THE LEAST INERT PRIME IN A REAL QUADRATIC FIELD

ENRIQUE TREVIÑO

ABSTRACT. In this paper, we prove that for any positive fundamental discriminant $D > 1596$, there is always at least one prime $p \leq D^{0.45}$ such that the Kronecker symbol $(D/p) = -1$. This improves a result of Granville, Mollin and Williams, where they showed that the least inert prime p in a real quadratic field of discriminant $D > 3705$ is at most $\sqrt{D}/2$. We use a "smoothed" version of the Pólya–Vinogradov inequality, which is very useful for numerically explicit estimates.

1. Introduction

In [6], Granville, Mollin and Williams prove the following theorem:

Theorem 1.1. *For any positive fundamental discriminant $D > 3705$, there is always at least one prime $p \leq \sqrt{D}/2$ such that the Kronecker symbol $(D/p) = -1$.*

Their proof consists of three parts. They verify the truth of the conjecture up to fairly large values of D computationally. They show using analytic methods that there are no counterexamples for $D > 10^{32}$ and they complete the proof using analytic methods combined with computation (what we'll refer to as the hybrid case).

Note that D is a fundamental discriminant if and only if either D is squarefree, $D \neq 1$, and $D \equiv 1 \pmod 4$ or $D = 4L$ with L squarefree and $L \equiv 2, 3 \pmod 4$. Since $(D/2) = -1$ for $D \equiv 5 \pmod 8$, we need only consider values of D such that $D = L \equiv 1 \pmod 8$ or $D = 4L$ with $L \equiv 2, 3 \pmod 4$.

For the computational aspect, they used the Manitoba Scalable Sieving Unit, a very powerful sieving machine (see [8] for more details). They ran the machine for a period of 5 months to produce three tables. From these tables the relevant information is the following:

If

(a) $L \equiv 1 \pmod 8$ with $(L/q) = 0$ or 1 for all odd $q \leq 257$,
(b) $L \equiv 2 \pmod 4$ with $(L/q) = 0$ or 1 for all odd $q \leq 283$, or
(c) $L \equiv 3 \pmod 4$ with $(L/q) = 0$ or 1 for all odd $q \leq 277$

then $L > 2.6 \times 10^{17}$.

From (a) we see that if D is odd and $D < 2.6 \times 10^{17}$ then there exists $q \leq 257$ for which $(D/q) = -1$, verifying the theorem for $D > 4(257)^2 = 264196$. From (b) and (c) we see that if D is even and $D = 4L < 4 \times 2.6 \times 10^{17} = 1.04 \times 10^{18}$ then there exists a $q \leq 283$ for which $(D/q) = -1$, verifying the theorem for

---

2000 *Mathematics Subject Classification.* Primary 11L40, 11Y40, 11R11.
Key words and phrases. Character Sums, Pólya–Vinogradov inequality, Quadratic fields.
This paper is essentially Chapter 3 of the author's Ph. D. Dissertation [16].

$D > 4(283)^2 = 320356$. Running a simple loop over all fundamental discriminants below 320356 we find that if we let

$$S = \{D| \text{ the least prime } p \text{ such that } (D/p) = -1 \text{ satisfies } p > \sqrt{D}/2\},$$

then

$$S = \{5, 8, 12, 13, 17, 24, 28, 33, 40, 57, 60, 73, 76, 88, 97, 105, 120, 124, 129, 136, 145, 156, 184, 204, 249, 280, 316, 345, 364, 385, 424, 456, 520, 561, 609, 616, 924, 940, 984, 1065, 1596, 2044, 3705\}.$$

We point out that in [6] they failed to mention that 120 and 561 are in S and they incorrectly claim $2244 \in S$ (note that 2244 is not a fundamental discriminant since $2244/4 = 561 \equiv 1 \pmod 4$)). Theorem 1.1 was first conjectured in Chapter 6 of [9] with a slightly different wording, focusing on the radicand instead of on the fundamental discriminant. When [6] translated radicands to discriminants there were mistakes; changing 561 to 2244 (this accounts for claiming $2244 \in S$ while neglecting that $561 \in S$) and we suspect that since $60 \in S$ they thought that the radicand 30 was already accounted for, therefore not including 120 in S.

For the analytical methods in the proof, i.e., to show that $D > 10^{32}$ works, the main tool in the paper is the Pólya–Vinogradov inequality. The Pólya–Vinogradov inequality states that there exists an absolute universal constant c such that for every character χ to the modulus q we have the inequality $\left|\sum_{n=M+1}^{M+N} \chi(n)\right| \leq c\sqrt{q}\log q$. This is the aspect on which we have been able to make some improvements by using the Smoothed Pólya–Vinogradov inequality, recently introduced by Levin, Pomerance, and Soundararajan [7].

To complete the proof, i.e., to show that when $D \leq 10^{32}$, $D > 2.6 \times 10^{17}$ works in the odd case and $D > 1.04 \times 10^{18}$ works in the even case, the authors combined the Pólya–Vinogradov inequality with computation. This aspect of their proof would not be needed if one uses the Smoothed Pólya–Vinogradov, however it is needed in our case to be able to improve their theorem.

In this paper we will prove

Theorem 1.2. *For any positive fundamental discriminant $D > 1596$, there is always at least one prime $p \leq D^{0.45}$ such that the Kronecker symbol $(D/p) = -1$.*

Note, that by using the tables provided in [6] the only even values of $D < 1.04 \times 10^{18}$ that can contradict the theorem satisfy $D < 283^{1/.45} < 280812$ and the only odd values of $D < 2.6 \times 10^{17}$ that can contradict the theorem satisfy $D < 257^{1/.45} < 226677$. Checking over all these values we find that the set of counterexamples S' is

$$S' = \{8, 12, 24, 28, 33, 40, 60, 105, 120, 156, 184, 204, 280, 364, 456, 520, 1596\}.$$

This set is sparser than S because for $D < 2^{20} = 1048576$, $\sqrt{D}/2$ is smaller than $D^{0.45}$.

In this paper, we are concerned with numerically explicit estimates. If we were interested in asymptotic results, then using the Burgess inequality (see [2]), it can be shown that the least inert prime in a real quadratic field of fundamental discriminant D is $\ll_\varepsilon D^{\frac{1}{4\sqrt{e}}+\varepsilon}$, where ε is a positive real number. We can do much better by assuming the extended Riemann Hypothesis, since in that case, Bach [1, Theorem

2, p. 372] proved that the least inert prime is at most $2(\log D)^2$. It is also worth pointing out that in this paper, we deal with the difficult case of D not necessarily being prime. If D were prime, then Norton [11] proved that the least inert prime is at most $3.9D^{1/4}\log D$, and the author [16] improved this to $0.9D^{1/4}\log D$.[1]

This paper is divided as follows: In section 2, we prove a slightly better smoothed Pólya–Vinogradov inequality, one that uses a little more information about the modulus of the character. This inequality will be key in our proof of Theorem 1.2. In section 3, we will prove many technical lemmas that will be used in the proof of the main theorem. In section 4 we prove the theorem for $D > 10^{24}$ and in the last section (section 5) we close the gap proving the theorem for $D > 10^{18}$ when D is even and $D > 10^{17}$ when D is odd.

2. Smoothed Pólya–Vinogradov

Theorem 2.1. *Let χ be a primitive character to the modulus $q > 1$, let M, N be real numbers with $0 < N \le q$. Then*

$$|S_\chi(M,N)| = \left|\sum_{M\le n\le M+2N} \chi(n)\left(1-\left|\frac{n-M}{N}-1\right|\right)\right| \le \frac{\phi(q)}{q}\sqrt{q} + 2^{(\omega(q)-1)}\frac{N}{\sqrt{q}}.$$

Proof. We follow the proof in [7]. Let

$$H(t) = \max\{0, 1-|t|\}.$$

We wish to estimate $|S_\chi(M,N)|$.
Using the identity (see Corollary 9.8 in [10])

$$\chi(n) = \frac{1}{\tau(\bar\chi)}\sum_{j=1}^{q}\bar\chi(j)e(nj/q),$$

where $e(x) := e^{2\pi i x}$ and $\tau(\chi) = \sum_{a=1}^{q}\chi(a)e(a/q)$ is the Gauss sum, we can deduce

$$S_\chi(M,N) = \frac{1}{\tau(\bar\chi)}\sum_{j=1}^{q}\bar\chi(j)\sum_{n\in\mathbb{Z}} e(nj/q)H\left(\frac{n-M}{N}-1\right).$$

The Fourier transform (see Appendix D in [10]) of H is

$$\widehat{H}(s) = \int_{-\infty}^{\infty} H(t)e(-st)dt = \frac{1-\cos 2\pi s}{2\pi^2 s^2} \text{ when } s\neq 0,\ \widehat{H}(0) = 1,$$

which is nonnegative for s real. In general, if $f(t) = e(\alpha t)H(\beta t+\gamma)$ with $\beta > 0$, then $\widehat{f}(s) = \frac{1}{\beta}e\left(\frac{s-\alpha}{\beta}\gamma\right)\widehat{H}\left(\frac{s-\alpha}{\beta}\right)$, using $\alpha = j/q$, $\beta = 1/N$ and $\gamma = -M/N-1$, then by Poisson summation we get

$$S_\chi(M,N) = \frac{N}{\tau(\bar\chi)}\sum_{j=1}^{q}\bar\chi(j)\sum_{n\in\mathbb{Z}} e\left(-(M+N)\left(n-\frac{j}{q}\right)\right)\widehat{H}\left(\left(n-\frac{j}{q}\right)N\right).$$

[1]Norton announced in [12] that he could prove that the least inert prime was at most $1.1D^{1/4}(\log D+4)$, but he did not prove it.

Using that if $(n,q)>1$ then $\chi(n)=0$, that $\widehat{H}$ is nonnegative and that $|\tau(\bar{\chi})|=\sqrt{q}$ for primitive characters, we have

$$\left|S_\chi(M,N)\right| \leq \frac{N}{\sqrt{q}} \sum_{\substack{j=1\\(j,q)=1}}^{q} \sum_{n\in\mathbb{Z}} \widehat{H}\left(\left(n-\frac{j}{q}\right)N\right) = \frac{N}{\sqrt{q}} \sum_{\substack{k\in\mathbb{Z}\\(k,q)=1}} \widehat{H}\left(\frac{kN}{q}\right).$$

Using inclusion-exclusion we get

$$|S_\chi(M,N)| \leq \frac{N}{\sqrt{q}} \sum_{d|q}\mu(d)\sum_{k\in\mathbb{Z}} \widehat{H}\left(\frac{kdN}{q}\right) = \sqrt{q}\sum_{d|q}\frac{\mu(d)}{d}\sum_{k\in\mathbb{Z}}\frac{dN}{q}\widehat{H}\left(\frac{kdN}{q}\right).$$

Since the Fourier transform of $H\left(\frac{qt}{Nd}\right)$ is $\frac{dN}{q}\widehat{H}\left(\frac{sdN}{q}\right)$, then by Poisson summation

(2.1)

$$\begin{aligned}
|S_\chi(M,N)| &\leq \sqrt{q}\sum_{d|q}\frac{\mu(d)}{d}\sum_{l\in\mathbb{Z}} H\left(\frac{ql}{Nd}\right) = \sqrt{q}\sum_{d|q}\frac{\mu(d)}{d}\left(1+2\sum_{1\leq l\leq \frac{Nd}{q}}\left(1-\frac{ql}{Nd}\right)\right)\\
&= \sqrt{q}\sum_{d|q}\frac{\mu(d)}{d} + 2\sqrt{q}\sum_{d|q}\frac{\mu(d)}{d}\sum_{1\leq l\leq \frac{Nd}{q}}\left(1-\frac{ql}{Nd}\right)\\
&= \frac{\phi(q)}{q}\sqrt{q} + 2\sqrt{q}\sum_{d|q}\frac{\mu(d)}{d}\sum_{1\leq l\leq \frac{Nd}{q}}\left(1-\frac{ql}{Nd}\right).
\end{aligned}$$

Note that for the last inner sum to be non-empty, $d\geq \frac{q}{N}$. Let's calculate the inner sum:

$$\sum_{1\leq l\leq \frac{Nd}{q}}\left(1-\frac{ql}{Nd}\right) = \left\lfloor\frac{Nd}{q}\right\rfloor\left(1-\frac{q}{2Nd}\left(\left\lfloor\frac{Nd}{q}\right\rfloor+1\right)\right).$$

Replacing $\left\lfloor\frac{Nd}{q}\right\rfloor$ with $\frac{Nd}{q}-\left\{\frac{Nd}{q}\right\}$ and multiplying through, we get:

$$\sum_{1\leq l\leq \frac{Nd}{q}}\left(1-\frac{ql}{Nd}\right) = \frac{Nd}{2q}-\frac{1}{2}+\frac{q}{2Nd}\left\{\frac{Nd}{q}\right\}\left(1-\left\{\frac{Nd}{q}\right\}\right). \tag{2.2}$$

Now,

$$\frac{q}{2Nd}\left\{\frac{Nd}{q}\right\}\left(1-\left\{\frac{Nd}{q}\right\}\right) \leq \frac{q}{8Nd} \leq \frac{1}{8}. \tag{2.3}$$

The last inequality follows from $d\geq\frac{q}{N}$. Combining (2.2) with (2.3) we get

$$0 \leq \sum_{l\leq\frac{Nd}{q}}\left(1-\frac{ql}{Nd}\right) < \frac{Nd}{2q}. \tag{2.4}$$

From (2.1) and (2.4) we get

$$\begin{aligned}
|S_\chi(M,N)| &< \frac{\phi(q)}{q}\sqrt{q} + 2\sqrt{q}\sum_{\substack{d|q\\ \mu(d)=1}}\frac{1}{d}\left(\frac{Nd}{2q}\right) \leq \frac{\phi(q)}{q}\sqrt{q} + \frac{N}{\sqrt{q}}\sum_{\substack{d|q\\ \mu(d)=1}} 1\\
&= \frac{\phi(q)}{q}\sqrt{q} + 2^{(\omega(q)-1)}\frac{N}{\sqrt{q}}.
\end{aligned}$$

□

3. Useful lemmas

We start by calculating a sum that pops up when dealing with the smoothed Pólya–Vinogradov inequality.

Lemma 3.1. *If x is a positive real number, then*

$$\sum_{n\le 2x}\left(1-\left|\frac{n}{x}-1\right|\right)=x-\frac{\|x\|^2}{x},$$

where $\|x\|$ is the distance from x to the nearest integer.

Proof. Let's work on the sum:

(3.1)

$$\begin{aligned}\sum_{n\le 2x}\left(1-\left|\frac{n}{x}-1\right|\right)&=\sum_{n\le x}\frac{n}{x}+\sum_{x<n\le 2x}\left(2-\frac{n}{x}\right)=\frac{2}{x}\sum_{n\le x}n-\frac{1}{x}\sum_{n\le 2x}n+2\lfloor 2x\rfloor-2\lfloor x\rfloor\\&=\frac{2}{x}\frac{\lfloor x\rfloor(\lfloor x\rfloor+1)}{2}-\frac{1}{x}\frac{\lfloor 2x\rfloor(\lfloor 2x\rfloor+1)}{2}+2\lfloor 2x\rfloor-2\lfloor x\rfloor\\&=\frac{\lfloor 2x\rfloor}{2x}\left(2x+\{2x\}-1\right)-\frac{\lfloor x\rfloor}{x}\left(x+\{x\}-1\right).\end{aligned}$$

Case 1: $\|x\|=\{x\}$. Then $\lfloor 2x\rfloor=2\lfloor x\rfloor$ and $\{2x\}=2\{x\}$. Using this and equation (3.1) we get

$$\begin{aligned}\sum_{n\le 2x}\left(1-\left|\frac{n}{x}-1\right|\right)&=\frac{\lfloor x\rfloor}{x}\left(2x+2\{x\}-1-x-\{x\}+1\right)\\&=\frac{\lfloor x\rfloor}{x}\left(x+\{x\}\right)=\frac{x^2-\{x\}^2}{x}=x-\frac{\|x\|^2}{x}.\end{aligned}$$

Case 2: $\|x\|=1-\{x\}$. Then $\lfloor 2x\rfloor=2\lfloor x\rfloor+1$ and $\{2x\}=2\{x\}-1$. Using this and equation (3.1) we get

$$\begin{aligned}\sum_{n\le 2x}\left(1-\left|\frac{n}{x}-1\right|\right)&=\frac{2\lfloor x\rfloor+1}{2x}\left(2x+2\{x\}-2\right)-\frac{\lfloor x\rfloor}{x}\left(x+\{x\}-1\right)\\&=\frac{\lfloor x\rfloor}{x}\left(x+\{x\}-1\right)+\frac{1}{2x}\left(2x+2\{x\}-2\right)=\frac{x+\{x\}-1}{x}\left(\lfloor x\rfloor+1\right)\\&=\frac{(x+(\{x\}-1))(x-(\{x\}-1))}{x}=\frac{x^2-(1-\{x\})^2}{x}=x-\frac{\|x\|^2}{x}.\end{aligned}$$

□

In the proof of the main theorem, we will need to consider the same sum but sieving out the numbers n that satisfy $\gcd(n,D)>1$. Therefore we prove the following result.

Lemma 3.2. *Let N be a positive real number and let D be a positive integer. Then*

$$\sum_{\substack{n\le 2N\\(n,D)=1}}\left(1-\left|\frac{n}{N}-1\right|\right)\ge\frac{\phi(D)}{D}N-2^{(\omega(D)-2)}.$$

Proof. Using Lemma 3.1,

(3.2)
$$\sum_{\substack{n\le 2N\\(n,D)=1}}\left(1-\left|\frac{n}{N}-1\right|\right)=\sum_{d|D}\mu(d)\sum_{n\le\frac{2N}{d}}\left(1-\left|\frac{nd}{N}-1\right|\right)=\sum_{d|D}\mu(d)\left(\frac{N}{d}-\frac{\|\frac{N}{d}\|^2}{\frac{N}{d}}\right)$$
$$=\sum_{d|D}\frac{\mu(d)}{d}N-\sum_{d|D}\mu(d)\frac{\|\frac{N}{d}\|^2}{\frac{N}{d}}=\frac{\phi(D)}{D}N-\sum_{d|D}\mu(d)\frac{\|\frac{N}{d}\|^2}{\frac{N}{d}}.$$

Now, since $\frac{\|\frac{N}{d}\|^2}{\frac{N}{d}}$ is nonnegative, we can bound the sum by summing over d such that $\mu(d)=1$. Also, if $d\ge 2N$ then $\|N/d\|=N/d$, so we can split it in two sums.

(3.3)
$$\sum_{d|D}\mu(d)\frac{\|\frac{N}{d}\|^2}{\frac{N}{d}}=\sum_{\substack{d\le 2N\\d|D}}\mu(d)\frac{\|\frac{N}{d}\|^2}{\frac{N}{d}}+\sum_{\substack{d>2N\\d|D}}\mu(d)\frac{N}{d}\le\sum_{\substack{d\le 2N\\d|D,\,\mu(d)=1}}\frac{d}{4N}+\sum_{\substack{d>2N\\d|D,\,\mu(d)=1}}\frac{N}{d}$$
$$\le\sum_{\substack{d\le 2N\\d|D,\,\mu(d)=1}}\frac{1}{2}+\sum_{\substack{d>2N\\d|D,\,\mu(d)=1}}\frac{1}{2}=\sum_{\substack{d|D\\\mu(d)=1}}\frac{1}{2}=2^{(\omega(D)-2)}.$$

Combining (3.2) and (3.3) we get the lemma.

□

The previous lemma has $2^{\omega(D)}$ in its error term, therefore it is useful to have explicit bounds on $2^{\omega(D)}$. We find such estimates in the following lemma.

Lemma 3.3. *Let D be a positive integer. Then $2^{\omega(D)}<4.8618\,D^{1/4}$. If $D>7.43\times10^{12}$ then $2^{\omega(D)}<2.4817\,D^{1/4}$. If $D>3.05\times10^{14}$, then $2^{\omega(D)}<1.9615\,D^{1/4}$. If $D>1.31\times10^{16}$ then $2^{\omega(D)}<1.532\,D^{1/4}$. Finally, if $D>3.26\times10^{19}$, then $2^{\omega(D)}<D^{1/4}$.*

Proof. Since 2^{ω} is multiplicative, we have
$$\frac{2^{\omega(D)}}{D^{1/4}}\le\prod_{p|D}\frac{2}{p^{1/4}}.$$
Since 13 is the last prime p with $p^{\frac14}<2$, then
$$\prod_{p|D}\frac{2}{p^{1/4}}\le\prod_{p\le 13}\frac{2}{p^{1/4}}\le 4.8618.$$
Let p_i be the i-th prime. Let $k\ge 6$ be an integer. Assume that
$$D\ge M(k):=\prod_{i=1}^{k}p_i.$$
We will show that
$$\frac{2^{\omega(D)}}{D^{1/4}}\le\prod_{i=1}^{k}\frac{2}{p_i}:=F(k). \tag{3.4}$$
This will yield the lemma, since $7.43\times10^{12}>M(12)$ and $F(12)>2.4817$. The other claims in the lemma coming from using $k=13$, $k=14$ and $k=16$, respectively.

Let's prove (3.4). We will do it in two cases, when $\omega(D) \le k$ and when $\omega(D) > k$. In the first case, we have

$$\frac{2^{\omega(D)}}{D^{1/4}} \le \frac{2^k}{M(k)^{1/4}} = F(k).$$

In the second case we have $\omega(D) > k$. Let $\omega(D) = r$. Since $M(r)$ is the smallest number with r distinct prime factors, we have that $D \ge M(r)$. Therefore

$$\frac{2^{\omega(D)}}{D^{1/4}} \le \frac{2^{\omega(M(r))}}{M(r)^{1/4}} = \left(\prod_{i=1}^{k} \frac{2}{p_i^{1/4}}\right)\left(\prod_{i=k+1}^{r} \frac{2}{p_i^{1/4}}\right) \le \left(\prod_{i=1}^{k} \frac{2}{p_i^{1/4}}\right).$$

The last inequality is true since $p_7^{1/4} > 2$, and $k+i \ge 7$ for $i = 1, 2, \ldots, r-k$. □

The proof of the main theorem also requires explicit estimates for the sum of primes. The following lemma (which is also of independent interest), gives lower and upper bounds on the sum of primes up to x.

Lemma 3.4. *For x a positive real number. If $x \ge a$ then there exist c_1 and c_2 depending on a such that*

$$\frac{x^2}{2\log x} + \frac{c_1 x^2}{\log^2 x} \le \sum_{p \le x} p \le \frac{x^2}{2\log x} + \frac{c_2 x^2}{\log^2 x}.$$

Table 1 gives us c_1 and c_2 for various values of a.

a	c_1	c_2
315437	0.205448	0.330479
468577	0.211359	0.32593
486377	0.212904	0.325537
644123	0.21429	0.322609
678407	0.214931	0.322326
758231	0.215541	0.321504
758711	0.215939	0.321489
10544111	0.239818	0.29251

TABLE 1. Bounds for the sum of primes.

Proof. To estimate the sum, we will use the very good estimates of $\theta(x)$ which can be found in Schoenfeld [14] and for the largest a we use an estimate of Dusart (see [4] and [5]). Let $x \ge a$, now let k_1 and k_2 satisfy

$$x - k_2\frac{x}{\log x} \le \theta(x) \le x + k_1\frac{x}{\log x}.$$

Table 2 has the values of k_1 and k_2 for different a and it also has a column for a constant C which will pop up later in the proof.

Now, let's work with the sum of primes using partial summation:

$$\sum_{p \le x} p = \sum_{p \le x} \log p \frac{p}{\log p} = \theta(x)\frac{x}{\log x} - \int_2^x \theta(t)\left(\frac{1}{\log t} - \frac{1}{\log^2 t}\right) dt.$$

For $x \geq a$	$\theta(x) \leq x + k_1 \frac{x}{\log x}$	$\theta(x) \geq x - k_2 \frac{x}{\log x}$	$\int_a^x \frac{t}{\log^3 t}\, dt \leq C \frac{x^2}{\log^2 x}$
a	k_1	k_2	C
315437	0.0201384	1/29	0.0371582
468577	0.0201384	1/35	0.0360657
486377	0.0201384	1/37	0.0359661
644123	0.0201384	1/39	0.0352333
678407	0.0201384	1/40	0.0351014
758231	0.0201384	1/41	0.0348216
758711	0.0201384	0.0239922	0.03482
10544111	0.006788	0.006788	0.0293063

TABLE 2. Bounds for $\theta(x)$

Then we can expand and get

$$\begin{aligned}(3.5)\quad \sum_{p \leq x} p &= \frac{\theta(x)x}{\log x} - \int_2^x \frac{\theta(t)}{\log t}\, dt + \int_2^x \frac{\theta(t)}{\log^2 t}\, dt \\ &= \frac{\theta(x)x}{\log x} - \int_2^a \frac{\theta(t)}{\log t}\, dt + \int_2^a \frac{\theta(t)}{\log^2 t}\, dt - \int_a^x \frac{\theta(t)}{\log t}\, dt + \int_a^x \frac{\theta(t)}{\log^2 t}\, dt.\end{aligned}$$

Now using this equation, we will work out an upper bound and then a lower bound.

Let's proceed with the upper bound. We start by pointing out that for $x \geq a$, we have

$$(3.6)\qquad \frac{\theta(x)x}{\log x} \leq \frac{x^2}{\log x} + \frac{k_1 x^2}{\log^2 x}.$$

Then we have

$$(3.7)\qquad -\int_a^x \frac{\theta(t)}{\log t}\, dt \leq -\int_a^x \frac{t - \frac{k_2 t}{\log t}}{\log t}\, dt = -\int_a^x \frac{t}{\log t}\, dt + k_2 \int_a^x \frac{t}{\log^2 t}\, dt.$$

We also have

$$(3.8)\qquad \int_a^x \frac{\theta(t)}{\log^2 t}\, dt \leq \int_a^x \frac{t}{\log^2 t}\, dt + k_1 \int_a^x \frac{t}{\log^3 t}\, dt.$$

By using integration by parts we get

$$(3.9)\qquad \int_a^x \frac{t}{\log t}\, dt = \frac{x^2}{2\log x} - \frac{a^2}{2\log a} + \int_a^x \frac{t}{2\log^2 t}\, dt,$$

and

$$(3.10)\qquad \int_a^x \frac{t}{\log^2 t}\, dt = \frac{x^2}{2\log^2 x} - \frac{a^2}{2\log^2 a} + \int_a^x \frac{t}{\log^3 t}\, dt.$$

Using (3.6), (3.7) and (3.8) on (3.5) yields

$$\begin{aligned}\sum_{p \leq x} p \leq \frac{x^2}{\log x} &+ \frac{k_1 x^2}{\log^2 x} - \int_2^a \frac{\theta(t)}{\log t}\, dt + \int_2^a \frac{\theta(t)}{\log^2 t}\, dt \\ &- \int_a^x \frac{t}{\log t}\, dt + (1 + k_2) \int_a^x \frac{t}{\log^2 t}\, dt + k_1 \int_a^x \frac{t}{\log^3 t}\, dt.\end{aligned}$$

Now, using (3.9) we get

$$\sum_{p\le x} p \le \frac{x^2}{\log x} + \frac{k_1x^2}{\log^2 x} - \int_2^a \frac{\theta(t)}{\log t}\,dt + \int_2^a \frac{\theta(t)}{\log^2 t}\,dt - \frac{x^2}{2\log x} + \frac{a^2}{2\log a} - \int_a^x \frac{t}{2\log^2 t}\,dt + (1+k_2)\int_a^x \frac{t}{\log^2 t}\,dt + k_1\int_a^x \frac{t}{\log^3 t}\,dt.$$

By simplifying and then using (3.10) we get that the right hand side equals

$$\frac{x^2}{2\log x} + \frac{k_1x^2}{\log^2 x} - \int_2^a \frac{\theta(t)}{\log t}\,dt + \int_2^a \frac{\theta(t)}{\log^2 t}\,dt + \frac{a^2}{2\log a} + \left(\frac{1}{2}+k_2\right)\left(\frac{x^2}{2\log^2 x} - \frac{a^2}{2\log^2 a} + \int_a^x \frac{t}{\log^3 t}\,dt\right) + k_1\int_a^x \frac{t}{\log^3 t}\,dt.$$

By rearranging further we get that this equals

$$\frac{x^2}{2\log x} + \left(\frac{1}{4}+k_1+\frac{k_2}{2}\right)\frac{x^2}{\log^2 x} - \int_2^a \frac{\theta(t)}{\log t}\,dt + \int_2^a \frac{\theta(t)}{\log^2 t}\,dt + \frac{a^2}{2\log a} - \left(\frac{1}{2}+k_2\right)\frac{a^2}{2\log^2 a} + \left(\frac{1}{2}+k_1+k_2\right)\int_a^x \frac{t}{\log^3 t}\,dt.$$

Now, $\int_2^a \frac{\theta(t)}{\log t}\,dt$, $\int_2^a \frac{\theta(t)}{\log^2 t}\,dt$ and $\int_2^a \frac{t}{\log^3 t}\,dt$ are constant. Also, $\int_a^x \frac{t}{\log^3 t}\,dt = o\left(x^2/(\log^2 x)\right)$ and hence, we can then find a constant C (see Table 2) such that

$$\frac{\int_a^x \frac{t}{\log^3 t}\,dt}{\frac{x^2}{\log^2 x}} \le C.$$

Therefore, for $x \ge a$, we have

$$\sum_{p\le x} p \le \frac{x^2}{2\log x} + \left(\frac{1}{4}+k_1+\frac{k_2}{2}+\left(\frac{1}{2}+k_1+k_2\right)C + A\right)\frac{x^2}{\log^2 x},$$

where

$$A = \max\left\{0, \frac{\int_2^a \frac{\theta(t)}{\log^2 t}\,dt - \int_2^a \frac{\theta(t)}{\log t}\,dt + \frac{a^2}{2\log a} - \left(\frac{1}{2}+k_2\right)\frac{a^2}{2\log^2 a}}{\frac{a^2}{\log^2 a}}\right\}.$$

We can now plug it into a calculator and get the third column in Table 1. This completes our work for the upper bound.

It is time to work on the lower bound. We proceed in the same way. In fact, every time you see a k_1 in the previous inequalities, you may replace it by $-k_2$ and vice versa. You would also replace the $\le$ symbol with $\ge$. After doing this, we reach the following inequality:

$$\sum_{p\le x} p \ge \frac{x^2}{2\log x} + \left(\frac{1}{4}-k_2-\frac{k_1}{2}\right)\frac{x^2}{\log^2 x} - \int_2^a \frac{\theta(t)}{\log t}\,dt + \int_2^a \frac{\theta(t)}{\log^2 t}\,dt + \frac{a^2}{2\log a} - \left(\frac{1}{4}-\frac{k_1}{2}\right)\frac{a^2}{\log^2 a} + \left(\frac{1}{2}-k_1-k_2\right)\int_a^x \frac{t}{\log^3 t}\,dt.$$

Working with the constant in the lower bound is a bit trickier than in the upper bound because we have to consider whether $\left(\frac{1}{2}-k_1-k_2\right)$ is positive or negative. In the case it is negative, we replace the integral with C, in the case it is positive we replace it with 0. Note that the expression is positive when $x \geq 599$ and it is negative when $x < 599$.

Therefore, we have two cases, for $x \geq a$ with $a < 599$ we have

$$\sum_{p \leq x} p \leq \frac{x^2}{2\log x} + \left(\frac{1}{4} - k_2 - \frac{k_1}{2} + \left(\frac{1}{2} - k_1 - k_2\right) C + A\right) \frac{x^2}{\log^2 x},$$

and for $a \geq 599$ we have

$$\sum_{p \leq x} p \leq \frac{x^2}{2\log x} + \left(\frac{1}{4} - k_2 - \frac{k_1}{2} + A\right) \frac{x^2}{\log^2 x},$$

where

$$A = \min\left\{0, \frac{\int_2^a \frac{\theta(t)}{\log^2 t}\,dt - \int_2^a \frac{\theta(t)}{\log t}\,dt + \frac{a^2}{2\log a} - \left(\frac{1}{2} - k_1\right)\frac{a^2}{2\log^2 a}}{\frac{a^2}{\log^2 a}}\right\}.$$

After plugging the numbers in the calculator we get the desired results, completing the lemma. □

Corollary 1. For x, y real numbers such that $x > y$. For $y \geq a$, there exist c_1 and c_2 depending on a such that

$$\frac{1}{2}\left(\frac{x^2}{\log x} - \frac{y^2}{\log y}\right) + \frac{c_1 x^2}{\log^2 x} - \frac{c_2 y^2}{\log^2 y} \leq \sum_{y < p \leq x} p \leq \frac{1}{2}\left(\frac{x^2}{\log x} - \frac{y^2}{\log y}\right) + \frac{c_2 x^2}{\log^2 x} - \frac{c_1 y^2}{\log^2 y}.$$

The values of c_1 and c_2 can be found in the table for Lemma 3.4.

Proof. It easily follows from the lemma once we write $\sum_{y<p\leq x} p = \sum_{p \leq x} p - \sum_{p \leq y} p$. □

Using the estimates on the sum of primes, we can then use these to estimate the sum which comes up in the proof of the main theorem. We do this in the following lemma.

Lemma 3.5. *Let $B \geq 315487$ and N be positive real numbers. For $n \leq \frac{2N}{B}$ a natural number we have the following inequality:*

$$\sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \leq \frac{N}{n \log B}.$$

Proof. If $n \leq \frac{N}{B}$ then

$$\sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) = \sum_{B < p \leq \frac{N}{n}} \frac{np}{N} + \sum_{\frac{N}{n} < p \leq \frac{2N}{n}} \left(2 - \frac{np}{N}\right), \tag{3.11}$$

and if $n > \frac{N}{B}$ then

$$\sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) = \sum_{B < p \leq \frac{2N}{n}} \left(2 - \frac{np}{N}\right) \leq \sum_{\frac{N}{n} < p \leq \frac{2N}{n}} \left(2 - \frac{np}{N}\right). \tag{3.12}$$

Since both sums require the bounding of $\sum_{\frac{N}{n} < p \leq \frac{2N}{n}} \left(2 - \frac{np}{N}\right)$, we'll estimate this first.

Dusart (see [4, Theorem 14, p.22] or [5, Theorem 6, p.57]) proved that for $x > 1$, $\pi(2x) - \pi(x) \leq \frac{x}{\log x}$. Combining that with Corollary 1 we have

$$\begin{aligned}(3.13)\qquad \sum_{\frac{N}{n}<p\leq\frac{2N}{n}} \left(2 - \frac{np}{N}\right) &= 2\left(\pi\left(\frac{2N}{n}\right) - \pi\left(\frac{N}{n}\right)\right) - \frac{n}{N}\sum_{\frac{N}{n}<p\leq\frac{2N}{n}} p \\ &\leq \frac{2N}{n\log\frac{N}{n}} - \frac{n}{N}\left(\frac{2N^2}{n^2\log\left(\frac{2N}{n}\right)} - \frac{N^2}{2n^2\log\left(\frac{N}{n}\right)} + \frac{4c_1N^2}{n^2\log^2\left(\frac{2N}{n}\right)} - \frac{c_2N^2}{n^2\log^2\left(\frac{N}{n}\right)}\right) \\ &= \frac{2N}{n\log\left(\frac{N}{n}\right)} - \frac{2N}{n\log\left(\frac{2N}{n}\right)} + \frac{N}{2n\log\left(\frac{N}{n}\right)} - \frac{4c_1N}{n\log^2\left(\frac{2N}{n}\right)} + \frac{c_2N}{n\log^2\left(\frac{N}{n}\right)},\end{aligned}$$

where c_1 and c_2 come from Table 1 in Lemma 3.4. Since

$$\frac{2N}{n\log\left(\frac{N}{n}\right)} - \frac{2N}{n\log\left(\frac{2N}{n}\right)} = \frac{(\log 4)N}{n\log\left(\frac{N}{n}\right)\log\left(\frac{2N}{n}\right)},$$

then the right hand side of (3.13) becomes

$$\frac{N}{2n\log\left(\frac{N}{n}\right)} + \frac{(\log 4)N}{n\log\left(\frac{N}{n}\right)\log\left(\frac{2N}{n}\right)} + \frac{c_2N}{n\log^2\left(\frac{N}{n}\right)} - \frac{4c_1N}{n\log^2\left(\frac{2N}{n}\right)}$$

which equals

$$(3.14)\qquad \frac{N}{2n\log\left(\frac{N}{n}\right)} + \frac{N}{n\log^2\left(\frac{N}{n}\right)}f(N,n),$$

where

$$f(N,n) = c_2 + (\log 4)\left(\frac{\log\left(\frac{N}{n}\right)}{\log\left(\frac{2N}{n}\right)}\right) - 4c_1\left(\frac{\log\left(\frac{N}{n}\right)}{\log\left(\frac{2N}{n}\right)}\right)^2.$$

Since $\log x/\log 2x$ is an increasing function for $x > 0$ and $\frac{\log x}{\log 2x} < 1$, then we can bound $f(N,n)$ by replacing the fraction with 1 in the positive term and by picking the smallest possible value of $\frac{N}{n}$ in the negative part. Since $n \leq \frac{2N}{B}$, then we have that $\frac{N}{n} \geq \frac{B}{2}$. Therefore

$$f(N,n) \leq c_2 + \log 4 - 4c_1\left(\frac{\log\left(\frac{B}{2}\right)}{\log B}\right)^2.$$

Using Lemma 3.4, for $B \geq 315487$, we have $c_1 = 0.205448$ and $c_2 = 0.330479$ and together with $\frac{N}{n} \geq \frac{B}{2}$ we get that $f(N,n) \leq 1$ yielding

$$(3.15)\qquad \sum_{\frac{N}{n}<p\leq\frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \leq \frac{N}{2n\log\left(\frac{N}{n}\right)} + \frac{N}{n\log^2\left(\frac{N}{n}\right)}.$$

To complete the estimate we care about, we must now bound $\frac{n}{N}\sum_{B<p\leq\frac{N}{n}} p$. We can do this by using Corollary 1:

$$\begin{aligned}\frac{n}{N}\sum_{B<p\leq\frac{N}{n}} p &\leq \frac{n}{N}\left(\frac{N^2}{2n^2\log\left(\frac{N}{n}\right)} - \frac{B^2}{2\log B} + \frac{c_2N^2}{n^2\log^2\left(\frac{N}{n}\right)} - \frac{c_1B^2}{\log^2 B}\right) \\ (3.16)\qquad &= \frac{N}{2n\log\left(\frac{N}{n}\right)} + \frac{c_2N}{n\log^2\left(\frac{N}{n}\right)} - \frac{c_1nB^2}{N\log^2 B} - \frac{nB^2}{2N\log B}.\end{aligned}$$

Now, for $n \le \frac{N}{B}$, by (3.11) and using the estimates of (3.15) and (3.16) we have

$$\sum_{B<p\le \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \le \frac{N}{n\log\left(\frac{N}{n}\right)} + \frac{(1+c_2)N}{n\log^2\left(\frac{N}{n}\right)} - \frac{c_1 nB^2}{N\log^2 B} - \frac{nB^2}{2N\log B}.$$

We want to prove that this is $\le \frac{N}{n\log B}$. We note that $\frac{N}{n\log B} - \frac{N}{n\log\left(\frac{N}{n}\right)} = \frac{N\log\left(\frac{N}{nB}\right)}{n\log B\log\left(\frac{N}{n}\right)}$, so what we want is

$$\frac{N\log\left(\frac{N}{nB}\right)}{n\log B\log\left(\frac{N}{n}\right)} + \frac{c_1 nB^2}{N\log^2 B} + \frac{nB^2}{2N\log B} \ge \frac{(1+c_2)N}{n\log^2\left(\frac{N}{n}\right)}.$$

After making the substition of $\frac{N}{n} = Bk$ we have that we want

$$\frac{Bk\log k}{\log B\log Bk} + \frac{c_1 B}{k\log^2 B} + \frac{B}{2k\log B} \ge \frac{(1+c_2)Bk}{\log^2 Bk}.$$

We can divide the whole inequality by B and multiply by $\log^2 Bk$, so we get

$$k\log k\frac{\log Bk}{\log B} + \frac{c_1}{k}\left(\frac{\log Bk}{\log B}\right)^2 + \frac{\log^2 Bk}{2k\log B} \ge (1+c_2)k.$$

For $k \ge 4$, using that for $B \ge 315487$, $c_2 = 0.330479$ we have

$$k\log k\frac{\log Bk}{\log B} + \frac{c_1}{k}\left(\frac{\log Bk}{\log B}\right)^2 + \frac{\log^2 Bk}{2k\log B} \ge k\log k \ge (1+c_2)k.$$

And for $1 \le k < 4$ using that $B \ge 315487$ we have

$$k\log k\frac{\log Bk}{\log B} + \frac{c_1}{k}\left(\frac{\log Bk}{\log B}\right)^2 + \frac{\log^2 Bk}{2k\log B} \ge k\log k + \frac{c_1}{k} + \frac{\log 315487}{2k} \ge (1+c_2)k.$$

This completes the proof of the lemma when $n \le \frac{N}{B}$.

For $n > \frac{N}{B}$, using (3.12) and (3.15) we have

$$\sum_{B<p\le \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \le \frac{N}{2n\log\left(\frac{N}{n}\right)} + \frac{N}{n\log^2\left(\frac{N}{n}\right)}.$$

Now using that $\frac{N}{B} < n \le \frac{2N}{B}$ we have that $\frac{B}{2} \le \frac{N}{n} \le B$. Using this we have

$$\frac{N}{n\log B} - \frac{N}{2n\log\left(\frac{N}{n}\right)} = \frac{N\log\left(\frac{N^2}{n^2 B}\right)}{2n\log B\log\left(\frac{N}{n}\right)} \ge \frac{N\log\left(\frac{B}{4}\right)}{2n\log B\log B}, \tag{3.17}$$

and

$$\frac{N}{n\log^2\left(\frac{N}{n}\right)} \le \frac{N}{n\log^2\left(\frac{B}{2}\right)}. \tag{3.18}$$

For $B \ge 73$ we have $\log(B/4)\log^2(B/2) \ge 2\log^2 B$ and hence from combining the inequalities (3.17) and (3.18) we get

$$\frac{N}{n\log B} - \frac{N}{2n\log\left(\frac{N}{n}\right)} \ge \frac{N}{n\log^2\left(\frac{N}{n}\right)},$$

completing the proof that for $n > \frac{N}{B}$

$$\sum_{B<p\le \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \le \frac{N}{n\log B}.$$

□

During the proof of the main theorem, one of the problems that arises comes from bounding

$$\frac{D}{\phi(D)} \sum_{\substack{n\leq x\\(n,D)=1}} \frac{1}{n}.$$

The difficulty is that when D has many prime factors $\frac{D}{\phi(D)}$ is big while the other factor is small. And if D has few prime factors we have the opposite situation. The following lemma allows us to simplify this situation by showing that we can reduce it to considering D having many small prime factors.

Lemma 3.6. *Let $M = \prod_{p\leq x} p$. For a positive integer D, let k be the positive integer that satisfies that $(D, M) = M/k$. Then*

$$\sum_{\substack{n\leq x\\(n,D)=1}} \frac{1}{n} \leq \frac{k}{\phi(k)}.$$

Proof. Note that if $n \leq x$ and $(n, D) = 1$ then any prime p that divides n also divides k. Therefore

$$\sum_{\substack{n\leq x\\(n,D)=1}} \frac{1}{n} \leq \prod_{p|k} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) = \prod_{p|k} \frac{p}{p-1} = \prod_{p|k} \frac{p}{\phi(p)} = \frac{k}{\phi(k)}.$$

□

The following lemma combines Lemmas 3.5 and 3.6 to give us the result we need in the proof of the main theorem.

Lemma 3.7. *For B and N positive real numbers and D a positive integer. Let $M = \prod_{p\leq \frac{2N}{B}} p$ and k be a positive integer such that $(D, M) = \frac{M}{k}$. Then, we have*

$$\sum_{B<p\leq 2N} \sum_{\substack{n\leq \frac{2N}{p}\\(n,D)=1}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \leq \frac{k}{\phi(k)} \frac{N}{\log B}.$$

Proof. Exchanging order of summation we get:

$$\sum_{B<p\leq 2N} \sum_{\substack{n\leq \frac{2N}{p}\\(n,D)=1}} \left(1 - \left|\frac{np}{N} - 1\right|\right) = \sum_{\substack{n\leq \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right).$$

The inner sum can be dealt with using Lemma 3.5 and then we will use Lemma 3.6 for the outer sum:

$$\sum_{\substack{n\leq \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \leq \sum_{\substack{n\leq \frac{2N}{B}\\(n,D)=1}} \frac{N}{n\log B} \leq \frac{k}{\phi(k)} \frac{N}{\log B}.$$

□

Finally, we end the section with an explicit estimate concerning the ratio $\frac{D}{\phi(D)}$ that will be needed in the proof of the main theorem.

Lemma 3.8. *For D a positive integer greater than $6 \cdot 10^{12}$ we have*

$$\frac{D}{\phi(D)} < 2 \log\log D.$$

Proof. Rosser and Schoenfeld [13] proved that for $D > 223092870$ the following inequality is true:

$$\frac{D}{\phi(D)} \leq e^{\gamma} \log\log D + \frac{2.5}{\log\log D}.$$

Therefore, $D/\phi(D) \leq 2\log\log D$ for $D > 6 \cdot 10^{12}$. □

4. Proof of the Theorem when $D > 10^{24}$

Theorem 4.1. *For D a fundamental discriminant larger than 10^{24} there exists a prime $p \leq D^{0.45}$ such that $\left(\frac{D}{p}\right) = -1$*

Proof. Assume to the contrary that no such p exists. Let $\chi(p) = \left(\frac{D}{p}\right)$. Since D is a fundamental discriminant, χ is a primitive character mod D.

Consider

$$S_{\chi}(N) = \sum_{n \leq 2N} \chi(n) \left(1 - \left|\frac{n}{N} - 1\right|\right).$$

By Theorem 2.1, we have

$$|S_{\chi}(N)| \leq \frac{\phi(D)}{D}\sqrt{D} + 2^{(\omega(D)-1)} \frac{N}{\sqrt{D}}. \tag{4.1}$$

However, using our assumption that $\chi(p) \neq -1$ for $p \leq D^{0.45} = B$ we can calculate $S_{\chi}(N)$ by separating the sum into $\chi(n) = 1, 0$ and -1. To account for $\chi(n) = 0$ we sum over the numbers relatively prime to D. The following is true when $B^2 > 2N$: In view of (2.1) of [6],

$$S_{\chi}(N) = \sum_{\substack{n \leq 2N \\ (n,D)=1}} \left(1 - \left|\frac{n}{N} - 1\right|\right) - 2 \sum_{\substack{B < p \leq 2N \\ \chi(p)=-1}} \sum_{\substack{n \leq \frac{2N}{p} \\ (n,D)=1}} \left(1 - \left|\frac{np}{N} - 1\right|\right). \tag{4.2}$$

Using Lemma 3.2 and (4.1), (4.2) we get

$$\frac{\phi(D)}{D}\sqrt{D} + 2^{(\omega(D)-1)} \frac{N}{\sqrt{D}} \geq \frac{\phi(D)}{D} N - 2^{(\omega(D)-2)} - 2 \sum_{\substack{n \leq \frac{2N}{B} \\ (n,D)=1}} \sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right). \tag{4.3}$$

Now, letting $N = c\sqrt{D}$ for some constant c we get that the inequality in (4.3) is equivalent to

$$0 \geq c - 1 - 2^{\omega(D)} \left(\frac{c}{2} + \frac{1}{4}\right) \frac{D}{\phi(D)\sqrt{D}} - \frac{2}{\sqrt{D}} \frac{D}{\phi(D)} \sum_{\substack{n \leq \frac{2N}{B} \\ (n,D)=1}} \sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right). \tag{4.4}$$

Using Lemma 3.7 we get that if $M = \prod_{p \leq \frac{2N}{B}} p$ and $(D, M) = \frac{M}{k}$ then

$$\sum_{\substack{n \leq \frac{2N}{B} \\ (n,D)=1}} \sum_{B < p \leq \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right) \leq \frac{N}{\log B} \frac{k}{\phi(k)} = \frac{c\sqrt{D}}{\log B} \frac{k}{\phi(k)}.$$

Therefore (4.4) becomes

$$0 \geq c - 1 - 2^{\omega(D)} \left(\frac{c}{2} + \frac{1}{4}\right) \frac{D}{\phi(D)\sqrt{D}} - \frac{2c}{\log B} \frac{D}{\phi(D)} \frac{k}{\phi(k)}. \tag{4.5}$$

Using Corollary 1 of Theorem 8 in [13], we get

$$\frac{D}{\phi(D)} \frac{k}{\phi(k)} = \prod_{p \leq \frac{2N}{B}} \frac{p}{p-1} \prod_{\substack{p > \frac{2N}{B} \\ p|D}} \frac{p}{p-1} \leq e^{\gamma} \left(1 + \frac{1}{\log^2\left(\frac{2N}{B}\right)}\right) \log\left(\frac{2N}{B}\right) \prod_{\substack{p > \frac{2N}{B} \\ p|D}} \frac{p}{p-1}.$$

Combining this with (4.5) yields

$$\begin{aligned} 0 \geq\ & c - 1 - 2^{\omega(D)} \left(\frac{c}{2} + \frac{1}{4}\right) \frac{D}{\phi(D)\sqrt{D}} \\ & - \frac{2c}{\log B} e^{\gamma} \left(1 + \frac{1}{\log^2\left(\frac{2N}{B}\right)}\right) \log\left(\frac{2N}{B}\right) \prod_{\substack{p > \frac{2N}{B} \\ p|D}} \frac{p}{p-1}. \end{aligned} \tag{4.6}$$

Now, let's pick $c = 8$. Now, D has at most 19 primes bigger than $\frac{2N}{B} = 16D^{0.05}$ dividing it. We have that $\frac{2N}{B} > 253$ and the product of $\frac{p}{p-1}$ for the first 19 primes bigger than 253 is smaller than 1.0642. We also have that for $D > 3.26 \times 10^{19}$, $2^{\omega(D)} < D^{1/4}$ by Lemma 3.3. Also, for $D > 10^{13}$ we have $\frac{D}{\phi(D)} < 2 \log\log D$ (Lemma 3.8). Combining these facts with (4.6) we get the inequality:

$$0 \geq 7 - 8.5 \frac{\log\log D}{D^{1/4}} - \frac{16}{\log B} e^{\gamma} \left(1 + \frac{1}{\log^2\left(\frac{2N}{B}\right)}\right) \log\left(\frac{2N}{B}\right) 1.0642. \tag{4.7}$$

If we let $B = D^{0.45}$, then $\frac{2N}{B} = 16D^{0.05}$ and the right hand side of (4.7) is $0.028836\ldots$ at $D = 10^{24}$. Since as D increases, the right hand side increases and at $D = 10^{24}$ it is already positive, we have arrived at a contradiction for all $D \geq 10^{24}$. $\square$

Remark 4.2. This proof with a few modifications would yield that for D a fundamental discriminant larger than 10^{16}, there exists a prime $p \leq \sqrt{D}/2$ such that $\left(\frac{D}{p}\right) = -1$. This gives us a proof of Theorem 1.1 without the need of the hybrid case.

5. Proof the theorem when $D \leq 10^{24}$

Theorem 5.1. *For D a fundamental discriminant such that $1596 < D \leq 10^{24}$, there exists a prime p such that $p < D^{0.45}$ and $\left(\frac{D}{p}\right) = -1$.*

Proof. Assume to the contrary that no such p exists. Following the same steps as in the proof of Theorem 4.1 we reach (4.4):

$$0 \geq c - 1 - 2^{\omega(D)}\left(\frac{c}{2}+\frac{1}{4}\right)\frac{D}{\phi(D)\sqrt{D}} - \frac{2}{\sqrt{D}}\frac{D}{\phi(D)}\sum_{\substack{n\leq \frac{2N}{B}\\(n,D)=1}}\sum_{B<p\leq\frac{2N}{n}}\left(1-\left|\frac{np}{N}-1\right|\right).$$

From the proof of Lemma 3.5 we can get tighter inequalities for the inner sum in the double sum above. If we combine (3.14) and (3.16) we get: For $n \leq \frac{N}{B}$

$$\sum_{B<p\leq\frac{2N}{n}}\left(1-\left|\frac{np}{N}-1\right|\right)$$
$$\leq \frac{N}{n\log\left(\frac{N}{n}\right)} + \frac{(f(N,n)+c_2)N}{n\log^2\left(\frac{N}{n}\right)} - \frac{c_1 nB^2}{N\log^2 B} - \frac{nB^2}{2N\log B} = g_1(N,n,B,c_1,c_2),$$

where c_1 and c_2 come from Table 1 in Lemma 3.4 and

$$f(N,n) = c_2 + (\log 4)\left(\frac{\log\left(\frac{N}{n}\right)}{\log\left(\frac{2N}{n}\right)}\right) - 4c_1\left(\frac{\log\left(\frac{N}{n}\right)}{\log\left(\frac{2N}{n}\right)}\right)^2.$$

Now, for $n > \frac{N}{B}$, using (3.14) we get

$$\sum_{B<p\leq\frac{2N}{n}}\left(1-\left|\frac{np}{N}-1\right|\right) \leq \frac{N}{2n\log\left(\frac{N}{n}\right)} + \frac{N}{n\log^2\left(\frac{N}{n}\right)}f(N,n) = g_2(N,n,B,c_1,c_2).$$

Something that will be important later on in the proof is that $f(N,n)$ is decreasing whenever $n < N/6.09$, therefore let's prove it now:

Claim 1. For a fixed integer n, if we let $c_1 = 0.239818$, then for $N > 6.09n$, $f(N,n)$ is a decreasing function.

Proof of the Claim: First note that if we let $x = \frac{\log\left(\frac{N}{n}\right)}{\log\left(\frac{2N}{n}\right)}$, then $f(N,n) = c_2 + (\log 4)x - 4c_1x^2$. We note that the maximum occurs when $x_0 = \frac{\log 4}{8c_1} = 0.722576\ldots$. For $N > 6.09n$ we have $x > x_0$ because x increases as N increases. Since $f(N,n)$ is decreasing once $x > x_0$, then as N grows, $f(N,n)$ decreases. This proves the claim.

Now, let $c = 7.8$, $c_1 = 0.239818$ and $c_2 = 0.29251$. Notice that $N = c\sqrt{D}$ depends only on D and $B = D^{0.45}$ also depends only on D. Now define

$$g(n,D) = \frac{1}{\sqrt{D}}\begin{cases} g_1(N,n,B,c_1,c_2) & : \; n \leq N/B; \\ g_2(N,n,B,c_1,c_2) & : \; n > N/B. \end{cases}$$

Therefore for $B \geq 10544111$, (4.4) becomes

$$0 \geq 7.8 - 1 - 2^{\omega(D)}(4.15)\frac{\sqrt{D}}{\phi(D)} - \frac{2D}{\phi(D)}\sum_{\substack{n\leq(15.6)D^{1/20}\\(n,D)=1}} g(n,D). \tag{5.1}$$

Now, let $M = \prod_{p\leq 41} p$ and let $m = \gcd(D,M)$. Note that since m is squarefree and 41 is the 13th prime, then there are 2^{13} possible values of m. Now, let's define a function $A(D,m,\omega,u)$ in the following way

$$A(D,m,\omega,u) = 6.8 - 2^{\omega}\,(4.15)\,\frac{\sqrt{D}}{\phi(D)} - \frac{2D}{\phi(D)} \sum_{\substack{n\le u\\(n,m)=1}} g(n,D).$$

Claim 2. Let m be a fixed positive integer. Let U be a fixed real number. Let $M = \prod_{p\le 41} p$. Let $D \le U$ be a positive integer such that $(D,M) = m$. Now let $u = \lfloor (15.6)U^{1/20} \rfloor$. Let ω be the maximum number of distinct primes a number below U can have. If $D \ge 4.05 \times 10^{15}$ then $0 \ge A(D,m,\omega,u)$.

Proof of the Claim: Let $D \le U$. We have $\omega(D) \le \omega$. We also have $u \ge \lfloor (15.6)D^{1/20} \rfloor$. Now, $D \ge 4.05 \times 10^{15} > 10544111^{1/0.45}$, therefore $B > 10544111$ and hence we have (5.1). Since $m|\,D$, if $(n,D) = 1$ then $(n,m) = 1$. Also note that $g(n,D) \ge 0$. Combining this with (5.1) we have

$$\begin{aligned} 0 &\ge 6.8 - 2^{\omega(D)}(4.15)\frac{\sqrt{D}}{\phi(D)} - \frac{2D}{\phi(D)} \sum_{\substack{n\le (15.6)D^{1/20}\\(n,D)=1}} g(n,D) \\ &\ge 6.8 - 2^{\omega}(4.15)\frac{\sqrt{D}}{\phi(D)} - \frac{2D}{\phi(D)} \sum_{\substack{n\le u\\(n,m)=1}} g(n,D) = A(D,m,\omega,u). \end{aligned}$$

This proves the claim.

For example, when $D \le 10^{24}$, we would have $U = 10^{24}$. Since any $D \le 10^{24}$ has at most 18 distinct prime factors, $\omega = 18$. Now, $u = \lfloor (15.6)U^{1/20} \rfloor = \lfloor 247.243 \rfloor = 247$. Once we fix an m, we get that if $D \ge 4.05 \times 10^{15}$ then $0 \ge A(D,m,18,247)$.

Therefore to reach a contradiction we must find values of D for which $A(D,m,18,247) > 0$.

Once U and m are fixed, it seems that $A(D,m,\omega,u)$ is increasing with D. The only cause for uncertainty comes from the factor $\frac{D}{\phi(D)}$ and from $g(n,D)$. Let's deal with this. Let p_i be the i-th prime. Note $p_{13} = 41$. Since we want to maximize $\frac{D}{\phi(D)}$ (to make $A(D,m,\omega,u)$ as small as possible), then we do is consider the product of the smallest primes bigger than 41 and consider $D_v(m) = m \times \prod_{13<i\le v} p_i$. Since we also have to deal with $g(n,D)$, what we will do is make it as big as possible in a range. Let's analyze the value of $g(n,D)$:

If $n \le \frac{N}{B}$, then

$$\begin{aligned} g(n,D) &= \frac{1}{\sqrt{D}}\left(\frac{N}{n\log\left(\frac{N}{n}\right)} + \frac{(f(N,n)+c_2)N}{n\log^2\left(\frac{N}{n}\right)} - \frac{c_1 n B^2}{N\log^2 B} - \frac{nB^2}{2N\log B} \right) \\ &= \frac{c}{n\log\left(\frac{c\sqrt{D}}{n}\right)} + \frac{(f(N,n)+c_2)c}{n\log^2\left(\frac{c\sqrt{D}}{n}\right)} - \frac{c_1 n}{cD^{1/10}\log^2\left(D^{.45}\right)} - \frac{n}{2cD^{1/10}\log\left(D^{.45}\right)} \\ &= H_1(n,D) - H_2(n,D), \end{aligned}$$

where $H_1(n,D)$ consists of the two positive terms and $H_2(n,D)$ consists of the two terms being substracted. Now, $f(N,n)$ is decreasing for $N > 6.09n$. Since $n \le u = 247$ we have that $N > 6.09n$. Therefore $f(N,n)$ is decreasing, showing that

$H_1(n,D)$ is decreasing. $H_2(n,D)$ is also a decreasing function, making $-H_2(n,D)$ an increasing function.

Now, for $n > \frac{N}{B}$, we have

$$g(n,D) = \frac{1}{\sqrt{D}}\left(\frac{N}{2n\log\left(\frac{N}{n}\right)} + \frac{N}{n\log^2\left(\frac{N}{n}\right)}f(N,n)\right)$$
$$= \frac{c}{2n\log\left(\frac{c\sqrt{D}}{n}\right)} + \frac{cf(N,n)}{n\log^2\left(\frac{c\sqrt{D}}{n}\right)} = H_3(n,D).$$

Again, because $f(N,n)$ is decreasing, the right hand side is decreasing.

All of this allows us to get the following claim:

Claim 3. Let D, D_1, D_2 be positive reals such that $D \in [D_1, D_2)$, and let

$$G(n,D_1,D_2) := \begin{cases} H_1(n,D_1) - H_2(n,D_2) & n \leq cD_1^{0.05}; \\ H_3(n,D_1) & n > cD_2^{0.05}; \\ \max\{H_1(n,D_1) - H_2(n,D_2), H_3(n,D_1)\} & \text{otherwise.} \end{cases}$$

Then $g(n,D) \leq G(n,D_1,D_2)$.

Proof of the Claim: If $n \leq cD_1^{0.05}$, then for any $D \in [D_1, D_2)$ we have $n \leq \frac{N}{B}$, therefore $g(n,D) = H_1(n,D) - H_2(n,D)$. But, since both H_1 and H_2 are decreasing functions, we have $g(n,D) \leq H_1(n,D_1) - H_2(n,D_2)$.

If $n > cD_2^{0.05}$, then for any $D \in [D_1, D_2)$ we have $n > \frac{N}{B}$, therefore $g(n,D) = H_3(n,D)$. Since H_3 is decreasing we have $g(n,D) \leq H_3(n,D_1)$.

For the few values of n such that $cD_1^{0.05} < n \leq cD_2^{0.05}$, we just take the maximum, so we have $g(n,D) \leq \max\{H_1(n,D_1) - H_2(n,D_2), H_3(n,D_1)\}$. This proves the claim.

Now, let's define a function similar to A called A_2 so that we can take this into account.

$$A_2(D,m,\omega,u,D_1,D_2) = 6.8 - \frac{2^{\omega}\,(4.15)}{\sqrt{D_1}}\frac{D}{\phi(D)} - \frac{2D}{\phi(D)}\sum_{\substack{n\leq u\\(n,m)=1}} G(n,D_1,D_2).$$

Claim 4. Let D be a positive integer. Let m be defined the same way as in Claim 2. Let v be an integer ≥ 13 such that $D_v(m) \geq 4.05 \times 10^{15}$. Let D_1 and D_2 be real numbers such that $[D_1, D_2) \subseteq [D_v(m), D_{v+1}(m))$. Let $\omega = \omega(m) + v - 13$. Let $u = \left\lfloor (15.6)D_2^{0.05} \right\rfloor$. Then, if $D \in [D_1, D_2)$, we have $0 \geq A_2(D_v(m), m, \omega, u, D_1, D_2)$.

Proof of the Claim: Since $m|\,D$ and $D < D_{v+1}(m)$ then $\omega(D) < \omega(m)+v+1-13 \leq \omega(m)+v-13 = \omega$. We also have

$$\frac{D}{\phi(D)} = \frac{m}{\phi(m)}\prod_{\substack{p>p_{13}\\p|D}}\frac{p}{p-1} \leq \frac{m}{\phi(m)}\prod_{13<i\leq v}\frac{p_i}{p_i-1} = \frac{D_v(m)}{\phi(D_v(m))}.$$

From Claim 3, we have $g(n,D) \leq G(n,D_1,D_2)$. Also, from Claim 2 using $U = D_2$ and because $\omega(D) \leq \omega$, we have for $D \geq 4.05 \times 10^{15}$, the inequality $0 \geq$

$A(D,m,\omega,u)$. Therefore, we have

$$\begin{aligned}0 \geq A(D,m,\omega,u) &= 6.8 - \frac{2^{\omega}(4.15)}{\sqrt{D}}\frac{D}{\phi(D)} - \frac{2D}{\phi(D)}\sum_{\substack{n\leq u\\(n,m)=1}} g(n,D)\\ &\geq 6.8 - \frac{2^{\omega}(4.15)}{\sqrt{D_1}}\frac{D_v(m)}{\phi(D_v(m))} - \frac{2D_v(m)}{\phi(D_v(m))}\sum_{\substack{n\leq u\\(n,m)=1}} G(n,D_1,D_2)\\ &= A_2(D_v(m),m,\omega,u,D_1,D_2).\end{aligned}$$

What this allows us to do is just check $A_2(D,m,\omega,u,D_1,D_2)$ for some numbers and cover a whole interval. Our implementation will run by checking

$$A_2(D_v(m),m,\omega,u,D_v(m),D_{v+1}(m)),$$

where $\omega=\omega(m)+v-13$ and $u=\lfloor(15.6)D_{v+1}(m)\rfloor$. The process is then to find for each m the first v such that

$$A_2(D_v(m),m,\omega,u,D_v(m),D_{v+1}(m))>0,$$

and

$$A_2(D_{v+i}(m),m,\omega,u,D_{v+i}(m),D_{v+i+1}(m))>0$$

for all positive integers i while $D_{v+i}(m)\leq 10^{24}$. We will denote this $D_v(m)$ by $K(m)$. Now, we find the maximum $K(m)$ among the 2^{13} possible m's. We denote this maximum by K and we note that for all $D\geq K$ with $D\leq 10^{24}$ we have $A(D,m,\omega,u)>0$, giving us a contradiction, yielding the desired theorem for $D\geq K$.

Since the odd cases are easier than the even ones (because $D/\phi(D)$ is smaller when D is odd), we split the process in dealing with the odd D's first and then with the even D's. After running a loop that computes $K(m)$ for every odd m and finds the maximum value K, we find that $K=21853026051351495<2.2\times10^{16}$. This implies that for all $D\geq 2.2\times10^{16}$, odd fundamental discriminants, the theorem is true. Since we had already dealt with the case $D\leq 2.6\times10^{17}$, this finishes the proof for odd D.

Now let's consider the case where D is even. In this case our goal is to prove it for all $D\geq 1.04\times10^{18}$, since we have computational tables proving the smaller D. Just as in the case for odd m, we run a loop that computes $K(m)$ for every even m and then find the maximum among this, which we call K. In this case, $K=1707159924755154870<1.71\times10^{18}$. Note that K is slightly larger than our desired outcome since it doesn't lead us all the way down to 1.04×10^{18}. This forces us to work a little harder to reach the theorem.

To get rid of this new obstacle we use the fact that in Claim 4 we have more flexibility than we've been using. We need not have $D_1=D_v(m)$ and $D_2=D_{v+1}(m)$ as we have been using so far, we could pick values in between. First of all, we found all the m values that have $D(m,U)>1.04\times10^{18}$. There are only twelve values of m. By the nature of the process the twelve counterexamples are of the form $D_v(m)$. Seven of the examples have $v=20$ and the other five have $v=19$. Therefore what we can do is consider $D_1=32D_{v-1}(m)$ and $D_2=D_v(m)$. After evaluating $A(D_v(m),m,\omega,u,D_1,D_2)$ for these twelve m's, we find that all of them are greater than zero. This completes the proof for even values.

Combining the result for even and odd values yields the theorem. □

As an extra note, this naive algorithm runs in around 15 minutes on a Pentium(R) Dual-Core CPU E5300 @ 2.60GHz.

Remark 5.2. With the same techniques we can prove that for D a fundamental discriminant satisfying $D > 10^{24}$, there exists a prime p such that $p \le D^{3/7}$ and the Kronecker symbol $(D/p) = -1$. Computations on pseudosquares (see [15] and [17]) suggest that sieving machines can check for the values below 10^{24} (such as MSSU computed the values under 10^{18}).

6. Acknowledgements

I would like to thank my advisor Carl Pomerance for his guidance in this problem. He has been very patient, insightful and inspiring. I would also like to thank Kannan Soundararajan for suggesting the problem. Finally, I would like to thank the anonymous referee for carefully reading the manuscript and making helpful suggestions.

References

[1] E. Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55(191):355–380, 1990.
[2] D. A. Burgess. On character sums and primitive roots. *Proc. London Math. Soc. (3)*, 12:179–192, 1962.
[3] R. Crandall and C. Pomerance. *Prime numbers*. Springer, New York, second edition, 2005. A computational perspective.
[4] P. Dusart. Sharper bounds for ψ, θ, π,p_k. *Laboratoire d'Arithmétique, de Calcul formel et d'Optimisation*, 1998.
[5] P. Dusart. Inégalités explicites pour $\psi(X)$, $\theta(X)$, $\pi(X)$ et les nombres premiers. *C. R. Math. Acad. Sci. Soc. R. Can.*, 21(2):53–59, 1999.
[6] A. Granville, R. A. Mollin, and H. C. Williams. An upper bound on the least inert prime in a real quadratic field. *Canad. J. Math.*, 52(2):369–380, 2000.
[7] M. Levin, C. Pomerance, and K. Soundararajan. Fixed points for discrete logarithms. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 6–15. 2010.
[8] R. F. Lukes, C. D. Patterson, and H. C. Williams. Some results on pseudosquares. *Math. Comp.*, 65(213):361–372, S25–S27, 1996.
[9] R. A. Mollin. *Quadratics*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1996.
[10] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.
[11] K. K. Norton. *Numbers with small prime factors, and the least kth power non-residue*. Memoirs of the American Mathematical Society, No. 106. American Mathematical Society, Providence, R.I., 1971.
[12] K. K. Norton. Bounds for sequences of consecutive power residues. I. In *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 213–220. Amer. Math. Soc., Providence, R.I., 1973.
[13] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.
[14] L. Schoenfeld. Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II. *Math. Comp.*, 30(134):337–360, 1976.
[15] J. P. Sorenson. Sieving for pseudosquares and pseudocubes in parallel using doubly-focused enumeration and wheel datastructures. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 331–339. 2010.
[16] E. Treviño. *Numerically explicit estimates for character sums*. 2011. Thesis (Ph.D.)–Dartmouth College.
[17] K. Wooding. *The sieve problem in one- and two-dimensions*. 2010. Thesis (Ph.D.)–University of Calgary.

Department of Mathematics, Dartmouth College, Hanover, New Hampshire 03755
E-mail address: enrique.trevino@dartmouth.edu