Annales Univ. Sci. Budapest., Sect. Comp. 53 (2022) 57–70

PRIMALITY PROOFS WITH ELLIPTIC CURVES: CONJECTURES FOR THE EXPECTED NUMBER OF CURVE ORDERS

Gábor Román (Budapest, Hungary)

Communicated by Antal Járai

(Received September 3, 2021; accepted July 29, 2022)

Abstract. In this article we state two conjectures, which enable us to give a satisfying answer to the question posed by the authors of article [4] concerning the expected number of curve orders for a given prime during the application of the elliptic curve primality proving method. The presented train of thoughts isolate the problematic aspects of this subject, and reveal the areas which require further development.

1. Introduction

We proceed with our investigation concerning the expected number of curve orders for a given prime during the application of the Atkin–Morain primality test, see articles [15, 16]. First, we briefly recall the key aspects of the topic.

Definition 1. We call a negative integer D as a negative fundamental discriminant if either $D \equiv 1 \pmod 4$, and D is square-free; or $D = 4k$, where $k \equiv 2, 3 \pmod 4$, and k is square-free.

Key words and phrases: Elliptic curve primality proving, negative fundamental discriminant, elliptic curve order, Legendre symbol, smooth number, class number, square-free number, random walk, quadratic (non-)residue, Siegel–Walfisz theorem, number of (distinct) prime factors, Abel's identity.
2010 Mathematics Subject Classification: 11Y11.

During the computation of the curve orders for the possible prime n, one processes those negative fundamental discriminants $D \geq -d(n)$, which satisfy the requirements

$$(D|n) = 1, \tag{1.1}$$

$$\forall\, p \in \mathbb{P},\ p|D,\ (n|p) = 1, \tag{1.2}$$

and $P(D) \leq d(n)^c$, for some $c \in (0,1)$. Here $P(x)$ denotes the largest prime factor of an integer x, with the convention that $P(1) = 1$; and $d(n)$ is a polylogarithmic function, so $d(n) \in o(n^{\varepsilon})$ for every $\varepsilon > 0$.

Now we present some notations to ease the discussion. Denote the negative fundamental discriminants, which fall into a certain interval as

$$\Delta_x^y := \{z \in \mathbb{Z} : x \leq |z| \leq y, \text{ and } z \text{ is a negative fundamental discriminant}\}$$

where x, and y are positive real numbers; furthermore introduce the sets, which contain the numbers satisfy requirement (1.1), and requirement (1.2) as

$$\Phi_x := \{z \in \mathbb{Z} : (z|x) = 1, \text{ and } \forall p \in \mathbb{P}, p|z, (x|p) = 1\}$$

where x is an integer. We will say that an integer is *well-structured* if it can be found in Φ_x.

During the computation of the curve orders for a given negative fundamental discriminant D, the probability of success can be taken as $1/h(D)$, where $h(D)$ is the class number of D. Based on this, the expected number of curve orders can be approximated with the following sum.

$$\sum_{\substack{D \in \Delta_3^{d(n)} \cap \Phi_n \\ P(D) \leq d(n)^c}} \frac{1}{h(D)} \tag{1.3}$$

We can take into consideration the fact that one must obtain the modular square-root of every negative fundamental discriminant D during the computations. As one builds the modular square-root of a discriminant D from the modular square-roots of its prime factors, the probability of success depends on the number of distinct prime factors of D. With every prime factor, our chances are doubled. So we can also approximate (supposedly better) the expected number of curve orders with the following sum.

$$\sum_{\substack{D \in \Delta_3^{d(n)} \cap \Phi_n \\ P(D) \leq d(n)^c}} \frac{2^{\omega(|D|)}}{h(D)} \tag{1.4}$$

Here $\omega(x)$ denotes the number of distinct prime factors of a natural number x, with the convention that $\omega(1) = 0$. Concerning how well this second sum approximates the expected number of curve orders, see the experimental results in [10]. We are going to give lower-, and upper bounds for these two sums.

2. Class numbers

The precision of our results will depend on the applied approximation for the class numbers, so we present a way to introduce the uncertainties as tuneable components into the results. The most basic lower-, and upper bound for the class number $h(D)$ can be expressed as

$$|D|^{1/2-\varepsilon} \ll h(D) \ll |D|^{1/2+\varepsilon}$$

for $\varepsilon > 0$, see Siegel [18]. (Taking $f, g \in \mathbb{R} \to \mathbb{R}$, by $f(x) \ll g(x)$ we mean that there exists a positive constant c, and a real constant x_0, such that for every real $x > x_0$, we have $|f(x)| \leq cg(x)$.) Better, but still unconditional bounds can be given as

$$\frac{\sqrt{|D|}}{\ln |D|} \ll h(D) \ll \sqrt{|D|} \ln |D|$$

see section 22.4 in [9], furthermore [16], and [3]. Using the Riemann hypothesis, one can squeeze out

$$\frac{\sqrt{|D|}}{\ln \ln |D|} \ll h(D) \ll \sqrt{|D|} \ln \ln |D|$$

see [12], and [3]. (For a more exhaustive historical recollection, see chapter 22 of [5], especially the concluding remarks.) Thus for some monotone increasing $\lambda_1, \lambda_2 : \mathbb{N} \to \mathbb{R}^+$, we have

$$\frac{\sqrt{|D|}}{\lambda_1(|D|)} \ll h(D) \ll \sqrt{|D|}\lambda_2(|D|) \tag{2.1}$$

where the left (respectively right) hand bound holds for every negative fundamental discriminant $D \leq D_{\lambda_1}$ (respectively $D \leq D_{\lambda_2}$), with $D_{\lambda_1}, D_{\lambda_2} \leq -3$ being fixed. The hidden constants are positive, and absolute; we are going to denote them as c_{λ_1} and c_{λ_2}.

3. Well structured discriminants

The way in which we are going to handle sum (1.3) requires a good lower-, and upper bound for the number of smooth, well structured negative fundamental discriminants. More precisely, we need good bounds for the number of $d(n)^c$-smooth elements in $\Delta_3^{d(n)} \cap \Phi_n$, where $c \in (0,1)$. The upper bound is trivially in $O(d(n))$, which will suffice for our needs. As for a useful lower bound, our scarce knowledge about the number of quadratic residues in short intervals hinders us in finding one. Nevertheless, we are going to present a conjectured lower bound, and the accompanying train of thoughts also. As a hint, we would want the lower bound to be in $\Omega(d(n))$, but it turns out that this might cannot be achieved.

Based on the structure of the negative fundamental discriminants, see definition 1, we have

$$|\Delta_3^{d(n)}| \in \Theta(Q(d(n)))$$

where $Q(x)$ is the number of square-free integers in $[1,x]$. It is known that $Q(x) \in \Theta(x)$, see for example theorem 2.2 in section 2.1 of [13], so we can conclude that the count of negative fundamental discriminants doesn't hinder us in reaching the sought bound, so we have to turn to the smoothness, and to the count of well structured integers. Proposition 1 from [17] suggests that by taking a big enough n, we could still have our lower bound for arbitrary $c \in (0,1)$ if we have enough well structured discriminants. We are going to construct a portion of these integers depending on the residue of n modulo 4.

- When $n \equiv 1 \pmod 4$, then take those primes p, for which $p \equiv 1\ (4)$, and $(n|p) = 1$ both hold. Construct numbers of the form $-4k \geq -d(n)$ from these primes, where k is square-free.
- When $n \equiv 3 \pmod 4$, then take those primes p, for which $p \equiv 3\ (4)$, and $(n|p) = 1$ both hold. Construct numbers of the form $-k \geq -d(n)$ from these primes, where k is square-free with odd number of prime factors.

By construction, these numbers will be negative fundamental discriminants, see again definition 1. Indeed, in the first case, when the numbers are of the form $-4k$, we have $-k = -p_1 \dots p_m \equiv -1 \pmod 4$; and in the second case, when they are of the form $-k$, we have $-k = -p_1 \dots p_m \equiv -3^m \equiv -3 \pmod 4$ because m is odd.

These numbers will satisfy requirement (1.2) in both cases, again by construction, so we just have to show that all of them satisfy requirement (1.1) too. In the first case we have

$$\left(\frac{-4k}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{4}{n}\right)\left(\frac{p_1}{n}\right)\dots\left(\frac{p_m}{n}\right)$$

where $(-1|n) = 1$, $(4|n) = 1$, so by using the law of quadratic reciprocity, we get

$$(-1)^{\frac{p_1-1}{2}\frac{n-1}{2}}\left(\frac{n}{p_1}\right)\dots(-1)^{\frac{p_m-1}{2}\frac{n-1}{2}}\left(\frac{n}{p_m}\right) = 1$$

because of the properties of p_i. In the second case we have

$$\left(\frac{-k}{n}\right)=\left(\frac{-1}{n}\right)\left(\frac{p_1}{n}\right)\dots\left(\frac{p_m}{n}\right)$$

where $(-1|n)=-1$, so by using the law of quadratic reciprocity again, we get that this is $(-1)^{m+1}$, which is 1, because m is odd.

From these we can deduce that what we essentially have to know, is the count of those primes $p\le d(n)$, which residue is either 1, or 3 modulo 4; and which satisfy $(n|p)=1$. Formally, this is

$$\sum_{\substack{p\le d(n)\\ p\equiv q(4)\\ (n|p)=1}}1=\frac{1}{2}\sum_{\substack{p\le d(n)\\ p\equiv q(4)}}\left(1+\left(\frac{n}{p}\right)\right)=\frac{\pi(d(n);4,q)}{2}+\frac{1}{2}\sum_{\substack{p\le d(n)\\ p\equiv q(4)}}\left(\frac{n}{p}\right)$$

where $\pi(x;4,q)$ is the count of primes $p\le x$, which are congruent to q modulo 4, with q being either 1, or 3; and the sum on the right hand side is equal to

$$\pm\frac{1}{2}\sum_{\substack{p\le d(n)\\ p\equiv q(4)}}\left(\frac{p}{n}\right)$$

based on the residue of p, and n modulo 4. The problem here is that for slowly growing d, the behaviour of this sum is not fully understood, so we cannot guarantee that it won't change the order of the term $\pi(d(n);4,q)/2$ too much. Treating the Legendre symbol with fixed modulus as a variable with Rademacher distribution, the sum becomes a one-dimensional random walk, so for faster growing $d(n)$ we expect that its value will be in $O(\sqrt{d(n)})$, see article [16]. As the Legendre symbol is not purely a variable with the mentioned distribution, this is only an approximation. However, based on the properties of the least quadratic non-residues, see article [11], it is probable that the sum starts to behave as a one-dimensional random walk when $d(n)\in\Omega(\ln^\delta n)$ for $\delta>1$. So using the Siegel–Walfisz theorem, see for example corollary 5.29 in section 5.9 of [9], we expect that the number of appropriate primes will be in $\Omega(\pi(d(n)))$.

Now we construct square-free numbers from these prime numbers. Taking only small primes, we can select even all of them to form square-free numbers, which aren't greater than $d(n)$. Then by the binomial theorem we have that the number of these products grow exponentially as the number of primes grow. So we expect that a logarithmic number of small primes should suffice to construct enough square-free numbers. As there are infinitely many primes n, which primes' least quadratic non-residue is in $\Omega(\ln n)$, see article [11], it seems that the count of our square-free numbers could reach the order of $d(n)$. However, as we cannot guarantee that there are enough primes, which are quadratic residues to n, it can happen that the number of our square-free numbers stay in $\Omega(\pi(d(n)))$.

So at the end of the day, we expect that the number of well structured discriminants will fall in $\Omega(\pi(d(n)))$, and also in $O(d(n))$. Take note that with this lower bound we cannot satisfy the requirements of the proposition from [17], so improvements would be required in the handling of the smoothness too.

Based on all of this, now we state our first conjecture.

Conjecture 1. *Let $d(n) \in \Omega(\ln^\delta n)$, where $\delta > 1$; $D_0 \geq 3$ be an integer; and $c \in (0,1)$. Then we have*

$$\frac{d(n)}{\ln d(n)} \ll \sum_{\substack{D \in \Delta_{D_0}^{d(n)} \cap \Phi_n \\ P(D) \leq d(n)^c}} 1 \ll d(n)$$

for every prime $n \geq n_0$, with n_0 depending on δ, D_0, and c.

To handle sum (1.4) we state a similar, but stronger conjecture, in which we incorporate the number of distinct prime factors of the examined negative fundamental discriminants. The distribution of natural numbers below x with $k > 0$ (distinct) prime factors can be approximated using the Poisson law with parameter $\ln \ln x$, see section 6.1 in part 2 of [19], furthermore [14], and [8]. So using the function

$$f_k(x) := \frac{1}{\ln x} \frac{(\ln \ln x)^{k-1}}{(k-1)!} \tag{3.1}$$

the number of positive integers below x having $k > 0$ (distinct) prime factors can be approximated as $x f_k(x)$. We expect that the distribution of well structured negative fundamental discriminants below $d(n)$ with $k > 0$ distinct prime factors follows this trend.

Conjecture 2. *Let $d(n) \in \Omega(\ln^\delta n)$, where $\delta > 1$; $D_0 \geq 3$ be an integer; $c \in (0,1)$; and $k > 0$. Then we have*

$$\frac{d(n) f_k(d(n))}{\ln d(n)} \ll \sum_{\substack{D \in \Delta_{D_0}^{d(n)} \cap \Phi_n \\ P(D) \leq d(n)^c \\ \omega(|D|) = k}} 1 \ll d(n) f_k(d(n))$$

for every prime $n \geq n_0$, with n_0 depending on δ, D_0, c, and k.

Take note that conjecture 1 follows from conjecture 2, as the integers in $\Delta_{D_0}^{d(n)}$ have at most a finite m number of distinct prime factors, one just has to accumulate the values of the sum in conjuncture 2 for $1 \leq k \leq m$, see the proof of proposition 2, and the proof of lemma 2.

4. Results

Using conjecture 1, first we present our bounds for the sum (1.3). Concerning the functions λ_1, and λ_2, see expression (2.1).

Proposition 1. *Let $d(n) \in \Omega(\ln^{\delta} n)$, where $\delta > 1$; and $c \in (0,1)$. Then based on conjecture 1, we have*

$$\frac{\sqrt{d(n)}}{\lambda_2(d(n)) \ln d(n)} \ll \sum_{\substack{D \in \Delta_3^{d(n)} \cap \Phi_n \\ P(D) \leq d(n)^c}} \frac{1}{h(D)} \ll \sqrt{d(n)} \lambda_1(d(n)) \tag{4.1}$$

for every prime $n \geq n_0$, with n_0 depending on δ, and c.

Take note that the right hand side bound is unconditional, so it doesn't actually depend on our conjecture. Now using conjecture 2, the bounds for the sum (1.4) can be given as follows.

Proposition 2. *Let $d(n) \in \Omega(\ln^{\delta} n)$, where $\delta > 1$; and $c \in (0,1)$. Then based on conjecture 2, we have*

$$\frac{\sqrt{d(n)}}{\lambda_2(d(n))} \ll \sum_{\substack{D \in \Delta_3^{d(n)} \cap \Phi_n \\ P(D) \leq d(n)^c}} \frac{2^{\omega(|D|)}}{h(D)} \ll \sqrt{d(n)} \lambda_1(d(n)) \ln d(n) \tag{4.2}$$

for every prime $n \geq n_0$, with n_0 depending on δ, and c.

5. Remarks

The following probabilistic viewpoint for the expected number of curve orders is based on the observations in article [4]. The probability that requirement (1.1), and requirement (1.2) are both satisfied for a discriminant D can be approximated with $2^{-\omega(|D|)}$, as we have a 50% chance to successfully compute a modular square root. Based on the theorem from Erdős and Kac, see article [7], we have

$$\lim_{x \to \infty} \frac{1}{x} \left| \left\{ n \leq x : a \leq \frac{\omega(n) - \ln \ln n}{\sqrt{\ln \ln n}} \leq b \right\} \right| = \frac{1}{\sqrt{2\pi}} \int\limits_a^b e^{-t^2/2}\, dt$$

so we can expect the above probability to be around $\ln^{-\ln 2} d(n)$. From this, we can argue that the expected number of well-structured discriminants should be around $d(n)\ln^{-\ln 2} d(n)$. Thus it seems possible that we can state the analog of proposition 1 as

$$\frac{\sqrt{d(n)}}{\lambda_2(d(n))\ln^{\ln 2} d(n)} \ll \sum_{\substack{D\in\Delta_3^{d(n)}\cap\Phi_n \\ P(D)\le d(n)^c}} \frac{1}{h(D)} \ll \frac{\sqrt{d(n)}}{\ln^{\ln 2} d(n)}\lambda_1(d(n))$$

and the analog of proposition 2 as

$$\frac{\sqrt{d(n)}}{\lambda_2(d(n))}\left(\frac{\ln\ln n}{\ln d(n)}\right)^{\ln 2} \ll \sum_{\substack{D\in\Delta_3^{d(n)}\cap\Phi_n \\ P(D)\le d(n)^c}} \frac{2^{\omega(|D|)}}{h(D)} \ll \sqrt{d(n)}\lambda_1(d(n))\left(\frac{\ln\ln n}{\ln d(n)}\right)^{\ln 2}$$

respectively for every big enough prime n. As we choose $d(n)$ to be logarithmic in n, the latter bounds suggest that the expected number of curve orders will be around $\sqrt{d(n)}$ as desired, disturbed only by $\lambda_1(d(n))$, and $\lambda_2(d(n))$. So it seems beneficial to include among the requirements that the selected discriminants must have at least around $\ln\ln n$ number of prime factors. (Another huge motivation would be that the running time of the proof construction during the test can be made faster by selecting discriminants with high prime factor count. For more details, see the Weber polynomials in section 7.3 of article [2].) Additional investigation is needed in the direction of this refinement.

6. Proofs

Our proof of proposition 1 is the following.

Proof.

- First we look at the lower bound in expression (4.1). As $d(n)$ is strictly monotone increasing, $d(n) > |D_{\lambda_2}|$ will hold for larger n, so for these n we can split our sum in expression (4.1) as

$$\sum_{\substack{D\in\Delta_3^{d(n)}\cap\Phi_n \\ P(D)\le d(n)^c}} \frac{1}{h(D)} = \sum_{\substack{D\in\Delta_{D_{\lambda_2}}^{d(n)}\cap\Phi_n \\ P(D)\le d(n)^c}} \frac{1}{h(D)} + \sum_{\substack{D\in\Delta_3^{D_{\lambda_2}}\cap\Phi_n \\ P(D)\le d(n)^c}} \frac{1}{h(D)}$$

where the second sum is smaller than a positive constant. Using the upper bound from expression (2.1), the first sum is greater than

$$c_{\lambda_2} \sum_{\substack{D \in \Delta_{D_{\lambda_2}}^{d(n)} \cap \Phi_n \\ P(D) \le d(n)^c}} \frac{1}{\sqrt{|D|}\lambda_2(|D|)} \gg \frac{1}{\lambda_2(d(n))} \sum_{\substack{D \in \Delta_{D_{\lambda_2}}^{d(n)} \cap \Phi_n \\ P(D) \le d(n)^c}} \frac{1}{\sqrt{|D|}} \tag{6.1}$$

because $d(n)$, and $\lambda_2(d(n))$ are monotone increasing. Let

$$A(x) := \sum_{m \le x} a(m)$$

where define $a(m)$ as 1 if $-m \in \Delta_{D_{\lambda_2}}^{d(n)} \cap \Phi_n$, and $P(m) \le d(n)^c$; otherwise define $a(m)$ as 0. Using Abel's identity, see theorem 4.2 in section 4.3 of [1], we have that the sum on the right hand side of expression (6.1) is equal to

$$\sum_{|D_{\lambda_2}|-1 < m \le d(n)} \frac{a(m)}{\sqrt{m}} = \frac{A(d(n))}{\sqrt{d(n)}} + \frac{1}{2} \int_{|D_{\lambda_2}|-1}^{d(n)} \frac{A(t)}{t^{3/2}}\, dt + O(1) \gg \frac{\sqrt{d(n)}}{\ln d(n)}$$

because of the bound for $A(d(n))$, see conjecture 1; and because the integral is positive.

- Now we look at the upper bound in expression (4.1). Similarly as in the previous case, $d(n) > |D_{\lambda_1}|$ will hold for larger n, so for these n we can split our sum in expression (4.1) as

$$\sum_{\substack{D \in \Delta_3^{d(n)} \cap \Phi_n \\ P(D) \le d(n)^c}} \frac{1}{h(D)} = \sum_{\substack{D \in \Delta_{D_{\lambda_1}}^{d(n)} \cap \Phi_n \\ P(D) \le d(n)^c}} \frac{1}{h(D)} + \sum_{\substack{D \in \Delta_3^{D_{\lambda_1}} \cap \Phi_n \\ P(D) \le d(n)^c}} \frac{1}{h(D)}$$

where the second sum is smaller than a positive constant. Using the lower bound from expression (2.1), the first sum is less than

$$c_{\lambda_1} \sum_{\substack{D \in \Delta_{D_{\lambda_1}}^{d(n)} \cap \Phi_n \\ P(D) \le d(n)^c}} \frac{\lambda_1(|D|)}{\sqrt{|D|}} \ll \lambda_1(d(n)) \int_{|D_{\lambda_1}|}^{d(n)} \frac{1}{\sqrt{t}}\, dt \ll \sqrt{d(n)}\lambda_1(d(n))$$

because $d(n)$, and $\lambda_1(d(n))$ are monotone increasing. ■

Before we present our proof for proposition 2, we prove two lemmas. Concerning the functions f_k, see definition (3.1).

Lemma 1. *Let $d(n) \in \Omega(\ln^{\delta} n)$, where $\delta > 1$; $c \in (0,1)$; and $k > 0$. Then based on Conjecture 2, we have*

$$\frac{\sqrt{d(n)}f_k(d(n))}{\lambda_2(d(n))\ln d(n)} \ll \sum_{\substack{D\in\Delta_3^{d(n)}\cap\Phi_n\\ P(D)\le d(n)^c\\ \omega(|D|)=k}} \frac{1}{h(D)} \ll \sqrt{d(n)}\lambda_1(d(n))f_k(d(n)) \tag{6.2}$$

for every prime $n \geq n_0$, with n_0 depending on δ, c, and k.

Proof. The proof will be very similar to the proof of proposition 1.

- First we look at the lower bound in expression (6.2). For those n, for which $d(n) > |D_{\lambda_2}|$, we can split the sum in expression (6.2) as

  $$\sum_{\substack{D\in\Delta_3^{d(n)}\cap\Phi_n\\ P(D)\le d(n)^c\\ \omega(|D|)=k}} \frac{1}{h(D)} = \sum_{\substack{D\in\Delta_{D_{\lambda_2}}^{d(n)}\cap\Phi_n\\ P(D)\le d(n)^c\\ \omega(|D|)=k}} \frac{1}{h(D)} + \sum_{\substack{D\in\Delta_3^{D_{\lambda_2}}\cap\Phi_n\\ P(D)\le d(n)^c\\ \omega(|D|)=k}} \frac{1}{h(D)}$$

  where the second sum is a positive constant. Using the upper bound from expression (2.1), we get that the first sum is greater than

  $$c_{\lambda_2} \sum_{\substack{D\in\Delta_{D_{\lambda_2}}^{d(n)}\cap\Phi_n\\ P(D)\le d(n)^c\\ \omega(|D|)=k}} \frac{1}{\sqrt{|D|}\lambda_2(|D|)} \gg \frac{1}{\lambda_2(d(n))} \sum_{\substack{D\in\Delta_{D_{\lambda_2}}^{d(n)}\cap\Phi_n\\ P(D)\le d(n)^c\\ \omega(|D|)=k}} \frac{1}{\sqrt{|D|}} \tag{6.3}$$

  because $d(n)$, and $\lambda_2(d(n))$ are monotone increasing. Let

  $$B_D(x) := \sum_{D\le m\le x} b_D(m)$$

  where define $b_D(m)$ as 1 if $-m \in \Delta_D^{d(n)} \cap \Phi_n$, $P(m) \leq d(n)^c$, furthermore $\omega(m) = k$; otherwise define $b_D(m)$ as 0. Using Abel's identity, we get that the sum on the right hand side of expression (6.3) is equal to

  $$\sum_{|D_{\lambda_2}|-1<m\le d(n)} \frac{b_{D_{\lambda_2}}(m)}{\sqrt{m}} = \frac{B_{D_{\lambda_2}}(d(n))}{\sqrt{d(n)}} + \frac{1}{2}\int_{|D_{\lambda_2}|-1}^{d(n)} \frac{B_{D_{\lambda_2}}(t)}{t^{3/2}}\,dt + O(1)$$

  from where we get our lower bound by using conjecture 2, and the fact that the integral is positive.

- Finally, we look at the upper bound in expression (6.2). For those n, for which $d(n) > |D_{\lambda_1}|$, we can split the sum in expression (6.2) as

$$\sum_{\substack{D\in\Delta_3^{d(n)}\cap\Phi_n\\ P(D)\le d(n)^c\\ \omega(|D|)=k}} \frac{1}{h(D)} = \sum_{\substack{D\in\Delta_{D_{\lambda_1}}^{d(n)}\cap\Phi_n\\ P(D)\le d(n)^c\\ \omega(|D|)=k}} \frac{1}{h(D)} + \sum_{\substack{D\in\Delta_3^{D_{\lambda_1}}\cap\Phi_n\\ P(D)\le d(n)^c\\ \omega(|D|)=k}} \frac{1}{h(D)}$$

where the second sum is a positive constant again. Using the lower bound from expression (2.1), the first sum is less than

$$c_{\lambda_1} \sum_{\substack{D\in\Delta_{D_{\lambda_1}}^{d(n)}\cap\Phi_n\\ P(D)\le d(n)^c\\ \omega(|D|)=k}} \frac{\lambda_1(|D|)}{\sqrt{|D|}} \ll \lambda_1(d(n)) \sum_{\substack{D\in\Delta_{D_{\lambda_1}}^{d(n)}\cap\Phi_n\\ P(D)\le d(n)^c\\ \omega(|D|)=k}} \frac{1}{\sqrt{|D|}}$$

because $d(n)$, and $\lambda_1(d(n))$ are monotone increasing. Applying Abel's identity again, we get that the sum on the right hand side is equal to

$$\sum_{|D_{\lambda_1}|-1<m\le d(n)} \frac{b_{D_{\lambda_1}}(m)}{\sqrt{m}} = \frac{B_{D_{\lambda_1}}(d(n))}{\sqrt{d(n)}} + \frac{1}{2}\int\limits_{|D_{\lambda_1}|-1}^{d(n)} \frac{B_{D_{\lambda_1}}(t)}{t^{3/2}}\,dt + O(1)$$

from where we get our upper bound as in the previous case. ∎

Lemma 2. *Take a function $m \in \mathbb{R} \to \mathbb{R}^+$, for which*

$$\lim_{x\to+\infty} \frac{m(x)}{\ln\ln x} = \infty$$

holds. Then we have

$$\sum_{k=1}^{\lfloor m(x)\rfloor} 2^k f_k(x) \in \Theta(\ln x).$$

Proof. Substitute f_k into the sum to get

$$\frac{1}{\ln x}\sum_{k=1}^{\lfloor m(x)\rfloor} 2^k \frac{(\ln\ln x)^{k-1}}{(k-1)!} = \frac{2}{\ln x}\sum_{k=0}^{\lfloor m(x)\rfloor-1} \frac{(2\ln\ln x)^k}{k!}$$

where we can use the results for the truncated exponential series, see section 9.2.1 of [6], to get

$$2\frac{\Gamma(\lfloor m(x)\rfloor, 2\ln\ln x)}{\Gamma(\lfloor m(x)\rfloor)}\ln x \in \Theta(\ln x)$$

based on the required property of m. ∎

Our proof for proposition 2 is the following.

Proof. The integers in $\Delta_3^{d(n)}$ can only have at most finite $m(d(n))$ number of distinct prime factors, where $m \in \mathbb{R} \to \mathbb{R}^+$ is a function, which can be defined for example as

$$m(x) := 2\frac{\ln x}{\ln \ln x}$$

see section 5.3 in part 1 of [19]. Using this function, we can can write the sum in expression (4.2) as

$$\sum_{\substack{D \in \Delta_3^{d(n)} \cap \Phi_n \\ P(D) \leq d(n)^c}} \frac{2^{\omega(|D|)}}{h(D)} = \sum_{k=1}^{\lfloor m(d(n)) \rfloor} 2^k \sum_{\substack{D \in \Delta_3^{d(n)} \cap \Phi_n \\ P(D) \leq d(n)^c \\ \omega(|D|)=k}} \frac{1}{h(D)}$$

Now we can use lemma 1 to bound the value of the inner sum.

- Using the lower bound from lemma 1, we get that the inner sum is bounded from below by

$$\frac{\sqrt{d(n)}}{\lambda_2(d(n)) \ln d(n)} \sum_{k=1}^{\lfloor m(d(n)) \rfloor} 2^k f_k(d(n))$$

  where the value of the sum cancels out the logarithmic part of the denominator, see lemma 2.

- Using the upper bound from lemma 1, we get that the inner sum is bounded from above by

$$\sqrt{d(n)} \lambda_1(d(n)) \sum_{k=1}^{\lfloor m(d(n)) \rfloor} 2^k f_k(d(n))$$

  from where we get our result by using lemma 2 again. ■

Acknowledgments. The author wishes to thank the reviewer for the helpful remarks.

References

[1] **Apostol, T.M.,** *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer–Verlag, 1976.

[2] **Atkin, A.O.L. and F. Morain,** Elliptic curves and primality proving, *Math. Comp.*, **61(203)** (1993), 29–68.

[3] **Bateman, P.T., S. Chowla and P. Erdős,** Remarks on the size of $L(1, \chi)$, *Publ. Math. Debrecen*, **1** (1950), 165–182.

[4] **Bosma, W., E. Cator, A. Járai and Gy. Kiss,** Primality Proofs With Elliptic Curves: Heuristics And Analysis, *Annales Univ. Sci. Budapest., Sect. Comp.*, **44** (2015), 3–27.

[5] **Elliott, P.D.T.A.,** *Probabilistic Number Theory II, Central Limit Theorems*, Springer–Verlag, 1980.

[6] **Erdélyi, A., editor,** *Higher Transcendental Functions, Vol. 2*, The Bateman Manuscript Project, McGraw-Hill, New York, 1953.

[7] **Erdős, P. and M. Kac,** The Gaussian Law of Errors in the Theory of Additive Number Theoretic Functions, *Am. J. Math.*, **62(1)** (1940), 738–742.

[8] **Hildebrand, A. and G. Tenenbaum,** On the number of prime factors of an integer, *Duke Math. J.*, **56(3)** (1988), 471–501.

[9] **Iwaniec, H. and E. Kowalski,** *Analytic Number Theory*, AMS, 2004.

[10] **Kiss, Gy.,** Primality Proofs With Elliptic Curves: Experimental Data, *Annales Univ. Sci. Budapest., Sect. Comp.*, **44** (2015), 197–210.

[11] **Lau, Y.-K. and J. Wu,** On the least quadratic non-residue, *Int. J. Number Theory*, **4(3)** (2008), 423–435.

[12] **Littlewood, J.E.,** On the class-number of the corpus $P(\sqrt{-k})$, *Proc. London Math. Soc.*, **27** (1928), 358–372.

[13] **Montgomery, H.L. and R.C. Vaughan,** *Multiplicative Number Theory: I. Classical Theory*, Cambridge University Press, 2006.

[14] **Pomerance, C.,** On the distribution of round numbers, K. Alladi (Ed.), *Number Theory*, (1984), 173–200.

[15] **Román, G.,** Primality Proofs With Elliptic Curves: Expected number of curve orders, *Annales Univ. Sci. Budapest., Sect. Comp.*, **46** (2017), 247–253.

[16] **Román, G.,** Primality Proofs With Elliptic Curves: Heuristic on the expected number of curve orders, *Annales Univ. Sci. Budapest., Sect. Comp.*, **51** (2020), 191–198.

[17] **Román, G.,** On sums of monotone functions over smooth numbers, *Acta Univ. Sapientiae Math.*, **13** (2021), 273–280.

[18] **Siegel, C.L.,** Über die Classenzahl quadratischer Zahlkörper, *Acta Arith.*, **1(1)** (1935), 83–86.

[19] **Tenenbaum, G.,** *Introduction to Analytic and Probabilistic Number Theory*, AMS, third edition, 2015.

G. Román
Department of Computer Algebra
Eötvös Loránd University
Budapest
Hungary
rogpaai@inf.elte.hu