Annales Univ. Sci. Budapest., Sect. Comp. 46 (2017) 247–253

PRIMALITY PROOFS WITH ELLIPTIC CURVES: EXPECTED NUMBER OF CURVE ORDERS

Gábor Román (Budapest, Hungary)

Dedicated to the memory of Professor Antal Iványi

Communicated by Antal Járai
(Received June 30, 2017; accepted September 20, 2017)

Abstract. In this paper, we are going to study the expected number of curve orders during the downrun part of the elliptic curve primality proving algorithm, when the applied negative fundamental discriminants are smooth.

1. Introduction

During the elliptic curve primality proving algorithm one proves the primality of a probable prime $n = n_0$ by recursively computing the monotone decreasing sequence of $n_1, \dots, n_k$ probable primes, until n_k is small enough that its primality can be shown easily. The details and an exact implementation can be read in [1]. The running time of this algorithm is investigated by many, and in [3] the authors reduced the heuristic running time to $o(\ln^4 n)$.

The part when one computes the decreasing sequence is called the downrun. During the step when we calculate n_{i+1} from n_i, the algorithm tries to obtain elliptic curve orders with the aid of D negative fundamental discriminants.

First, one verifies the validity of

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

Key words and phrases: Elliptic curve primality proving, negative fundamental discriminants, class numbers, elliptic curve orders, square-free numbers.
2010 Mathematics Subject Classification: 11Y11.

for every p prime factor of a given D. Then we obtain the elliptic curve orders by reducing a binary quadratic form which is computed from this discriminant D. The probability of success is driven by the $h(D)$ class number of D. So the expected number of curve orders in a step can be calculated with

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

where $d(n_i)$ is a limit which depends on n_i. The authors of [3] ask the question that what kind of asymptotic behaviour is shown by this sum, when the D numbers are smooth and they satisfy the (1.1) requirements. First, we state the following.

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

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

where D runs over the set of negative fundamental discriminants.

The sought result is that for some $c < 1/2$, the (1.2) sum is close to $\sqrt{d(n_i)}$ when the summation runs through the $d(n_i)^c$-smooth negative fundamental discriminants, or at least for $c = 1/2$. For this, we state the following.

Proposition 2. *Proposition 1 still holds when D runs over the d^δ-smooth negative fundamental discriminants, where $\delta > 0$.*

Another dominating factor during a step of the downrun part is the computation of the modular square-root of D. Here, instead of taking the modular square-root of D, we take the modular square-root of its prime factors, and compute the actual modular square-root using multiplications. With every prime factor, our chances are doubled. Let us denote the number of prime divisors of a natural number n with $\omega(n)$.

Proposition 3. *There exists a constant $c > 0$, such that*

$$c\sqrt{d} \leq \sum_{-d\leq D\leq -7} \frac{2^{\omega(|D|)}}{h(D)},$$

when d tends to $+\infty$, and D runs over the set of negative fundamental discriminants.

Of course, this sum is trivially bounded by $2d$, because every D can give us two curve orders. Obtaining a non-trivial upper bound, or a generalisation to smooth discriminants here is still a problem.

Further research is required for incorporating (1.1) requirements into these sums. One could read about the experimental behaviour of the sum with these requirements in [7].

2. Proofs

For our proofs, we are going to need the following lemma, which reduces the counting of fundamental discriminants back to the counting of square-free numbers. Let us denote the set of positive square-free numbers with Q.

Lemma 1. *For $a > 0$ we have*

$$\sum_{-a \le D} 1 \ge \sum_{\substack{n \in Q \\ n \le \frac{a}{4}}} 1$$

where D runs over the set of negative fundamental discriminants.

Proof of Lemma 1. According the definition of fundamental discriminants, D is a fundamental discriminant if

- $D \equiv 1 \pmod 4$ and D is square-free, or
- $D = 4m$ where $m \equiv 2, 3 \pmod 4$ and m is square-free.

Relying on this, for D negative fundamental discriminants

$$\sum_{-a \le D} 1 = \sum_{\substack{n \in Q \\ n \le a \\ -n \equiv 1 (4)}} 1 + \sum_{\substack{n \in Q \\ n \le \frac{a}{4} \\ -n \equiv 2,3 (4)}} 1 \ge \sum_{\substack{n \in Q \\ n \le \frac{a}{4}}} 1. \qquad \blacksquare$$

Proof of Proposition 1. Using the connection between the class numbers and the L-functions (see Proposition 5.3.12 in [5]), for every D negative fundamental discriminant, according [2] we have $h(D) \in O(\sqrt{|D|} \ln |D|)$, furthermore assuming the generalised Riemann hypothesis, according [8] we have $h(D) \in O(\sqrt{|D|} \ln \ln |D|)$, so

$$h(D) \in O(|D|^{\frac{1}{2}+\varepsilon})$$

for every $\varepsilon > 0$. Using this,

$$\sum_{-d \le D \le -7} \frac{1}{h(D)} \ge \sum_{-d \le D \le -7} \frac{1}{c_\varepsilon |D|^{\frac{1}{2}+\varepsilon}} \ge \frac{1}{c_\varepsilon d^{\frac{1}{2}+\varepsilon}} \sum_{-d \le D \le -7} 1,$$

where $c_\varepsilon > 0$ depends on ε. According [10], the asymptotic number of square-free numbers less than or equal to x is $6x\pi^{-2} + O(\sqrt{x})$. Applying Lemma 1 on the sum and using this result, we get our lower bound.

For the upper bound, according the results of [12], for every $\varepsilon > 0$, there exists a c_ε positive constant such $c_\varepsilon |D|^{\frac{1}{2}-\varepsilon} < h(D)$ holds. Now for $0 < \varepsilon < \frac{1}{2}$ one has

$$\sum_{-d \le D \le -7} \frac{1}{h(D)} \le \sum_{-d \le D \le -7} \frac{1}{c_\varepsilon |D|^{\frac{1}{2}-\varepsilon}} \le \frac{1}{c_\varepsilon} \int_6^d \frac{1}{x^{\frac{1}{2}-\varepsilon}} dx,$$

which gives us our upper bound after integration. ■

Proof of Proposition 2. The proven upper bound in Proposition 1 will still hold for smooth negative fundamental discriminants. For the lower bound, we are going to use the following result. For large enough x, the count of x^δ-smooth square-free numbers in the $[x \dots x + x^{\frac{1}{2}+\varepsilon}]$ interval is

$$\Omega\left(\frac{x^{\frac{1}{2}+\varepsilon}}{\ln^{\lfloor \delta^{-1} \rfloor + 1} x}\right),$$

where $0 < \varepsilon < \frac{1}{2}$ and $\delta > 0$, according to [4].

Assume that d is large enough, that the mentioned theorem is valid for $x \ge \sqrt{d} \ge 2$. Then in the

$$\left[\frac{d}{2^i} \dots \frac{d}{2^i} + \left(\frac{d}{2^i}\right)^{\frac{1}{2}+\varepsilon}\right] \subseteq \left[\frac{d}{2^i} \dots \frac{d}{2^{i-1}}\right] \quad \left(i = 1, 2, \dots, \left\lfloor \frac{\log_2 d}{2} \right\rfloor\right)$$

intervals the count of $\left(\frac{d}{2^i}\right)^\delta$-smooth square-free numbers is at least

$$c \frac{\frac{d}{2^i}}{\ln^{\lfloor \delta^{-1} \rfloor + 1} \frac{d}{2^i}}.$$

Now if D runs over the d^δ-smooth negative fundamental discriminants, then

$$\sum_{-d \le D \le -7} 1 \ge c \sum_{i=1}^{\left\lfloor \frac{\log_2 d}{2} \right\rfloor} \frac{\frac{d}{2^i}}{\ln^{\lfloor \delta^{-1} \rfloor + 1} \frac{d}{2^i}} \ge c \frac{d}{\ln^{\lfloor \delta^{-1} \rfloor + 1} d} \sum_{i=1}^{\left\lfloor \frac{\log_2 d}{2} \right\rfloor} \frac{1}{2^i},$$

where the later sum is less than 1 and greater than $\frac{1}{2}$, so

$$\sum_{-d \le D \le -7} 1 \ge \frac{c}{2} \frac{d}{\ln^{\lfloor \delta^{-1} \rfloor + 1} d}.$$

If we follow the method in the proof of Proposition 1, but substituting this result instead of the asymptotic number of square-free numbers, we get our lower bound. ■

For the proof of Proposition 3 we will need the following lemma.

Lemma 2. *For an $a > 0$ positive number*

$$\sum_{-a \le D} 2^{\omega(|D|)} \ge \sum_{\substack{n \in Q \\ n \le \frac{a}{4}}} 2^{\omega(n)}$$

where D runs over the set of negative fundamental discriminants.

Proof of Lemma 2. As in the proof of Lemma 1, we separate the sum according the definition of fundamental discriminants. So

$$\sum_{-a \le D} 2^{\omega(|D|)} = \sum_{\substack{n \in Q \\ n \le a \\ -n \equiv 1(4)}} 2^{\omega(n)} + \sum_{\substack{n \in Q \\ n \le \frac{a}{4} \\ -n \equiv 2(4)}} 2^{\omega(4n)} + \sum_{\substack{n \in Q \\ n \le \frac{a}{4} \\ -n \equiv 3(4)}} 2^{\omega(4n)} =$$

$$= \sum_{\substack{n \in Q \\ n \le a \\ -n \equiv 1(4)}} 2^{\omega(n)} + \sum_{\substack{n \in Q \\ n \le \frac{a}{4} \\ -n \equiv 2(4)}} 2^{\omega(n)} + 2 \sum_{\substack{n \in Q \\ n \le \frac{a}{4} \\ -n \equiv 3(4)}} 2^{\omega(n)} \ge \sum_{\substack{n \in Q \\ n \le \frac{a}{4}}} 2^{\omega(n)}. \qquad ■$$

Proof of Proposition 3. When x tends to $+\infty$, according to [11] and [6] one has

$$\sum_{\substack{n \in Q \\ n \le x}} z^{\omega(n)} = xG(z)(\ln x)^{z-1} + O(x(\ln x)^{\Re z - 2}),$$

with an arbitrary z complex number and

$$G(z) = \frac{1}{\Gamma(z)} \prod_{p} \left(1 + \frac{z}{p}\right) \left(1 - \frac{1}{p}\right)^{z},$$

where p in the product runs over the set of prime numbers. Using this result and Lemma 2, when d is large enough, we get

$$\sum_{-d \le D \le -7} 2^{\omega(|D|)} \ge \sum_{\substack{n \in Q \\ n \le \frac{d}{4}}} 2^{\omega(n)} - 12 \ge \frac{d}{4} G(2) \ln \frac{d}{4} - c_1 \frac{d}{4} - 12$$

where $G(2)$ is a positive constant [9], and $c_1 \in \mathbb{R}$ is for handling the asymptotic part of the cited result. Recalling the mentioned results in the proof of Proposition 1, we have such $c_2 > 0$ that

$$\sum_{-d \leq D \leq -7} \frac{2^{\omega(|D|)}}{h(D)} \geq \frac{c_2}{\sqrt{d} \ln d} \sum_{-d \leq D \leq -7} 2^{\omega(|D|)}.$$

Substituting the estimation for the sum, we get that the right hand side is greater than

$$G(2) \frac{c_2}{4} \sqrt{d} \left(1 - \frac{\ln 4}{\ln d}\right) - \sqrt{d} \frac{c_1 c_2}{4 \ln d} - 12 \frac{c_2}{\sqrt{d} \ln d}$$

which gives us our lower bound. ■

References

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

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

[3] **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.

[4] **Charles, D. X.,** Squarefree integers without large prime factors in short intervals, *University of Wisconsin, Madison, Computer Science Department*, Technical report 1432 (2001), 1–5.

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

[6] **Delange, H.,** Sur des formules de Atle Selberg, *Acta Arithmetica*, **19(2)** (1971), 105–146.

[7] **Kiss, Gy.,** Primality proofs with elliptic curves: Experimental data, *Annales Univ. Sci. Budapest., Sect. Comp.*, **44** (2015), 197–210.

[8] **Littlewood, J. E.,** On the class-number of the corpus $P(\sqrt{-k})$, *Proc. London Math. Soc.*, **27(2)** (1928), 358–372.

[9] **Moree, P.,** Counting carefree couples, *arXiv* (2005), 1–12. `https://arxiv.org/abs/math/0510003`

[10] **Nagell, T.** *Introduction to Number Theory*, Wiley, New York, 1951.

[11] **Selberg, A.** Note on a paper by L. G. Sathe, *Journ. Indian Math. Soc.*, **18** (1954), 83–87.

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

G. Román
Department of Computer Algebra
Faculty of Informatics
Eötvös Loránd University
H-1117 Budapest
Pázmány Péter sétány 1/C
Hungary
romangabor@caesar.elte.hu