Annales Univ. Sci. Budapest., Sect. Comp. 52 (2021) 279–291

PRIMALITY PROOFS WITH ELLIPTIC CURVES: ON THE DISTRIBUTION AND THE EXPECTED VALUE OF THE GAIN DURING DOWNRUN

Gábor Román (Budapest, Hungary)

Communicated by Antal Járai

(Received December 18, 2020; accepted July 8, 2021)

Abstract. In this article, we give heuristic approximation for the distribution, and the expected value of the gain during one step of the downrun part of the elliptic curve primality proving method.

1. Introduction

The elliptic curve primality proving method was introduced by Goldwasser and Kilian, see article [7]. Their technique is based on the following theorem.

Theorem 1. *Let $n \neq 1$ be an integer coprime to 6, and E_n be an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$. Assume that we know an integer m, and a point $P \in E_n$ satisfying the following conditions.*

1. *There exists a prime divisor q of m such that $q > (\sqrt[4]{n}+1)^2$ holds,*
2. *$mP = 0_{E_n} = (0:1:0)$,*
3. *and $(m/q)P = (x:y:t)$ with $t \in \mathbb{Z}/n\mathbb{Z}^*$.*

Then n is a prime. (It is assumed the all the computations are possible.)

Key words and phrases: Elliptic curve primality proving, elliptic curve order, primes in short intervals, smooth numbers in short intervals, Dickman function.
2010 Mathematics Subject Classification: 11Y11.

This theorem enables us to compute a probable prime q which is smaller than our initial probable prime n. The question of how to choose the required m is answered by the following theorem.

Theorem 2. *Let n be an integer coprime to 6, E_n be an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$, and $m := |E_n|$. If m has a prime divisor q satisfying $q > (\sqrt[4]{n}+1)^2$, then there exists a point $P \in E_n$ such that $mP = 0_{E_n}$, and $(m/q)P = (x : y : t)$ with $t \in \mathbb{Z}/n\mathbb{Z}^*$.*

So by selecting an elliptic curve, and by computing the number of points on it, we get a useful m. Atkin and Morain switched the order of computation, as they construct the elliptic curve for a previously computed curve order, effectively rendering the method useful in practice, see article [3].

Proceeding recursively, we get a decreasing sequence of probable primes n_i, until a point, where the primality of the actual probable prime can be verified more easily by some other method. This descent is called the "downrun".

The number of levels is governed by the difference between $\ln n_i$ and $\ln n_{i+1}$, which essentially depends on how much time we are willing to spend on the factorisation of a given curve cardinality. Spending too much time renders the method slow, so an important control point of the factorisation is the applied smoothness bound $b : \mathbb{N} \to \mathbb{R}^+$, which is a monotone increasing function. We require that $b(n) \in o(n^\xi)$ should hold for every $\xi > 0$.

This smoothness bound is chosen to be $(\ln n)^\alpha$, where α is a positive constant. Take note that we can still use the presented results if we can give inequalities $(\ln n)^{\alpha_1} \leq b(n) \leq (\ln n)^{\alpha_2}$, where $\alpha_1 < \alpha_2$ are positive constants. The authors of article [4] ask the following question.

Suppose that, applying the different factorisation methods with various parameters to find prime factors, one succeeds in factoring completely the cardinality of a given elliptic curve modulo n, what is the expected value and distribution of the "gain", defined as log of the "smooth part" of the cardinality?

Concerning the distribution, we have the following heuristic proposition.

Heuristic proposition 1. *Let the currently examined probable prime be n. Assuming that we successfully find the complete factorisation of the curve orders, using the above defined smoothness bound, the probability that the gain will be $\lambda \ln_2 n$ for positive $\lambda \leq \lambda_{\max}$ can be approximated with*

$$\frac{\rho(\lambda/\alpha)}{\ln n - \lambda \ln_2 n}\left(1 + O\left(\frac{\ln(\lambda/\alpha + 1)}{\alpha \ln_2 n}\right)\right),$$

where ρ is the Dickman function.

Here $\ln_k$ is the k-fold iterated logarithm. Take note that the variable $\lambda_{\max}$ is just a technicality, for more information regarding it, see Section 4, where

we are going to demonstrate this proposition based on certain heuristics, after describing the required tools in Section 2 and 3. (The reader can find more information about the Dickman function in Section 3.)

Assume that we have arrived at a certain level of the downrun, and let's denote the currently examined probable prime as n. Taking into consideration point 1 of theorem 1, the size of the smooth part of the cardinality is well below $\sqrt{n}$. Based on our smoothness bound, looking for the smooth part in the size of n^λ for $\lambda \in (0, 1/2)$ is too optimistic, and we expect a size of $(\ln n)^\lambda$ for some small $\lambda > 0$.

Heuristic proposition 2. *The expected value of λ in Heuristic proposition 1 can be approximated with $e^\gamma \alpha + o_n(1)$.*

We will verify this proposition in Section 5. This result coincides with the expectations of the authors of article [4], namely that the gain remains $\asymp \ln b(n)$ independently of the applied factorisation method. What we have sketched here is that if the applied factorisation method *can* produce the complete factorisation of a curve cardinality, then the properties of the curve cardinalities supposedly won't hinder us in reaching this gain of $\ln b(n)$.

Next to the concretisation of these observations, examining the distribution, and the expected value while using $b(n) := (\ln n)^{\alpha(n)}$, with $\alpha : \mathbb{N} \to \mathbb{R}^+$ being a monotone increasing function would be another important task.

2. Primes in short intervals

Based on the prime number theorem, one would expect that for certain functions Φ, the asymptotic relation

$$\pi(x + \Phi(x)) - \pi(x) \sim \frac{\Phi(x)}{\ln x} \tag{2.1}$$

holds as x tends to positive infinity. When the function Φ grows fast, then this statement certainly holds; the real question here is that how slowly increasing Φ can be to still have this relation. We recall the concise summary of the results of this area from [21].

It has been shown that one can choose $\Phi(x) = x^{7/12-\varepsilon(x)}$, where $\varepsilon(x)$ goes to zero as x tends to positive infinity, see the article of Heath-Brown [11]. It is briefly explained in this article that by using the Riemann hypothesis, one can reach $\Phi(x) = x^{1/2+\varepsilon}$, where $\varepsilon > 0$.

If we are willing to throw away some numbers, then we can choose even slower functions. Indeed, using the results from the article of Huxley [14], relation (2.1) still holds for the functions $\Phi(x) = x^{1/6+\varepsilon}$ for almost all x, where

$\varepsilon > 0$. Selberg showed in his article [19], that by assuming the Riemann hypothesis, relation (2.1) is true for almost all x, if $\Phi(x)/(\ln x)^2$ goes to positive infinity with x.

On the other hand, Φ should grow with a certain speed, which can be also seen from the relation

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{(\ln n)(\ln_2 n)(\ln_4 n)/(\ln_3 n)^2} > 0,$$

where p_n is the nth prime, see the article of Rankin [18]. Based on probabilistic arguments, Cramér stated in his article [6] that $p_{n+1} - p_n \in O((\ln p_n)^2)$ holds, however Maier showed in his article [17] that

$$\limsup_{x\to\infty} \frac{\pi(x + \Phi(x)) - \pi(x)}{\Phi(x)/\ln x} > 1, \text{ and } \liminf_{x\to\infty} \frac{\pi(x + \Phi(x)) - \pi(x)}{\Phi(x)/\ln x} < 1$$

for $\Phi(x) = (\ln x)^\lambda$, where $\lambda > 1$.

3. Smooth numbers in short intervals

Extensive investigation has been made concerning the number of smooth integers defined as

$$\Psi(x, y) := |\{1 \le n \le x : P(n) \le y\}|$$

where $P(n)$ denotes the greatest prime divisor of n, with the convention that $P(1) = 1$, see for example article [13]. It is shown that $\Psi(x, y) \sim x\rho(u)$, where ρ is the Dickman function, and u is defined as $(\ln x)/\ln y$. Similarly to the prime number theorem in Section 2, this result suggests that

$$\Psi(x + z, y) - \Psi(x, y) \sim z\rho(u)$$

should hold at least when z is not too small. The following theorem is proved by Hildebrand, see article [12].

Theorem 3. *For any fixed $\varepsilon > 0$, uniformly in the range $y \ge 2$,*

$$1 \le u \le \exp((\ln y)^{3/5-\varepsilon})$$

and for $xy^{-5/12} \le z \le x$, we have that the equality

$$\Psi(x + z, y) - \Psi(x, y) = z\rho(u)\left(1 + O\left(\frac{\ln(u + 1)}{\ln y}\right)\right)$$

holds.

The Dickman function ρ is a continuously differentiable on $\mathbb{R}^+ \setminus \{1\}$, and it satisfies the delay differential equation

$$u\rho'(u) + \rho(u-1) = 0 \tag{3.1}$$

for $u > 1$, with the initial condition $\rho(u) = 1$ for $0 \le u \le 1$. This function keeps to zero quite fast as u grows, namely it can be shown that the inequality $\rho(u) \le 1/\Gamma(u+1)$ holds for $u \ge 0$, see theorem 5.7 in [20]. So we have

$$\lim_{u\to+\infty} u^k \rho(u) = 0 \tag{3.2}$$

for fixed $k \in \mathbb{Z}$. Based on the delay differential equation (3.1), one can show that

$$\rho(u) = \frac{1}{u} \int\limits_{u-1}^{u} \rho(v)\, dv \tag{3.3}$$

holds when $u \ge 1$, see theorem 5.7 in [20]. (Take note that the $1/u$ part is missing in the reference due to a typographical error.) It can be also shown that

$$\int\limits_{0}^{u} \rho(v)\, dv = e^{\gamma} + O(e^{-u}) \tag{3.4}$$

as $u \to \infty$, see article [5], and article [16]. Now we are going to demonstrate the generalisation of this result.

Lemma 1. *Let k be a non-negative integer. Then we have that the equality*

$$\int\limits_{0}^{u} v^k \rho(v)\, dv = c_k e^{\gamma} + O(e^{-u})$$

holds as $u \to \infty$, where $c_0 := 1$, and

$$c_k := \frac{1}{k} \sum_{l=0}^{k-1} \binom{k}{l} c_l$$

for $k > 0$.

Proof. We are going to prove our statement by using induction. Equality (3.4) covers the case $k = 0$. Assuming that our equality holds until $k-1$, with

k being positive, we are going to show that it holds for k also. Integrating by parts, we get the equality

$$(k+1)\int_0^u v^k\rho(v)\,dv = \left[v^{k+1}\rho(v)\right]_0^u - \int_0^u v^{k+1}\rho'(v)\,dv. \tag{3.5}$$

By using equality (3.1), we get

$$u^{k+1}\rho(u) + \int_1^u v^k\rho(v-1)\,dv = u^{k+1}\rho(u) + \int_0^{u-1}(t+1)^k\rho(t)\,dt$$

where we substituted $t = v-1$. Looking only at the integral alone, we can apply the binomial theorem to get

$$\int_0^{u-1}\rho(t)\sum_{l=0}^{k-1}\binom{k}{l}t^l\,dt + \int_0^{u-1}t^k\rho(t)\,dt,$$

where we can write the last integral as

$$\int_0^{u-1}t^k\rho(t)\,dt = \int_0^u t^k\rho(t)\,dt - \int_{u-1}^u t^k\rho(t)\,dt.$$

Looking at our initial expression on the left hand side of equality (3.5), by joining the terms computed so far, and by doing some rearrangements, we get the equality

$$\int_0^u v^k\rho(v)\,dv = \frac{1}{k}\sum_{l=0}^{k-1}\binom{k}{l}\int_0^{u-1}v^l\rho(v)\,dv + \frac{u^{k+1}}{k}\rho(u) - \frac{1}{k}\int_{u-1}^u v^k\rho(v)\,dv,$$

where by using equality (3.3), and (3.2), we can show that the last two terms on the right hand side keep to zero, and based on the rate of decrease of the Dickman function, they do it much faster than e^{-u} does. Substituting the asymptotic for the integrals inside the sum, we get our statement.

One last thing that needs to be considered is the accumulating error term

$$\frac{1}{k}\sum_{l=0}^{k-1}\binom{k}{l}O(e^{-u}) = O(e^{-u})\frac{2^k-1}{k}$$

but for a fixed k, these stay in $O(e^{-u})$ as u tends to positive infinity. ■

Take note that one could prove this statement also by using

$$\int_0^t \tau^k \rho(\tau)\, d\tau = \mathcal{L}^{-1}\left\{\frac{1}{s}\mathcal{L}\{\tau^k \rho(\tau)\}(s)\right\}(t)$$

as the Laplace transform of the Dickman function is known, see Theorem 5.10 in [20], and it behaves well under differentiation, but this path is a bit more complicated.

Using the constants c_k defined for $k \geq 0$ in lemma 1, introduce

$$C_r(x) := \sum_{k=0}^{r} c_k x^k,$$

where r is a non-negative integer.

Lemma 2. *Let r be a positive integer. Then for $x \geq 0$ we have*

$$C_r(x) = 1 - \ln(1-x) + R_r(x),$$

where

$$\lim_{x \to 0^+} R_r(x) = 0$$

holds.

What is important for us here is actually the logarithmic part of $C_r(x)$, as it will help us in the cancellation of certain terms later.

Proof. By using the definition of c_k from lemma 1, we get

$$C_r(x) - 1 = \sum_{k=1}^{r} c_k x^k = \sum_{k=1}^{r}\sum_{l=0}^{k-1} \binom{k}{l} c_l \frac{x^k}{k} = \sum_{l=0}^{r-1} c_l \sum_{k=l+1}^{r} \binom{k}{l} \frac{x^k}{k},$$

where we have switched the order of summation. By shifting the index of the innermost sum, we get

$$\sum_{l=0}^{r-1} c_l x^{l+1} \sum_{k=0}^{r-l-1} \binom{k+l+1}{l} \frac{x^k}{k+l+1} = \sum_{l=0}^{r-1} c_l x^{l+1} \sum_{k=0}^{r-l-1} \binom{k+l}{l} \frac{x^k}{k+1}$$

because of the properties of the binomial coefficients. Separating the case $l = 0$ from the sum, we get

$$x \sum_{k=0}^{r-1} \frac{x^k}{k+1} + \sum_{l=1}^{r-1} c_l x^{l+1} \sum_{k=0}^{r-l-1} \binom{k+l}{l} \frac{x^k}{k+1},$$

where the first sum is equal to

$$\int_0^x \sum_{k=0}^{r-1} u^k\,du = \int_0^x \frac{1-u^r}{1-u}\,du = -\ln(1-x) - \int_0^x u^r(1-u)^{-1}\,du.$$

Substituting as $u = xt$, we get

$$x^{r+1}\int_0^1 t^r(1-xt)^{-1}\,dt = \frac{x^{r+1}}{r+1}{}_2F_1(1, r+1; r+2; x),$$

where we have used the integral representation of the Gauss hypergeometric function, see equation 15.3.1 in [1]. Now we can define

$$R_r(x) := -\frac{x^{r+1}}{r+1}{}_2F_1(1, r+1; r+2; x) + \sum_{l=1}^{r-1} c_l x^{l+1} \sum_{k=0}^{r-l-1} \binom{k+l}{l} \frac{x^k}{k+1}$$

which keeps to zero as x tends to zero from the right, as the hypergeometric function is continuous for $|x| < 1$, and it is equal to 1 when $x = 0$, furthermore all the other parts keep to zero. ■

4. The distribution

Let's assume that we've succeeded in factoring completely the cardinality of a given elliptic curve modulo a prime n, into the form fq, where f should be $b(n)$-smooth, and q should be a prime of the right size. Now we are going to look at the probability of these events separately.

First we look at the probability of finding a $b(n)$-smooth f in a small interval around $(\ln n)^\lambda$. When $0 \le \lambda \le \alpha$, then this probability is one, which coincides with $\rho(\lambda/\alpha)$ for such λ, otherwise we can use theorem 3 to have

$$\frac{\Psi((\ln n)^\lambda + z, (\ln n)^\alpha) - \Psi((\ln n)^\lambda, (\ln n)^\alpha)}{z} = \rho(\lambda/\alpha)\left(1 + O\left(\frac{\ln(\lambda/\alpha + 1)}{\alpha \ln_2 n}\right)\right),$$

when

$$1 < \lambda/\alpha \le \tau(n) < e^{(\alpha \ln_2 n)^{3/5-\varepsilon}}$$

for fixed $\varepsilon > 0$, and where z can be chosen conveniently according the conditions presented in Theorem 3. Take note that the asymptotic error term here disappears as n goes to infinity. The threshold $\tau : \mathbb{N} \to \mathbb{R}^+$ should be a strictly monotone increasing function, however one should choose it in a manner so that f remains in $o(n^\xi)$ for $\xi > 0$.

For such $b(n)$-smooth f, we have to choose a big enough prime q. Taking Theorem 2 into consideration, we have to recall an important result from the theory of elliptic curves. The following theorem is conjectured by Artin, see article [2], and proven by Hasse, see articles [8, 9, 10].

Theorem 4. *Let $p > 3$ be a prime. Then for the order m of an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$ we have that the inequality*

$$|p - (m + 1)| \leq 2\sqrt{p}$$

holds.

Lenstra showed, see proposition (1.9) in [15], that for any prime $p > 3$, the probability that the order m of an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$ will satisfy the inequality $|p - (m + 1)| \leq \sqrt{p}$ is in $\mathcal{O}(1/\ln p)$. Note that this can be improved to $\mathcal{O}(1/\ln_2 p)$ if we assume that the Riemann hypothesis holds. So we can suppose that the curve orders will be distributed uniformly in the interval in Theorem 4, or at least in the middle of the interval.

Based on these, for a given f, we have to choose uniformly a prime q from the interval $[(n - 2\sqrt{n} + 1)/f, (n + 2\sqrt{n} + 1)/f]$. Taking into consideration the maximal size of f, this interval is not empty, and a prime from it will satisfy point 1. of Theorem 1. Using the results concerning the number of primes in short intervals presented in Section 2, we can approximate the probability of success as

$$\frac{1}{\ln(n/f)} \approx \frac{1}{\ln n - \lambda \ln_2 n}.$$

The event of finding a smooth number, and the event of finding a prime in a given interval can be treated as independent events, so after multiplying the two probabilities, we get our Heuristic proposition 1.

5. The expected value

Now we demonstrate Heuristic proposition 2 by approximating the expected value of λ in Heuristic proposition 1 with the integrals

$$\int_0^{\tau(n)} \frac{\lambda\rho(\lambda/\alpha)}{\ln n - \lambda \ln_2 n}\, d\lambda + \frac{c}{\alpha \ln_2 n} \int_\alpha^{\tau(n)} \frac{\lambda\rho(\lambda/\alpha)\ln(\lambda/\alpha + 1)}{\ln n - \lambda \ln_2 n}\, d\lambda,$$

where c is some real constant. We are going to look at the integrals separately.

- First we look at the first integral. Substituting as $\lambda = \alpha u$, we get

$$\int_0^{\tau(n)} \frac{\lambda\rho(\lambda/\alpha)}{\ln n - \lambda \ln_2 n}\, d\lambda = \frac{\alpha^2}{\ln n} \int_0^{\tau(n)/\alpha} \frac{u\rho(u)}{1 - u\frac{\alpha \ln_2 n}{\ln n}}\, du.$$

Now we subtract and add back the integral

$$\frac{\alpha^2}{\ln n}\int_0^{\tau(n)/\alpha} u\rho(u)\frac{(u\frac{\alpha\ln_2 n}{\ln n})^r}{1-u\frac{\alpha\ln_2 n}{\ln n}}\,du$$

for some fixed positive integer r, to get on the one hand

$$\frac{\alpha^2}{\ln n}\int_0^{\tau(n)/\alpha} u\rho(u)\frac{1-(u\frac{\alpha\ln_2 n}{\ln n})^r}{1-u\frac{\alpha\ln_2 n}{\ln n}}\,du$$

and on the other hand

$$\frac{\alpha^{r+2}(\ln_2 n)^r}{(\ln n)^{r+1}}\int_0^{\tau(n)/\alpha}\frac{u^{r+1}\rho(u)}{1-u\frac{\alpha\ln_2 n}{\ln n}}\,du.$$

Now we are going to look at the two terms separately.

– Using the formula for the sum of the geometric progression, and switching the order of integration and summation, we get that the first term is

$$\frac{\alpha^2}{\ln n}\sum_{k=0}^{r-1}\left(\frac{\alpha\ln_2 n}{\ln n}\right)^k\int_0^{\tau(n)/\alpha} u^{k+1}\rho(u)\,du.$$

Using Lemma 1, we get

$$e^\gamma\frac{\alpha^2}{\ln n}\sum_{k=0}^{r-1}c_{k+1}\left(\frac{\alpha\ln_2 n}{\ln n}\right)^k+\frac{\alpha^2}{\ln n}O(e^{-\tau(n)/\alpha})\sum_{k=0}^{r-1}\left(\frac{\alpha\ln_2 n}{\ln n}\right)^k$$

where the second part goes to zero as n tends to positive infinity. The first part however is equal to

$$e^\gamma\frac{\alpha}{\ln_2 n}\sum_{k=0}^{r-1}c_{k+1}\left(\frac{\alpha\ln_2 n}{\ln n}\right)^{k+1}=e^\gamma\frac{\alpha}{\ln_2 n}\left(C_r\left(\frac{\alpha\ln_2 n}{\ln n}\right)-1\right),$$

where we can use Lemma 2 to have

$$e^\gamma\frac{\alpha}{\ln_2 n}\ln\frac{1}{1-\frac{\alpha\ln_2 n}{\ln n}}+e^\gamma\frac{\alpha}{\ln_2 n}R_r\left(\frac{\alpha\ln_2 n}{\ln n}\right)$$

which is equal to $e^\gamma\alpha+o_n(1)$.

– As for the second term, by using integration by parts, we get

$$-\frac{\alpha^{r+1}(\ln_2 n)^{r-1}}{(\ln n)^r}\left[\ln\left(1-u\frac{\alpha\ln_2 n}{\ln n}\right)u^{r+1}\rho(u)\right]_0^{\tau(n)/\alpha}$$

which is in $o_n(1)$, and

$$\frac{\alpha^{r+1}(\ln_2 n)^{r-1}}{(\ln n)^r}\int_0^{\tau(n)/\alpha}\ln\left(1-u\frac{\alpha\ln_2 n}{\ln n}\right)\frac{d}{du}u^{r+1}\rho(u)\,du.$$

The absolute value of this expression is smaller than

$$\frac{3\alpha^{r+2}(\ln_2 n)^r}{2(\ln n)^{r+1}}\int_0^{\tau(n)/\alpha}u\frac{d}{du}u^{r+1}\rho(u)\,du$$

for large enough n, see inequality 4.1.35 in [1]. Integrating by parts again, we get

$$\frac{3\alpha^{r+2}(\ln_2 n)^r}{2(\ln n)^{r+1}}\left([u^{r+2}\rho(u)]_0^{\tau(n)/\alpha}-\int_0^{\tau(n)/\alpha}u^{r+1}\rho(u)\,du\right)$$

where both terms are in $o_n(1)$.

- Now we turn to the second integral. The logarithmic part of the numerator is positive and we have

$$\ln(\lambda/\alpha+1)<\ln\lambda-\ln\alpha+\frac{\alpha}{\lambda} \tag{5.1}$$

because $\lambda/\alpha\geq 1$, so at the end of the day, we only have to deal with the expression

$$\frac{c}{\alpha\ln_2 n}\int_\alpha^{\tau(n)}\frac{\lambda\rho(\lambda/\alpha)\ln\lambda}{\ln n-\lambda\ln_2 n}\,d\lambda$$

because the integrals containing the terms other than $\ln\lambda$ at the right hand side of the inequality (5.1) will be in $o_n(1)$ based on the previous computations. By substituting $\exp((\alpha\ln_2 n)^{3/5-\varepsilon})$ inside the logarithmic part of the integrand for some fixed $\varepsilon>0$, we do an overestimation. As

$$\frac{(\alpha\ln_2 n)^{3/5-\varepsilon}}{\ln_2 n}$$

goes to zero as n tends to positive infinity, we get that this last expression does too, yet again based on the previously computed integrals.

Collecting all the terms we have calculated, we get our Heuristic proposition 2.

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

References

[1] **Abramowitz, M. and I.A. Stegun,** *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, Applied Mathematics Series 55, tenth printing, Dover publications, 1972.

[2] **Artin, E.,** Quadratische Körper im Gebiete der höheren Kongruenzen. I. (Arithmetischer Teil.), *Math. Z.*, **19** (1924), 207–246.

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

[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] **de Bruijn, N.G.,** The asymptotic behaviour of a function occurring in the theory of primes, *J. Indian Math. Soc.* (*N.S.*), **15** (1951), 25–32.

[6] **Cramér, H.,** On the order of magnitude of the difference between consecutive prime numbers, *Acta Arith.*, **2(1)** (1936), 23–46.

[7] **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.

[8] **Hasse, H.,** Zur Theorie der abstrakten elliptischen Funktionenkörper I. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung. *J. Reine Angew. Math.*, **175** (1936), 55–62.

[9] **Hasse, H.,** Zur Theorie der abstrakten elliptischen Funktionenkörper II. Automorphismen und Meromorphismen. Das Additionstheorem. *J. Reine Angew. Math.*, **175** (1936), 69–88.

[10] **Hasse, H.,** Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung. *J. Reine Angew. Math.*, **175** (1936), 193–208.

[11] **Heath-Brown, D.R.,** The number of primes in a short interval, *J. reine angew. Math.*, **389** (1988), 22–63.

[12] **Hildebrand, A.,** On the number of positive integers $\leq x$ and free of prime factors $> y$, *J. Number Theory*, **22** (1986), 289–307.

[13] **Hildebrand, A. and G. Tenenbaum,** Integers without large prime factors, *J. Théor. Nr. Bordx*, **5(2)** (1993), 411–484.

[14] **Huxley, M.N.,** On the difference between consecutive primes, *Inventiones Math.*, **15** (1972), 164–170.

[15] **Lenstra, H.W., Jr.,** Factoring integers with elliptic curves, *Ann. of Math.*, **126** (1987), 649–673.

[16] **van Lint, J.H. and H.E. Richert,** Über die Summe $\sum_{\substack{n\leq x\\ p(n)<y}} \frac{\mu^2(n)}{\varphi(n)}$, in: *Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen: Series A: Mathematical Sciences*, **67(5)** (1964), 582–587.

[17] **Maier, H.,** Primes in short intervals, *Michigan Math. J.*, **32(2)** (1985), 221–225.

[18] **Rankin, R.A.,** The difference between consecutive primes, *J. London Math. Soc.*, **13(4)** (1938), 242–247.

[19] **Selberg, A.,** On the normal density of primes in small intervals, and the difference between consecutive primes, *Arch. Math. Naturvid*, **47(6)** (1943), 87–105.

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

[21] **Yildirim, C.Y.,** A survey of results on primes in short intervals, in: *Number Theory and its Applications* (*Ankara, 1996*), Lecture Notes in Pure and Appl. Math. 204, Dekker, New York, 1999.

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