MATHEMATICS OF COMPUTATION
Volume 81, Number 278, April 2012, Pages 1093–1110
S 0025-5718(2011)02543-3
Article electronically published on September 29, 2011

ON THE NUMBER OF ISOGENY CLASSES OF PAIRING-FRIENDLY ELLIPTIC CURVES AND STATISTICS OF MNT CURVES

JORGE JIMÉNEZ URROZ, FLORIAN LUCA, AND IGOR E. SHPARLINSKI

Abstract. We give an upper bound on the number of finite fields over which elliptic curves of cryptographic interest with a given embedding degree and small complex multiplication discriminant may exist, and present some heuristic arguments which indicate that this bound is tight. We also refine some heuristic arguments on the total number of so-called MNT curves with prime cardinalities which have been recently presented by various authors.

1. Introduction

1.1. **Motivation.** Following the pioneering works [6, 7, 15, 16, 25, 26], a diverse scope of cryptographic applications of the Tate, Weil, and other pairings has been discovered (see [1, 5, 10] and references therein). For a background on elliptic curves, see [4, 27].

In this context, the notion of *embedding degree* plays the central role. Recall that an elliptic curve $\mathbf{E}$ over the finite field $\mathbb{F}_q$ of q elements has embedding degree k with respect to the subgroup $\mathcal{G}$ of the group $\mathbf{E}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on $\mathbf{E}$, if $\#\mathcal{G} \mid q^k - 1$, and k is the smallest positive integer with this property. Typically, only subgroups $\mathcal{G}$ of prime order ℓ of $\mathbf{E}(\mathbb{F}_q)$ are of interest.

The above applications have naturally led to two mutually complementing problems:

- Estimating the probability that a "random" elliptic curve (in some sense) has a small embedding degree with respect to a subgroup $\mathcal{G}$ of $\mathbf{E}(\mathbb{F}_q)$ of large prime order ℓ.
- Finding explicit constructions of elliptic curves having a small embedding degree with respect to some subgroup $\mathcal{G}$ of $\mathbf{E}(\mathbb{F}_q)$ of large prime order ℓ.

The first problem has been tackled in [2, 8, 20, 21]. The results of these papers show that a "random" curve (for different types of randomization) tends to have a very large embedding degree with respect to large prime order subgroups of $\mathbf{E}(\mathbb{F}_q)$. In particular, this means that the so-called *MOV attack* of [25] is not likely to succeed on a "random" curve. On the other hand, this also means that "random" curves are useless for the purposes of pairing-based cryptography, thus making the second problem even more important.

Received by the editor February 23, 2010 and, in revised form, February 11, 2011.
2010 *Mathematics Subject Classification.* Primary 11G07, 11T71, 14H52.
Key words and phrases. Elliptic curves, pairing based cryptography, embedding degree, MNT curves.

It is also well known that *supersingular* curves over a finite field of characteristic p satisfy the above condition with respect to the full group $\mathcal{G} = \mathbf{E}(\mathbb{F}_q)$ of points over $\mathbb{F}_q$ with a value of k satisfying

$$k \le \begin{cases} 4, & \text{if } p = 2, \\ 6, & \text{if } p = 3, \\ 2, & \text{if } p \ge 5 \end{cases}$$

(see [1, Proposition 6.20]). This certainly limits the range of their possible applications, as sometimes larger values of k (such as $k = 12$) are necessary to provide the desired level of security. Besides, since there seems to be a widespread belief, not yet substantiated by any theoretic results or heuristic predictions, that supersingular curves may have some cryptographic weaknesses, it seems important to find *ordinary* curves with small embedding degrees. Motivated by this observation, many ingenious constructions of "pairing-friendly" ordinary curves have been proposed. An exhaustive survey can be found in [10], as well as in the more recent papers [17, 18, 29]. Despite multiple efforts of many researchers, only a few rather thin families of such curves are known and even these have only been heuristically analyzed.

In this paper, we continue the counting approach of [22, 23] to "pairing-friendly" curves, and show that, unfortunately, the appropriate curves are very scarce, providing in this way some partial explanation as to why all known constructions output only very sparse sequences of curves. We also present some heuristic predictions which indicate that in some cases our bound should be tight.

Furthermore, we examine and clarify the heuristic, given in [22], on the so-called MNT curves introduced by A. Miyaji, M. Nakabayashi and S. Takano [24]; see also [1, 5]. In [22], two of the current authors gave some heuristic arguments suggesting the upper bound $O(z/(\log z)^2)$ on the number of MNT curves of prime cardinality having CM discriminant at most z. Furthermore, it is suggested in the same paper that even the upper bound $z^{o(1)}$ on the number of such curves may hold as $z \to \infty$. However, in the recent paper [18] it has been shown that this number is very likely to be at least $0.49\sqrt{z}/(\log z)^2$. Here, we revisit the heuristic arguments from [18] and obtain a stronger lower bound (in particular, with only one $\log z$ in the denominator), which seems to be in better agreement with the numerical results presented in [18].

We remark that although the cryptographic significance of MNT curves has decreased as new constructions have been discovered, we believe that our technique is of independent value and for example can be used to analyse these more practically important constructions of pairing-friendly curves.

1.2. **Notation.** We fix some notation. For a positive integer k we put

$$\Phi_k(X) = \prod_{\substack{j=1 \\ \gcd(j,k)=1}}^{k} (X - \exp(2\pi\iota j/k)) \in \mathbb{Z}[X]$$

for the kth *cyclotomic polynomial*. Here, we write $\iota = \sqrt{-1}$. We recall that by the well-known formula

$$X^k - 1 = \prod_{m \mid k} \Phi_m(X),$$

it follows easily that if for a prime ℓ we have $\ell \mid q^k - 1$ but $\ell \nmid q^m - 1$ for all positive integers $m < k$, then $\ell \mid \Phi_k(q)$.

The known constructions of ordinary curves with small embedding degree mentioned in the Introduction typically work in two steps:

Step 1: Find a prime ℓ, integers $k \geq 2$ and t, and a prime power q such that

$$|t| \leq 2q^{1/2}, \quad \gcd(t, q) = 1, \quad t \neq 1, 2, \quad \ell \mid q + 1 - t, \\ \ell \mid q^k - 1, \quad \ell \nmid q^m - 1, \quad m < k. \tag{1}$$

Step 2: Find an elliptic curve $\mathbf{E}$ over $\mathbb{F}_q$ in the isogeny class defined by the pair (q, t); that is, having $\#\mathbf{E}(\mathbb{F}_q) = q + 1 - t$.

In particular,

$$\ell \mid \Phi_k(q).$$

Note that the condition $\ell \mid q^k - 1$ and $\ell \nmid q^m - 1$, for all positive integers $m < k$ implies that k is the multiplicative order of q modulo ℓ and thus $\ell \equiv 1 \pmod{k}$. In the above construction, k should be reasonably small, while the ratio $\log \ell / \log q$ should be as large as possible, preferably close to 1. Unfortunately, Step 2 above is feasible only if $t^2 - 4q$ has a very small squarefree part; that is, if

$$t^2 - 4q = -r^2 s, \tag{2}$$

with some integers r and s, where s is a small squarefree positive integer (see [1, Section 18.1]). In this case, either $-s$ or $-4s$ is the fundamental discriminant of the complex multiplication field, or the *CM discriminant* of the corresponding elliptic curve, according to the residue class of s modulo 4.

Throughout the rest of the paper we use the Landau symbols O and o and the Vinogradov symbols $\gg$ and $\ll$ with their usual meaning. The implied constants in these symbols are absolute. We recall that the assertions $U = O(V)$ and $U \ll V$ are both equivalent to the inequality $|U| \leq cV$ with some constant $c > 0$, while $U = o(V)$ means that $U/V \to 0$.

2. Statistics of pairing-friendly curves

2.1. **Previous results.** In [22, 23], for positive real numbers x, y and z, the function $Q_k(x, y, z)$ is defined as being the number of prime powers $q \leq x$ for which there exist a prime $\ell \geq y$ and an integer t satisfying the conditions (1) and (2) with some squarefree positive integer $s \leq z$. Improving upon the estimates obtained in [22], it has been shown in [23] that for any fixed integer $k \geq 2$ and any positive real numbers x, y and z, the bound

$$Q_k(x, y, z) \ll \varphi(k) x^{3/2} y^{-1} z^{1/2} \frac{\log x}{\log \log x} \tag{3}$$

holds. In particular, in the case when x, y and z tend to infinity in such a way that $y = x^{1+o(1)}$ and $z = x^{o(1)}$, which is the instance of main practical interest, we see from the above estimate (3) that there are at most $x^{1/2+o(1)}$ fields of cardinality q for which one may find such a curve that is much smaller than the total number $(1 + o(1))x/\log x$ of all such fields.

2.2. **Upper bounds on the number of pairing-friendly curves.** Here, we introduce a new ingredient to the approaches of [22, 23] and instead estimate a different function $I_k(x, y, z)$ which is defined as the number of pairs (q, t) of prime powers $q \le x$ and integers t such that the conditions (1) and (2) are satisfied with some prime $\ell \ge y$ and some squarefree positive integer $s \le z$. Thus, $I_k(x, y, z)$ is just the total number of isogeny classes of the corresponding elliptic curves. Our result here is the following:

Theorem 1. *For any integer $k \ge 2$ and positive real numbers x, y and z, the following bound holds:*

$$I_k(x, y, z) \ll \varphi(k) \left(xy^{-1} + x^{1/2}\right) z^{1/2} \frac{\log x}{\log\log x}.$$

Proof. Since $\ell \mid q + 1 - t$ and $\ell \mid \Phi_k(q)$, we have

$$\ell \mid \Phi_k(t - 1). \tag{4}$$

Using (1), we see that

$$\ell m = q + 1 - t$$

holds with some integer m, which together with (2) implies that

$$(t - 2)^2 + r^2 s = 4\ell m.$$

Hence,

$$\ell \mid (t - 2)^2 + r^2 s. \tag{5}$$

Comparing (4) and (5), we conclude that ℓ divides the resultant $R_k(r^2 s)$ of the polynomials $\Phi_k(X)$ and $(X - 1)^2 + r^2 s$; that is,

$$\ell \mid R_k(r^2 s) = \operatorname{Res}\left(\Phi_k(X), (X - 1)^2 + r^2 s\right). \tag{6}$$

Since $\Phi_k(X)$ is an irreducible polynomial of degree $\varphi(k)$, where $\varphi(k)$ is the Euler function, we see that $R_k(r^2 s)$ does not vanish if $k \ne 1, 2, 3, 4, 6$, because $\Phi_k(X)$ is irreducible of degree $\varphi(k) \ge 3$ for $k \ne 1, 2, 3, 4, 6$. For $k = 2$, we have $\Phi_k(X) = X + 1$, and it is obvious that -1 is not a root of $(X-1)^2 + r^2 s$ for $s \ge 1$. For $k = 3, 4, 6$, we have that $\varphi(k) = 2$. Thus, $R_k(r^2 s) = 0$ implies that $\Phi_k(X) = (X - 1)^2 + r^2 s$, which is impossible (it is enough to substitute $X = 0$ to see this). Hence, we have shown that in all cases $R_k(r^2 s) \ne 0$.

Let $\omega(n)$ denote the number of prime divisors of an integer n. Using the trivial inequality $\omega(n)! \le n$ and the Stirling formula, we derive that

$$\omega(n) \ll \frac{\log n}{\log\log(n + 2)}.$$

We now see from (6) that if the product $r^2 s$ is fixed, then ℓ can take at most

$$\omega(|R_k(r^2 s)|) \ll \frac{\log |R_k(r^2 s)|}{\log\log |R_k(r^2 s)|} \ll \frac{\varphi(k) \log(r^2 s)}{\log\log(r^2 s)} \ll \varphi(k) \frac{\log x}{\log\log x} \tag{7}$$

possible values provided that x is large enough.

We see from (2) that $r^2 s \le 4x$ if $q \le x$. Thus, the total number of such products can be bounded by

$$\sum_{\substack{s \le z \\ s \text{ squarefree}}} \sum_{r \le \sqrt{4x/s}} 1 = \left(\frac{24}{\pi^2} + o(1)\right) \sqrt{xz}. \tag{8}$$

The above estimate has been derived in [23, Section 3] by partial summation from the well-known fact that there are $(6/\pi^2 + o(1))z$ positive squarefree integers $s \le z$ as $z \to \infty$ (see [13, Theorem 334]).

When the positive integers $r^2 s$ and ℓ satisfying (6) are fixed, we see from the divisibility condition (5) that t belongs to at most two residue classes modulo ℓ. Since $|t| \le 2x^{1/2}$, it follows that t may take at most

$$2\left(\frac{4x^{1/2}+1}{\ell}+1\right) \ll x^{1/2}/y + 1 \tag{9}$$

values. When all three numbers ℓ, $r^2 s$ and t are fixed, the value of q is uniquely defined from equation (2). Combining (7), (8) and (9), we conclude the proof. □

Assume that $y \ge x^{1/2+o(1)}$ and $z = x^{o(1)}$ which is the most interesting case from the cryptographic point of view. Then Theorem 1 implies that

$$I_k(x, y, z) \le x^{1/2+o(1)}$$

which can be compared with the total number $x^{3/2+o(1)}$ of all possible isogeny classes (that is, of pairs (q, t)) of elliptic curves over finite fields of cardinality $q \le x$.

Since we also have the trivial inequality

$$Q_k(x, y, z) \le I_k(x, y, z),$$

we see that Theorem 1 gives a substantial improvement upon the inequality (3) (except for the case of $y = x^{1+o(1)}$ when it is of the same strength). We record this as follows:

Corollary 2. *For any integer $k \ge 2$ and positive real numbers x, y and z, the following bound holds:*

$$Q_k(x, y, z) \ll \varphi(k)\left(xy^{-1} + x^{1/2}\right) z^{1/2} \frac{\log x}{\log\log x}.$$

2.3. **Some heuristic arguments.** In [11], heuristic predictions are given suggesting that for a fixed integer k and $x \to \infty$, there are $x^{1/2+o(1)}$ prime powers $q \le x$ for which there is an ordinary elliptic curve $\mathbf{E}$ over $\mathbb{F}_q$ satisfying $\#\mathbf{E}(\mathbb{F}_q) \mid \Phi_k(q)$. These heuristic predictions apply to all curves without any restriction on either the arithmetic structure of $\#\mathbf{E}(\mathbb{F}_q)$, or on the size of the discriminant of the field of complex multiplication. Here, we provide somewhat different heuristic arguments which take these two conditions into account and suggest that the bound of Theorem 1 is of correct order of magnitude in a wide range of y and z versus x.

We start with the shape of the prime divisors ℓ of the resultant

$$R_k(u) = \operatorname{Res}\left(\Phi_k(X), (X-1)^2 + u\right).$$

Lemma 3. *Assume that $k \ge 1$ and u are integers and ℓ is a prime with $\ell \mid R_k(u)$ and such that $-u$ is a quadratic residue modulo ℓ. Then either $\ell \mid k$ or $\ell \equiv 1 \pmod{k}$.*

Proof. Since $-u$ is a quadratic residue modulo ℓ, there is an integer solution t to the congruence

$$(t-2)^2 + u \equiv 0 \pmod{\ell}. \tag{10}$$

Since $\ell \mid R_k(u)$, we can also assume that t is chosen in such a way that

$$\Phi_k(t-1) \equiv 0 \pmod{\ell}. \tag{11}$$

Let $\mathbb{K} = \mathbb{Q}[\iota\sqrt{s}]$, where s is the squarefree part of u. Since $-u$ is a quadratic residue modulo ℓ, so is $-s$. Therefore, ℓ is either ramified or splits in $\mathbb{K}$.

If ℓ is ramified in $\mathbb{K}$, then $\ell \mid s$. Therefore, $\ell \mid t-2$ (see (10)). Thus, from (11), we obtain that $\ell \mid \Phi_k(1)$. However, it is well known that $\Phi_k(1) = 1$ unless k is a power of a prime ℓ, in which case $\Phi_k(1) = \ell$.

When ℓ splits in $\mathbb{K}$ we denote by

$$\alpha = 1 + \iota\sqrt{u} \qquad \text{and} \qquad \beta = 1 - \iota\sqrt{u}$$

the roots of $(X-1)^2 + u$. Then

$$R_k(u) = \Phi_k(\alpha)\Phi_k(\beta) = \mathrm{Nm}_{\mathbb{K}/\mathbb{Q}}\left(\Phi_k(\alpha)\right),$$

where $\mathrm{Nm}_{\mathbb{K}/\mathbb{Q}}(\tau)$ is the norm of $\tau \in \mathbb{K}$ in $\mathbb{Q}$.

We have

$$\lambda \mid \Phi_k(\alpha)$$

for some prime ideal λ dividing ℓ in the ring of algebraic integers $\mathcal{O}_{\mathbb{K}}$ of $\mathbb{K}$. Hence, $\alpha^k \equiv 1 \pmod{\lambda}$. Let m be the order of α modulo λ. Clearly,

$$m \mid k.$$

If $m = k$, then k divides the order of α in $\mathcal{O}_{\mathbb{K}}/\lambda$, which is the field $\mathbb{F}_\ell$ of ℓ elements. Hence, $k \mid \ell - 1$, leading to $\ell \equiv 1 \pmod{k}$.

If $m < k$, then $k = mk_0$, with some integer $k_0 > 1$ and λ divides both $\alpha^m - 1$ and

$$(\alpha^m)^{k_0-1} + \cdots + 1 = \frac{\alpha^k - 1}{\alpha^m - 1} = \prod_{\substack{d \mid k \\ d \nmid m}} \Phi_d(\alpha)$$

(since it divides $\Phi_k(\alpha)$). Reducing the above relation modulo λ, we obtain

$$k_0 \equiv \prod_{\substack{d \mid k \\ d \nmid m}} \Phi_d(\alpha) \equiv 0 \pmod{\lambda}.$$

Therefore, $\ell \mid k_0 \mid k$, which completes the proof. □

Thus, we see from (1) and Lemma 3 that the prime factors ℓ of $R_k(r^2 s)$ are either divisors of k or are congruent to 1 modulo k.

Next, we recall that from well-known results concerning the distribution of divisors of a "random" integer in intervals (see [9, 12], for example), for any two fixed real numbers $0 < \alpha < \beta < 1$, there is a number $\eta > 0$ depending on α and β, such that for a sufficiently large positive number U there are at least ηU positive integers $n \le U$ which have a prime divisor $\ell \in [U^\alpha, U^\beta]$.

However, we model the values $|R_k(r^2 s)|$ not as "typical" integers, but rather as random positive integers whose prime factors are either divisors of k, or congruent to 1 modulo k according to Lemma 3. Let $\mathcal{A}_k$ be the set of all such integers. Let us show that integers in $\mathcal{A}_k$ have the same property as above with respect to the distribution of their prime factors in large intervals. For this, we start by observing that a well-known theorem of Wirsing [30] implies that the counting function $A_k(U) = \#\mathcal{A}_k(U)$, where

$$\mathcal{A}_k(U) = \mathcal{A}_k \cap [1, U],$$

satisfies the asymptotic formula

$$A_k(U) = (c_k + o(1))\frac{U}{(\log U)^{1-1/\varphi(k)}}$$

as $U \to \infty$, where c_k is some positive constant depending only on k. Let us show that for the integers in $\mathcal{A}_k$ with a prime divisor of a prescribed size a similar density result also holds. More precisely, for real numbers $0 < \alpha < \beta < 1$, we denote by $A_k(U; \alpha, \beta)$ the number of integers $n \in \mathcal{A}_k(U)$ with a prime divisor $\ell \in [U^\alpha, U^\beta]$.

Lemma 4. *For any fixed real numbers $0 < \alpha < \beta < 1$ and integer $k \geq 1$, there is a constant $\eta_k > 0$ such that*

$$A_k(U; \alpha, \beta) \geq (\eta_k(\alpha, \beta) + o(1))\, A_k(U)$$

as $U \to \infty$.

Proof. Let us fix a prime number $\ell \equiv 1 \pmod k$ in the above interval. Any integer $n \in \mathcal{A}_k(U)$ which is a multiple of ℓ is of the form $n = \ell m$ where $m \in \mathcal{A}_k(U/\ell)$. Thus, the number $A_k(U, \ell)$ of such integers $n \in \mathcal{A}_k(U)$ which are multiples of ℓ is

$$A_k(U, \ell) = (c_k + o(1))\frac{U}{\ell(\log(U/\ell))^{1-1/\varphi(k)}} \geq (d_k + o(1))\frac{U}{\ell(\log U)^{1-1/\varphi(k)}}$$

as $U \to \infty$, where we can take

$$d_k(\alpha) = c_k/(1-\alpha)^{1-1/\varphi(k)}.$$

Now we sum up the above estimate over all primes $\ell \equiv 1 \pmod k$ in $[U^\alpha,\ U^\beta]$, getting

$$\sum_{\substack{\ell \equiv 1 \pmod k \\ \ell \in [U^\alpha, U^\beta]}} A_k(U, \ell) \geq (d_k(\alpha) + o(1))\frac{U}{(\log U)^{1-1/\varphi(k)}} \sum_{\substack{\ell \equiv 1 \pmod k \\ \ell \in [U^\alpha,\ U^\beta]}} \frac{1}{\ell}.$$

We now recall that for any modulus k and integer a coprime with k we have

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod k}} \frac{1}{p} = \frac{1}{\varphi(k)} \log\log x + C(a, k) + o(1), \tag{12}$$

where the constant $C(a, k)$ depends only on a and k (see, for example, [19, Corollary 3 and Theorem 4]). Hence, we obtain

$$\sum_{\substack{\ell \equiv 1 \pmod k \\ \ell \in [U^\alpha, U^\beta]}} \mathcal{A}_k(U, \ell) \geq (e_k(\alpha, \beta) + o(1))\frac{U}{(\log U)^{1-1/\varphi(k)}}, \tag{13}$$

as $U \to \infty$, where

$$e_k(\alpha, \beta) = d_k(\alpha)\frac{\log(\beta/\alpha)}{\varphi(k)}.$$

Finally, let us observe that a number $n \leq U$ can have at most $1/\alpha$ prime divisors $\ell \in [U^\alpha,\ U^\beta]$. Thus, every positive integer in $\mathcal{A}_k(U)$ having a prime factor ℓ in the above interval is counted at most $1/\alpha$ times in the sum on the left-hand side of (13). This shows that

$$A_k(U; \alpha, \beta) \geq (\alpha e_k(\alpha, \beta) + o(1))\frac{U}{(\log U)^{1-1/\varphi(k)}} \qquad \text{as } U \to \infty.$$

Taking

$$\eta_k(\alpha,\beta) = \frac{\alpha e_k(\alpha,\beta)}{c_k} = \frac{\alpha \log(\beta/\alpha)}{\varphi(k)(1-\alpha)^{1-1/\varphi(k)}},$$

we conclude the proof. □

Next we estimate the size of $R_k(r^2s)$. The roots

$$\alpha = 1 + r\sqrt{s} \qquad \text{and} \qquad \beta = 1 - r\sqrt{s}$$

of the quadratic polynomial $(X-1)^2 + r^2 s$ have absolute values $\sqrt{1+r^2s}$. Since all the roots ζ of $\Phi_k(X)$ have absolute value 1 and both polynomials are monic, we get that

$$|R_k(r^2s)| \le (1+\sqrt{1+r^2s})^{2\varphi(k)} \le (3(1+r^2s))^{\varphi(k)} \le (4r^2s)^{\varphi(k)}, \tag{14}$$

where in the above inequalities we used also the fact that $r^2 s \ge 3$, which follows since if $r^2 s \in \{1,2\}$, then $r = 1$ and $s = 1,\ 2$, but none of the equations $4q = t^2+1$, or $4q = t^2+2$ has integer solutions q and t. Observe also that since for $\zeta = \cos\vartheta + \iota \sin\vartheta$, where again $\iota = \sqrt{-1}$, we have

$$\begin{aligned} |(\alpha-\zeta)(\beta-\zeta)| &= \left|\left(\iota r\sqrt{s} + (1-\zeta)\right)\left(-\iota r\sqrt{s} + (1-\zeta)\right)\right| \\ &= \left|r^2 s + (1-\zeta)^2\right| = \left|\left(r^2 s + 2 - 2\cos\vartheta\right) - 2\iota\sin\vartheta\right| \\ &\ge r^2 s + (2 - 2\cos\vartheta) \ge r^2 s, \end{aligned}$$

we get that

$$|R_k(r^2s)| \ge (r^2 s)^{\varphi(k)}. \tag{15}$$

Thus, making the assumption that the prime factors of $R_k(r^2s)$ are distributed in intervals according to the same distribution law governing the divisors of a "random" integer, we infer from Lemma 4 and the bounds (14) and (15), that it is natural to expect that for a positive proportion $\gamma_k(\varepsilon)$ of these products $r^2 s$, where $\gamma_k(\varepsilon)$ depends only on k and $\varepsilon > 0$, the resultant $R_k(r^2s)$ has a prime divisor ℓ with $y \le \ell \le y^{1+\varepsilon}$.

Moreover, it is natural to expect that for about 50% of these values of ℓ, the quadratic polynomial $(X-1)^2 + r^2 s$ has a root $u \in [0, \ell/2]$ modulo ℓ. Assuming further that the fractions u/ℓ are uniformly distributed in the interval $[0, 1/2]$, we then see that the "expectation" that $0 \le u \le x^{1/2}$ is about

$$x^{1/2}/\ell \ge x^{1/2} y^{-1-\varepsilon}. \tag{16}$$

In this case, the equality $t = u - 1$ is a valid value for the isogeny class of elliptic curves $\mathbf{E}$ over $\mathbb{F}_p$ with $p + 1 \pm t$ points. Recall that by (8), we have about $\sqrt{xz}$ admissible products $r^2 s$ and, by (16), a positive proportion of at least $x^{1/2} y^{-1+\varepsilon}$ of them yields a valid isogeny class. All the above arguments suggest that for any fixed k and $\varepsilon > 0$, once x is large and $x^{1/2} \le y \le x^{1-\varepsilon}$, the lower bound

$$I_k(x,y,z) \ge c(\varepsilon,k)\sqrt{xz}\, x^{1/2} y^{-1+\varepsilon} = c(\varepsilon,k) x y^{-1+\varepsilon} z^{1/2}$$

holds, where $c(\varepsilon,k)$ depends only on ε and k. But in our range, the above lower bound is of about the same order of magnitude as the upper bound of Theorem 1.

3. Statistics of MNT curves

3.1. **Background on MNT curves.** It is clear that the condition (2) is hard to satisfy since "random" integers tend to have only very small square divisors, and thus a large squarefree part. However, as we have already mentioned in the Introduction, there are some explicit constructions of such sets of parameters (see [10, 17, 18, 29] for a survey, as well as [17, 18, 29] for more recent results). Here, we concentrate on the historically first constructions of this kind given by A. Miyaji, M. Nakabayashi and S. Takano [24] whose aim is to produce pairing-friendly curves with embedding degrees $k = 3, 4, 6$. As in [22], here we only deal with the technically (and typographically) simpler case of the MNT curves with embedding degree $k = 6$ written as MNT_6. The same analysis can be carried over to the other two cases as well without any further technical complication. By [24, Theorem 4], we know that if p is a large enough prime, then an ordinary elliptic curve $\mathbf{E}$ over $\mathbb{F}_p$ has a prime number of $\mathbb{F}_p$ points $\#\mathbf{E}(\mathbb{F}_p) = p + 1 - t$ and embedding degree $k = 6$ if and only if for some integer n we have both $p = 4n^2 + 1$ and $t = 1 \pm 2n$. Thus, $\#\mathbf{E}(\mathbb{F}_p) = 4n^2 \mp 2n + 1$.

In order to find the parameters of an elliptic curve with this number of points and the CM discriminant s, we have to find integer solutions (n, s, m), with s, m positive, to the Pell-type equation

$$(6n + 1)^2 + 8 = 3sm^2. \tag{17}$$

After this, if s is not too large, then the *complex multiplication method* (see [1, Section 18.1]) can be applied to find the corresponding curve. The bound $s < 10^{10}$ is given in [18] as a practical bound and has been recently extended to $s < 10^{13}$ in [28].

Accordingly, we say that an ordinary elliptic curve $\mathbf{E}$ over $\mathbb{F}_p$ is an MNT_6 *curve of discriminant* s if it comes from an integer n satisfying the Pell equation (17). Thus, as a first step, it is natural to estimate the number $E(z)$ of MNT_6 curves of discriminant $s \leq z$.

3.2. **Previous results.** As we have mentioned, in [22] a heuristic argument is presented leading to a conjectured upper bound on $E(z)$ of the form

$$E(z) \ll \frac{z}{(\log z)^2}.$$

In the same paper, it is even suggested that the upper bound $E(z) \ll z^{o(1)}$ may hold as $z \to \infty$. However, K. Karabina and E. Teske [18] have shown a heuristic argument in favor of the lower bound

$$E(z) \geq 0.49 \frac{\sqrt{z}}{(\log z)^2} \tag{18}$$

being valid for z sufficiently large. The idea of K. Karabina and E. Teske [18] is to compute the solutions to the Pell equation (17) having only $m = 1$. Thus, the CM discriminants s are chosen to satisfy $3s = (6n + 1)^2 + 8$. The lower bound (18) is then derived after some heuristic calculation involving the Prime Number Theorem. However, the numerical calculations in [18] show that (18) falls short by a constant factor of the numerical values of $E(z)$.

3.3. **Our approach.** There are two possible ways to improve the lower bound of K. Karabina and E. Teske [18].

First, one can take into account not only the value $m = 1$ but also other suitable values of $m > 1$. Let us observe that if in the equation (17) m is large, say comparable with n, then s is automatically small.

Second, in order to improve this bound one can carefully apply the standard heuristic predictions on the distribution of primes in polynomial sequences. Indeed, while $1/\log \ell$ is the expectation of a "random" integer ℓ to be prime, this is no longer the case when ℓ is a value of a fixed polynomial, since now the result depends on the "local" properties of the polynomial corresponding to each individual prime. This is in fact the content of the so-called Bateman-Horn Conjecture (see [3]), which we now include for convenience. Given any finite set $\mathcal{F} = \{f_1, \dots, f_\nu\}$ consisting of irreducible polynomials $f_1(T), \dots, f_\nu(T) \in \mathbb{Z}[T]$ with positive leading coefficients and such that the products $f_1(n) \dots f_\nu(n)$, $n = 1, 2, \dots$, have no fixed prime divisor, that is, there is no prime ℓ with

$$\ell \mid f_1(n) \dots f_\nu(n)$$

for every $n = 1, 2, \dots$, we have

$$\begin{aligned} &\#\{n \le X \ : \ f_1(n), \dots, f_\nu(n) \text{ are simultaneously prime}\} \\ &\qquad \sim \frac{C(\mathcal{F})}{\deg f_1 \dots \deg f_\nu} \int_2^X \frac{du}{(\log u)^\nu}, \end{aligned} \tag{19}$$

where

$$C(\mathcal{F}) = \prod_{p \ge 2 \text{ prime}} \frac{(1 - \omega_p(\mathcal{F})/p)}{(1 - 1/p)^\nu},$$

and

$$\omega_p(\mathcal{F}) = \{1 \le n \le p \ : \ f_1(n) \dots f_\nu(n) \equiv 0 \pmod p\}.$$

The use of this conjecture would have the effect of improving the constant 0.49 in front of the lower bound (18).

Combining the above two observations, in the remainder of this paper we improve upon the bound (18), subject to the truth of the Bateman-Horn Conjecture [3].

Our strategy to find MNT_6 curves is for each fixed m to find integers n such that $4n^2 + 1$ and $4n^2 + 2n + 1$ or $4n^2 - 2n + 1$ are primes and, furthermore,

$$s = \frac{1}{3m^2}((6n + 1)^2 + 8)$$

is a squarefree integer.

3.4. **The generalized Bateman-Horn conjecture.** In studying questions related to the distribution of prime numbers, it is customary to use the *Cramér model*; that is, to think of this distribution as a collection of independent Bernoulli distributions $X(n)$ with value 1 with probability $1/\log n$. In other words, a number n is prime with probability $1/\log n$ given by the Prime Number Theorem. In general, the Cramér model gives a very good heuristic answer to problems that are, otherwise, intractable. However, there is an important caveat in the reasoning. For example, in the study of the *twin prime conjecture*, we want to guess an asymptotic

for $\pi_2(X)$, which is the number of integers $n \leq X$ such that both n and $n+2$ are prime. The naïve prediction

$$\pi_2(x) \sim \int_2^X \frac{du}{(\log u)^2} \sim \frac{x}{(\log x)^2}$$

is wrong as the two events "n is prime" and "$n+2$ is prime" are clearly dependent. Indeed, if we want both to be prime, then in particular, they must be coprime with all primes $\ell < \sqrt{n+2}$; but if n is odd, automatically $n+2$ is also odd. In the same way, both are coprime with 3 only when $n \equiv 1 \pmod 3$, and so on. Thus, in order to find the correct constant, one has to measure the dependence between n and $n+2$ with respect to each prime p. In this way, one finds that

$$\pi_2(x) \sim \mathfrak{S} \frac{x}{(\log x)^2}, \tag{20}$$

where

$$\mathfrak{S} = 2 \prod_{p>2 \text{ prime}} \left(1 - \frac{2}{p}\right) \left(1 - \frac{1}{p}\right)^{-2},$$

which gives, for each prime p, the probability of $n(n+2)$ not being a multiple of p, divided by the probability of two random numbers not being multiples of p. A more advanced form of this argument leads to the Bateman-Horn Conjecture (19). We now incorporate the squarefreeness property into this model and make the following *Generalized Bateman-Horn Conjecture*.

Conjecture 5. *Let $\mathcal{F} = \{f_1, \ldots, f_\nu\}$ and $\mathcal{G} = \{g_1, \ldots, g_\mu\}$ be two finite sets of irreducible polynomials $f_1(T), \ldots, f_\nu(T), g_1(T), \ldots, g_\mu(T) \in \mathbb{Q}[T]$ such that the products $f_1(n) \ldots f_\nu(n) g_1(n), \ldots, g_\mu(n)$, $n = 1, 2, \ldots$, have no fixed prime divisor. Then, for large X, we have*

$$\begin{aligned} \#\{n \leq X \ :\ & f_1(n), \ldots, f_\nu(n) \text{ are simultaneously prime} \\ & \text{and } g_1(n), \ldots, g_\mu(n) \text{ are simultaneously squarefree}\} \\ & \sim \frac{C(\mathcal{F}, \mathcal{G})}{\deg f_1 \ldots \deg f_\nu} \int_2^X \frac{du}{(\log u)^\nu}, \end{aligned} \tag{21}$$

where

$$C(\mathcal{F}, \mathcal{G}) = \prod_{p \geq 2 \text{ prime}} \frac{(1 - \Omega_p(\mathcal{F}, \mathcal{G})/p^2)}{(1 - 1/p)^{\nu+\mu}},$$

and

$$\Omega_p(\mathcal{F}, \mathcal{G}) = \#\left\{1 \leq n \leq p^2 \ :\ \prod_{i=1}^{\nu} f_i(n)^2 \prod_{j=1}^{\mu} g_j(n) \equiv 0 \pmod{p^2}\right\}.$$

3.5. **Preparations.** Let m be a fixed odd integer. Since the equation (17) fixes the congruence class of n modulo m^2 in at most $m^{o(1)}$ ways as $m \to \infty$, we expect the main contribution to $E(z)$ to come from systems of parameters where $m \leq z^{1/2-\varepsilon}$ with a small error term depending on ε. From now on, we always assume this upper bound for the variable m. Recall that we are looking for integers n such that :

- $4n^2 + 1$ is prime,
- $4n^2 + 2n + 1$ or $4n^2 - 2n + 1$ is prime,
- $((6n+1)^2 + 8)/(3m^2)$ is a squarefree integer.

The next result is a straightforward application of the Chinese Remainder Theorem.

Let, as usual, (a/p) denote the Legendre symbol of a with respect to p.

Lemma 6. *Let m be a fixed integer and let $B(m)$ be the set of residues modulo m^2 which give solutions to the equation*

$$(6n+1)^2+8 \equiv 0 \pmod{3m^2}.$$

Then $\#B(m) = \rho(m)$, where $\rho(m)$ is the multiplicative function defined at prime powers p^α by

$$\rho(p^\alpha) = \begin{cases} 0 & \text{if } p = 2, \\ 1 & \text{if } p = 3, \\ 1 + \left(\dfrac{-2}{p}\right) & \text{if } p \geq 5. \end{cases}$$

From now on, we fix an integer m and a residue class $\beta \in B(m)$. Observe that, by Lemma 6, this is possible only if every prime divisor of m is congruent to either 1 or 3 modulo 8. We denote by $E_{m,\beta}(z)$ the number of positive integers of the form $n = \beta + km^2$ (that is, $n \equiv \beta \pmod{m^2}$), which yield MNT_6 curves with discriminant at most z. From the bound $s \leq z$, we get

$$36k^2m^4 \leq (6n+1)^2 + 8 \leq 3zm^2,$$

so $0 \leq k \leq \sqrt{z}/(\sqrt{12}m)$.

Since the cases of polynomials $4n^2+2n+1$ or $4n^2-2n+1$ are completely symmetric (and three pairwise distinct polynomials are simultaneously prime for $O(x/(\log x)^3)$ arguments $n \leq x$), we consider only the polynomial $4n^2+2n+1$ and then double the result.

Assuming the independence of the events:

- $4n^2+1$ is prime,
- $4n^2+2n+1$ is prime,
- $((6n+1)^2+8)/(3m^2)$ is a squarefree integer,

the Cramér model gives us

$$F_{m,\beta}(z) \sim \frac{\sqrt{z}}{\zeta(2)\sqrt{12}m(\log(zm^2))^2} \tag{22}$$

positive integers n yielding MNT_6 curves of discriminant $s \leq z$ for the fixed values of m and $\beta \in B(m)$. Indeed, note that the numbers $4n^2+1$ and $4n^2+2n+1$ are of size about zm^2 and recall that the probability of a number to be squarefree is exactly $1/\zeta(2)$. Analogously, as in the twin prime conjecture, in order to adjust the dependence of these three events, we have to count the number of solutions modulo each prime. Observe that for each integer n, any prime $p \neq 3$ divides at most one of $4n^2+1$, $4n^2+2n+1$ and $((6n+1)^2+8)/m^2$. Hence, we just have to count the number of solutions modulo p individually and then add them together.

Let us define

$$C_2 = 0, \qquad C_3 = 4, \tag{23}$$

and

$$C_p = \begin{cases} 4p+2 & \text{if } p \equiv 1 \pmod{24}, \\ 2p & \text{if } p \equiv 5,7 \pmod{24}, \\ 2 & \text{if } p \equiv 11 \pmod{24}, \\ 4p & \text{if } p \equiv 13 \pmod{24}, \\ 2p+2 & \text{if } p \equiv 17,19 \pmod{24}, \\ 0 & \text{if } p \equiv 23 \pmod{24}. \end{cases} \tag{24}$$

Lemma 7. *Let m be a fixed odd integer, $\beta \in B(m)$, p a prime, and let N_p be the number of solutions to the congruence*

$$((4n^2+1)(4n^2+2n+1))^2 \frac{(6n+1)^2+8}{3m^2} \equiv 0 \pmod{p^2},$$

in the arithmetic progression $n \equiv \beta \pmod{m^2}$. Then, $N_p = 1$ for all $p \mid m$, and $N_p = C_p$ otherwise.

Proof. Suppose first that $p \nmid m$. Then we can drop the extra condition given by $n \equiv \beta \pmod{m^2}$, and count the solutions to $4n^2+1$, $4n^2+2n+1$, and $(6n+1)^2+8$ separately since p can divide at most one of those factors. In fact, it does so depending on whether -1, -3 or -2 is a quadratic residue modulo p. Hence, the condition modulo 24 given in C_p. Observe that each solution to $4n^2+1 \equiv 0 \pmod{p}$ or $4n^2+2n+1 \equiv 0 \pmod{p}$ gives p solutions to our congruence modulo p^2. Now, if $p \mid m$, then it is easy to see that $p \nmid (4n^2+1)(4n^2+2n+1)$, whereas the congruence

$$\frac{1}{3m^2}((6(\beta+km^2)+1)^2+8) \equiv 0 \pmod{p^2}$$

has only one solution modulo p^2. The case $p = 3$ is dealt with separately. □

Now, as in the twin prime conjecture, we multiply all the local factors, and divide by the probability of the independent events. We get from (22) the following lower bound valid for any $\beta \in B(m)$:

$$\begin{aligned} E_{m,\beta}(z) &\geq 2 \prod_p \left(1 - \frac{N_p}{p^2}\right)\left(1 - \frac{1}{p}\right)^{-2}\left(1 - \frac{1}{p^2}\right)^{-1} F_{m,\beta}(z) \\ &\sim \frac{1}{\sqrt{3}} \prod_p \left(1 - \frac{N_p}{p^2}\right)\left(1 - \frac{1}{p}\right)^{-2} \frac{\sqrt{z}}{m(\log(zm^2))^2}, \end{aligned} \tag{25}$$

where the factor 2 at the front account for the two independent cases of primality of $4n^2+2n+1$ or $4n^2-2n+1$.

3.6. **Lower bound on** MNT_6 **curves.** Here we obtain a lower bound on $E(z)$ under the Generalized Bateman-Horn Conjecture 5. In fact, only the contribution from solutions to the Pell equation (17) with squarefree m are taken into account. Using our method one can include the contribution from all integer m and obtain a better constant in our estimate, however, it involves significant technical complications as the function $f(m)$ is multiplicative but not completely multiplicative if we consider it supported on all integers m.

Let us define the product

$$\mathfrak{S}_0 = \frac{1}{2\sqrt{3}} \prod_p \left(1 - \frac{C_p}{p^2}\right)\left(1 - \frac{1}{p}\right)^{-1}\left(1 + \frac{f(p)}{p}\right) = 0.237615\ldots, \tag{26}$$

where

$$f(m) = \prod_{p|m} \left(1 - \frac{1}{p}\right)^2 \left(1 - \frac{C_p}{p^2}\right)^{-1} \rho(p),$$

and the constants C_p are given by (23) and (24) and $\rho(p)$ is defined in Lemma 6. The convergence of $\mathfrak{S}_0$ follows from (12). To see it, it is enough to consider $\log \mathfrak{S}$ and use (12) with $k = 24$, and the definition of C_p in (24) and $\rho(p)$ in Lemma 6.

It might be interesting to note that the definition of C_p ensures convergence of $\mathfrak{S}_0$ but not absolute convergence, which is not the case with the constant $\mathfrak{S}$ in the twin prime conjecture (20).

Theorem 8. *Let $E(z)$ be the number of* MNT_6 *curves having CM discriminant $s \leq z$. Then, assuming the Generalized Bateman-Horn Conjecture* 5*, the lower bound*

$$E(z) \geq (\mathfrak{S}_0 + o(1)) \frac{\sqrt{z}}{\log z}$$

holds as $z \to \infty$, where $\mathfrak{S}_0$ is given by (26)*.*

Proof. Let us define the products

$$\mathfrak{S}_1 = \prod_p \left(1 - \frac{C_p}{p^2}\right) \left(1 - \frac{1}{p}\right)^{-2} \tag{27}$$

and

$$\mathfrak{S}_2 = \prod_p \left(1 - \frac{1}{p}\right) \left(1 + \frac{f(p)}{p}\right). \tag{28}$$

As in the case of $\mathfrak{S}_0$, we note that the convergence of $\mathfrak{S}_1$ and of $\mathfrak{S}_2$ follows from (12). To see it, take logarithms in the finite products

$$\prod_{p \leq x} \left(1 - \frac{C_p}{p^2}\right) \left(1 - \frac{1}{p}\right)^{-2} \qquad \text{and} \qquad \prod_{p \leq x} \left(1 - \frac{1}{p}\right) \left(1 + \frac{f(p)}{p}\right),$$

and use (12) with $k = 24$. Clearly, we have

$$\mathfrak{S}_0 = \frac{1}{2\sqrt{3}} \mathfrak{S}_1 \mathfrak{S}_2. \tag{29}$$

Let us fix some $\varepsilon > 0$ and assume that z is large enough.

In order to get the lower bound for $E(z)$, we sum the lower bound (25) over all possible squarefree $m \leq z^{1/2-\varepsilon}$ and $\beta \in B(m)$ obtaining

$$E(z) \geq \sum_{m \leq z^{1/2-\varepsilon}} \sum_{\beta \in B(m)} E_{m,\beta}(z) \geq \frac{\mathfrak{S}_1}{\sqrt{3}} \sqrt{z} \sum_{m \leq z^{1/2-\varepsilon}} \frac{f(m)}{m(\log(zm^2))^2}, \tag{30}$$

where $\mathfrak{S}_1$ is given by (27). We observe that

$$f(p) = \begin{cases} 2 + O\left(1/p\right) & \text{if } p \equiv 1, 3 \pmod 8, \\ 0 & \text{otherwise.} \end{cases} \tag{31}$$

Observe also that $f(p) \geq 1$ for all primes $p \equiv 1, 3 \pmod 8$. We need an asymptotic formula for

$$S(T) = \sum_{m \leq T} \mu^2(m) \frac{f(m)}{m},$$

where, as usual, $\mu(m)$ is the Möbius function (that is, the summation is restricted to squarefree integers m). To do so, we use [14, Theorem 1.1] and hence, we need a crude estimate for $S(T)$ and an asymptotic formula for the sum restricted to primes. We have

$$S(T) \le \prod_{p \le T} \left(1 + \frac{f(p)}{p}\right) \ll \log T, \tag{32}$$

where in the above calculation we have used (31) and the Prime Number Theorem in the arithmetic progressions modulo 8. Finally, again a simple application of the Prime Number Theorem in the arithmetic progressions modulo 8 combined with (31), gives

$$\sum_{p \le t} \frac{f(p) \log p}{p} = \log t + O(1).$$

Now we just apply [14, Theorem 1.1] to obtain

$$S(t) = \mathfrak{S}_2 \log t + O(1), \tag{33}$$

where $\mathfrak{S}_2$ is given by (28). We now use partial summation in (30) to obtain

$$E(z) \ge \frac{\mathfrak{S}_1}{(2-2\varepsilon)^2\sqrt{3}} \frac{\sqrt{z}}{(\log z)^2} S(z^{1/2-\varepsilon}) + 4\mathfrak{S}_1\sqrt{z} \int_1^{z^{1/2-\varepsilon}} \frac{S(t)}{t(\log zt^2)^3} dt.$$

By a simple change of variables, we get from (33),

$$S(z^{1/2-\varepsilon}) = \left(\frac{1}{2} - \varepsilon\right) \mathfrak{S}_2 \log z + O(1)$$

and

$$\int_1^{z^{1/2-\varepsilon}} \frac{S(t)}{t(\log zt^2)^3} dt \ge \left(\frac{\mathfrak{S}_2}{32} - \varepsilon\right) \frac{1}{\log z},$$

which, after taking into account that ε is arbitrary and recalling (29), immediately implies the desired result. □

We note that the arguments used in the proof of (32) also allow us to estimate the sum

$$\widetilde{S}(T) = \sum_{m \le T} \frac{f(m)}{m},$$

which is an analogue of the sum $S(T)$ except that the summation is extended to all positive integers m. Indeed, since every positive integer can be represented in a unique way as a product of a perfect square and squarefree integer, we have for any T,

$$\widetilde{S}(T) = \sum_{u \le \sqrt{T}} \frac{1}{u^2} \sum_{\substack{n \le T/u^2 \\ \mu^2(n)=1}} \frac{f(nu^2)}{n}.$$

Using the fact that either $f(p) = 0$ or $f(p) \geq 1$, we get $f(nu^2) \leq f(n)f(u)$. Thus,

$$\begin{aligned}\widetilde{S}(T) &\leq \sum_{u \leq \sqrt{T}} \frac{f(u)}{u^2} \sum_{\substack{n \leq T/u^2 \\ \mu^2(n)=1}} \frac{f(n)}{n} \leq \sum_{u \leq \sqrt{T}} \frac{f(u)}{u^2} \prod_{p \leq T/u^2} \left(1 + \frac{f(p)}{p}\right) \\ &\ll \log T \sum_{u \leq \sqrt{T}} \frac{f(u)}{u^2} \ll \log T,\end{aligned}$$

since $f(m) = m^{o(1)}$ as $m \to \infty$.

3.7. MNT_6 **curves and average values of class numbers.** Theorem 8 reduces the gap between heuristic estimates on $E(z)$ and numerical results reported in [18]. However, there still is a discrepancy. For example, calculations show that $E(2^{40}) \geq 27587$ (as there are at least that many curves with over fields of $q \leq 2^{1000}$ elements), while the bound of [18] predicts $E(2^{40}) \geq 668$ and our bound predicts $E(2^{40}) \geq 8986$.

An alternative approach to obtaining tighter upper and lower bounds on $E(z)$ is via directly counting solutions to the Pell equation

$$u^2 + 8 = 3sv^2, \qquad u, v \in \mathbb{Z}$$

with $u \equiv 1 \pmod 6$ and working out the standard primality predicting heuristics. In turn, the size of the smallest solution of the above equation is related to the size of the regulator $R(3s)$ of the field $\mathbb{Q}(\sqrt{-3s})$. In particular, this suggests a link between $E(z)$ and sums of the type

$$\sum_{s \leq z} \frac{1}{R(3s)^2},$$

which are beyond the reach of the present methods.

Acknowledgements

The authors are grateful to Andrew Sutherland for fruitful discussions and also computing the constant $\mathfrak{S}_0$, given by (26) and for the estimates of $E(2^{40})$ in Section 3.7.

During the preparation of this paper, J. J. U. was partially supported by MEC of Spain, DGICYT Grants MTM2006-15038-C02-02, TSI2006-02731 and MTM2009-11068, F. L. by Grant SEP-CONACyT 79685 and I. E. S. by ARC Grant DP1092835 and NRF Grant CRP2-2007-03.

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Elliptic and hyperelliptic curve cryptography: Theory and practice*, CRC Press, 2005.

[2] R. Balasubramanian and N. Koblitz, 'The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm', *J. Cryptology*, **11** (1998), 141–145. MR1620936 (2000f:94024)

[3] P. T. Bateman and R. A. Horn, 'A heuristic asymptotic formula concerning the distribution of prime numbers', *Math. Comp.*, **16** (1962), 363–367. MR0148632 (26:6139)

[4] I. Blake, G. Seroussi and N. Smart, *Elliptic curves in cryptography*, London Math. Soc., Lecture Note Series, **265**, Cambridge Univ. Press, 1999. MR1771549 (2001i:94048)

[5] I. Blake, G. Seroussi and N. Smart, *Advances in elliptic curves in cryptography*, London Math. Soc., Lecture Note Series, **317**, Cambridge Univ. Press, 2005.

[6] D. Boneh and M. Franklin, 'Identity-based encryption from the Weil pairing', *SIAM J. Comp.*, **32** (2003), 586–615. MR2001745 (2004m:94035)
[7] D. Boneh, B. Lynn and H. Shacham, 'Short signatures from the Weil pairing', *J. Cryptology*, **17** (2004), 297–319. MR2090559 (2005h:94040)
[8] A. C. Cojocaru and I. E. Shparlinski, 'On the embedding degree of reductions of an elliptic curve', *Inform. Proc. Letters*, **109** (2009), 652–654. MR2527697 (2010d:11066)
[9] K. Ford, 'The distribution of integers with a divisor in a given interval', *Annals Math.*, **168** (2008), 367–433. MR2434882 (2009m:11152)
[10] D. Freeman, M. Scott and E. Teske, 'A taxonomy of pairing-friendly elliptic curves', *J. Cryptology*, **23** (2010), 224–280. MR2578668 (2011a:11112)
[11] S. D. Galbraith, J. McKee and P. Valenca, 'Ordinary abelian varieties having small embedding degree', *Proc. Workshop on Math. Problems and Techniques in Cryptology*, CRM, Barcelona, 2005, 29–45.
[12] R. R. Hall and G. Tenenebaum, *Divisors*, Cambridge University Press, Cambridge, 1988. MR964687 (90a:11107)
[13] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979. MR568909 (81i:10002)
[14] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004. MR2061214 (2005h:11005)
[15] A. Joux, 'A one round protocol for tripartite Diffie–Hellman', *Lect. Notes in Comp. Sci.*, vol. 1838, Springer-Verlag, Berlin, 2000, 385–393. MR1850619 (2002i:14029)
[16] A. Joux and K. Nguyen, 'Separating decision Diffie-Hellman from computational Diffie-Hellman in cryptographic groups', *J. Cryptology*, **16** (2000), 239–247. MR2002044 (2004h:94045)
[17] E. J. Kachisa, E. F. Schaefer and M. Scott, 'Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field', *Lect. Notes in Comp. Sci.*, vol. 5209 Springer-Verlag, Berlin, 2008, 126–135.
[18] K. Karabina and E. Teske, 'On prime-order elliptic curves with embedding degrees $k = 3$, 4 and 6', *Lect. Notes in Comp. Sci.*, vol. 5011, Springer-Verlag, Berlin, 2008, 102–117. MR2467839 (2010a:11114)
[19] A. Languasco and A. Zaccagnini, 'A note on Mertens formula for arithmetic progressions', *Number Theory*, **127** (2007), 37–46. MR2351662 (2009g:11136)
[20] F. Luca, D. J. Mireles and I. E. Shparlinski, 'MOV attack in various subgroups on elliptic curves', *Illinois J. Math.*, **48** (2004), 1041–1052. MR2114268 (2005h:11126)
[21] F. Luca and I. E. Shparlinski, 'On the exponent of the group of points on elliptic curves in extension fields', *Intern. Math. Research Notices*, **2005** (2005), 1391–1409. MR2152235 (2006h:11072)
[22] F. Luca and I. E. Shparlinski, 'Elliptic curves with low embedding degree', *J. Cryptology*, **19** (2006), 553–562. MR2267556 (2007h:14034)
[23] F. Luca and I. E. Shparlinski, 'On finite fields for pairing based cryptography', *Adv. Math. of Commun.*, **1** (2007), 281–286. MR2327047 (2008d:11059)
[24] A. Miyaji, M. Nakabayashi and S. Takano, 'New explicit conditions of elliptic curve traces for FR-reduction', *IEICE Trans. Fundamentals*, **E84-A** (2001), 1234–1243.
[25] A. Menezes, T. Okamoto and S. A. Vanstone, 'Reducing elliptic curve logarithms to logarithms in a finite field', *IEEE Transactions on Information Theory*, **39** (1993), 1639–1646. MR1281712 (95e:94038)
[26] R. Sakai, K. Ohgishi and M. Kasahara, 'Cryptosystems based on pairing', *Proc. Symp.on Cryptography and Inform. Security, SCIS'2000*, Okinawa, Japan, 2000.
[27] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.
[28] A. V. Sutherland, 'Computing Hilbert class polynomials with the Chinese Remainder Theorem', *Math. Comp*, **80** (2011), 501–538. MR2728992
[29] S. Tanaka and K. Nakamula, 'Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials', *Lect. Notes in Comp. Sci.*, vol. 5209 Springer-Verlag, Berlin, 2008, 136–145.
[30] E. Wirsing, 'Das asymptotische Verhalten von Summen uber multip- likative Funktionen,' *Math. Ann.*, **143** (1961), 75–102. MR0131389 (24:A1241)

Departamento de Matemática Aplicada IV, Universidad Politecnica de Catalunya, Barcelona, 08034, España
E-mail address: jjimenez@ma4.upc.edu

Instituto de Matemáticas, Universidad Nacional Autonoma de México, C.P. 58089, Morelia, Michoacán, México
E-mail address: fluca@matmor.unam.mx

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: igor.shparlinski@mq.edu.au