Annales Univ. Sci. Budapest., Sect. Comp. 51 (2020) 191–198

PRIMALITY PROOFS WITH ELLIPTIC CURVES: HEURISTIC ON THE EXPECTED NUMBER OF CURVE ORDERS

Gábor Román (Budapest, Hungary)

Dedicated to the 70th birthday of Professor Antal Járai

Communicated by Gábor Farkas

(Received December 1, 2019; accepted April 25, 2020)

Abstract. In article [14] we have shown that during the downrun part of the elliptic curve primality proving algorithm, the expected number of curve orders for a given probable prime grows asymptotically as the square root of the limit until we take the negative fundamental discriminants, even if these discriminants are smooth. In this article, based on a heuristic assumption, we are going to show that this behaviour is still expectable if we only use those smooth negative fundamental discriminants which are quadratic residues modulo the tested probable prime number.

1. Introduction

The elliptic curve primality proving method, which is invented by Goldwasser and Kilian [8] then rendered useful in pactice by Atkin and Morain [2] is a recursive procedure, during which one computes a monotone decreasing sequence of probable primes in a step called the "downrun."

Key words and phrases: Elliptic curve primality proving, negative fundamental discriminant, class number, elliptic curve order, quadratic residue, Khintchine inequality, square-free number, Dirichlet L-series.
2010 Mathematics Subject Classification: 11Y11.

During the computation of the subsequent probable primes, the algorithm attempts to obtain elliptic curve orders with the aid of negative fundamental discriminants. If the current probable prime is n, then one verifies that

$$(D|n) = 1 \text{ and } (n|p) = 1 \tag{1.1}$$

holds for every p prime factor of a given D discriminant. If these requirements are satisfied, then one calculates the elliptic curve orders using the given discriminant. The probability of success during this step is driven by the $h(D)$ class number. Hence, the expected number of curve orders for a given n prime can be calculated as

$$\sum_{-d(n)\leq D\leq -7} \frac{1}{h(D)} \tag{1.2}$$

where $d(n)$ is a limit depending on n. The authors of [4] asked that what kind of asymptotic behaviour does this sum shows when the D discriminants are smooth and they satisfy requirements (1.1).

In article [14] we have showed that the expected number of curve orders behaves asymptotically as the square root of the limit $d(n)$, and showed separately that this behaviour is still present when the applied negative fundamental discriminants are smooth. The two statements can be joined as follows.

Proposition 1. *For every $\varepsilon > 0$, there exist c_1, c_2 positive real constants such that, for every large enough d one has*

$$c_1 d^{1/2-\varepsilon} \leq \sum_{-d\leq D\leq -7} \frac{1}{h(D)} \leq c_2 d^{1/2+\varepsilon}$$

where D runs over the set of d^δ-smooth negative fundamental discriminants, where $\delta > 0$.

Note that we have used a limit d in place of the previously mentioned limit $d(n)$. This is because the n probable prime doesn't have an effect on the sum while we don't include requirements (1.1) into it.

Now we are going to include the $(D|n) = 1$ condition into expression (1.2). Because of this new condition, we have to use $d(n)$ instead of d. It is sufficient to chose a strictly monotone increasing function for $d(n)$, because this way, by choosing a large enough n prime, we will be able to use the results which require a large enough d limit.

Another assumption is that $d(n) < n$ should hold, but this is not a troubling requirement as $d(n)$ should be taken as $\ln^\alpha n$ where an $\alpha \in (0, 2]$ suffices, see article [4]. (It worth mentioning that the optimal value of α depends on the factorization strategy which we apply during the downrun.)

2. The heuristic

For the rest of the article we are going to assume that n is an odd prime. We start by including the $(D|n)=1$ condition into expression (1.2), and transform it as

$$\sum_{\substack{-d(n)\le D\le -7\\(D|n)=1}} \frac{1}{h(D)} = \sum_{-d(n)\le D\le -7} \left(1+\left(\frac{D}{n}\right)\right)\frac{1}{2h(D)}$$

so when the Legendre symbol is minus one, then the given term disappears, otherwise we multiply the given term with two. This is the reason why we have included 2 in the denominator of every term. (Based on the requirements posed on n and $d(n)$, the $(D|n)=0$ case cannot arise in the sum.) We can split this finite sum as

$$\frac{1}{2}\left(\sum_{-d(n)\le D\le -7}\frac{1}{h(D)} + \sum_{-d(n)\le D\le -7}\left(\frac{D}{n}\right)\frac{1}{h(D)}\right) \tag{2.1}$$

where the behaviour of the first sum is known. Handling the second sum seems unmanagable because of the nature of the Legendre symbol, so we will live with a heuristic assumption in order to be able to guess its value. If n is an odd prime, then half of the

$$\left(\frac{1}{n}\right),\left(\frac{2}{n}\right),\ldots,\left(\frac{n-1}{n}\right)$$

sequence takes the value of 1, while the rest takes the value of -1, see theorem 9.1 in Apostol [1]. Based on this, we are going to handle the values of the Legendre symbol like they are independent and identically distributed random variables, and they are forming a sequence with Rademacher distribution. (A random variable X has Rademacher distribution if $P(X=\pm 1)=1/2$ holds.)

If we live with this heuristic assumption, then we can utilise the following inequality, see Haagerup [9].

Theorem 1. (Khintchine inequality.) *Let $\{\eta_n\}_{n=1}^N$ be mutually independent random variables with Rademacher distribution. Let $0<p<\infty$ and $x_1,\ldots,x_N$ be real numbers. Then*

$$A_p\left(\sum_{n=1}^N |x_n|^2\right)^{1/2} \le E\left(\left|\sum_{n=1}^N \eta_n x_n\right|^p\right)^{1/p} \le B_p\left(\sum_{n=1}^N |x_n|^2\right)^{1/2}$$

for some real constants $A_p, B_p>0$ depending only on p, where $E(\cdot)$ denotes the mean of a random variable.

For more information regarding the size of the constants A_p and B_p in the theorem, see the article of Haagerup [9]. Combining the previously described heuristic together with this theorem, we are going to verify the following proposition.

Heuristic proposition 1. *Let $d : \mathbb{N} \to \mathbb{R}^+$ be a strictly monotone increasing function which is in $o(n)$. If n is a large enough odd prime, then for every $\varepsilon > 0$, there exist c_1, c_2 positive real constants such that one has*

$$c_1 d(n)^{1/2-\varepsilon} \leq \sum_{\substack{-d(n)\leq D\leq -7 \\ (D|n)=1}} \frac{1}{h(D)} \leq c_2 d(n)^{1/2+\varepsilon}$$

where D runs over the set of $d(n)^\delta$-smooth negative fundamental discriminants, where $\delta > 0$.

3. Proofs

Our goal now is to bound the value of the second sum in expression (2.1). By combining our heuristic with the inequalities given in theorem 1 we note that we have to bound

$$\sum_{-d\leq D\leq -7} \frac{1}{|h(D)|^2} \tag{3.1}$$

essentially. We are going to search for an appropriate lower bound for $h(D)$, so we can give an upper bound for the sum (3.1). The most fundamental result in this area is from Siegel [15], which states, that for every $\varepsilon > 0$, there exists a c_ε positive constant, such that $c_\varepsilon |D|^{1/2-\varepsilon} < h(D)$ holds. Based on this, expression (3.1) is less than or equal to

$$\frac{1}{c_\varepsilon^2} \sum_{-d\leq D\leq -7} \frac{1}{|D|^{1-2\varepsilon}} \tag{3.2}$$

which we are going to examine first. Either by using

$$\sum_{n\leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s})$$

when $s > 0$ and $s \neq 1$, see theorem 3.2 in Apostol [1], or by approximating from above with the

$$\frac{1}{c_\varepsilon^2} \int_6^d \frac{1}{x^{1-2\varepsilon}}\, dx$$

definite integral, one can see that expression (3.2) behaves as $O(d^{2\varepsilon})$ asymptotically. Because the number of negative fundamental discriminant up to a given limit is similar to the number of square-free integers, and because the number of square-free integers up to an $x > 0$ bound can be approximated with

$$\frac{6}{\pi^2}x + O(\sqrt{x})$$

see for example page 130 of Nagell [13], it seems that we cannot squeeze out a better asymptotic from the sum by using the result of Siegel, so we have to use more subtle results. For a χ Dirichlet character define the Dirichlet L-series as

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

when $\Re(s) > 0$. (Regarding Dirichlet characters and L-series, see chapter 6 of Apostol [1].) It is known due to Dirichlet, that when $\chi(n) := (D|n)$ where $D < -4$ is a negative discriminant, then

$$h(D) = \frac{\sqrt{|D|}}{\pi} L(1,\chi) \tag{3.3}$$

holds, see section 5.3.3 of Cohen [6]. Efficient lower bounds can be given for the value of $L(1,\chi)$, see Tatuzawa [16], Hoffstein [10], Ji and Lu [11] and finally the following result from Chen [5].

Theorem 2. (Chen) *Let $0 < \varepsilon < 1/(6\ln 10)$ and χ be a real primitive Dirichlet character modulo k with $k > e^{1/\varepsilon}$. Then, with at most one exception,*

$$L(1,\chi) > \min\left\{\frac{1}{7.732\ln k}, \frac{1.5\cdot 10^6\varepsilon}{k^{\varepsilon}}\right\}$$

Using these results, the authors of [7] gave finer lower bounds for $h(D)$. Their arXiv article is marked as a preliminary version at the time of the writing of this paper, so we present a proof for their result.

Lemma 1. *For every large enough D negative fundamental discriminant,*

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

holds, where c is a real positive constant.

Proof. Let $\varepsilon := 1/\ln|D|$, and $\chi(n) := (D|n)$, which is a real primitive Dirichlet character. Solving the inequality posed on ε, we get that we can apply

Theorem 2, if $10^6 < |D|$ holds. Let us assume that this inequality is satisfied, then we have that

$$L(1,\chi) > \min\left\{\frac{1}{7.732\ln|D|}, \frac{1.5\cdot 10^6}{e\ln|D|}\right\}$$

with at most one exception. Using this in equality (3.3), we get our result. ■

Lemma 2. *For every large enough positive d one has*

$$\sum_{-d\le D\le -7}\frac{1}{|h(D)|^2}\in O(\ln^3 d)$$

where D runs over the negative fundamental discriminants.

Proof. Chose a $d > 10^6$, see proof of Lemma 1. Split the sum into two parts as

$$\sum_{-d\le D<-10^6}\frac{1}{|h(D)|^2}+\sum_{-10^6\le D\le -7}\frac{1}{|h(D)|^2} \tag{3.4}$$

where the value of the second sum can be viewed as a δ constant, and we can use the lower bound from Lemma 1 in the terms in the first sum. By these, we have that expression (3.4) is smaller than or equal to

$$\delta + c\sum_{-d\le D<-10^6}\frac{\ln^2|D|}{|D|}\le \delta + c\int_1^d\frac{\ln^2 x}{x}\,dx \tag{3.5}$$

where the expression on the right hand side is in $O(\ln^3 d)$. ■

It's worth noting that if one assumes the validity of the Generalized Riemann Hypothesis, then it can be shown that

$$h(D)\in\Omega\left(\frac{\sqrt{|D|}}{\ln\ln|D|}\right)$$

holds, see Littlewood [12]. Using this result one can prove that expression (3.1) behaves as $O(\ln d)$ asymptotically. For more results concerning $L(1,\chi)$, see [3].

Proof of the Heuristic proposition 1. We required that $d(n)\in o(n)$ should be a strictly monotone increasing function, so for large enough n, the bounds given in Proposition 1 will still hold for the first sum in expression (2.1), because $d(n)$ will be large enough.

Based on our heuristic assumption, and Lemma 2, we can apply Theorem 1 with $p = 1$, to get that the expected absolute value of the second sum in expression (2.1) can be regarded as $O(\ln^{3/2} d)$.

Let $\{\eta_n\}_{n=1}^N$ be mutually independent random variables with Rademacher distribution, and $x_1, \ldots, x_N$ be real numbers. Then because of the mutual independence-, the zero mean-, and the finite variance of the variables, one has

$$V\left(\sum_{n=1}^{N} \eta_n x_n\right) = E\left(\left|\sum_{n=1}^{N} \eta_n x_n\right|^2\right) \tag{3.6}$$

where $V(\cdot)$ donates the variance of a random variable. Based on our heuristic assumption, equality (3.6), and Lemma 2, we can apply Theorem 1 with $p = 2$, to get that the variance of the second sum in expression (2.1) can be taken as $O(\ln^3 d)$. ■

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] **Chen, Y.G.,** On the Siegel–Tatuzawa–Hoffstein theorem, *Acta Arith.*, **130(4)** (2007), 361–367.

[6] **Cohen, H.,** *A Course In Computational Algebraic Number Theory*, Springer–Verlag, third, corrected printing (1996).

[7] **Elsenhans, A.S., J. Klüners and F. Nicolae,** Imaginary quadratic number fields with class groups of small exponent, 2018, https://arxiv.org/abs/1803.02056

[8] **Goldwasser, S. and J. Kilian,** Almost all primes can be quickly certified, in: *Proceeding STOC '86 Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, (1986), 316–329.

[9] **Haagerup, U.,** The best constants in the Khintchine inequality, *Stud. Math.*, **70(3)** (1981), 231–283.

[10] **Hoffstein, J.,** On the Siegel–Tatuzawa theorem, *Acta Arith.*, **38** (1980), 167–174.

[11] **Ji, C.G. and H.W. Lu,** Lower bound of real primitive L-function at $s = 1$, *Acta Arith.*, **111(4)** (2004), 405–409.

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

[13] **Nagell, T.,** *Introduction to Number Theory*, New York, Wiley, (1951).

[14] **Román, G.,** Primality proofs with elliptic curves: Expected number of curve orders, *Annales Univ. Sci. Budapest., Sect. Comp.*, **46** (2017), 247–253.

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

[16] **Tatuzawa, T.,** On a theorem of Siegel, *Jap. J. Math.*, **21** (1951), 163–178.

G. Román
Department of Computer Algebra
Eötvös Loránd University
Budapest
Hungary
romangabor@caesar.elte.hu