Divisibility of class numbers of imaginary quadratic fields whose discriminant has only three prime factors

Kostadinka Lapkova

Department of Mathematics and its Applications, Central European University
Nador u. 9, 1051 Budapest, HUNGARY
email:lapkova_kostadinka@ceu-budapest.edu

January 3, 2012

Abstract

We prove the existence of infinitely many imaginary quadratic fields whose discriminant has exactly three distinct prime factors and whose class group has an element of a fixed large order. The main tool we use is solving an additive problem via the circle method.

1 Introduction

In this work we establish the existence of infinitely many imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ with discriminant d of only three distinct prime factors such that in the class group $Cl(-d)$ there is an element of order 2ℓ for any integer $\ell \geq 2$ and $5, 3 \nmid \ell$. The result extends naturally the one in [3], where the same problem is considered for $d = pq$ − product of two distinct primes. We show without a proof how with the same techniques an analogous result can be stated for any fixed number of prime divisors of d and any $\ell \geq 2$. Whereas in [3] the infinite number of solutions of a certain additive problem is borrowed by a strong estimate in [2], we will derive a weaker asymptotic formula following closely the method of §5 in [1]. The idea of generating such imaginary quadratic fields comes from [1] and [7], as stated in [3].

The main motivation for considering the questions of the present work was Theorem 1.1 from [6] which solves class number one problem for a certain type of real quadratic fields.

Lemma 1.1 (Lapkova). *If $d = (an)^2 + 4a$ is square-free for odd positive integers a and n such that n is divisible by $43 \cdot 181 \cdot 353$, then $\#Cl(d) > 1$.*

Key words and phrases: class number, quadratic field, circle method.
2010 *Mathematics Subject Classification*: Primary 11R29; Secondary 11P55.

Here $\#G$ represents the order of the group G. The particular parameter dividing n was chosen from a table of class numbers which showed that the 2-part of the class group $Cl(-43\cdot 181\cdot 353)$ has a high order. More specifically, $\#Cl(-43\cdot 181\cdot 353) = 2^9\cdot 3$, and we also needed that $43\cdot 181\cdot 353 \equiv 3 \pmod 4$. We will show how the main result of this paper implies existence of an infinite family of parameters $q = p_1p_2p_3$, where p_i are distinct primes, and $q \equiv 3 \pmod 4$, such that for square-free $d = (an)^2 + 4a$ with odd positive a and n, and q dividing n, we have $\#Cl(d) > 1$.

Let $\ell \geq 2$ be any integer. Consider the additive problem

$$4m^\ell = p_1 + p_2p_3\,, \tag{1.1}$$

where m is an odd integer and the primes p_1, p_2, p_3 are different. Let Δ be a fixed positive integer such that $(15,\Delta) = 1$ and the variables in (1.1) satisfy

$$\begin{gathered} x^{1/8} < p_1 \leq x, \quad p_1 \equiv -5 \pmod{\Delta}\,; \\ x^{1/8} < p_2 \leq x^{1/4} < p_3,\ p_2p_3 \leq x, \quad p_2, p_3 \equiv 3 \pmod{\Delta}\,. \end{gathered} \tag{1.2}$$

If we write

$$4m^\ell = U + V \tag{1.3}$$

for any positive integers U, V and assume that $U > V$, then for $n = (U-V)/2$ we have

$$4m^{2\ell} - n^2 = (2m^\ell - n)(2m^\ell + n) = \left(\frac{U+V}{2} - \frac{U-V}{2}\right)\left(\frac{U+V}{2} + \frac{U-V}{2}\right) = V\cdot U.$$

This way having infinitely many solutions of (1.1) we will find infinitely many corresponding discriminants $d = p_1p_2p_3 = 4m^{2\ell} - n^2$.

The following statement shows that under some conditions, which are satisfied from the solutions of (1.1), discriminants of the type $d = 4m^{2\ell} - n^2$ yield existence of an element of large order in the class group $Cl(-d)$.

Lemma 1.2 (See [3]). *For integer $\ell \geq 2$ let m and n be integers with $(n,2) = 1$ and $2m^\ell - n > 1$. If d is a square-free integer for which*

$$d = 4m^{2\ell} - n^2\,,$$

then $Cl(-d)$ contains an element of order 2ℓ.

With the notation $e(\alpha) = e^{2\pi i\alpha}$ we introduce the generating functions

$$f_1(\alpha) = \sum_{p_1} e(p_1\alpha) = \sum_{n\leq x} b_n e(n\alpha), \tag{1.4}$$

$$f_2(\alpha) = \sum_{p_2,p_3} e(p_2p_3\alpha) = \sum_{n\leq x} c_n e(n\alpha), \tag{1.5}$$

$$g(\alpha)=\sum_{m}\ell m^{\ell-1}e(m^{\ell}\alpha)=\sum_{m\le M}\omega_m e(m^{\ell}\alpha), \tag{1.6}$$

where p_i satisfy (1.2) and

$$m\le M=\left(\frac{x}{2}\right)^{1/\ell}\quad\text{and}\quad (m,\Delta)=1. \tag{1.7}$$

Remark that we will generally omit all the conditions on the parameters at which we make the summation in (1.4), (1.5), (1.6), but they will always satisfy (1.2) or (1.7), unless it is specified otherwise. We will use the circle method and in its setting it is sensible to consider

$$R(x):=\sum_{p_1+p_2p_3=4m^{\ell}}\ell m^{\ell-1}=\int_0^1 f_1(\alpha)f_2(\alpha)g(-4\alpha)d\alpha. \tag{1.8}$$

For this integral we state the following asymptotic formula which proof will be the main focus of this paper starting from section §3 .

Theorem 1.3. *Suppose that Δ,ℓ are positive integers for which $16\ell^2\mid\Delta$ and $(15,\Delta)=1$. Then*

$$R(x)=4\ell(2,\ell)\prod_{p\mid\Delta}(\ell,p-1)f_1(0)f_2(0)+\mathcal{O}\left(\frac{x^2}{\log^3 x}\right).$$

Note that the main term in the upper formula is larger than the error term. Indeed, the prime number theorem for arithmetic progressions implies

$$\pi(x,q,b)=\frac{\pi(x)}{\varphi(q)}+\mathcal{O}\left(\frac{x}{\log^C x}\right) \tag{1.9}$$

for any fixed integers $C>0$, b coprime to q. Here $\pi(x)\sim x/\log x$ is the usual prime counting function, and $\pi(x,q,b)$ counts the primes $p\le x$ in the residue class b modulo q. Therefore, taking $C=2$,

$$f_1(0)=\sum_{\substack{x^{1/8}<p_1\le x\\ p_1\equiv -5 \pmod{\Delta}}}1=\pi(x,\Delta,-5)-\pi(x^{1/8},\Delta,-5)=\frac{\pi(x)}{\varphi(\Delta)}+\mathcal{O}\left(\frac{x}{\log^2 x}\right),$$

hence

$$f_1(0)\asymp\frac{x}{\log x}. \tag{1.10}$$

We also have

$$f_2(0)=\sum_{p_2,p_3}1\asymp\frac{x}{\log x}. \tag{1.11}$$

This estimate follows from a more general result, Lemma 2.1, which is stated and proved in the next section.

Estimates (1.10) and (1.11) show that the main term in Theorem 1.3 exceeds the error term. Note that the primes p_1,p_2,p_3, counted in $R(x)$, are growing to infinity with x.

In a similar way as in [1], taking into account that the weights in $g(\alpha)$ are $\ll M^{\ell-1}\ll x^{1-1/\ell}$, we can finally deduce

Corollary 1.4. *Let $\ell \geq 2$ and Δ be positive integers for which $16\ell^2 \mid \Delta$ and $(15, \Delta) = 1$. If $R^\sharp(X)$ denotes the number of positive integers $d \leq X$ of the form*

$$d = p_1p_2p_3 = 4m^{2\ell} - n^2 \,,$$

where p_1, p_2, p_3 are distinct primes which satisfy (1.2) with $x = \sqrt{X}$, then

$$R^\sharp(X) \gg \frac{X^{1/2+1/(2\ell)}}{\log^2 X} \,.$$

Now the result of Theorem 1.1 can be extended:

Corollary 1.5. *There is an infinite family of parameters $q = p_1p_2p_3$, where p_1, p_2, p_3 are distinct primes, and $q \equiv 3 \pmod 4$, with the following property. If $d = (an)^2 + 4a$ is square-free for odd positive integers a and n, and q divides n, then $\#Cl(d) > 1$.*

Proof. The main identity to prove Theorem 1.1 is

$$q.\#Cl(-q).\#Cl(-qd) = n\left(a + \left(\frac{a}{q}\right)\right)\frac{1}{6}\prod_{p|q}(p^2-1)\,, \tag{1.12}$$

which holds if we assume that $\#Cl(d) = 1$ and $q \equiv 3 \pmod 4$. According to Claim 5.1 [6] if $\#Cl(d) = 1$ for the square-free discriminant $d = (an)^2 + 4a$, then a and $an^2 + 4$ are primes. Something more, for any prime $r \neq a$ such that $2 < r < an/2$ we have $\left(\frac{d}{r}\right) = -1$. Then by the genus theory it follows that $a \equiv 3 \pmod 4$. Also if we further assume $an/2 > 353$, we get $\left(\frac{a}{q}\right) = -1$, so $a + \left(\frac{a}{q}\right) = a - 1 \equiv 2 \pmod 4$.

Now consider $q = p_1p_2p_3$ from Corollary 1.4. Take ℓ such that $\ell = 2^g$ for $g \geq 9$. From conditions (1.2) and $16 \mid \Delta$ we see that $p_i \equiv 3 \pmod 8$, $q \equiv 3 \pmod 4$, and $2^9 \| \prod_{p_i}(p_i^2 - 1)$. Then the right-hand side of the above identity has 2-part exactly 2^9. The left-hand side, on the other hand, is divisible by the class number $\#Cl(-p_1p_2p_3)$ and 2ℓ divides this class number. This is a contradiction. Therefore $\#Cl(d) > 1$. □

At this point it becomes clear why we solve the additive problem (1.1) with a factor 4 instead of the original equation

$$2m^\ell = AU + BV \tag{1.13}$$

from [1]. We need discriminant d which is a product of exactly three primes, thus in our application we take $A = B = 1$. Something more, we want to control the 2-part in the right-hand side of (1.12). We do this by imposing $p_i \equiv 3 \pmod 8$. Then $p_1 + p_2p_3 \equiv 4 \pmod 8$ but $2m^\ell \not\equiv 4 \pmod 8$. So we need to change the coefficient 2 to 4 in (1.13). We can still keep the skeleton of the proof the same as in [1] and only work out slight modifications in the corresponding estimates.

2 Generalizations: Divisibility of Class Numbers

Let us fix any integers $\ell \geq 2$ and $k \geq 3$. Consider the additive problem

$$4m^{\ell} = p_1 + p_2 \dots p_k \,, \tag{2.1}$$

where m is an odd integer and the primes $p_1, p_2, \dots, p_k$ are different. Let Δ be an integer such that $(c_0(4 - c_0^{k-1}), \Delta) = 1$ and for the variables in (2.1) assume that $p_1 \equiv 4 - c_0^{k-1} \pmod{\Delta}$ and $p_2, \dots, p_k \equiv c_0 \pmod{\Delta}$. Denote $y = x^{1/2^{\ell+2}}$ and first assume that $y < p_1 \leq x$. Clearly there are positive real numbers $1 < \alpha_2 < \dots < \alpha_{k-1}$ such that $\sum_{2 \leq i \leq k-1} \alpha_i < 2^{\ell+2} - 1$ and with them being fixed we further require

$$y < p_2 \leq y^{\alpha_2} < p_3 \leq y^{\alpha_3} < \dots \leq y^{\alpha_{k-1}} < p_k \text{ and } p_2 p_3 \dots p_k \leq x \,. \tag{2.2}$$

The latter guarantees that $p_2, \dots, p_k$ are different while the lower bound for each of them $x^{1/2^{\ell+2}}$ is applied during the proof of Theorem 1.3.

Here we show a statement we already used in the previous section:

Lemma 2.1. *Let $n \geq 2$ be an integer and $q_1, q_2, \dots, q_n$ be primes from the same arithmetic progression that also satisfy*

$$y < q_1 \leq y^{\alpha_1} < q_2 \leq y^{\alpha_2} < \dots \leq y^{\alpha_{n-1}} < q_n \text{ and } q_1 q_2 \dots q_n \leq x,$$

where $y = x^{1/\beta}$ for some real $\beta > 1$ and $\sum_{1 \leq i \leq n-1} \alpha_i < \beta - 1$. Then if $f_n(\alpha) = \sum\limits_{q_1, \cdots, q_n} e(q_1 \dots q_n \alpha)$, we have

$$f_n(0) = \sum_{q_1, \cdots, q_n} 1 \asymp \frac{x}{\log x} \,.$$

Proof. We note that

$$x^{1 - \frac{1}{\beta}(\alpha_1 + \dots + \alpha_{n-1})} = \frac{x}{y^{\alpha_1 + \dots + \alpha_{n-1}}} \leq \frac{x}{q_1 \cdots q_{n-1}} \leq \frac{x}{y^{1 + \alpha_1 + \dots + \alpha_{n-2}}} = x^{1 - \frac{1}{\beta}(1 + \alpha_1 + \dots + \alpha_{n-2})} \,.$$

Then, since β and $\alpha_1, \dots, \alpha_{n-1}$ are fixed, we have $\log \dfrac{x}{q_1 \cdots q_{n-1}} \asymp \log x$. In that case after the Prime number theorem, similarly to (1.10), we get

$$f_n(0) \;=\; \sum_{q_1, \cdots, q_{n-1}} \sum_{q_n > x^{\frac{\alpha_{n-1}}{\beta}}}^{x/(q_1 \dots q_{n-1})} 1 \asymp \sum_{q_1, \cdots, q_{n-1}} \frac{x/(q_1 \cdots q_{n-1})}{\log x} \,.$$

Obviously, with the notation $\alpha_0 = 1$,

$$\sum_{q_1, \cdots, q_{n-1}} \frac{1}{q_1 \cdots q_{n-1}} = \prod_{i=1}^{n-1} \sum_{y^{\alpha_{i-1}} < q_i \leq y^{\alpha_i}} \frac{1}{q_i}$$

and every interval $(y^{\alpha_{i-1}}, y^{\alpha_i}]$ can be divided into $\asymp \log x$ intervals of type $(A, 2A]$. If the primes p run over an arithmetic progression modulo some fixed q, then

$$\sum_{A < p \leq 2A} \frac{1}{p} \asymp \frac{1}{\varphi(q)} \frac{1}{A} \frac{A}{\log A} \asymp \frac{1}{\log A} \,.$$

Therefore every factor $\sum_{q_i} \frac{1}{q_i} \asymp 1$ and

$$\sum_{q_1,\ldots,q_{n-1}} \frac{1}{q_1 \ldots q_{n-1}} \asymp 1\,.$$

This finishes the proof of the lemma. □

From all these we can conclude that without much effort, following literally the method in this paper for discriminants of only three prime factors, one can show an analogue of Corollary 1.4 for the solutions of (2.1). Then from Lemma 1.2 it follows

Lemma 2.2. *If for any fixed integers $k \geq 3$ and $\ell \geq 2$ there exist integers c_0, Δ with $16\ell^2 \mid \Delta$ and $\left(c_0(4 - c_0^{k-1}), \Delta\right) = 1$, then there are infinitely many discriminants $d = p_1 p_2 \ldots p_k$ such that the group $Cl(-d)$ consists of an element of order 2ℓ.*

Observe that when $3 \mid \ell$ and $k-1$ is even, we always have $1 \equiv 4 \equiv c_0^{k-1} \pmod 3$ for any $(c_0, 3) = 1$. Therefore $(4 - c_0^{k-1}, \ell) > 1$ and we cannot use the same methods for (2.1). The situation can be remedied by considering

$$2m^\ell = p_1 + p_2 \ldots p_k\,. \tag{2.3}$$

We require m to be an odd integer and the primes $p_1, \ldots, p_k$ to be different elements of the same arithmetic progression with difference Δ and $p_i \equiv 1 \pmod \Delta$. Let the variables in (2.3) satisfy $x^{1/2^{\ell+1}} < p_1 \leq x$ and conditions (2.2), with the difference that $y = x^{1/2^{\ell+1}}$ and we demand in extra $2^{\ell+1} - 1 < 1 + \alpha_2 + \ldots + \alpha_{k-1} < 2^{\ell+1}$. This way we assure $d = p_1 \ldots p_k \geq m^\ell$ and the different power in the definition of y comes from the difference between our Lemma 3.4 and the corresponding estimate in [1].

Proceeding exactly like in the paper of Balog and Ono we can show

Lemma 2.3. *For any fixed integers $k \geq 3$ and $\ell \geq 2$ there exists Δ with $4\ell^2 \mid \Delta$ such that there are infinitely many solutions of the equation (2.3).*

In order to apply the original lemmata from [1] we also need

Lemma 2.4 (Proposition 1,[7]). *Let $\ell \geq 2$ be an integer and let $d \geq 63$ be a square-free integer for which*

$$dt^2 = m^{2\ell} - n^2\,,$$

where m and n are integers with $(m, 2n) = 1$ and $m^\ell \leq d$. Then $Cl(-d)$ contains an element of order 2ℓ.

We can conclude that

Theorem 2.5. *Let $\ell \geq 2$ and $k \geq 3$ be integers. Then there are infinitely many imaginary quadratic fields whose ideal class group has an element of order 2ℓ and whose discriminant has exactly k distinct prime divisors.*

On the one hand, in order to generalize Theorem 1.1 for real quadratic fields we have to solve equation (1.1) and modify some lemmata from [1]. On the other hand, to obtain Theorem 2.5 for imaginary quadratic fields we have to define the proper additive problem (1.13), which, however, we can solve after direct application of the statements from §5 of [1].

3 Estimates of $g(\alpha)$ and $G(q,a)$

For the integers $u\,,q$ we denote by $u(q)$ the fact that u runs through a whole system of residues modulo q. For integers $q \geq 1$ and a we require the Gaussian sum

$$G(q,a) = \sum_{\substack{u(q)\\(u,q,\Delta)=1}} e\left(\frac{au^\ell}{q}\right)$$

and the auxiliary function

$$V(\eta) = \sum_{n \leq x/2} e(n\eta).$$

In this section we state the lemmata required for the estimate on the 'minor arcs' and more refined expressions of $g(\alpha)$ and $G(q,a)$. These are variants of Lemma 5.2 to Lemma 5.8 from §5 of [1] and some statements needed for the Hardy-Littlewood's circle method application taken from [8].

We start with the Dirichlet's approximation lemma

Lemma 3.1. *Let α denote a real number. Then for each real number $N \geq 1$ there exists a rational number a/q with $(a,q)=1$, $1 \leq q \leq N$ and*

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qN}\,.$$

Proof. This is Lemma 2.1 from [8]. □

Lemma 3.2 (Weyl). *Let α denote a real number and a/q is a rational number with $(a,q)=1$ and $|\alpha - a/q| \leq 1/q^2$. Then for any positive ϵ we have*

$$\sum_{m \leq y} e(\alpha m^\ell) \ll y^{1+\epsilon}\left(\frac{1}{q} + \frac{1}{y} + \frac{q}{y^\ell}\right)^{2^{1-\ell}}.$$

Proof. This is Lemma 2.4 from [8]. □

Lemma 3.3. *If a and $q \geq 1$ are integers and η is a real number, then*

$$g\left(\frac{a}{q}+\eta\right) = \frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta}G(q,a)V(\eta) + \mathcal{O}\left(qM^{\ell-1}(1+|\eta|M^\ell)\right)$$

Here and afterwards in the paper we mean $\varphi(a,b) := \varphi((a,b))$.

Proof. This is Lemma 5.2 from [1] without any modifications. □

Lemma 3.4. *Let $M^{1/2} < q \leq N := M^{\ell-1/2}$, $(a,q)=1$ and $|\alpha - a/q| \leq 1/qN$. Then we have*

$$g(4\alpha) \ll M^{\ell - 2^{-(\ell+2)}}$$

Proof. We give here modified version of the proof of Lemma 5.3 [1]. Note that we could only show the slightly weaker estimate $g(4\alpha) \ll M^{\ell-2^{-(\ell+2)}}$ than $g(2\alpha) \ll M^{\ell-2^{-(\ell+1)}}$ from [1]. Also there is a slight difference in the approximation we make below that comes from considering $g(4\alpha)$ in our case instead of $g(2\alpha)$. The inequality we want to prove is essentially Weyl's inequality from Lemma 3.2.

Recall that

$$g(4\alpha) = \sum_{\substack{m\leq M\\(m,\Delta)=1}} \ell m^{\ell-1} e(4\alpha m^\ell) = \sum_{d|\Delta} \mu(d)\ell d^{\ell-1} \sum_{m\leq M/d} m^{\ell-1} e(4\alpha d^\ell m^\ell)$$

and applying summation by parts we get

$$g(4\alpha) = \sum_{d|\Delta} \mu(d)\ell d^{\ell-1} \left([M/d]^{\ell-1}\Sigma_{[M/d]} - \sum_{y=1}^{[M/d]-1} \Big((y+1)^{\ell-1} - y^{\ell-1}\Big)\Sigma_y \right), \tag{3.1}$$

where

$$\Sigma_y := \sum_{m\leq y} e(4\alpha d^\ell m^\ell).$$

Notice that when $y \leq M^{1-2^{-(\ell+1)}}$ trivially

$$|\Sigma_y| \leq M^{1-2^{-(\ell+1)}} < M^{1-2^{-(\ell+2)}}.$$

Now assume that $y > M^{1-2^{-(\ell+1)}}$. To estimate Σ_y we will apply Weyl's inequality with some rational approximation of $4\alpha d^\ell$. To find such we apply Lemma 3.1 – there exist $(a', q') = 1$ and $1 \leq q' \leq 2N$ such that

$$\left|4d^\ell\alpha - \frac{a'}{q'}\right| < \frac{1}{q'(2N)} < \frac{1}{(q')^2}.$$

Now we consider the two possibilities

1. $4d^\ell a/q = a'/q'$. Here we can write $4d^\ell a = a'r$ and $q = q'r$ for $r = 4d^\ell a/a' \in \mathbb{Z}$. If there is a prime p such that $p \mid a$ but $p \nmid a'$ it follows that $p \mid r$, so $p \mid q$. But this yields the contradiction $p \mid (a,q) = 1$. In the same way we see that if $p^k \mid a$ we need to have $p^k \mid a'$. Therefore $a \mid a'$ and $a/a' \leq 1$. So $r \leq 4d^\ell$, $q = q'r \leq q'4d^\ell$ and $q' \geq q/(4d^\ell)$. By the assumptions on q we get

$$\frac{M^{1/2}}{4d^\ell} < q' \leq 2N. \tag{3.2}$$

2. $4d^\ell a/q \neq a'/q'$. In this case we form the difference

$$\begin{aligned}\frac{1}{qq'} &\leq \left|4d^\ell\frac{a}{q} - \frac{a'}{q'}\right| = \left|4d^\ell\alpha - 4d^\ell\alpha + 4d^\ell\frac{a}{q} - \frac{a'}{q'}\right| \leq \left|4d^\ell\alpha - \frac{a'}{q'}\right| + 4d^\ell\left|\alpha - \frac{a}{q}\right| \\ &\leq \frac{1}{q'(2N)} + \frac{4d^\ell}{qN} = \frac{q + 8q'd^\ell}{2Nqq'}.\end{aligned}$$

When we multiply both sides of the outermost members of the inequality by $qq'2N$ we get $2N \leq q + 8d^\ell q'$. Again by the lemma's assumptions $q \leq N$ and we should have $8d^\ell q' \geq N$, otherwise $q + 8d^\ell q' < 2N$. We conclude that

$$\frac{N}{8d^\ell} \leq q' \leq 2N\,. \tag{3.3}$$

Now we apply Weyl's inequality for $\left|4d^\ell\alpha - a'/q'\right| < 1/(q')^2$ where we combine (3.2) and (3.3) for the lower bound of q' : $\min(M^{1/2}/(4d^\ell), N/(8d^\ell)) \leq q' \leq 2N$ and we take $\epsilon = 2^{-(\ell+2)}$. Then

$$\Sigma_y \ll y^{1+2^{-(\ell+2)}}\left(\frac{1}{q'} + \frac{1}{y} + \frac{q'}{y^\ell}\right)^{2^{1-\ell}}\,.$$

We have

$$(q')^{-1} \leq \max\left(\frac{4d^\ell}{M^{1/2}}, \frac{8d^\ell}{M^{\ell-1}.M^{1/2}}\right) = \frac{4d^\ell}{M^{1/2}}\max\left(1, \frac{2}{M^{\ell-1}}\right) = \frac{4d^\ell}{M^{1/2}}$$

when $\ell \geq 2$ and x is large enough, and $1/y < 1/M^{1-2^{-(\ell+1)}}$. It follows that

$$\Sigma_y \ll y^{1+2^{-(\ell+2)}}\left(\frac{1}{q'} + \frac{1}{y} + \frac{q'}{y^\ell}\right)^{2/2^\ell} \ll M^{1+2^{-(\ell+2)}}\left(\frac{1}{q'} + \frac{1}{y} + \frac{q'}{y^\ell}\right)^{2/2^\ell}\,.$$

The expression in the brackets is

$$\begin{aligned} &\ll \frac{1}{M^{1/2}} + \frac{1}{y} + \frac{N}{y^\ell} \ll \frac{1}{M^{1/2}} + \frac{1}{y} + \frac{M^\ell}{M^{1/2}(M^{1-1/2^{\ell+1}})^\ell} = \frac{1}{M^{1/2}} + \frac{1}{y} + \frac{M^{\ell/2^{\ell+1}}}{M^{1/2}} \\ &\ll M^{-1/2} + M^{-1+1/2^{\ell+1}} + M^{-1/2+\ell/2^{\ell+1}} \ll M^{-1/4}\,, \end{aligned}$$

because for $l \geq 2$ the last summand makes the biggest contribution. But then

$$\Sigma_y \ll M^{1+2^{-(\ell+2)}}M^{-1/2^{\ell+1}} = M^{1-2^{-(\ell+2)}}\,.$$

Now we insert the last estimate into (3.1). Using that $\sum_{d|\Delta} \ll 1$, $d \ll 1$, $(y+1)^{\ell-1} - y^{\ell-1} \ll y^{\ell-2}$, we get

$$g(4\alpha) \ll M^{\ell-2^{-(\ell+2)}}\,.$$

□

Lemma 3.5. *If* $(q_1, q_2) = 1$, *then* $G(q_1, a_1)G(q_2, a_2) = G(q_1q_2, a_1q_2 + a_2q_1)$.

Proof. This is Lemma 5.4 from [1] and follows from Lemma 2.10, [8]. □

Lemma 3.6. *If* p *is prime and* a *is integer coprime to* p, *then* $|G(p, a)| \leq (\ell, p-1)p^{1/2}$

Proof. This is Lemma 5.5 of [1] and follows from Lemma 4.3, [8]. □

Lemma 3.7. *Suppose that* $p \mid \Delta$ *is prime and let* $s := ord_p(4\ell)$. *If* $p \nmid a$ *and* $k \geq \max(2, 2s+1)$, *then* $G(p^k, a) = G(p^k, 4a) = 0$.

Proof. First we show that $G(p^k, 4a) = 0$. From the assumptions we have $k - s - 1 \geq s \geq 0$, so we can represent the residues $\pmod{p^k}$ in the form $u + vp^{k-s-1}$ where u runs through the residues $\pmod{p^{k-s-1}}$ and v – the residues $\pmod{p^{s+1}}$.

Since $p \mid \Delta$, the condition $(u, p, \Delta) = 1$ is equivalent to $p \nmid u$, and

$$G(p^k, 4a) = \sum_{\substack{u(p^k) \\ p \nmid u}} e\left(\frac{4au^\ell}{p^k}\right) = \sum_{\substack{u(p^{k-s-1}) \\ p \nmid u}} \sum_{v(p^{s+1})} e\left(\frac{4a(u + vp^{k-s-1})^\ell}{p^k}\right).$$

By the binomial polynomial theorem $(u + vp^{k-s-1})^\ell = \sum_{m=0}^{\ell} \binom{\ell}{m} u^{\ell-m}(vp^{k-s-1})^m$. Consider the possibilities

1. $s = 0$, $m \geq 2$. Here $m(k - s - 1) = m(k - 1) \geq 2(k - 1) \geq 2$ whenever $k \geq 2$, which is true.
2. $s \geq 1$, $m \geq 3$. Now $m(k - s - 1) \geq 3(k - s - 1) \geq k$ if $2k \geq 3s + 3$. We know that $k \geq \max(2, 2s + 1)$, hence $2k \geq 4s + 2 \geq 3s + 3$ if and only if $s \geq 1$. This is true in the regarded case.
3. $s \geq 1$, $m = 2$. We can have $2(k-s-1) \geq k$ following from $k \geq 2s+2$. The only possible problem might arise for $k = 2s + 1$. However in this case

$$\frac{4a\binom{\ell}{2}u^{\ell-2}(vp^s)^2}{p^{2s+1}} = \frac{au^{\ell-2}(2\ell)(\ell-1)v^2}{p}$$

   and, as $ord_p(4\ell) = s \geq 1$, in any case $p \mid 2\ell$.

All these show that for $m \geq 2$ the summands from the binomial polynomial contribute integers as arguments of the exponent $e(x)$ so we can write

$$G(p^k, 4a) = \sum_{\substack{u(p^{k-s-1}) \\ p \nmid u}} e\left(\frac{4au^\ell}{p^k}\right) \sum_{v(p^{s+1})} e\left(\frac{4\ell au^{\ell-1}v}{p^{s+1}}\right).$$

Now $p \nmid a$, $p \nmid u$, and $ord_p(4\ell) = s$. Therefore, if we write $4\ell = p^s \ell_1$ with $(\ell_1, p) = 1$,

$$\sum_{v(p^{s+1})} e\left(\frac{4\ell au^{\ell-1}v}{p^{s+1}}\right) = \sum_{v(p^{s+1})} e\left(\frac{\ell_1 au^{\ell-1}v}{p}\right) = p^s.0 = 0\,.$$

Hence $G(p^k, 4a) = 0$.

The proof that $G(p^k, a) = 0$ is identical for $p \neq 2$. If $p = 2$, notice that

$$\sum_{\substack{u(2^k) \\ 2 \nmid u}} e\left(\frac{4au^\ell}{2^k}\right) = 4 \sum_{\substack{u(2^{k-2}) \\ 2 \nmid u}} e\left(\frac{au^\ell}{2^{k-2}}\right), \tag{3.4}$$

i.e. $G(2^k, a) = G(2^{k+2}, 4a)/4$. When k is not smaller than $\max(2, 2s + 1)$, so is $k + 2$. This shows that $G(p^k, a) = 0$. □

Lemma 3.8. *If* $(q,a)=1$, *then*

$$G(q,4a) \ll q^{1-1/\ell}\,.$$

Proof. Using Lemma 3.5, 3.6, 3.7 we reduce the statement to Theorem 4.2 from [8] . In [8] one considers the sum

$$S(a,q)=\sum_{x(q)} e\left(\frac{ax^{\ell}}{q}\right)$$

and for it we have $S(q,a) \ll q^{1-1/\ell}$ when $(q,a)=1$.

We can reformulate Lemma 3.5: for $(q_1,q_2)=1$ and $q_1\bar{q}_1 \equiv 1 \pmod{q_2}$, $q_2\bar{q}_2 \equiv 1 \pmod{q_1}$ we have

$$G(q_1q_2,a)=G(q_1,a\bar{q}_2)G(q_2,a\bar{q}_1)\,. \tag{3.5}$$

Still $(q_1,a\bar{q}_2)=(q_2,a\bar{q}_1)=1$ and the desired estimate of $G(q,4a)$ does not depend on the second argument, so it suffices to consider only $G(p^k,4a)$.

Let $p\neq 2$. Then $(p,4a)=1$. If $p\nmid\Delta$ the condition $(u,p^k,\Delta)=1$ is trivial, so $G(p^k,4a)=S(p^k,4a)$ and Theorem 4.2 [8] applies. When $p\mid\Delta$ we consider only, because of Lemma 3.7, $k<\max(2,2s+1)$. When this maximum is 2, then $k=1$. In that case, as $\ell\geq 2$, we have

$$G(p,4a)\ll p^{\frac{1}{2}}\ll p^{1-\frac{1}{\ell}}$$

after Lemma 3.6. Now assume that $s>0$, i.e. $s\geq 1$. Then

$$G(p^k,4a)=\sum_{\substack{u(p^k)\\ p\nmid u}} e\left(\frac{4au^{\ell}}{p^k}\right)=\sum_{u(p^k)} e\left(\frac{4au^{\ell}}{p^k}\right)-\sum_{\substack{u(p^k)\\ p\mid u}} e\left(\frac{4au^{\ell}}{p^k}\right)=S(p^k,4a)+\mathcal{O}(p^{k-1})\,. \tag{3.6}$$

By Theorem 4.2 [8] $S(p^k,4a)\ll p^{k(1-1/\ell)}$. Obviously we will have $G(p^k,4a)\ll p^{k(1-1/\ell)}$ if $k\leq\ell$.
Assume that $k>\ell$. As p is odd we have $3^s\leq\ell<k\leq 2s$, which is not true for $s\geq 1$.

When $p=2$ in analogous way as in (3.4) we can show that $G(2^k,4a)=4G(2^{k-2},a)$ for $k\geq 2$. We could freely omit to consider the smaller powers of 2 since they contribute small constants to the upper bound we try to show. Also, if $2\nmid\Delta$, then again $G(2^{k-2},a)=S(2^{k-2},a)$. So further regard $2\mid\Delta$. Like in (3.6), if $k-2\leq\ell$ the estimate follows. Assume the contrary – then $2^{s-2}\leq\ell<k-2\leq 2s-2$ which holds only for $s\leq 4$. But this gives $k\leq 8$ – again these contribute only constant to the whole estimate of $G(q,4a)$. This proves the Lemma. □

Lemma 3.9. *Suppose that* $|\beta|\leq 1/2$ *and* n *is a positive integer. Then for*

$$\nu(\beta)=\sum_{m=1}^{n} e(\beta m)$$

we have $\nu(\beta)\ll\min(n,|\beta|^{-1})$.

Proof. This is Lemma 2.8 from [8] when $k = 1$. □

The following is Bombieri's theorem on the large sieve.

Lemma 3.10. *For any complex numbers c_n we have*

$$\sum_{q\le Q}\sum_{(a,q)=1}\left|\sum_{n\le x} c_n e\left(\frac{an}{q}\right)\right|^2 \le (x+Q^2)\sum_{n\le x}|c_n|^2 .$$

Proof. This is Theorem 2 of §23 in [4]. □

4 The circle method

With the conditions from Theorem 1.3 in this section our main aim is to prove the following

Theorem 4.1. *For any $1 \le Q \le M^{\min(1/6,\ell/2^{\ell+2})}$ we get*

$$R(x) = \sum_{q\le Q}\sum_{(a,q)=1}\frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta}G(q,-4a)f_1\left(\frac{a}{q}\right)f_2\left(\frac{a}{q}\right) + \mathcal{O}\left(\frac{x^2}{Q^{1/\ell}}\right).$$

Proof. We recall that we search for the number of solutions of (1.1) satisfying condition (1.2) and

$$p_1 \equiv -5 \pmod{\Delta}, \qquad p_2, p_3 \equiv 3 \pmod{\Delta},$$

so that $p_1 + p_2p_3 \equiv 4 \pmod 8$ because $16\ell^2 \mid \Delta$. We also use the parameters

$$M = \left(\frac{x}{2}\right)^{1/\ell}, \qquad N = M^{\ell-1/2} \asymp \frac{x}{M^{1/2}}, \qquad Q \le M^{\min\left(1/6,\ell/2^{(\ell+2)}\right)}. \tag{4.1}$$

By Lemma 3.1 for any real α such that $1/N \le \alpha < 1 + 1/N$ there exists approximation $|\alpha - a/q| < 1/(qN)$ with $1 \le a \le q \le N$ and $(a,q) = 1$. We denote this 'major arc' by

$$\mathfrak{M}(a/q) = \left(\frac{a}{q} - \frac{1}{qN}, \frac{a}{q} + \frac{1}{qN}\right).$$

One easily sees that the major arcs are non-overlaping so we can define the set of the 'minor arcs'

$$\mathfrak{m} = \left[\frac{1}{N}, 1 + \frac{1}{N}\right) \setminus \bigcup_{q\le M^{1/2}}\bigcup_{(a,q)=1}\mathfrak{M}(a/q).$$

Later we will also need the orthogonality relation

$$\int_0^1 e(\alpha h)d\alpha = \begin{cases} 1 & \text{when } h = 0, \\ 0 & \text{when } h \ne 0. \end{cases} \tag{4.2}$$

As f_1, f_2 and g are periodic functions with period 1, we have

$$\begin{aligned} R(x) &= \int_{1/N}^{1+1/N} f_1(\alpha)f_2(\alpha)g(-4\alpha)d\alpha = \sum_{q\le M^{1/2}}\sum_{(a,q)=1}\int_{\mathfrak{M}(a/q)} f_1(\alpha)f_2(\alpha)g(-4\alpha)d\alpha \\ &+ \int_{\mathfrak{m}} f_1(\alpha)f_2(\alpha)g(-4\alpha)d\alpha . \end{aligned}$$

When α is in $\mathfrak{m}$, it is approximated by a/q where $M^{1/2} < q < N$ and we use Lemma 3.4 to get $g(-4\alpha) \ll M^{\ell - 2^{-(\ell+2)}}$. Then

$$\int_{\mathfrak{m}} f_1(\alpha) f_2(\alpha) g(-4\alpha) d\alpha \ll M^{\ell - 2^{-(\ell+2)}} \int_{\mathfrak{m}} |f_1(\alpha) f_2(\alpha)| \, d\alpha$$

By Cauchy-Schwartz inequality, Parseval's identity and the fact that in (1.4) and (1.5) $b_n, c_n \leq 2 \ll 1$, we have

$$\begin{aligned} \int_{\mathfrak{m}} |f_1(\alpha) f_2(\alpha)| \, d\alpha &< \int_0^1 |f_1(\alpha) f_2(\alpha)| \, d\alpha < \left(\int_0^1 |f_1(\alpha)|^2 d\alpha \int_0^1 |f_2(\alpha)|^2 d\alpha \right)^{1/2} \\ &= \left(\sum_{n \leq x} |b_n|^2 \sum_{n \leq x} |c_n|^2 \right)^{1/2} \ll (x.x)^{1/2} = x \,. \end{aligned}$$

Thus

$$\int_{\mathfrak{m}} f_1(\alpha) f_2(\alpha) g(-4\alpha) d\alpha \ll M^{\ell - 2^{-(\ell+2)}} x = M^\ell x . M^{-2^{-(\ell+2)}} \ll \frac{x^2}{M^{2^{-(\ell+2)}}} \,. \tag{4.3}$$

On the 'major arc' $\mathfrak{M}(a/q)$ we use the bound in Lemma 3.3. Note that when $q \leq M^{1/2}$ and $a/q + \eta \in \mathfrak{M}(a/q)$ we have $|\eta| < 1/(qN)$. Then the error term from Lemma 3.3 is $\mathcal{O}(qM^{\ell-1}(1 + |\eta| x)) = \mathcal{O}\left(qM^{\ell-1}(1 + M^\ell/(qM^{\ell-1/2}))\right) = \mathcal{O}\left(qM^{\ell-1} + M^{\ell-1}M^{1/2}\right) = \mathcal{O}(M^{\ell-1/2})$. Then, by Cauchy-Schwarz inequality and Parseval's identity, for the error term we get

$$\begin{aligned} &\sum_{q \leq M^{1/2}} \sum_{(a,q)=1} \int_{\mathfrak{M}(a/q)} \left| f_1(\frac{a}{q} + \eta) f_2(\frac{a}{q} + \eta) \right| M^{\ell-1} q (1 + |\eta| x) d\eta \\ &\ll M^{\ell - 1/2} \int_0^1 |f_1(\alpha) f_2(\alpha)| \, d\alpha \ll M^{\ell-1/2} x \ll \frac{x^2}{M^{1/2}} \,. \end{aligned}$$

The latter error term is smaller than the one in (4.3). Therefore, after Lemma 3.3

$$\begin{aligned} R(x) &= \sum_{q \leq M^{1/2}} \sum_{(a,q)=1} \frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta} G(q,-4a) \int_{-1/qN}^{1/qN} f_1\left(\frac{a}{q} + \eta\right) f_2\left(\frac{a}{q} + \eta\right) V(-4\eta) d\eta \\ &\quad + \mathcal{O}\left(\frac{x^2}{M^{2^{-(\ell+2)}}}\right) \end{aligned}$$

We will use Lemma 3.9 – for $|\beta| \leq 1/2$ we have $V(\beta) \ll \min(x, |\beta|^{-1})$. As $|4\eta| \leq 4/qN \leq 1/2$, because $N \asymp x^{1-1/2\ell}$ is greater than 8 for large enough x, we get

$$V(-4\eta) \ll \min(x, |\eta|^{-1}) \,.$$

To estimate the contribution of the terms with $Q < q \leq M^{1/2}$ we use the latter inequality and Lemma 3.8 .

$$\begin{aligned}
&\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta}G(q,-4a)\int_{-1/qN}^{1/qN}f_1\left(\frac{a}{q}+\eta\right)f_2\left(\frac{a}{q}+\eta\right)V(-4\eta)d\eta\\
\ll\ &\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta}q^{1-1/\ell}\int_{-1/qN}^{1/qN}\left|f_1\left(\frac{a}{q}+\eta\right)f_2\left(\frac{a}{q}+\eta\right)V(-4\eta)\right|d\eta\\
\ll\ &Q^{-1/\ell}\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\int_{-1/2}^{1/2}|\ldots|\,d\eta\\
\ll\ &Q^{-1/\ell}\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\left|f_1\left(\frac{a}{q}+\eta\right)f_2\left(\frac{a}{q}+\eta\right)\right|d\eta\\
\ll\ &Q^{-1/\ell}\left(\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\left|f_1\left(\frac{a}{q}+\eta\right)\right|^2d\eta\right)^{1/2}.\\
&\left(\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\left|f_2\left(\frac{a}{q}+\eta\right)\right|^2d\eta\right)^{1/2}
\end{aligned}$$

As

$$f_1\left(\frac{a}{q}+\eta\right)=\sum_{n\le x}b_ne(n\eta)e\left(n\frac{a}{q}\right)\qquad\text{and}\qquad f_2\left(\frac{a}{q}+\eta\right)=\sum_{n\le x}c_ne(n\eta)e\left(n\frac{a}{q}\right),$$

when we apply the large sieve for the sum in the upper integrals and use the trivial estimate $\sum_{n\le x}|b_ne(n\eta)|^2\ll x/\log x$ after (1.10), and $\sum_{n\le x}|c_ne(n\eta)|^2\ll x/\log x$ after (1.11), we see that the last considered error term is

$$\ll Q^{-1/\ell}\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})(x+M)\frac{x}{\log x}d\eta\ll Q^{-1/\ell}\frac{x^2}{\log x}\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})d\eta\,.$$

The latter integral is $\ll\log x$. Indeed, for $|\eta|^{-1}\ge x$, i.e. $1/x\ge|\eta|$, we have $\min(x,|\eta|^{-1})=x$. So

$$\begin{aligned}
\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})d\eta\ &=\ \int_{-1/x}^{1/x}xd\eta+\int_{-1/2}^{-1/x}\frac{d\eta}{-\eta}+\int_{1/x}^{1/2}\frac{d\eta}{\eta}=x\left(\frac{1}{x}+\frac{1}{x}\right)\\
&+\ 2\int_{1/x}^{1/2}\frac{d\eta}{\eta}=2-2\log 2+2\log x\ll\log x\,.
\end{aligned}$$

Hence the contribution to $R(x)$ of the terms with $Q<q\le M^{1/2}$ is $\mathcal{O}(x^2Q^{-1/\ell})$.

We are left with $q\le Q$. When we extend the range of integration in the corresponding integral from $(-1/qN,1/qN)$ to $(-1/2,1/2)$ we get an error term which we estimate by Parseval's identity, Lemma 3.8, and using that $V(-4\eta)\ll|\eta|^{-1}\le qN$ for $1/(qN)\le|\eta|\le 1/2$.

The error term in question is

$$2\sum_{q\le Q}\sum_{(a,q)=1}\frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta}|G(q,-4a)|\int_{1/qN}^{1/2}\left|f_1\left(\frac{a}{q}+\eta\right)f_2\left(\frac{a}{q}+\eta\right)V(-4\eta)\right|d\eta$$

$$\ll N\sum_{q\le Q}\sum_{(a,q)=1}q^{1-1/\ell}\int_0^1\left|f_1\left(\frac{a}{q}+\eta\right)f_2\left(\frac{a}{q}+\eta\right)\right|d\eta\ll Nx\sum_{q\le Q}\sum_{(a,q)=1}q^{1-1/\ell}$$

$$\ll Nx\sum_{q\le Q}q^{1-1/\ell}.q=Nx\sum_{q\le Q}q^{2-1/\ell}\le NxQ^{2-1/\ell}\sum_{q\le Q}1\le NxQ^{3-1/\ell}.$$

Now recall the parameters conditions (4.1). It follows that

$$NxQ^{3-1/\ell}\ll x^2M^{-1/2}M^{1/2}Q^{-1/\ell}=x^2Q^{-1/\ell}.$$

Until now we got the error terms $\mathcal{O}\left(x^2/M^{2^{-(\ell+2)}}\right)$ and $\mathcal{O}(x^2Q^{-1/\ell})$. After (4.1) $Q\le M^{\ell.2^{-(\ell+2)}}$, so $Q^{-1/\ell}\ge M^{-2^{-(\ell+2)}}$ and the larger error term is $\mathcal{O}(x^2Q^{-1/\ell})$. Collecting all up to now we arrive at

$$R(x)=\sum_{q\le Q}\sum_{(a,q)=1}\frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta}G(q,-4a)\int_0^1 f_1\left(\frac{a}{q}+\eta\right)f_2\left(\frac{a}{q}+\eta\right)V(-4\eta)d\eta+\mathcal{O}\left(\frac{x^2}{Q^{1/\ell}}\right).$$

The integral, after the orthogonality property, counts $e(p_1\frac{a}{q})e(p_2p_3\frac{a}{q})$ exactly when $p_1+p_2p_3=4n\le 2x$, thus its value is exactly $f_1(a/q)f_2(a/q)$ and this proves the claim. □

Further we need to compute $f_1\left(a/q\right)$ and $f_2\left(a/q\right)$. For $q\le Q$ we write $q=dq'$, where d is composed only from primes dividing Δ and $(q',\Delta)=1$. If $p^k\mid d$ but $p^k\nmid\Delta$, then from $16\ell^2\mid\Delta$ and $s=ord_p(4\ell)$ we have $k\ge 2s+1$. Clearly there is no $p\mid d$ such that $p\nmid\Delta$, so $k\ge 2$. Thus $k\ge\max(2,2s+1)$ and after Lemma 3.7 we get $G(p^k,4a)=0$. Combining this with Lemma 3.5, and (3.5), we get $G(q,4a)=0$ unless $d\mid\Delta$.

Recall that $p_1\equiv -5 \pmod{\Delta}$ and $p_2p_3\equiv 9 \pmod{\Delta}$. Let us write $r_1\equiv -5 \pmod{\Delta}$ and $r_2\equiv 9 \pmod{\Delta}$. If $d\mid\Delta$ we have

$$f_1\left(\frac{a}{q}\right)=\sum_{x^{1/8}<p_1\le x}e\left(p_1\frac{a}{q}\right)=\sum_{(b,q)=1}e\left(b\frac{a}{q}\right)\sum_{\substack{x^{1/8}<p_1\le x\\ p_1\equiv b(q)}}1=\sum_{\substack{(b,q)=1\\ b\equiv r_1(d)}}e\left(b\frac{a}{q}\right)\sum_{\substack{x^{1/8}<p_1\le x\\ p_1\equiv b(q')}}1$$

and

$$f_2\left(\frac{a}{q}\right)=\sum_{n\le x}c_ne\left(n\frac{a}{q}\right)=\sum_{(b,q)=1}e\left(b\frac{a}{q}\right)\sum_{\substack{n\le x\\ n\equiv b(q)}}c_n=\sum_{\substack{(b,q)=1\\ b\equiv r_2(d)}}e\left(b\frac{a}{q}\right)\sum_{\substack{n\le x\\ n\equiv b(q')}}c_n$$

because $c_n=0$ unless $n=p_2p_3\equiv 3^2\equiv r_2 \pmod{\Delta}$. Also in the two functions always $(b,q)=1$, as $x^{1/8}<p_1,p_2,p_3$ and $q\le Q\le M^{\frac{\ell}{2^{\ell+2}}}<x^{1/2^{\ell+2}}<x^{1/8}$ for $\ell\ge 2$. Thus $(p_1,q)=1$ and $n=p_2p_3$ is composed by primes larger than q and $(n,q)=1$.

Similarly to (1.9) we see that

$$\sum_{\substack{x^{1/8}<p_1\le x\\ p_1\equiv b(q')}} 1 = \frac{1}{\varphi(q')}\sum_{x^{1/8}<p_1\le x} 1 + \mathcal{O}\left(\frac{x}{\log^C x}\right) = \frac{1}{\varphi(q')} f_1(0) + \mathcal{O}\left(\frac{x}{\log^C x}\right).$$

The analogous sum, again by (1.9), is

$$\sum_{\substack{n\le x\\ n\equiv b(q')}} c_n = \sum_{p_2}\sum_{\substack{x^{1/4}<p_3\le x/p_2\\ p_3\equiv b/p_2(q')}} 1 = \frac{1}{\varphi(q')}\sum_{p_2}\sum_{p_3} 1 + \mathcal{O}\left(\frac{x}{\log^C x}\right) = \frac{1}{\varphi(q')} f_2(0) + \mathcal{O}\left(\frac{x}{\log^C x}\right).$$

Here we again used that $\sum_{x^{1/8}<p_2\le x^{1/4}} \frac{1}{p_2} \ll 1$ as was shown in the proof of Lemma 2.1. The latter estimates with $f_i(0)$ are uniform in b and the main term is independent on b. Thus for $i = 1, 2$ we can write

$$f_i\left(\frac{a}{q}\right) = \frac{1}{\varphi(q')} f_i(0) \sum_{\substack{(b,q)=1\\ b\equiv r_i(d)}} e\left(\frac{ab}{q}\right) + \mathcal{O}\left(\frac{q'x}{\log^C x}\right). \tag{4.4}$$

Each b in the sum above can be written as $b = r_i q'\overline{q'} + b'd$, where $(b', q') = 1$ and $q'\overline{q'} \equiv 1 \pmod d$. Also recall that for the Ramanujan sum for any positive integer q we have(Theorem 272,[5])

$$\sum_{(b,q)=1} e\left(\frac{ab}{q}\right) = \varphi(q)\frac{\mu(q/(a,q))}{\varphi(q/(a,q))}.$$

Then, since $(a, q) = (a, q') = 1$, we have

$$\begin{aligned}\sum_{\substack{(b,q)=1\\ b\equiv r_i(d)}} e\left(\frac{ab}{q}\right) &= \sum_{(b',q')=1} e\left(\frac{a(r_i q'\overline{q'} + b'd)}{q}\right) = e\left(\frac{ar_i\overline{q'}}{d}\right)\sum_{(b',q')=1} e\left(\frac{ab'}{q'}\right)\\ &= e\left(\frac{ar_i\overline{q'}}{d}\right)\varphi(q')\frac{\mu(q'/(a,q'))}{\varphi(q'/(a,q'))} = \mu(q')e\left(\frac{ar_i\overline{q'}}{d}\right).\end{aligned}$$

Recall also Theorem 327, [5] stating that for every positive δ $\varphi(n)/n^{1-\delta} \to \infty$. Thus $n/\varphi(n) < n^\delta$ for large enough n.

Let us take $Q \le \log^{C/2} x$. Then for $q \le Q$ we have $q/\varphi(q) \ll \log x$ and when we multiply $f_1(a/q)$ with $f_2(a/q)$ from (4.4) the error terms are

$$\mathcal{O}\left(\frac{f_i(0)}{\varphi(q')}.\frac{q'x}{\log^C x}\right) = \mathcal{O}\left(\frac{x}{\log x}\log x\frac{x}{\log^C x}\right) = \mathcal{O}\left(\frac{x^2}{\log^C x}\right)$$

and

$$\mathcal{O}\left(\frac{q'x}{\log^C x}\right)^2 = \mathcal{O}\left(\frac{x\log^{C/2} x}{\log^C x}\right)^2 = \mathcal{O}\left(\frac{x^2}{\log^C x}\right).$$

Also note that $r_1 + r_2 \equiv -5 + 9 \equiv 4 \pmod \Delta$, thus

$$f_1\left(\frac{a}{q}\right) f_2\left(\frac{a}{q}\right) = \frac{\mu(q')^2}{\varphi(q')^2} e\left(\frac{4a\overline{q'}}{d}\right) f_1(0)f_2(0) + \mathcal{O}\left(\frac{x^2}{\log^C x}\right).$$

Then Theorem 4.1 transforms into

$$\begin{aligned} R(x) &= f_1(0)f_2(0)\frac{\varphi(\Delta)}{\Delta}\sum_{d|\Delta}\sum_{\substack{q'\leq Q/d\\(q',\Delta)=1}}\frac{\mu(q')^2(q',\Delta)}{q'\varphi(q')^2\varphi(d)\varphi(q',\Delta)}\sum_{(a,dq')=1}G(dq',-4a)e\left(\frac{4a\overline{q'}}{d}\right)\\ &+ \mathcal{O}\left(\frac{x^2}{Q^{1/\ell}}\right)+\mathcal{O}\left(\frac{x^2Q^{2-1/\ell}}{\log^C x}\right). \end{aligned}$$

The last error term comes from

$$\sum_{q\leq Q}\sum_{(a,q)=1}\frac{1}{q}G(q,-4a)\ll\sum_{q\leq Q}\sum_{(a,q)=1}\frac{q^{1-1/\ell}}{q}\ll\sum_{q\leq Q}q.q^{-1/\ell}\leq Q.Q^{1-1/\ell}.$$

Of course $(q',\Delta)=1$. At this stage we also take $Q=\log^{3\ell}x$ with $C=6\ell$. Then

$$\frac{x^2Q^{2-1/\ell}}{\log^C x}=\frac{x^2(\log^{3\ell}x)^{2-1/\ell}}{\log^{6\ell}x}=\frac{x^2}{\log^3 x}$$

and
(4.5)

$$R(x)=f_1(0)f_2(0)\frac{\varphi(\Delta)}{\Delta}\sum_{d|\Delta}\sum_{\substack{q'\leq Q/d\\(q',\Delta)=1}}\frac{\mu(q')^2}{q'\varphi(q')^2\varphi(d)}\sum_{(a,dq')=1}G(dq',-4a)e\left(\frac{4a\overline{q'}}{d}\right)+\mathcal{O}\left(\frac{x^2}{\log^3 x}\right)$$

In order to examine further the asymptotic formula for $R(x)$ we need to investigate the innermost sum in (4.5). Let us introduce a notation for it:

$$\varkappa(q)=\begin{cases}\sum_{(a,q)=1}G(q,-4a)e\left(\frac{4a\overline{q'}}{d}\right) & \text{for } q=dq'\,,(q',\Delta)=1\,,\mu(q')^2=1\,,\text{and } d\mid\Delta\,,\\ 0 & \text{otherwise}\,.\end{cases}$$

5 The sum $\varkappa(q)$

We can easily check that $\varkappa(q)$ is multiplicative function using Chinese remainder theorem. In particular, $\kappa(q'd)=\kappa(q')\kappa(d)$. Observe that because of the factor $\mu(q')^2$ in (4.5) we will have a contribution of 0 always when $q'\nmid\Delta$ and q' is not square-free. Thus for every $p\nmid\Delta$ we need to compute only $\varkappa(p)$, and for every $p^k\mid\Delta$ we will look at $\varkappa(p^k)$.

$\underline{p \nmid \Delta}$ Here p should be odd and

$$\begin{aligned}
\varkappa(p) &= \sum_{(a,p)=1} G(p,-4a) e\left(4a\overline{p}/1\right) = \sum_{(a,p)=1} \sum_{\substack{u(p)\\(u,p,\Delta)=1}} e\left(\frac{-4au^\ell}{p}\right) \\
&= \sum_{\substack{u(p)\\(u,(p,\Delta))=1}} \sum_{(a,p)=1} e\left(\frac{-4au^\ell}{p}\right) = \sum_{u(p)} \sum_{(a,p)=1} e\left(\frac{-4au^\ell}{p}\right) \\
&= \sum_{(u,p)=1} \sum_{(a,p)=1} e\left(\frac{-4au^\ell}{p}\right) + \sum_{(a,p)=1} e\left(-4ap^{\ell-1}\right) \\
&= \sum_{(u,p)=1} (-1) + \varphi(p) = -\varphi(p) + \varphi(p) = 0\,.
\end{aligned}$$

But then in (4.5) we actually have only $q' = 1$ and

$$R(x) = f_1(0) f_2(0) \frac{\varphi(\Delta)}{\Delta} \sum_{d|\Delta} \frac{\varkappa(d)}{\varphi(d)} + \mathcal{O}\left(\frac{x^2}{\log^3 x}\right). \tag{5.1}$$

When $d \mid \Delta$ we have

$$\begin{aligned}
\varkappa(d) &= \sum_{(a,d)=1} \sum_{\substack{u(d)\\(u,d,\Delta)=1}} e\left(\frac{-4au^\ell}{d}\right) e\left(\frac{4a}{d}\right) = \sum_{(a,d)=1} \sum_{(u,d)=1} e\left(\frac{-4au^\ell}{d}\right) e\left(\frac{4a}{d}\right) \\
&= \sum_{(a,d)=1} \sum_{(u,d)=1} e\left(\frac{-4a(u^\ell - 1)}{d}\right)
\end{aligned}$$

We introduce the notation

$$\rho(p^k) = \#\{u(p^k) : \, u^\ell \equiv 1 \pmod{p^k}\}\,.$$

We have the following

Lemma 5.1.

$$\rho(p^k) = (\ell, p-1)(\ell, p^{k-1}) \ \textit{if}\ p \neq 2\,,$$
$$\rho(2^k) = \begin{cases} 1 & , \ \textit{if}\ 2 \nmid \ell \\ (2\ell, 2^{k-1}) & , \ \textit{if}\ 2 \mid \ell\,. \end{cases}$$

Proof. See the discussion before Lemma 2.13 in §2.6, [8]. □

$\underline{p \mid \Delta\,, p \neq 2}$

$$\begin{aligned}
\sum_{(a,p)=1} \sum_{(u,p)=1} e\left(\frac{-4a(u^\ell-1)}{p}\right) &= \sum_{\substack{(u,p)=1\\u^\ell \equiv 1(p)}} \sum_{(a,p)=1} e\left(\frac{-4a(u^\ell-1)}{p}\right) \\
&\quad + \sum_{\substack{(u,p)=1\\u^\ell \not\equiv 1(p)}} \sum_{(a,p)=1} e\left(\frac{-4a(u^\ell-1)}{p}\right) \\
= \rho(p)\varphi(p) + (p - 1 - \rho(p))\,(-1) &= \rho(p)(p-1) - (p-1) + \rho(p) = p(\ell, p-1) - (p-1)
\end{aligned}$$

or

$$\varkappa(p) = p(\ell, p-1) - (p-1)\,. \tag{5.2}$$

<u>$p^k \mid \Delta\,, k \geq 2\,, p \nmid 2\ell$</u> If $p \nmid 2\ell$, we have $ord_p(4\ell) = s = 0$ and, as $k \geq 2$, from Lemma 3.7 it follows that $G(p^k, -4a) = 0$. Thus

$$\varkappa(p^k) = 0\,. \tag{5.3}$$

So further we assume that $s \geq 1$:

<u>$p^k \mid \Delta\,, k \geq 2\,, p \mid \ell\,, p \neq 2$</u> Here we have

$$\begin{aligned} \varkappa(p^k) &= \sum_{(u,p^k)=1} \sum_{(a,p^k)=1} e\left(\frac{-4a(u^\ell - 1)}{p^k}\right) = \sum_{\substack{(u,p^k)=1 \\ u^\ell \equiv 1 (p^k)}} \dots + \sum_{\substack{(u,p^k)=1 \\ u^\ell \not\equiv 1 (p^k)}} \cdots \\ &= \rho(p^k)\varphi(p^k) + \sum_{n=0}^{k-1} \sum_{\substack{(u,p^k)=1 \\ p^n \| u^\ell - 1}} \sum_{(a,p^k)=1} e\left(\frac{-4a(u^\ell - 1)}{p^k}\right)\,. \end{aligned}$$

Obviously $4(u^\ell - 1) = Up^n$ with some $p \nmid U$, and the inner sum becomes p^n copies of the Ramanujan sum regarding p^{k-n}(,i.e. $p^n\mu(p^{k-n})$). Therefore, as $\mu(p^{k-n}) = 0$ for $n \leq k-2$ and $\mu(p) = -1$, we have

$$\begin{aligned} \varkappa(p^k) &= \rho(p^k)\varphi(p^k) + \sum_{n=0}^{k-1} \sum_{\substack{(u,p^k)=1 \\ p^n \| u^\ell - 1}} p^n \mu(p^{k-n}) = \rho(p^k)\varphi(p^k) - p^{k-1} \sum_{\substack{(u,p^k)=1 \\ p^{k-1} \| u^\ell - 1}} 1 \\ &= \rho(p^k)\varphi(p^k) - p^{k-1}\left(p\rho(p^{k-1}) - \rho(p^k)\right) = \rho(p^k)p^{k-1}(p-1) - p^k\rho(p^{k-1}) \\ &\quad + p^{k-1}\rho(p^k) = p^k(\rho(p^k) - \rho(p^{k-1}))\,. \end{aligned}$$

After Lemma 5.1 in our case we have $\rho(p^k) = (\ell, p-1)(\ell, p^{k-1})$ and

$$\varkappa(p^k) = p^k(\ell, p-1)\left((\ell, p^{k-1}) - (\ell, p^{k-2})\right)\,.$$

Regard the case $2 \leq k \leq s+1$. Then $1 \leq k-1 \leq s = ord_p(4\ell)$ and as $p \neq 2$, we have $(\ell, p^{k-1}) = p^{k-1}$ and $(\ell, p^{k-2}) = p^{k-2}$. If $k \geq s+2$, then $k-2 \geq s$ and $(\ell, p^{k-2}) = (\ell, p^{k-1}) = p^s$. We combine the result in the considered case:

$$\varkappa(p^k) = \begin{cases} (\ell, p-1)(p^{2k-1} - p^{2k-2}) & \text{if } 2 \leq k \leq s+1\,, \\ 0 & \text{if } k \geq s+2\,. \end{cases} \tag{5.4}$$

$\underline{p=2}$ We will show that

$$\varkappa(2^k) = \begin{cases} 1 & \text{if}\, k=1\,, \\ 4 & \text{if}\, k=2\,, \\ 16 & \text{if}\, k=3\,, \\ 2^{2k-2} & \text{if}\, 4 \le k \le s+2\, \text{and}\, 2 \mid \ell, \\ 0 & \text{otherwise}\,, \end{cases} \tag{5.5}$$

where 'otherwise' means either $k \ge 4$ and $2 \nmid \ell$, or $k \ge s+3$ and $2 \mid \ell$.

Clearly $\varkappa(2) = 1$, $\varkappa(4) = 4$ and

$$\varkappa(8) = \sum_{(u,8)=1} \sum_{(a,8)=1} e\left(\frac{-4a(u^\ell - 1)}{8}\right) = \sum_{(u,8)=1} \sum_{(a,8)=1} e\left(\frac{-a(u^\ell - 1)}{2}\right) = 4.4 = 16\,.$$

For $k \ge 4$

$$\begin{aligned} \varkappa(2^k) &= \sum_{(u,2^k)=1} \sum_{(a,2^k)=1} e\left(\frac{-4a(u^\ell - 1)}{2^k}\right) = \sum_{(u,2^k)=1} \sum_{(a,2^k)=1} e\left(\frac{-a(u^\ell - 1)}{2^{k-2}}\right) \\ &= \sum_{\substack{(u,2^k)=1 \\ u^\ell \equiv 1 (2^{k-2})}} \ldots + \sum_{\substack{(u,2^k)=1 \\ u^\ell \not\equiv 1 (2^{k-2})}} \ldots \\ &= 2^2 \rho(2^{k-2}) \varphi(2^k) + \sum_{n=0}^{k-3} \sum_{\substack{(u,2^k)=1 \\ 2^n \| u^\ell - 1}} \sum_{(a,2^k)=1} e\left(\frac{a(u^\ell - 1)}{2^{k-2}}\right) \\ &= 4\rho(2^{k-2})\varphi(2^k) + \sum_{n=0}^{k-3} \sum_{\substack{(u,2^k)=1 \\ 2^n \| u^\ell - 1}} 2^{n+2} \mu(2^{k-2-n}) = 4\rho(2^{k-2})\varphi(2^k) - 2^{k-1} \sum_{\substack{(u,2^k)=1 \\ 2^{k-3} \| u^\ell - 1}} 1 \\ &= 4\rho(2^{k-2})\varphi(2^k) - 2^{k-1}\left(2^3\rho(2^{k-3}) - 2^2\rho(2^{k-2})\right)\,. \end{aligned}$$

According to Lemma 5.1 $\rho(2^k) = 1$ if $2 \nmid \ell$, so in this case $\varkappa(2^k) = 4\varphi(2^k) - 2^{k-1}(8-4) = 4.2^{k-1} - 2^{k-1}.4 = 0$.

If 2 divides ℓ we have $\rho(2^k) = (2\ell, 2^{k-1})$,so $\varkappa(2^k) = 4(2\ell, 2^{k-3}).2^{k-1} - 2^{k-1}\left(2^3(2\ell, 2^{k-4}) - 2^2(2\ell, 2^{k-3})\right)$. If $k-3 \le s-1$, then $(2\ell, 2^{k-3}) = 2^{k-3}$ because $2^{s-1} \mid 2\ell$ and $2^{k-3} \mid 2^{s-1}$. Similarly $(2\ell, 2^{k-4}) = 2^{k-4}$. Then $\varkappa(2^k) = 4.2^{k-3}.2^{k-1} - 2^{k-1}(2^3.2^{k-4} - 2^2.2^{k-3}) = 2^{2k-2}$.

If $k-3 > s-1$, then also $k-4 \ge s-1$ and $(2\ell, 2^{k-3}) = (2\ell, 2^{k-4}) = 2^{s-1}$. Then

$$\varkappa(2^k) = 2^2.2^{s-1}.2^{k-1} - 2^{k-1}(2^3.2^{s-1} - 2^2.2^{s-1}) = 0,$$

and finally this proves (5.5).

6 Proof of Theorem 1.3

Here we complete the proof of the main theorem. We need to compute the sum in (5.1). Let us use the shorter notation

$$\kappa = \sum_{d|\Delta} \frac{\varkappa(d)}{\varphi(d)}\,.$$

We only have to combine the results of (5.2), (5.3), (5.4) and (5.5). We get

$$\kappa = \prod_{\substack{p|\Delta \\ p\nmid 2\ell}} \left(1 + \frac{\varkappa(p)}{\varphi(p)}\right) \prod_{p|2\ell} \left(1 + \frac{\varkappa(p)}{\varphi(p)} + \frac{\varkappa(p^2)}{\varphi(p^2)} + \dots\right)\,.$$

The first product equals

$$\prod_{\substack{p|\Delta \\ p\nmid 2\ell}} \left(1 + \frac{p(\ell, p-1) - \varphi(p)}{\varphi(p)}\right) = \prod_{\substack{p|\Delta \\ p\nmid 2\ell}} \frac{p}{\varphi(p)}(\ell, p-1)\,.$$

According to the cases considered in §5 we split the other product into two factors

$$\prod_{p|2\ell} = \prod_{\substack{p|2\ell \\ p\neq 2}} \cdot \prod_{p=2} =: \Pi_1 \Pi_2\,.$$

For the first factor we have

$$\begin{aligned}
\Pi_1 &= \prod_{\substack{p|2\ell \\ p\neq 2}} \left(1 + \frac{p(\ell, p-1) - \varphi(p)}{\varphi(p)} + \sum_{k=2}^{s+1} \frac{(\ell, p-1)(p^{2k-1} - p^{2k-2})}{\varphi(p^k)}\right) \\
&= \prod_{\substack{p|2\ell \\ p\neq 2}} \left(\frac{p}{\varphi(p)}(\ell, p-1) + (\ell, p-1) \sum_{k=2}^{s+1} \frac{p^{2k-2}(p-1)}{p^{k-1}(p-1)}\right) \\
&= \prod_{\substack{p|2\ell \\ p\neq 2}} (\ell, p-1) \left(\frac{p}{\varphi(p)} + \sum_{k=2}^{s+1} p^{k-1}\right) \\
&= \prod_{\substack{p|2\ell \\ p\neq 2}} (\ell, p-1) \left(\frac{p}{\varphi(p)} + p\frac{p^s - 1}{p-1}\right) = \prod_{\substack{p|2\ell \\ p\neq 2}} (\ell, p-1) \left(\frac{p}{\varphi(p)} + \frac{p}{\varphi(p)}(p^s - 1)\right) \\
&= \prod_{\substack{p|2\ell \\ p\neq 2}} (\ell, p-1) \frac{p}{\varphi(p)} p^s
\end{aligned}$$

For $p = 2$ and $2 \nmid \ell$ the factor Π_2 is of the form $1 + 1/\varphi(2) + 4/\varphi(2^2) + 16/\varphi(2^3) = 1 + 1 + 2 + 4 = 8$. For $2 \mid \ell$ we have the factor

$$\begin{aligned}
\Pi_2 &= 1 + 1 + 2 + 4 + \sum_{k=4}^{s+2} \frac{2^{2k-2}}{\varphi(2^k)} = 8 + \sum_{k=4}^{s+2} 2^{k-1} \\
&= 8 + 8\sum_{k=4}^{s+2} 2^{k-4} = 8 + 8(2^{s-1} - 1) = 4.2^s
\end{aligned}$$

Notice that in any case we have

$$\Pi_2 = \frac{2}{\varphi(2)}(2,\ell)2^s\,,$$

because for $(2,\ell)=1$ we have $s = ord_2(4\ell) = 2$ and $2^s = 4$. Putting all these together we arrive at

$$\kappa = \frac{2}{\varphi(2)}(2,\ell)2^s \prod_{\substack{p|\Delta \\ p\nmid 2\ell}} \frac{p}{\varphi(p)}(\ell,p-1) \prod_{\substack{p|2\ell \\ p\neq 2}} \frac{p}{\varphi(p)}(\ell,p-1)p^s = 4\ell(2,\ell)\prod_{p|\Delta}\frac{p}{\varphi(p)}(\ell,p-1)\,.$$

Note that $\varphi(\Delta)/\Delta = \prod_{p|\Delta}\varphi(p)/p$ because for any $k \geq 2$ we have $\varphi(p^k)/p^k = p^{k-1}\varphi(p)/p^k = \varphi(p)/p$. That is why when we substitute the expression for κ we achieved above into (5.1), we get

$$\begin{aligned} R(x) &= f_1(0)f_2(0)\frac{\varphi(\Delta)}{\Delta}4\ell(2,\ell)\prod_{p|\Delta}\frac{p}{\varphi(p)}(\ell,p-1) + \mathcal{O}\left(\frac{x^2}{\log^3 x}\right) \\ &= 4\ell(2,\ell)\prod_{p|\Delta}(\ell,p-1)f_1(0)f_2(0) + \mathcal{O}\left(\frac{x^2}{\log^3 x}\right)\,. \end{aligned}$$

This completes the proof of Theorem 1.3.

Acknowledgments

I am grateful to Antal Balog for his suggestions how to simplify the present paper and for pointing out some inaccuracies. I am also indebted to my supervisor András Biró for the valuable regular discussions on my work.

References

[1] A. Balog and K. Ono, Elements of class groups and Shafarevich-Tate groups of elliptic curves, Duke Math. J. (2003), no.1, 35–63

[2] J. Brüdern, K. Kawada and T. D. Wooley, Additive representation in thin sequences, II: The binary Goldbach problem, Mathematica, 47(2000), no.1-2, 117–125

[3] D. Byeon, Sh. Lee, Divisibility of class numbers of imaginary quadratic fields whose discriminant has only two prime factors, Proc. Japan Acad., 84, Ser. A (2008), 8–10

[4] H. Davenport, Multiplicative Number Theory, Third Edition, Springer (2000)

[5] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford Univ. Press (New York, 1979)

[6] K. Lapkova, Class number one problem for real quadratic fields of certain type, to appear in Acta Arith.

[7] K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, J. London Math. Soc.(2), 61(2000),no.3, 681–690

[8] R. C. Vaughan, The Hardy-Littlewood Method, Cambridge Tracts in Math., 80, Cambridge Univ. Press (Cambridge, 1981)