and  $b = \ell b' \equiv \ell n t^{-1} \pmod{\ell m}$  as claimed.  $\square$

The above parameterization suggests a local relation of type

$$m^k = n^2 + t^2 d \quad \Rightarrow \quad m^k \equiv n^2 \pmod{t^2}.$$

We now give a local parameterization of solutions to this congruence.

**Proposition 4.2.** *Let  $N > 0$  be an integer and  $k \geq 1$  be odd. Define*

$$S_N = \{(m, n) \in ((\mathbb{Z}/N\mathbb{Z})^\times)^2 : m^k \equiv n^2 \pmod{N}\}$$

and

$$S'_N = \{(m, n) \in ((\mathbb{Z}/4N\mathbb{Z})^\times)^2 : m^k - n^2 \equiv 2N \pmod{4N}\}.$$

The sets  $S_N$  and  $S'_N$  have the local parameterization

$$\begin{aligned} S_N &= \{(w^2, w^k) : w \in (\mathbb{Z}/N\mathbb{Z})^\times\}, \\ S'_N &= \{(m + 2N, n) : (m, n) \in S_{4N}\}. \end{aligned}$$

Furthermore, given  $(m, n) \in \mathbb{Z}^2$ ,  $(mn, N) = 1$  solving  $m^k \equiv n^2 \pmod{N^2}$ , one has the parameterization

$$\begin{aligned} & \{(m', n') \in (\mathbb{Z}/N^2\mathbb{Z})^2 : (m', n') \equiv (m, n) \pmod{N}, m'^k \equiv n'^2 \pmod{N^2}\} \\ &= \{(m + aN, n + a'N) : a, a' \in \mathbb{Z}/N\mathbb{Z}, kam^{k-1} \equiv 2a'n \pmod{N}\}. \end{aligned}$$

**Proof.** To prove the parameterization, note that

$$w \mapsto (w^2, w^k) \quad \text{and} \quad (m, n) \mapsto m^{-\frac{k-1}{2}} n$$

are inverse maps between  $(\mathbb{Z}/N\mathbb{Z})^\times$  and  $S_N$ . The remaining claims are simple modular arithmetic.  $\square$

Ultimately we will solve for  $d$  in the parameterization of Proposition 4.1, and sieve for  $d$  that are fundamental discriminants. In bounding the error from the sieve in Section 7 we require the following estimate for the number of primitive ideals of bounded norm in a given ideal class.

**Proposition 4.3.** *Fix an ideal class  $[\mathfrak{a}] \in H(-4d)$ . Let  $Y > 0$ . We have the bound*

$$|\{\mathfrak{b} \text{ primitive} : [\mathfrak{b}] = [\mathfrak{a}], N\mathfrak{b} \leq Y\sqrt{d}\}| \ll 1 + Y.$$

**Proof.** The condition  $N\mathfrak{b} \leq Y\sqrt{d}$  is equivalent to  $\Im z_{\mathfrak{b}} \geq Y^{-1}$ . Since  $z_{\mathfrak{b}} = \gamma \cdot z_{[\mathfrak{a}]}$  for some  $\gamma \in \Gamma_{\infty} \backslash \Gamma$  the result is a consequence of the simple geometric estimate, valid for any  $z$  in the strip  $\Gamma_{\infty} \backslash \mathbb{H}$ ,

$$|\{\gamma \in \Gamma_{\infty} \backslash \Gamma : \Im \gamma z \geq Y^{-1}\}| \ll 1 + Y;$$

see [10, Lemma 2.11]. □

We close this section with a bound for certain complete exponential sums. Let

$$(6) \quad S_k(A, B; q) = \sum_{w \bmod q}^{\times} e\left(\frac{Aw^2 + Bw^k}{q}\right).$$

This sum factors as a product over prime power sums,

$$S_k(A, B; q) = \prod_{p^j \parallel q} S(A\bar{q}_p, B\bar{q}_p; p^j),$$

$$q_p = \frac{q}{p^j}, \quad \bar{q}_p q_p \equiv 1 \pmod{p^j}.$$

For the prime power sums we record the following lemma.

**Lemma 4.4.** *We have the following evaluation and bounds for  $S_k(A, B; p^n)$ .*

- (i) *If  $p^n \mid (A, B)$  then  $S_k(A, B; p^n) = (p - 1)p^{n-1}$ .*
- (ii) *If  $p^j \parallel (A, B)$  with  $j < n$  then  $S_k(A, B; p^n) = p^j S_k(\frac{A}{p^j}, \frac{B}{p^j}; p^{n-j})$*
- (iii) *If  $p \nmid (A, B)$  then  $|S_k(A, B; p^n)| \ll_k p^{\frac{n}{2}}$ .*

*In particular,*

$$|S_k(A, B; p^n)| \ll_k \text{GCD}(A, B, p^n)^{\frac{1}{2}} p^{\frac{n}{2}}.$$

**Proof.** Items (i) and (ii) are obvious. In case (iii) the bound holds for  $n = 1$  by Weil's bounds. For  $n > 1$  this is elementary. □

## 5 Function notation and properties

We adopt the following notation regarding Fourier transforms. For a smooth integrable function  $f$  in several variables denote by

$$\begin{aligned} f^1(u, y, z) &= \int_{-\infty}^{\infty} f(x, y, z)e(-ux)dx, \\ f^2(x, v, z) &= \int_{-\infty}^{\infty} f(x, y, z)e(-vy)dy, \\ f^{1,2}(u, v, z) &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y, z)e(-ux - vy)dxdy \end{aligned}$$

the function with the Fourier transform taken in the first, second, or both first and second slots.

**Lemma 5.1.** *Let  $F \in \mathcal{S}(\mathbb{R}^2)$  be a Schwarz-class function and set*

$$f(x, y) = F(A + Bx, C + Dx + Ey), \quad B, E \neq 0.$$

*Then*

$$f^{1,2}(u, v) = \frac{1}{BE} e\left(\frac{A}{B}u + \left(\frac{C}{E} - \frac{AD}{BE}\right)v\right) F^{1,2}\left(\frac{1}{B}u - \frac{D}{BE}v, \frac{1}{E}v\right).$$

Throughout,  $\phi \in C_c^\infty(\mathbb{R}^+)$  is the smooth function of the Theorems, and also fix once and for all a function  $\sigma \in C_c^\infty(\mathbb{R})$  satisfying

$$(7) \quad \sigma \geq 0, \quad \text{supp}(\sigma) \subset [-2, 2], \quad \sum_{n \in \mathbb{Z}} \sigma(n+x) = 1.$$

Letting  $\sigma^\times(x) = \sigma(\log x)$  we obtain a related non-negative function of compact support on  $\mathbb{R}^+$  satisfying

$$(8) \quad \sum_{n \in \mathbb{Z}} \sigma^\times(e^n x) = 1.$$

In addition to the fixed  $\phi$ , let  $\{\psi_j\}_{j \in \mathbb{Z}}$  be smooth functions on  $\mathbb{R}^+$  satisfying uniform support and  $C^k$  bounds

$$(9) \quad \text{supp}(\psi_j) \subset [e^{-6}, e^6], \quad \forall j \in \mathbb{Z}, \forall k \geq 0, \quad \|\psi_j\|_{C^k} = O_k(1).$$

Note in particular that  $\phi$  and  $\psi_j$  have Mellin transforms  $\tilde{\phi}, \tilde{\psi}_j$  that are entire, and satisfy uniform bounds

$$(10) \quad \forall A > 0, \forall s \in \mathbb{C}^\times, \quad |\tilde{\phi}(s)|, |\tilde{\psi}_j(s)| \ll_A |s|^{-A}.$$

For positive parameters  $X, Y$ , a frequency  $f \in \mathbb{Z}$  and a smooth bounded function  $\psi$  on  $\mathbb{R}^+$ , supported away from 0, define

$$(11) \quad \Phi_{X,Y,f}(x, y, z|\psi) = \phi\left(\frac{x^k - y^2}{Xz^2}\right) \psi\left(\frac{x^k - y^2}{Y^2 x^2 z^2}\right) e\left(-\frac{fy}{xz}\right),$$

with the interpretation that  $\phi$  and  $\psi$  vanish at negative argument. This is the typical function packaging the ‘Archimedean’ data of our analysis. Also set, for  $M > 0$  and  $F \in \mathbb{R}$ ,

$$(12) \quad \Psi_{M,F}(x, y|\psi) = \phi(x^k - y^2) \psi\left((x^k - y^2) \frac{M}{x^2}\right) e\left(-\frac{Fy}{x}\right).$$

The appropriate  $\psi$  will generally be clear from the context, in which case the last argument is dropped. Note that for fixed  $x$ , and for  $\psi_j$  satisfying support condition (9),  $\Psi_{M,F}(\psi_j)$  is supported on  $x^k - y^2 \asymp 1$  so that

$$\text{meas}(\{y : \Psi_{M,F}(x, y|\psi_j) \neq 0\}) \ll x^{-\frac{k}{2}}.$$

Also,  $\Psi_{M,F}(\psi_j)$  is supported on  $x \asymp \sqrt{M}$ . In particular,

$$(13) \quad \|\Psi_{M,F}(\psi_j)\|_1 \ll M^{-\frac{k-2}{4}}.$$

**Lemma 5.2.** *The Fourier transforms of  $\Phi$  and  $\Psi$  are related as follows:*

$$(14) \quad \begin{aligned} \Phi_{X,Y,f}^{1,2}(u, v, z) &= (z^2 X)^{\frac{1}{2} + \frac{1}{k}} \Psi_{M,F}^{1,2}(z^{\frac{2}{k}} X^{\frac{1}{k}} u, z X^{\frac{1}{2}} v), \\ M &= \frac{X^{1-\frac{2}{k}}}{Y^2 z^{\frac{4}{k}}}, \quad F = \frac{f X^{\frac{1}{2}-\frac{1}{k}}}{z^{\frac{2}{k}}}. \end{aligned}$$

**Proof.** We have

$$(15) \quad \begin{aligned} \Phi_{X,Y,f}^{1,2}(u, v, z) &= \int_{\mathbb{R}^2} \phi\left(\frac{x^k - y^2}{Xz^2}\right) \psi\left(\frac{x^k - y^2}{Y^2 x^2 z^2}\right) e\left(-\frac{fy}{xz} - ux - vy\right) dx dy \\ &= (Xz^2)^{\frac{1}{2} + \frac{1}{k}} \int_{\mathbb{R}^2} \phi(x^k - y^2) \psi\left(\frac{x^k - y^2}{x^2} \frac{X^{1-\frac{2}{k}}}{Y^2 z^{\frac{4}{k}}}\right) \\ &\quad \times e\left(-\frac{f X^{\frac{1}{2}-\frac{1}{k}} y}{x z^{\frac{2}{k}}} - (Xz^2)^{\frac{1}{k}} ux - (Xz^2)^{\frac{1}{2}} vy\right) dx dy \\ &= (Xz^2)^{\frac{1}{2} + \frac{1}{k}} \Psi_{M,F}^{1,2}(X^{\frac{1}{k}} z^{\frac{2}{k}} u, X^{\frac{1}{2}} z v). \end{aligned} \quad \square$$

**Lemma 5.3.** *The function  $\Psi_{M,F}$  satisfies, for all  $i_1, i_2 \geq 0$ ,*

$$\begin{aligned} D_1^{i_1} D_2^{i_2} \Psi_{M,F}(x, y) \\ \ll_{i_1, i_2} (M^{\frac{k-1}{2}} + |F| M^{\frac{k}{4}-1})^{i_1} \left(M^{\frac{k}{4}} + \frac{|F|}{\sqrt{M}}\right)^{i_2} \|\phi\|_{C^{i_1+i_2}} \|\psi\|_{C^{i_1+i_2}}, \end{aligned}$$

and therefore, for  $u, v \neq 0$ ,

$$(16) \quad \Psi_{M,F}^{1,2}(u, v | \psi_j) \ll_{i_1, i_2} M^{-\frac{k-2}{4}} \left( \frac{M^{\frac{k-1}{2}} + |F| M^{\frac{k}{4}-1}}{|u|} \right)^{i_1} \left( \frac{M^{\frac{k}{4}} + \frac{|F|}{\sqrt{M}}}{|v|} \right)^{i_2} \|\phi\|_{C^{i_1+i_2}} \|\psi\|_{C^{i_1+i_2}}.$$

In terms of the frequency  $F$ , for  $F \neq 0$ ,

$$(17) \quad \left| \Psi_{M,F}^{1,2}(u, 0) \right| \ll \frac{M^{\frac{k}{4}+\frac{1}{2}}}{|F|} \|\Psi_{M,0}\|_1.$$

**Proof.** The bounds on the derivatives are straightforward from the observation  $x \ll \sqrt{M}$  and  $y \ll x^{\frac{k}{2}}$ , and the bound on the Fourier transform is deduced by integration by parts.

To prove the bound (17), integrate (15) by parts with respect to  $y$  (note that  $v = 0$ ) and use the bounds  $x \ll \sqrt{M}$ ,  $y \ll M^{\frac{k}{4}}$ .  $\square$

**Lemma 5.4.** Let  $\delta > 0$  and  $\psi \in C^\infty(\mathbb{R}^+)$  supported in  $[\delta, \infty]$ , satisfying, for all  $a, j \geq 0$ ,  $D^j(\psi(x) - 1)x^a \rightarrow 0$  as  $x \rightarrow \infty$ . Set

$$H(z) = \Psi_{z^{-1}, 0}^{1,2}(0, 0 | \psi).$$

For  $s \neq 0$  and  $\frac{2}{k}s + \frac{1}{2} + \frac{1}{k} \neq -n$ ,  $n \in \mathbb{Z}_{\geq 0}$ ,

$$\tilde{H}(s) = \frac{1}{k} \frac{\Gamma(\frac{1}{2})\Gamma(\frac{1}{2} - \frac{1}{k} + \frac{2}{k}s)}{\Gamma(1 - \frac{1}{k} + \frac{2}{k}s)} \tilde{\phi}\left(\frac{1}{2} + \frac{1}{k} + \frac{k-2}{k}s\right) \tilde{\psi}(-s).$$

**Proof.** For  $\Re s > 0$ ,

$$\begin{aligned} \tilde{H}(s) &= 2 \int_0^\infty \int_0^\infty \int_0^\infty \phi(x^k - y^2) \psi\left(\frac{x^k - y^2}{x^2 z}\right) x y z^s \frac{dz}{z} \frac{dy}{y} \frac{dx}{x} \\ &= \int_0^\infty \int_0^1 \int_0^\infty \phi(x^k(1-y)) \psi(x^{k-2}(1-y)z) x^{1+\frac{k}{2}} y^{-\frac{1}{2}} z^{-s} \frac{dz}{z} dy \frac{dx}{x} \\ &= \frac{1}{k} \int_0^\infty \phi(x) x^{\frac{1}{2}+\frac{1}{k}+\frac{k-2}{k}s} \frac{dx}{x} \int_0^1 (1-y)^{\frac{2s}{k}-\frac{1}{2}-\frac{1}{k}} y^{-\frac{1}{2}} dy \int_0^\infty \psi(z) z^{-s} \frac{dz}{z} \\ &= \frac{1}{k} \frac{\Gamma(\frac{1}{2})\Gamma(\frac{1}{2} - \frac{1}{k} + \frac{2}{k}s)}{\Gamma(1 - \frac{1}{k} + \frac{2}{k}s)} \tilde{\phi}\left(\frac{1}{2} + \frac{1}{k} + \frac{k-2}{k}s\right) \tilde{\psi}(-s). \end{aligned}$$

The conditions on  $\psi$  guarantee that  $\tilde{\psi}$  extends to a meromorphic function, with a single simple pole of residue  $-1$  at  $s = 0$ . The formula thus holds for  $s$  not equal to a pole of the right-hand side, by analytic continuation.  $\square$



## 6 Proof of Theorems

The initial steps in the proofs of Theorems 3.1 and 3.2 are made together, and then the argument splits depending on  $k = 3$  or  $k > 3$ , and  $f = 0$  or  $f \neq 0$  when it is necessary to choose parameters.

The sums which appear in Theorems 3.1 and 3.2 may be written

$$(18) \quad \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \sum_{\substack{\alpha \in P_k(-4d) \\ \alpha = [a, b + \sqrt{-d}]}} e\left(\frac{fb}{a}\right) \psi\left(\frac{\sqrt{d}}{Ta}\right).$$

To introduce the parameterization, let  $H_k(-D)^*$  denote those classes in the class group whose  $k$ th power is principal, and write

$$(19) \quad \mathcal{S}_{X,Y,f} = \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \sum_{\substack{(1) \neq \alpha \text{ primitive,} \\ [\alpha]^k = [(1)] \in H(-4d) \\ \alpha = [a, b + \sqrt{-d}]}} e\left(\frac{fb}{a}\right) \psi\left(\frac{\sqrt{d}}{Ta}\right).$$

This sum counts ideals from classes that are order dividing  $k$ , but those of order less than  $k$  do not appear due to the conditions which are imposed upon  $T$  and the support of  $\psi$ .

In the case that  $\psi \equiv 1$  near  $\infty$  it is convenient to localize further, so as to consider Heegner points having imaginary part in dyadic intervals. Let  $\sigma^\times$  be the smooth multiplicative partition of the unity function of the previous section (see (7)), so that  $\sum_{j \in \mathbb{Z}} \sigma^\times(e^j x) = 1$ . Define, for  $j \in \mathbb{Z}$ , and real  $x$

$$Y_j = e^j, \quad \psi_j(x) = \begin{cases} \psi\left(\frac{Y_j x^{\frac{1}{2}}}{T}\right) \sigma^\times(x^{\frac{1}{2}}), & x > 0, \\ 0, & x \leq 0. \end{cases}$$

If  $j < \log T - 12$  the support condition gives  $\psi_j \equiv 0$ . We may now write

$$(20) \quad \begin{aligned} \mathcal{S}_{X,Y,f} &= \sum_j \sum_{\substack{d \equiv 2 \pmod{4} \\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \sum_{\substack{(1) \neq \alpha \text{ primitive,} \\ [\alpha]^k = [(1)] \in H(-4d) \\ \alpha = [a, b + \sqrt{-d}]}} e\left(\frac{fb}{a}\right) \psi_j\left(\frac{d}{Y_j^2 a^2}\right) \\ &= \sum_{\log T - 12 \leq j \ll \log X} \mathcal{S}_j. \end{aligned}$$

**6.1 Global parameterization.** We now appeal to the global parameterization in Proposition 4.1. Recall the definition from (11),

$$\Phi_{X,Y,f}(x, y, z | \psi) = \phi\left(\frac{x^k - y^2}{Xz^2}\right) \psi\left(\frac{x^k - y^2}{Y^2 x^2 z^2}\right) e\left(-\frac{fy}{xz}\right).$$

Solving  $d = \frac{\ell m^k - \ell^2 n^2}{t^2}$ , and observing the property of fractions

$$\frac{nt^{-1}}{m} \equiv \frac{-nm^{-1}}{t} + \frac{n}{mt} \pmod{1},$$

where  $tt^{-1} \equiv 1 \pmod{m}$  and  $mm^{-1} \equiv 1 \pmod{t}$ , write

$$(21) \quad \mathcal{S}_j = \sum_{\substack{\ell, m, t \in \mathbb{Z}^+, n \in \mathbb{Z} \\ \mathcal{C}_1}} e\left(\frac{f n m^{-1}}{t}\right) \Phi_{X, Y_j, f}(\ell m, \ell^{\frac{k+1}{2}} n, \ell^{\frac{k-1}{2}} t | \psi_j) \sum_{s^2 | \frac{\ell m^k - \ell^2 n^2}{t^2}} \mu(s).$$

In this expression,  $\mathcal{C}_1$  indicates the local conditions

$$\mathcal{C}_1 = \{\ell \text{ } \square\text{-free}, (\ell m n, t) = (2\ell, m) = 1, \ell m^k - \ell^2 n^2 \equiv 2t^2 \pmod{4t^2}\}.$$

Note that the condition  $(2\ell, m) = 1$  may be imposed since it is implied by  $d \equiv 2 \pmod{4}$  and  $d$  square-free.

The support of  $\psi_j$  and  $\phi$  imposes the following restrictions on the summations variables:

$$(22) \quad \ell m \ll \frac{\sqrt{X}}{Y}, \quad \ell^{\frac{k-1}{2}} t \ll X^{\frac{k-2}{4}} Y^{-\frac{k}{2}}.$$

Splitting the sum over  $s$  at parameter  $Z$  write  $\mathcal{S}_j = \mathcal{M}_j + \mathcal{E}_j$  as a main term plus an error term. Observe that  $(s, \ell) = 1$  holds, since  $\ell$  and  $m$  are required to be co-prime. In the main term, pass the summation over  $s$  to the front, keeping the restriction  $(s, \ell) = 1$ , then perform Möbius inversion with variable  $s_1$ , necessarily co-prime to  $s$ , to eliminate the co-primality condition between  $\ell$  and  $m$ . Write  $s_1 \ell := \ell$ ,  $s_1 m := m$ . Thus<sup>4</sup>

$$(23) \quad \begin{aligned} \mathcal{M}_j &= \sum_{s < Z, s_1} \mu(ss_1) \sum_{\substack{\ell, m, t \in \mathbb{Z}^+, n \in \mathbb{Z} \\ \mathcal{C}_2}} e\left(\frac{f n s_1^{-1} m^{-1}}{t}\right) \Phi(s_1^2 \ell m, (s_1 \ell)^{\frac{k+1}{2}} n, (s_1 \ell)^{\frac{k-1}{2}} t | \psi_j); \\ \mathcal{C}_2 &= \begin{cases} \ell \text{ square-free}, \\ (s_1 \ell m n, t) = (\ell, s s_1) = 1, \\ s_1^{k+1} \ell m^k - s_1^2 \ell^2 n^2 \equiv 2s^2 t^2 \pmod{4s^2 t^2} \end{cases} \end{aligned}$$

and

$$\mathcal{E}_j = \sum_{\substack{\ell, m, t \in \mathbb{Z}^+, n \in \mathbb{Z} \\ \mathcal{C}_1}} e\left(\frac{f n m^{-1}}{t}\right) \Phi(\ell m, \ell^{\frac{k+1}{2}} n, \ell^{\frac{k-1}{2}} t | \psi_j) \sum_{\substack{s^2 | \frac{\ell m^k - \ell^2 n^2}{t^2} \\ s \geq Z}} \mu(s).$$

The next section is concerned with proving the following evaluation of the main term.

---

<sup>4</sup>The subscripts  $X, Y_j, f$  are suppressed.

**Proposition 6.1.** *Let  $k \geq 3$ , be odd, and let  $c_k$  be the constant of Theorem 2.4. In the case  $f = 0$ , in the range  $Z \ll T^{\frac{k}{4}} X^{\frac{1}{2} - \frac{k}{8} - \epsilon}$ ,  $\mathcal{M} = \sum \mathcal{M}_j$  satisfies*

$$\begin{aligned} \mathcal{M} &= \frac{6}{\pi^3} \tilde{\phi}(1) \tilde{\psi}(-1) \frac{X}{T} + \psi(\infty) \tilde{\phi}\left(\frac{1}{2} + \frac{1}{k}\right) c_k X^{\frac{1}{2} + \frac{1}{k}} \\ &\quad + O(X^{\frac{1}{2} + \frac{1}{(2k-2)} + \epsilon}) + O(X^{1+\epsilon} T^{-1} Z^{-1}) + O(X^{\frac{k}{4} + \epsilon} T^{-\frac{k}{2}}). \end{aligned}$$

When  $f \neq 0$ , for  $Z \ll |f|^{-\frac{1}{2}} X^{\frac{-k}{8} + \frac{1}{2} - \epsilon} T^{\frac{k}{4} - \frac{1}{2}}$ ,

$$\mathcal{M}_f = O(X^{\frac{k}{4} + \epsilon} T^{-\frac{k}{2}}) + O(X^{\frac{1}{2} + \frac{1}{k} + \epsilon}) + \delta_{k=3} O(X^{\frac{7}{8} + \epsilon} T^{-\frac{1}{4}}).$$

In the final section, Section 7, the sieving error term is estimated.

**Proposition 6.2.** *We have*

$$\mathcal{E} = \sum_j \mathcal{E}_j \ll \frac{X^{1+\epsilon}}{TZ} + \frac{X^{\frac{k}{4} + \epsilon}}{T^{\frac{k}{2}}}.$$

One easily obtains by Mellin inversion

$$(24) \quad \sum_{\substack{d \equiv 2 \pmod{4} \\ d \square\text{-free}}} \phi\left(\frac{d}{X}\right) = \frac{2}{\pi^2} \tilde{\phi}(1) X + O(X^{\frac{1}{2}}).$$

The deductions, Theorems 3.1 and 3.2, are as follows.

**Proof of Theorem 3.1.** Recall that this treats the case  $k = 3$ .

When  $f = 0$ , choose  $Z = T^{\frac{3}{4}} X^{\frac{1}{8} - \epsilon}$  to obtain the asymptotic of the Theorem with error term bounded by

$$O\left(\frac{X^{\frac{7}{8} + \epsilon}}{T^{\frac{7}{4}}}\right) + O(X^{\frac{3}{4} + \epsilon}).$$

When  $f \neq 0$ , choose  $Z = |f|^{-\frac{1}{2}} T^{\frac{1}{4}} X^{\frac{1}{8} - \epsilon}$  to obtain the bound

$$O\left(|f|^{\frac{1}{2}} \frac{X^{\frac{7}{8}}}{T^{\frac{3}{4}}}\right) + O(X^{\frac{5}{6} + \epsilon})$$

as required. □

**Proof of Theorem 3.2.** When  $f = 0$ , choose  $Z = T^{\frac{k}{4}} X^{\frac{1}{2} - \frac{k}{8} - \epsilon}$  to obtain the asymptotic of the Theorem with error terms of size  $O\left(\frac{X^{\frac{k}{4} + \epsilon}}{T^{\frac{k}{2}}}\right) + O(X^{\frac{1}{2} + \frac{1}{2k-2} + \epsilon})$ .

When  $f \neq 0$ , choose  $Z = |f|^{-\frac{1}{2}} T^{\frac{k}{4} - \frac{1}{2}} X^{\frac{-k}{8} + \frac{1}{2} - \epsilon}$  to obtain a bound of

$$O\left(\frac{X^{\frac{k}{4} + \epsilon}}{T^{\frac{k}{2}}}\right) + O\left(\frac{|f|^{\frac{1}{2}} X^{\frac{k}{8} + \frac{1}{2} + \epsilon}}{T^{\frac{k}{4} + \frac{1}{2}}}\right) + O(X^{\frac{1}{2} + \frac{1}{k} + \epsilon}).$$

□

**6.2 Evaluation of the main term.** Control the local conditions in  $\mathcal{M}_j$  by setting  $s_2 = (s, t)$  and  $s_3 = \text{GCD}(s, m, n)$ . Then replace  $s_2 t := t$ ,  $s_3 m := m$ ,  $s_3 n := n$ . Thus<sup>5</sup>

$$\begin{aligned} \mathcal{M}_j &= \sum_{\substack{s < Z, s_1 \\ s = s_2 s_3 s_4 \\ \text{odd}}} \mu(ss_1) \\ &\times \sum_{(\ell, t) \in (\mathbb{Z}^+)^2} \sum_{\substack{(m, n) \in \mathbb{Z}^2 \\ \mathcal{C}_3}} e\left(\frac{fns_1^{-1}m^{-1}}{s_2 t}\right) \Phi(s_1^2 s_3 \ell m, (s_1 \ell)^{\frac{k+1}{2}} s_3 n, (s_1 \ell)^{\frac{k-1}{2}} s_2 t); \\ \mathcal{C}_3 &= \begin{cases} \ell \text{ square-free,} \\ (t, s_1 s_3 s_4) = (\ell, ss_1 t) = 1, \\ m \text{ odd,} \\ (mn, s_2 s_4 t) = 1 \\ \ell s_1^{k+1} s_3^k m^k - \ell^2 s_1^2 s_3^2 n^2 \equiv 2s_2^4 s_4^2 t^2 \pmod{4s_2^4 s_4^2 t^2}. \end{cases} \end{aligned}$$

Set  $\mathcal{M}_j = \mathcal{M}_{j,e} + \mathcal{M}_{j,o}$  according as  $\ell$  is even or odd. When  $\ell$  is even the condition at 2 is guaranteed so that on replacing  $\ell$  by  $\frac{\ell}{2}$ ,

$$\begin{aligned} \mathcal{M}_{j,e} &= \sum_{\substack{s < Z, s_1 \\ s = s_2 s_3 s_4 \\ \text{odd}}} \mu(ss_1) \\ &\times \sum_{(\ell, t) \in (\mathbb{Z}^+)^2} \sum_{\substack{(m, n) \in \mathbb{Z}^2 \\ \mathcal{C}_{4,e}}} e\left(\frac{fs_1^{-1}nm^{-1}}{s_2 t}\right) \Phi(2s_1^2 s_3 \ell m, (2s_1 \ell)^{\frac{k+1}{2}} s_3 n, (2s_1 \ell)^{\frac{k-1}{2}} s_2 t) \\ \mathcal{C}_{4,e} &= \begin{cases} \ell \text{ square-free,} \\ (\ell, 2s_1 st) = (t, 2s_1 s_3 s_4) = 1, \\ m \text{ odd,} \\ (mn, s_2 s_4 t) = 1, \\ (2s_1^2 s_3 \ell m)^k \equiv ((2s_1 \ell)^{\frac{k+1}{2}} s_3 n)^2 \pmod{4s_2^4 s_4^2 t^2}. \end{cases} \end{aligned}$$

Setting apart the sum over  $m$  and  $n$ , write

$$\mathcal{M}_{j,e} = \sum_{\substack{s = s_2 s_3 s_4 < Z, s_1 \\ \text{odd}}} \mu(ss_1) \sum_{\substack{(\ell, t) \in (\mathbb{Z}^+)^2 \\ \ell \square\text{-free} \\ (\ell, 2s_1 st) = (t, 2s_1 s_3 s_4) = 1}} \mathcal{M}_{j,e,s,\ell,t}.$$

---

<sup>5</sup>In this section the indices  $X, Y, f$  are suppressed.

When  $\ell$  is odd,

$$\begin{aligned} \mathcal{M}_{j,o} &= \sum_{\substack{s < Z, s_1 \\ s = s_1 s_2 s_3 s_4 \\ \text{odd}}} \mu(ss_1) \\ &\times \sum_{(\ell, t) \in (\mathbb{Z}^+)^2} \sum_{\substack{(m, n) \in \mathbb{Z}^2 \\ \mathcal{C}_{4,o}}} e\left(\frac{fs_1^{-1}nm^{-1}}{s_2 t}\right) \Phi(s_1^2 s_3 \ell m, (s_1 \ell)^{\frac{k+1}{2}} s_3 n, (s_1 \ell)^{\frac{k-1}{2}} s_2 t); \\ \mathcal{C}_{4,o} &= \begin{cases} \ell \text{ square-free,} \\ (t, s_1 s_3 s_4) = (\ell, 2s_1 s t) = 1, \\ m \text{ odd,} \\ (mn, s_2 s_4 t) = 1, \\ (s_1^2 s_3 \ell m)^k - ((s_1 \ell)^{\frac{k+1}{2}} s_3 n)^2 \equiv 2s_2^4 s_4^2 t^2 \pmod{4s_2^4 s_4^2 t^2}. \end{cases} \end{aligned}$$

As above, write

$$\mathcal{M}_{j,o} = \sum_{\substack{s = s_2 s_3 s_4 < Z, s_1 \\ \text{odd}}} \mu(ss_1) \sum_{\substack{(\ell, t) \in (\mathbb{Z}^+)^2 \\ \ell \square\text{-free, odd} \\ (\ell, s_1 s t) = (t, s_1 s_3 s_4) = 1}} \mathcal{M}_{j,o,s,\ell,t}.$$

We show the analysis in the even case. The odd case may be handled similarly.

**6.3 Local parameterization.** By Proposition 4.2 the sum over  $(m, n)$  in  $\mathcal{M}_{j,e}$  is parametrized by setting

$$\begin{aligned} 2s_1^2 s_3 \ell m &= (2s_1 s_3 \ell w)^2 + (2a + 1) \cdot 2s_1^2 s_3 \ell \cdot N, \\ (2s_1 \ell)^{\frac{k+1}{2}} s_3 n &= (2s_1 s_3 \ell w)^k + (2a + 1) \cdot \frac{k}{2} (2s_1 s_3 \ell w)^{k-2} (2s_1^2 s_3 \ell) \cdot N \\ &\quad + b \cdot (2s_1 \ell)^{\frac{k+1}{2}} s_3 \cdot N^2, \end{aligned}$$

where

$$(25) \quad a, b \in \mathbb{Z}, \quad w \in (\mathbb{Z}/N\mathbb{Z})^\times, \quad N = s_2^2 s_4 t.$$

Thus<sup>6</sup>

$$\mathcal{M}' = \frac{1}{s_2^2 s_4 t} \sum_{\substack{0 \leq w < s_2^4 s_4^2 t^2 \\ (w, s_2 s_4 t) = 1}} \sum_{a, b \in \mathbb{Z}} e\left(\frac{\tilde{f} w^{k-2}}{s_2 t}\right) \Phi(A + Ba, C + Da + Eb, z),$$

---

<sup>6</sup>In this section we abbreviate  $\mathcal{M}' = \mathcal{M}_{j,e,s,\ell,t}$ .

where

$$\begin{aligned}
A &= (2\ell s_1 s_3 w)^2 + 2\ell s_1^2 s_3 \cdot s_2^2 s_4 t, \\
B &= 4\ell s_1^2 s_3 \cdot s_2^2 s_4 t, \\
C &= (2\ell s_1 s_3 w)^k + k \cdot s_1^2 s_3 \ell (2s_1 s_3 \ell w)^{k-2} \cdot s_2^2 s_4 t, \\
D &= 2k \cdot s_1^2 s_3 \ell (2s_1 s_3 \ell w)^{k-2} \cdot s_2^2 s_4 t, \\
E &= (2s_1 \ell)^{\frac{k+1}{2}} s_3 \cdot s_2^4 s_4^2 t^2, \\
\tilde{f} &= f \cdot 2^{\frac{k-3}{2}} s_1^{\frac{k-3}{2}} s_3^{k-2} \ell^{\frac{k-3}{2}}, \\
z &= (2s_1 \ell)^{\frac{k-1}{2}} s_2 t.
\end{aligned}$$

**Lemma 6.3.** *Keep the definitions of  $A - E$ ,  $\tilde{f}$ ,  $z$  above, and set*

$$(26) \quad M = \frac{X^{1-\frac{2}{k}}}{Y_j^2 (2s_1 \ell)^{2-\frac{2}{k}} (s_2 t)^{\frac{2}{k}}}, \quad F = \frac{f X^{\frac{1}{2}-\frac{1}{k}}}{(2s_1 \ell)^{1-\frac{1}{k}} (s_2 t)^{\frac{2}{k}}}.$$

Define

$$U_0 = \frac{s X^{\frac{k-3}{2}}}{Y_j^{k-1} (s_1 \ell)^{k-3} s_2 t}, \quad \forall f \neq 0, \quad U_f = \frac{|f| s X^{\frac{k}{4}-1}}{Y_j^{\frac{k}{2}-2} (s_1 \ell)^{\frac{k}{4}-1}}.$$

Subject to the constraint on  $Z$

$$Z \leq \begin{cases} X^{\frac{1}{2}-\frac{k}{8}-\epsilon} T^{\frac{k}{4}}, & f = 0, \\ |f|^{-\frac{1}{2}} X^{\frac{1}{2}-\frac{k}{8}-\epsilon} T^{\frac{k}{4}-\frac{1}{2}}, & f \neq 0, \end{cases}$$

for any  $N > 0$ ,

$$\begin{aligned}
\mathcal{M}' &= O_N(X^{-N}) + \Delta_f + E_f, \\
\Delta_f &= \frac{(z^2 X)^{\frac{1}{2}+\frac{1}{k}}}{BE} S_{k-2}(0, \tilde{f} s_2 s_4 t; s_2^2 s_4 t) \Psi_{M,F}(0, 0), \\
E_f &= \frac{(z^2 X)^{\frac{1}{2}+\frac{1}{k}}}{BE} \sum_{0 \neq |u| \leq U_f X^\epsilon} (-1)^u S_{k-2}(\ell s_3 u, \tilde{f} s_2 s_4; s_2^2 s_4 t) \Psi_{M,F}^{1,2}\left(\frac{(z^2 X)^{\frac{1}{k}} u}{B}, 0\right).
\end{aligned}$$

**Proof.** Applying Poisson summation in the  $a$  and  $b$  variables, and evaluating the Fourier transform by applying Lemma 5.1,

$$\begin{aligned}
\mathcal{M}' &= \frac{1}{BE} \frac{1}{s_2^2 s_4 t} \sum_{\substack{0 \leq w < s_2^4 s_4^2 t^2 \\ (w, s_2 s_4 t)=1}} \sum_{u, v \in \mathbb{Z}} e\left(\frac{\tilde{f} w^{k-2}}{s_2 t} + \frac{Au}{B} + \left(\frac{BC - AD}{BE}\right)v\right) \\
&\quad \times \Phi^{1,2}\left(\frac{u}{B} - \frac{Dv}{BE}, \frac{v}{E}, z\right).
\end{aligned}$$

Applying Lemma 5.3,

$$(27) \quad \begin{aligned} \mathcal{M}' &= \frac{(z^2 X)^{\frac{1}{2} + \frac{1}{k}}}{B E s_2^2 s_4 t} \sum_{\substack{0 \leq w < s_2^4 s_4^2 t^2 \\ (w, s_2 s_4 t) = 1}} \sum_{u, v \in \mathbb{Z}} e\left(\frac{\tilde{f} w^{k-2}}{s_2 t} + \frac{A u}{B} + \left(\frac{B C - A D}{B E}\right) v\right) \\ &\times \Psi_{M, F}^{1,2}\left(\frac{(z^2 X)^{\frac{1}{k}}}{B}\left(u - \frac{D v}{E}\right), \frac{z X^{\frac{1}{2}} v}{E}\right). \end{aligned}$$

Decay of the Fourier transform is now used to truncate the ranges of summation. By rapid decay of  $\Psi_{M, F}^{1,2}$  in the first and second slots ((16) of Lemma 5.3), the sums over  $u, v$  and  $w$  above are bounded in length by polynomials in  $X$ , with negligible error.

We first argue that we may discard all terms with  $v \neq 0$  with negligible error. By decay in the second slot, those terms satisfying

$$\left[M^{\frac{k}{4}} + \frac{|F|}{\sqrt{M}}\right] \left(\frac{s_1 s_2^3 s_3 s_4^2 \ell t}{X^{\frac{1}{2}}}\right) < X^{-\epsilon}, \quad \epsilon > 0$$

are bounded, for all  $N > 0$ , by  $O_N(X^{-N})$ . Suppose first that  $f = 0$  so that  $F = 0$ . Then, using (22),

$$s_1^{\frac{k+1}{2}} s_2 \ell^{\frac{k-1}{2}} t \ll X^{\frac{k-2}{4}} Y^{-\frac{k}{2}}, \quad M = \frac{X^{1-\frac{2}{k}}}{Y_j^2 (2s_1 \ell)^{2-\frac{2}{k}} (s_2 t)^{\frac{4}{k}}},$$

we have

$$M^{\frac{k}{4}} \frac{s_1 s_2^3 s_3 s_4^2 \ell t}{X^{\frac{1}{2}}} \ll \frac{X^{\frac{k}{4}-1} s_2^2 s_3 s_4^2}{Y_j^{\frac{k}{2}}} \ll X^{\frac{k}{4}-1} T^{-\frac{k}{2}} Z^2$$

and so the condition  $Z \ll X^{\frac{1}{2}-\frac{k}{8}-\epsilon} T^{\frac{k}{4}}$  suffices.

When  $f \neq 0$ , one must consider, in addition,

$$\frac{|F|}{\sqrt{M}} \frac{s_1 s_2^3 s_3 s_4^2 \ell t}{X^{\frac{1}{2}}} = |f| s_1 s_2^3 s_3 s_4^2 \ell t X^{\frac{-1}{2}} Y_j \ll |f| s_2^2 s_3 s_4^2 X^{\frac{k}{4}-1} Y_j^{-\frac{k}{2}+1},$$

where in the last inequality we again use (22). Therefore, for  $f \neq 0$  the condition  $Z \ll |f|^{-\frac{1}{2}} X^{\frac{1}{2}-\frac{k}{8}-\epsilon} T^{\frac{k}{4}-\frac{1}{2}}$  suffices.

Thus in the given ranges for  $Z$  we may assume that  $v = 0$  and now truncate the sum over  $u$ . This is negligible beyond the range

$$|u| \ll X^\epsilon [M^{\frac{k-1}{2}} + |F| M^{\frac{k}{4}-1}] \frac{s_1^{1+\frac{1}{k}} s_2^{2-\frac{2}{k}} s_3 s_4 \ell^{\frac{1}{k}} t^{1-\frac{2}{k}}}{X^{\frac{1}{k}}}.$$

When  $f = 0$ , this gives the restriction

$$(28) \quad |u| \leq U_0 X^\epsilon.$$

When  $f \neq 0$  the second term dominates, and we have the restriction

$$(29) \quad |u| \leq U_f X^\epsilon.$$

With  $v = 0$ , the inner sum over  $w$  in (27) becomes the complete sum

$$(-1)^u s_2^2 s_4 t \cdot S_{k-2}(\ell s_3 u, \tilde{f} s_2 s_4; s_2^2 s_4 t),$$

completing the evaluation.  $\square$

**6.3.1 Evaluation of the diagonal  $\Delta_0$ .** When  $f = 0$ ,  $\Delta_0$  is a diagonal main term contribution. Write  $\Delta_{0,j,e}$  to indicate  $\Delta_0$  for the even terms attached to  $\mathcal{M}_j$ . Since  $S_{k-2}(0, 0; s_2^2 s_4 t) = \varphi(s_2^2 s_4 t)$  we have

$$\Delta_{0,j,e} = \sum_{\substack{s=s_2 s_3 s_4 < Z, s_1 \\ \text{odd}}} \mu(ss_1) \sum_{\substack{(\ell, t) \in (\mathbb{Z}^+)^2 \\ \ell \square\text{-free} \\ (\ell, 2st) = (t, 2s_1 s_3 s_4) = 1}} \frac{X^{\frac{1}{2} + \frac{1}{k}} \varphi(s_2^2 s_4 t) \Psi_{M_j, 0}^{1,2}(0, 0)}{2^{2 + \frac{1}{k}} s_1^{2 + \frac{1}{k}} s_2^{5 - \frac{2}{k}} s_3^2 s_4^3 \ell^{1 + \frac{1}{k}} t^{2 - \frac{2}{k}}}$$

where

$$M_j = \frac{X^{1 - \frac{2}{k}}}{Y_j^2 (2s_1 \ell)^{2 - \frac{2}{k}} (s_2 t)^{\frac{1}{k}}}.$$

As a first step we remove the restriction  $s < Z$ . It follows from (13) that  $\Psi_{M_j, 0}^{1,1}(0, 0) \ll X^\epsilon M_j^{-\frac{k-2}{4}}$ . Substituting this bound, the sum over  $s \geq Z$  is bounded by (use  $Y \ll X^{\frac{1}{2} - \frac{1}{k}}$  in bounding the sum over  $s_1 \ell$ )

$$\sum_{s=s_2 s_3 s_4 \geq Z} \sum_{\substack{(s_1 \ell)^{\frac{k-1}{2}} s_2 t \\ \ll X^{\frac{k-2}{4}} Y_j^{\frac{k}{2}}}} \frac{X^{\frac{3}{2} - \frac{k}{4} + \epsilon} Y_j^{\frac{k-2}{2}}}{s_1^{\frac{7}{2} - \frac{k}{2}} s_2^2 s_3^2 s_4^2 \ell^{\frac{5}{2} - \frac{k}{2}}} \ll X^{1+\epsilon} Y_j^{-1} Z^{-1}.$$

Next remove the partition of unity. Recall that  $Y_j = e^j$ , and that  $\psi_j$  is supported on  $x > 0$ , defined there by

$$\psi_j(x) = \psi\left(\frac{Y_j x^{\frac{1}{2}}}{T}\right) \sigma^\times(x^{\frac{1}{2}}).$$

Put  $\psi_{\frac{1}{2}}(x) = \psi(\frac{x^{\frac{1}{2}}}{T})$  for  $x > 0$ ,  $\psi_{\frac{1}{2}}(x) = 0$  for  $x \leq 0$ .

**Lemma 6.4.** *For arbitrary  $M > 0$  we have the equality*

$$\sum_j \Psi_{\frac{M}{Y_j^2}, 0}^{1,2}(0, 0 | \psi_j) = \Psi_{M, 0}^{1,2}(0, 0 | \psi_{\frac{1}{2}}).$$



**Proof.** The left hand side is

$$\int_{\mathbb{R}^2} \phi(x^k - y^2) \left[ \sum_j \psi_j \left( (x^k - y^2) \frac{M}{Y_j^2 x^2} \right) \right] dx dy = \Psi_{M,0}^{1,2}(0, 0 | \psi_{\frac{1}{2}}). \quad \square$$

Applying the lemma,

$$\begin{aligned} \Delta_{0,e} &= \sum_j \Delta_{0,j,e} = O(X^{1+\epsilon} T^{-1} Z^{-1}) \\ &\quad + X^{\frac{1}{2}+\frac{1}{k}} \sum_{s=s_1 s_2 s_3 s_4} \mu(s) \sum_{\substack{(\ell, t) \in (\mathbb{Z}^+)^2 \\ \ell \square\text{-free} \\ (\ell, 2st)=(t, 2s_1 s_3 s_4)=1}} \frac{\varphi(s_2^2 s_4 t) \Psi_{*,0}^{1,2}(0, 0 | \psi_{\frac{1}{2}})}{2^{2+\frac{1}{k}} s_1^{2+\frac{1}{k}} s_2^{5-\frac{2}{k}} s_3^2 s_4^3 \ell^{1+\frac{1}{k}} t^{2-\frac{2}{k}}} \end{aligned}$$

where  $*$  stands in for  $\frac{X^{1-\frac{2}{k}}}{(2s_1 \ell)^{2-\frac{2}{k}} (s_2 t)^{\frac{4}{k}}}$ .

Dropping the error, we now evaluate the main term by Mellin inversion, using the formula of Lemma 5.4 for the Mellin transform of  $\Psi_{z^{-1},0}^{1,2}(0, 0)$ . This yields the main term as the integral

$$\frac{\Gamma(\frac{1}{2})}{k} \frac{X^{\frac{1}{2}+\frac{1}{k}}}{2^{2+\frac{1}{k}}} \oint_{(2)} \frac{\Gamma(\frac{1}{2} - \frac{1}{k} + \frac{2\alpha}{k})}{\Gamma(1 - \frac{1}{k} + \frac{2\alpha}{k})} \tilde{\phi}\left(\frac{1}{2} + \frac{1}{k} + \frac{k-2}{k}\alpha\right) \tilde{\psi}_{\frac{1}{2}}(-\alpha) \frac{X^{(1-\frac{2}{k})\alpha}}{2^{(2-\frac{2}{k})\alpha}} F(\alpha) d\alpha,$$

where  $\tilde{\psi}_{\frac{1}{2}}(\alpha) = 2T^{2\alpha} \tilde{\psi}(2\alpha)$  and

$$\begin{aligned} F(\alpha) &= \sum_{\substack{s_1 s_2 s_3 s_4 = s \\ \text{odd}}} \frac{\mu(s)}{s_1^{2+\frac{1}{k}+(2-\frac{2}{k})\alpha} s_2^{5-\frac{2}{k}+\frac{4\alpha}{k}} s_3^2 s_4^3} \sum_{\substack{(\ell, t) \in (\mathbb{Z}^+)^2 \\ \ell \square\text{-free} \\ (\ell, 2st)=1 \\ (t, 2s_1 s_3 s_4)=1}} \frac{\varphi(s_2^2 s_4 t)}{\ell^{1+\frac{1}{k}+(2-\frac{2}{k})\alpha} t^{2-\frac{2}{k}+\frac{4\alpha}{k}}} \\ &= \zeta\left(1 - \frac{2}{k} + \frac{4\alpha}{k}\right) G(\alpha), \end{aligned}$$

where

$$\begin{aligned} G(\alpha) &= \left(1 - \frac{1}{2^{1-\frac{2}{k}+\frac{4\alpha}{k}}}\right) \prod_{p \text{ odd}} \left[1 - \frac{2}{p^2} + \frac{1}{p^3} + \frac{1}{p^{1+\frac{1}{k}+(2-\frac{2}{k})\alpha}} - \frac{1}{p^{2-\frac{1}{k}+(2+\frac{2}{k})\alpha}} - \frac{1}{p^{2-\frac{2}{k}+\frac{4\alpha}{k}}} \right. \\ &\quad \left. + \frac{1}{p^{3-\frac{2}{k}+\frac{4\alpha}{k}}} - \frac{1}{p^{2+\frac{1}{k}+(2-\frac{2}{k})\alpha}} + \frac{1}{p^{3-\frac{1}{k}+(2+\frac{2}{k})\alpha}}\right]; \end{aligned}$$

$G$  is holomorphic in  $\Re(\alpha) > \frac{-1}{2k-2}$ . Shifting the contour to  $\Re(\alpha) = \frac{-1}{2k-2} + \epsilon$ , we pass a pole at  $\frac{1}{2}$ , and, depending on  $\psi$ , possibly a second pole at  $\alpha = 0$ . We have  $G(\frac{1}{2}) = \frac{32}{\pi^4}$  and

$$G(0) = \frac{8}{\pi^2} \left(1 - \frac{1}{2^{1-\frac{2}{k}}}\right) \prod_{p \text{ odd}} \left[1 + \frac{1}{p+1} \left(\frac{1}{p^{\frac{1}{k}}} - \frac{1}{p^{1-\frac{2}{k}}} - \frac{1}{p^{1-\frac{1}{k}}} - \frac{1}{p}\right)\right].$$

Thus

$$\begin{aligned} \Delta_{0,e} = & O\left(X^{\frac{1}{2} + \frac{1}{(2k-2)} + \epsilon}\right) + O(X^{1+\epsilon} T^{-1} Z^{-1}) + \frac{2}{\pi^3} \tilde{\phi}(1) \tilde{\psi}(-1) \frac{X}{T} \\ & + \psi(\infty) \tilde{\phi}\left(\frac{1}{2} + \frac{1}{k}\right) \frac{1}{k\pi^{\frac{3}{2}}} \frac{\Gamma(\frac{1}{2} - \frac{1}{k})}{\Gamma(1 - \frac{1}{k})} X^{\frac{1}{2} + \frac{1}{k}} \left(2^{1-\frac{1}{k}} - 2^{\frac{1}{k}}\right) \\ & \times \prod_{p \text{ odd}} \left[1 + \frac{1}{p+1} \left(\frac{1}{p^{\frac{1}{k}}} - \frac{1}{p^{1-\frac{2}{k}}} - \frac{1}{p^{1-\frac{1}{k}}} - \frac{1}{p}\right)\right]. \end{aligned}$$

The analysis of  $\Delta_{0,o}$  is entirely analogous. It yields

$$\begin{aligned} \Delta_{0,o} = & O(X^{\frac{1}{2} + \frac{1}{(2k-2)} + \epsilon}) + O(X^{1+\epsilon} T^{-1} Z^{-1}) + \frac{4}{\pi^3} \tilde{\phi}(1) \tilde{\psi}(-1) \frac{X}{T} \\ & + \psi(\infty) \tilde{\phi}\left(\frac{1}{2} + \frac{1}{k}\right) \frac{1}{k\pi^{\frac{3}{2}}} \frac{\Gamma(\frac{1}{2} - \frac{1}{k})}{\Gamma(1 - \frac{1}{k})} X^{\frac{1}{2} + \frac{1}{k}} \\ & \times \prod_{p \text{ odd}} \left[1 + \frac{1}{p+1} \left(\frac{1}{p^{\frac{1}{k}}} - \frac{1}{p^{1-\frac{2}{k}}} - \frac{1}{p^{1-\frac{1}{k}}} - \frac{1}{p}\right)\right]. \end{aligned}$$

Combining these two expressions together yields the main term of Proposition 6.1.

**6.3.2 Bound for the off-diagonal  $f = 0, u \neq 0$ .** Write  $E_{0,j,e,s,\ell,t}$  for the even terms associated to  $E_0$  coming from  $\mathcal{M}_j$ . It follows from Lemma 4.4 that

$$|S_{k-2}(\ell s_3 u, 0; s_2^2 s_4 t)| \ll (u, s_2^2 s_4 t)^{\frac{1}{2}} (s_2^2 s_4 t)^{\frac{1}{2} + \epsilon}.$$

Actually we could quite easily extract the sign and get much more cancellation, but anyway, this is not the limiting error term.

In view of the restriction  $u \ll U_0 X^\epsilon$  (see (28)) we obtain

$$\begin{aligned} E_{0,j,e,s,\ell,t} & \ll \frac{X^{\frac{1}{2} + \frac{1}{k}} \|\Psi_{M,0}(\psi_j)\|_1}{s_1^{2+\frac{1}{k}} s_2^{4-\frac{2}{k}} s_3^{\frac{5}{2}} s_4^{\frac{1}{k}} \ell^{1+\frac{1}{k}} t^{\frac{3}{2}-\frac{2}{k}}} \sum_{0 < |u| \ll U_0 X^\epsilon} (u, s_2^2 s_4 t)^{\frac{1}{2}} \\ & \ll \frac{X^{\frac{1}{2} + \frac{1}{k}} \|\Psi_{M,0}(\psi_j)\|_1}{s_1^{2+\frac{1}{k}} s_2^{4-\frac{2}{k}} s_3^{\frac{5}{2}} s_4^{\frac{1}{k}} \ell^{1+\frac{1}{k}} t^{\frac{3}{2}-\frac{2}{k}}} \sum_{d|s_2^2 s_4 t} d^{\frac{1}{2}} \sum_{0 < |u| \ll \frac{U_0 X^\epsilon}{d}} 1. \end{aligned}$$

For the  $L^1$  norm  $\|\Psi_{M,0}(\psi_j)\|_1$  recall (13), namely

$$\|\Psi_{M,0}(\psi_j)\|_1 \ll X^\epsilon M^{-\frac{k-2}{4}}.$$

Substituting this bound and the bound  $U_0 \ll \frac{X^{\frac{k-3}{2}}}{Y_j^{k-1}(s_1 \ell)^{k-3} s_2 t}$  in (28), we obtain

$$E_{0,j,e,s,\ell,t} \ll \frac{X^{\frac{k}{4} + \epsilon}}{T^{\frac{k}{2}} s_1^{\frac{k}{2} - \frac{1}{2}} s_3^{\frac{5}{2}} s_4^{\frac{1}{k}} \ell^{1+\frac{1}{k}} t^{\frac{3}{2}}}$$

and thus

$$E_{0,j,e} = \sum_{s,\ell,t} E_{0,j,e,s,\ell,t} \ll \frac{X^{\frac{k}{4}+\epsilon}}{T^{\frac{k}{2}}}.$$

Since there are  $O(\log X)$  components  $\psi_j$  in the partition of unity, we deduce that the total contribution of terms  $E_{0,j,e}$  to  $\mathcal{M}$  is  $O(X^{\frac{k}{4}+\epsilon}T^{-\frac{k}{2}})$ , with an analogous contribution from the odd component. Combined with the evaluation of the diagonal in the previous section, this proves Proposition 6.1 in the case  $f = 0$ .

**6.3.3 Bound for  $\Delta_f$ ,  $f \neq 0$ .** Following our convention, write  $\Delta_{f,j,e}$  to indicate the even term from  $\mathcal{M}_j$ . Bound

$$|S_{k-2}(0, \tilde{f}s_2s_4; s_2^2s_4t)| \ll (s_2^2s_4)(f, t)^{\frac{1}{2}}t^{\frac{1}{2}+\epsilon}$$

to obtain

$$\Delta_{f,j,e,s,\ell,t} \ll \frac{X^{\frac{1}{2}+\frac{1}{k}+\epsilon}}{s_1^{2+\frac{1}{k}}s_2^{2-\frac{2}{k}}s_3^{\frac{3}{2}}s_4^{\frac{3}{2}}\ell^{1+\frac{1}{k}}t^{\frac{3}{2}-\frac{2}{k}-\epsilon}}(f, t)^{\frac{1}{2}}|\Psi_{M,F}^{1,2}(0, 0)|.$$

Bound

$$|\Psi_{M,F}^{1,2}(0, 0)| \leq \|\Psi_{M,0}\|_1 \ll X^\epsilon M^{-\frac{k-2}{4}}$$

to obtain

$$\begin{aligned} \Delta_{f,j,e} &\ll X^{\frac{3}{2}-\frac{k}{4}+\epsilon}Y_j^{\frac{k}{2}-1} \sum_{s=s_1s_2s_3s_4} \sum_{\substack{(s_1\ell)^{\frac{k-1}{2}}s_2t \\ \ll X^{\frac{k-2}{4}+\epsilon}Y_j^{-\frac{k}{2}}}} \frac{s_1^{\frac{k}{2}-\frac{7}{2}}\ell^{\frac{k}{2}-\frac{5}{2}}(f, t)^{\frac{1}{2}}}{s^2t^{\frac{1}{2}}} \\ &\ll X^{\frac{3}{2}-\frac{k}{4}}Y_j^{\frac{k}{2}-1}(X^{\frac{k-2}{4}}Y_j^{-\frac{k}{2}})^{\max(\frac{1}{2}, \frac{k-3}{k-1})}. \end{aligned}$$

For  $k = 3$  this gives a bound of

$$\Delta_f \ll X^{\frac{7}{8}+\epsilon}T^{-\frac{1}{4}}.$$

For  $k \geq 5$  this gives a bound of

$$\Delta_f \ll X^{\frac{1}{2}+\frac{1}{2(k-1)}+\epsilon}Y_j^{\frac{1}{k-1}} \ll X^{\frac{1}{2}+\frac{1}{k}+\epsilon}.$$

**6.3.4 Bound for  $E_f$ ,  $f \neq 0$ .** When  $u \neq 0$ , bound

$$|S_{k-2}(\ell s_3u, \tilde{f}s_2s_4; s_2^2s_4t)| \ll (u, s_2^2s_4t)^{\frac{1}{2}}(s_2^2s_4t)^{\frac{1}{2}+\epsilon}$$

and apply the bound (17) of Lemma 5.3 to bound  $\Psi_{M,F}^{1,2}$  by

$$|\Psi_{M,F}^{1,2}(\cdot, 0)| \ll \frac{M^{\frac{k}{4}+\frac{1}{2}}}{|F|} \|\Psi_{M,0}(\psi_j)\|_1.$$

In view of the bound for the  $L^1$  norm (13), we have

$$|\Psi_{M,F}^{1,2}(\cdot, 0)| \ll X^\epsilon \frac{M}{|F|} \ll \frac{X^{\frac{1}{2}-\frac{1}{k}+\epsilon}}{|f|(s_1\ell)^{1-\frac{1}{k}}(s_2t)^{\frac{2}{k}}T^2}.$$

This yields

$$E_{f,j,e,s,\ell,t} \ll \frac{X^{1+\epsilon}}{|f|T^2s_1^3s_2^4s_3^2s_4^{\frac{5}{2}}\ell^2t^{\frac{3}{2}}} \sum_{d|s_2^2s_4t} d^{\frac{1}{2}} \sum_{u \ll \frac{1}{d} \frac{|f|sX^{\frac{k}{4}-1+\epsilon}}{T^{\frac{k}{2}-2}}} 1 \ll \frac{X^{\frac{k}{4}+\epsilon}}{T^{\frac{k}{2}}s_1^2s_2^3s_3^2s_4^{\frac{3}{2}}\ell^2t^{\frac{3}{2}}},$$

so that, summing over  $s, \ell, t$ , the contribution of these terms to  $E_{f,j,e}$  is bounded by  $\frac{X^{\frac{k}{4}+\epsilon}}{T^{\frac{k}{2}}}$ .

Combined with the estimate for  $\Delta_f$  above and corresponding estimates in the odd case, we obtain Proposition 6.1 in the case  $f \neq 0$ .

## 7 The sieving error term

The goal of this section is to prove the bound for the sieving error term claimed in Proposition 6.2. The crucial ingredient in the sieve is the following lemma, which associates to non-square-free  $d = d_1q^2$  and parameterization equation  $\ell m^k = \ell^2 n^2 + t^2 d$ , a genuine primitive ideal in the ring of integers of  $\mathbb{Q}(\sqrt{-d_1})$ , and of class lying in a prescribed coset of the  $k$ -part of the class group  $H(-4d_1)$ , with the number of such cosets appearing bounded by a divisor function of  $q$ .

Given  $q \geq 1$ , indicate by

$$\text{sq}(p_1^{e_1} \cdots p_r^{e_r}) = p_1^{\lfloor \frac{e_1}{2} \rfloor} \cdots p_r^{\lfloor \frac{e_r}{2} \rfloor}, \quad \text{kr}(p_1^{e_1} \cdots p_r^{e_r}) = p_1^{\lceil \frac{e_1}{k} \rceil} \cdots p_r^{\lceil \frac{e_r}{k} \rceil}$$

the largest number whose square divides  $q$ , resp. the least  $k$ th power divisible by  $q$ .

**Lemma 7.1.** *Let  $(\ell, m, n, t, q, d) \in (\mathbb{Z}^+)^6$  satisfy  $\ell m^k - \ell^2 n^2 = t^2 q^2 d$  with  $q^2 d \equiv 2 \pmod{4}$ ,  $d$  square-free,  $(\ell m n, t) = (\ell, m) = 1$  and  $\ell$  square-free. Set*

$$q_1 = \text{sq}(\gcd(m^k, n^2)), \quad q_2 = \frac{q}{q_1}.$$

Further, set also

$$q_{10} = \text{kr}(q_1^2).$$

Then define

$$m' = \frac{m}{q_{10}}, \quad n' = \frac{n}{q_1}, \quad q' = \frac{q_{10}^k}{q_1^2}.$$

The congruence conditions  $(m', \ell n') = (m' n' q', q_2) = (\ell, q) = 1$  hold. Also, the ideal  $(q')$  factors in  $\mathbb{Q}(\sqrt{-d})$  as  $(q') = \mathfrak{q}\bar{\mathfrak{q}}$ . Moreover, there is a primitive ideal  $\mathfrak{a}$  of  $\mathbb{Q}(\sqrt{-d})$  of norm  $\ell m'$  and solving  $\mathfrak{q}\mathfrak{a}^k = \ell^{\frac{k-1}{2}}(\ell n' + tq_2\sqrt{-d})$ .

**Proof.** Dividing both sides by  $q_1^2$ , the equation  $\ell m^k - \ell^2 n^2 = t^2 q^2 d$  may be rewritten as

$$(30) \quad \ell m'^k q' - \ell^2 n'^2 = t^2 q_2^2 d.$$

The condition  $(\ell, q) = 1$  follows from  $(\ell, m) = 1$  and  $\ell$  square-free. Notice  $(m'^k q', n'^2)$  is square-free, and therefore  $(m', n') = 1$  and also  $(q', n')$  is square-free. Then  $(m', \ell n') = 1$  implies  $(m', q_2) = 1$  and  $(q', \ell) = 1$  implies  $(q', q_2) = 1$  since a common factor would divide  $n'$ , but any prime factor of  $(q', n')$  divides  $\ell m'^k q'$  only once. It thus follows that  $(n', q_2) = 1$ , so we have proven all of the congruence conditions.

Equation (30) gives a factorization of ideals

$$(\ell m'^k q') = (\ell n' + tq_2 \sqrt{-d})(\ell n' - tq_2 \sqrt{-d})$$

in  $\mathbb{Q}(\sqrt{-d})$ . Notice that  $p|\ell \Rightarrow p|t^2 q_2^2 d$  so  $p|d$ , and therefore  $(\ell) = \mathfrak{h}^2$  for some  $\mathfrak{h}$  dividing the different  $\mathfrak{d}$ . We claim that  $p|q'$  implies  $p$  is ramified or split in  $\mathbb{Q}(\sqrt{-d})$ . Indeed, if  $p$  is inert then

$$(p)|((\ell n' + tq_2 \sqrt{-d}), (\ell n' - tq_2 \sqrt{-d})) \Rightarrow p|n'$$

since  $p \nmid 2\ell$ . But then  $(p)^2 | m'^k q'$ , which contradicts  $(m'^k q', n'^2)$  square-free. Since all primes dividing  $(q')$  are ramified or split, we obtain the factorization  $(q') = \mathfrak{q}\bar{\mathfrak{q}}$  with  $\mathfrak{q} | (\ell n' + tq_2 \sqrt{-d})$ .

Set  $\mathfrak{b} = (\ell n' + tq_2 \sqrt{-d})\mathfrak{h}^{-1}\mathfrak{q}^{-1}$  so that  $\mathfrak{b}\bar{\mathfrak{b}} = (m')^k$ . Note that

$$(\mathfrak{b}, \bar{\mathfrak{b}}) | (2\ell n', m') = (1)$$

and, therefore,  $\mathfrak{b}$  is primitive, and co-prime to  $\mathfrak{d}$ . Therefore there exists primitive ideal  $\mathfrak{c}$  satisfying  $\mathfrak{c}^k = \mathfrak{b}$ , and furthermore,  $\mathfrak{a} = \mathfrak{h}\mathfrak{c}$  remains primitive. Clearly  $N(\mathfrak{a}) = \ell m'$  and  $\mathfrak{q}\mathfrak{a}^k = \ell^{\frac{k-1}{2}}(\ell n' + tq_2 \sqrt{-d})$  as wanted.  $\square$

Before turning to the sieve upper bound, we record bounds regarding the average number of  $k$ -torsion elements in the class group.

**Proposition 7.2.** *We have the bounds*

$$\sum_{\substack{\frac{X}{2} < d < X \\ d \equiv 2 \pmod{4} \\ \square\text{-free}}} \sum_{\substack{[(1)] \neq [\mathfrak{a}] \in H(-4d) \\ [\mathfrak{a}]^k = [(1)]}} 1 \ll \begin{cases} X, & k = 3, \\ X^{\frac{5}{4}}, & k = 5, \\ X^{\frac{3}{2}}, & k \geq 7. \end{cases}$$

**Proof.** For  $k = 3$  this follows from the Davenport–Heilbronn theorem. For  $k = 5$  this follows from the method of Soundararajan [13]. When  $k \geq 7$  this is the result of bounding the number of  $k$ -torsion elements by the size of the full class group.  $\square$

We now prove our basic estimate for the sieve.

**Proposition 7.3.** *Let  $\phi$  and  $\psi$  be non-negative smooth functions having compact support on  $\mathbb{R}^+$ . Let  $1 \leq T \ll X^{\frac{1}{2}-\frac{1}{k}}$ . We have the bound*

$$\sum_{q > Z} \sum_{\substack{q^2 d \equiv 2 \pmod{4} \\ d \square\text{-free}}} \sum_{\substack{(\ell, m, n, t) \in (\mathbb{Z}^+)^4 \\ (\ell mn, t) = (\ell, t) = 1 \\ \ell m^k - \ell^2 n^2 = t^2 q^2 d \\ \ell \square\text{-free}}} \phi\left(\frac{q^2 d}{X}\right) \psi\left(\frac{q^2 d}{T^2 \ell^2 m^2}\right) \ll \frac{X^{1+\epsilon}}{TZ} + \frac{X^{\frac{k}{4}+\epsilon}}{T^{\frac{k}{2}}}.$$

**Proof.** Keep the meaning of  $q_{ij}$  etc. from Lemma 7.1, in particular  $q = q_1 q_2$  and  $q' q_1^2 = q_{10}^k$ . The sum in question is

$$\sum_{\substack{q=q_1 q_2 > Z \\ q \text{ odd} \\ q' q_1^2 = q_{10}^k}} \sum_{\substack{d \equiv 2 \pmod{4} \\ d \square\text{-free}}} \sum_{\substack{(\ell, m', n', t) \in (\mathbb{Z}^+)^4 \\ \mathcal{C}_5}} \phi\left(\frac{q^2 d}{X}\right) \psi\left(\frac{q^2 d}{T^2 \ell^2 m'^2 q_{10}^2}\right);$$

$$\mathcal{C}_5 = \begin{cases} \ell \text{ square-free,} \\ m' \text{ odd,} \\ (\ell m' n' q', t q_2) = (\ell, m' q) = (m', n') = 1, \\ \ell m'^k q' - \ell^2 n'^2 = t^2 q_2^2 d \end{cases}$$

**Case 1.**  $\sqrt{d} \gg \ell m' \asymp \frac{\sqrt{X}}{T q_{10}}$ .

In the first case, set  $t' = t q_2$  to obtain, for a suitable non-negative  $\psi_0 \in C_c^\infty(\mathbb{R}^+)$ ,

$$\ll X^\epsilon \sum_{\substack{q=q_1 q_2 \\ q \text{ odd} \\ q' q_1^2 = q_{10}^k}} \sum_{\substack{(\ell, m', n', t') \in (\mathbb{Z}^+)^4, q_2 | t' \\ \mathcal{C}_6}} \psi_0\left(\frac{\sqrt{X}}{T \ell m' q_{10}}\right);$$

$$\mathcal{C}_6 = \begin{cases} (\ell m' n' q', t') = (m', \ell n') = 1, \\ \ell m'^k q' - \ell^2 n'^2 = t'^2 d, \\ d \equiv 2 \pmod{4}, \text{ square-free,} \\ \frac{X}{T^2 q_{10}^2} \ll d < \min\left(\frac{X}{Z^2}, \frac{X}{q^2}\right). \end{cases}$$

Controlling the size of  $d$  with a partition of unity, the inner sum is bounded by (we write  $t$  for  $t'$ )

$$(31) \quad \sum_{\substack{\max(1, \frac{X}{t^2 q_{10}^2}) \\ < e^a < \min(\frac{X}{Z^2}, \frac{X}{q^2})}} \sum_{\substack{(\ell q', t)=1 \\ \ell \square\text{-free} \\ (\ell t)^2 \ll \frac{q' X^{\frac{k}{2}}}{e^a T^k q_{10}^k}}} \sum_{\substack{(m', 2\ell t)=1 \\ m' \asymp \frac{\sqrt{X}}{t q_{10} \ell}}} \psi_0\left(\frac{\sqrt{X}}{T \ell m' q_{10}}\right) \\ \times \sum_{\substack{(n', m' t)=1 \\ \ell m'^k q' - \ell^2 n'^2 \\ \equiv 2t^2 \pmod{4t^2}}} \sigma^\times\left(\frac{\ell m'^k q' - \ell^2 n'^2}{t^2 e^a}\right).$$

Splitting the sum over  $n'$  into blocks of length  $t^2$ , this sum is

$$\ll X^\epsilon \left( O(1) + \frac{1}{t^2} \frac{t^2 e^a}{\ell^{\frac{3}{2}} m'^{\frac{k}{2}} q'^{\frac{1}{2}}} \right) \ll X^\epsilon \left( O(1) + \frac{e^a}{\ell^{\frac{3}{2}} m'^{\frac{k}{2}} q'^{\frac{1}{2}}} \right).$$

Bounding the sums over  $m'$  and  $\ell t$  by their length (recall that  $q_2 | t$ ), the  $O(1)$  term contributes

$$\ll \frac{X^{\frac{k}{4} + \frac{1}{2} + \epsilon}}{T^{\frac{k}{2} + 1}} \sum_{\substack{Z < q = q_1 q_2 < X^{\frac{1}{2}} \\ q' q_1^2 = q_{10}^k}} \frac{q'^{\frac{1}{2}}}{q_{10}^{\frac{k+2}{2}} q_2} \sum_{\substack{\max(1, \frac{X}{t^2 q_{10}^2}) < e^a}} \frac{1}{e^{\frac{a}{2}}} \ll \frac{X^{\frac{k}{4} + \epsilon}}{T^{\frac{k}{2}}}.$$

The second term contributes

$$\begin{aligned} &\ll X^\epsilon \sum_{\substack{Z < q_1 q_2 < X^{\frac{1}{2}} \\ q' q_1^2 = q_{10}^k}} \frac{1}{q'^{\frac{1}{2}}} \sum_{e^a < \frac{X}{Z^2}} e^a \sum_{\substack{(\ell t)^2 \ll \frac{q' X^{\frac{k}{2}}}{e^a T^k q_{10}^k} \\ q_2 | t}} \frac{1}{\ell^{\frac{3}{2}}} \sum_{m' \gg \left(\frac{t^2 e^a}{\ell q'}\right)^{\frac{1}{k}}} \frac{1}{m'^{\frac{k}{2}}} \\ &\ll X^\epsilon \sum_{\substack{Z < q_1 q_2 < X^{\frac{1}{2}} \\ q' q_1^2 = q_{10}^k}} \frac{1}{q'^{\frac{1}{k}}} \sum_{e^a < \frac{X}{Z^2}} e^{(\frac{1}{2} + \frac{1}{k})a} \sum_{\substack{(\ell t)^2 \ll \frac{q' X^{\frac{k}{2}}}{e^a T^k q_{10}^k} \\ q_2 | t}} \frac{1}{\ell^{1 + \frac{1}{k}} t^{1 - \frac{2}{k}}} \\ &\ll \frac{X^{\frac{1}{2} + \epsilon}}{T} \sum_{q < X^{\frac{1}{2}}} \frac{1}{q} \sum_{e^a < \frac{X}{Z^2}} e^{\frac{a}{2}} \ll \frac{X^{1 + \epsilon}}{TZ}. \end{aligned}$$

**Case 2.**  $\sqrt{d} \ll \ell m' \asymp \frac{\sqrt{X}}{T q_{10}}.$

Recall from Lemma 4.3 that the number of ideals of  $\mathbb{Q}(\sqrt{-d})$  of a fixed class, and with norm bounded by  $Y\sqrt{d}$ , is  $\ll (1 + Y)$ . Using this, we find that the second

case gives

$$X^\epsilon \sum_{\substack{q=q_1 q_2 > Z \\ q' q_1^2 = q_{10}^k}} \sum_{\substack{d \equiv 2 \pmod{4} \\ \square\text{-free} \\ d \asymp \frac{X}{q^2}}} \sum_{\substack{(q')=q\bar{q} \\ \text{in } \mathbb{Q}(\sqrt{-d})}} \sum_{\substack{\mathfrak{a} \text{ primitive in } \mathbb{Q}(\sqrt{-d}) \\ [\mathfrak{a}^k] = [(1)], N\mathfrak{a} \gg \sqrt{d}}} \psi_0\left(\frac{\sqrt{X}}{T q_{10} N \mathfrak{a}}\right).$$

The support of  $\psi_0$  imposes  $q_{10} \ll \frac{\sqrt{X}}{T}$ . Also, knowing the ideal  $\mathfrak{a}$  we recover  $q_2 t$ , and hence  $q_2$  up to a divisor function. Putting these together, we obtain

$$\ll \frac{X^{\frac{1}{2}+\epsilon}}{T} \sum_{q_{10} \ll \frac{\sqrt{X}}{T}} \frac{1}{q_{10}} \sum_{\substack{d \equiv 2 \pmod{4}, \square\text{-free} \\ d < \min(\frac{X}{Z^2}, \frac{X}{T^2 q_{10}^2})}} \frac{1}{\sqrt{d}} \sum_{\substack{[\mathfrak{a}] \in H(-4d) \\ [\mathfrak{a}]^k = [(1)]}} 1.$$

Substituting the bounds for the average number of  $k$ -torsion elements (Proposition 7.2) we obtain a bound of  $\ll \frac{X^{1+\epsilon}}{TZ}$  for  $k = 3$ ,  $\ll \frac{X^{\frac{5}{4}+\epsilon}}{T^{\frac{5}{2}}}$  for  $k = 5$ ,  $\ll \frac{X^{\frac{3}{2}+\epsilon}}{T^3}$  for  $k \geq 7$ . This completes the proof.  $\square$

**Proof of Proposition 6.2.** We bound  $\mathcal{E}_j$  by

$$\begin{aligned} \mathcal{E}_j &\leq \sum_{\substack{\ell, m, t \in \mathbb{Z}^+, n \in \mathbb{Z} \\ (\ell mn, t) = (\ell, m) = 1 \\ \ell \square\text{-free} \\ \ell m^k - \ell^2 n^2 \equiv 2t^2 \pmod{4t^2}}} \Phi\left(\ell m, \ell^{\frac{k+1}{2}} n, \ell^{\frac{k-1}{2}} t \mid \psi_j\right) \sum_{s^2 \mid \frac{\ell m^k - \ell^2 n^2}{t^2}, s > Z} 1 \\ &\ll X^\epsilon \sum_{q > Z} \sum_{\substack{q^2 d \equiv 2 \pmod{4} \\ d \square\text{-free}}} \sum_{\substack{(\ell, m, n, t) \in (\mathbb{Z}^+)^4 \\ (\ell mn, t) = 1, \ell \square\text{-free} \\ \ell m^k - \ell^2 n^2 = t^2 q^2 d}} \phi\left(\frac{q^2 d}{X}\right) \psi_j\left(\frac{\ell m^k - \ell^2 n^2}{Y_j^2 \ell^2 m^2 t^2}\right), \end{aligned}$$

which reduces to the sum estimated in Proposition 7.3.  $\square$

**Acknowledgments.** The problem of proving equidistribution was suggested to me by graduate advisor Soundararajan. The possibility of calculating a negative secondary term related to  $k$ -torsion was suggested to me by Akshay Venkatesh.

#### REFERENCES

- [1] N. C. Ankeny and S. Chowla, *On the divisibility of the class number of quadratic fields*, Pacific J. Math. **5** (1955), 321–324.
- [2] M. Bhargava and P. Harron, *The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields*, Compos. Math. **152**, (2016), 1111–1120.
- [3] M. Bhargava, A. Shankar and J. Tsimerman, *On the Davenport–Heilbronn theorem and second order terms*, Invent. Math. **193** (2013), 439–499.



- [4] D. Byeon and E. Koh, *Real quadratic fields with class number divisible by 3*, Manuscripta Math. **111** (2003), 261–263.
- [5] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups*, in *Number Theory (New York, 1982)*, Springer, Berlin, 1984, pp. 26–36.
- [6] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), 405–420.
- [7] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*, Invent. Math. **92** (1988), 73–90.
- [8] D. R. Heath-Brown, *Quadratic class numbers divisible by 3*, Funct. Approx. Comment. Math. **37** (2007), 203–211.
- [9] B. Hough, *Distribution Problems in Analytic Number Theory*, PhD. thesis, Stanford University, Stanford, CA, 2012.
- [10] H. Iwaniec, *Spectral Methods of Automorphic Forms*, American Mathematical Society, Providence, RI, 2002.
- [11] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society, Providence, RI, 2004.
- [12] Yu. V. Linnik, *Ergodic Properties of Algebraic Fields*, Springer, New York, 1968.
- [13] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc. **61** (2000), 681–690.
- [14] T. Taniguchi and F. Thorne, *Secondary terms in the counting functions for cubic fields*, Duke Math. J. **162** (2013), 2451–2508.
- [15] D. Terr, *The Distribution of Shapes of Cubic Orders*, PhD. Thesis, University of California, Berkeley, CA, 1997.

*Bob Hough*

DEPARTMENT OF MATHEMATICS

STANFORD UNIVERSITY

450 SERRA MALL

STANFORD, CA, 94305, USA

*current address*

INSTITUTE FOR ADVANCED STUDY

PRINCETON, NJ 08540, USA

email: hough@math.ias.edu

(Received September 5, 2016 and in revised form February 25, 2017)