Elliptic Curves with Low Embedding Degree

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

October 8, 2005

Abstract

Motivated by the needs of the *pairing based cryptography*, Miyaji, Nakabayashi and Takano have suggested a construction of so-called MNT elliptic curves with low embedding degree. We give some heuristic arguments which suggest that there are only about $z^{1/2+o(1)}$ of MNT curves with complex multiplication discriminant up to z. We also show that there are very few finite fields over which elliptic curves with small embedding degree and small complex multiplication discriminant may exist (regardless of the way they are constructed).

1 Introduction

Since the pioneering works [8, 9, 14, 15, 20, 21, 25], several other cryptographic applications of the Tate or Weil pairing on elliptic curves have been discovered (see, for example, [1, 7]). In particular, for these applications, the following problem is of primal interest: Find an efficient construction of elliptic curves $\mathcal{E}$ over the finite field $\mathbb{F}_q$ of q elements, such that $\#\mathcal{E}(\mathbb{F}_q)$, the number of $\mathbb{F}_q$-rational points on $\mathcal{E}$, has a sufficiently large prime divisor $\ell \mid \#\mathcal{E}(\mathbb{F}_q)$ which also satisfies $\ell \mid q^k - 1$ for a reasonably small value of the positive integer k. In what follows, we refer to [6, 23] for a background on elliptic curves.

It is easy to see that *supersingular curves* are the natural candidates for such constructions. However, one can also suspect that supersingular curves have some cryptographic weaknesses and thus ask for constructions generating *ordinary curves* with the above property. It follows from results of [2, 17, 18] that such curves are very rare and brute force search is not likely to succeed. On the other hand, several such constructions have recently been proposed (see [3, 4, 5, 10, 13, 19, 22] and the references therein). Unfortunately, none of these constructions has been rigorously analyzed and, in fact, even heuristic analysis is not immediate, and may take significant efforts. For example, see [12, 13] for several examples of such analysis of various aspects of the above constructions.

Let

$$\Phi_k(X) = \prod_{\substack{j=0 \\ \gcd(j,k)=1}}^{k} (X - \exp(2\pi\iota j/k))$$

be the kth *cyclotomic polynomial*, where $\iota = \sqrt{-1}$. Typically, the above mentioned constructions work into two steps:

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

$$|t| \leq 2q^{1/2}, \qquad t \neq 0, 1, 2, \qquad \ell \mid q + 1 - t, \qquad \ell \mid \Phi_k(q). \tag{1}$$

Step 2 Construct an elliptic curve $\mathcal{E}$ over $\mathbb{F}_q$ with $\#\mathcal{E}(\mathbb{F}_q) = q + 1 - t$.

In the above construction, k should be reasonable small (for example $k = 2, 3, 4, 6$ are typical values), while the ratio $\log \ell / \log q$ should be as large as possible, preferably close to 1.

Unfortunately, there is no efficient algorithm for Step 2, except for the case when the $t^2 - 4q$ has a very small square-free part; that is, when

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

with some integers r and s, where s is a small square-free positive integer. In this case either $-s$ or $-4s$ is the fundamental discriminant of the complex multiplication field of the corresponding elliptic curve.

Accordingly, for positive real numbers x, y and z we denote by $Q_k(x, y, z)$ the number of prime powers $q \le x$ for which there exist a prime $\ell \ge y$ and an integer t satisfying (1) and (2) with a square-free positive integer $s \le z$. In this note, we obtain an upper bound on $Q_k(x, y, z)$ which suggests that finite fields suitable for pairing based cryptography are very rare, at least using the current algorithms for constructing elliptic curves with a given number of points.

For example, if $z = O(1)$, that is, if the complex multiplication discriminant is bounded by an absolute constant, and the cardinality of the curve must be prime, then our bound implies that there are at most $x^{1/2+o(1)}$ such possible fields $\mathbb{F}_q$ with $q \le x$. On the other hand, heuristically, the construction proposed in [5] should lead to about $x^{1/4+o(1)}$ examples of suitable fields and elliptic curves. It would be very interesting to close the gap and give, if not rigorous then at least convincing heuristic, tight upper and lower bounds on the number of suitable finite fields.

We also examine in more detail one of the first constructions of the above type, namely the construction of the MNT curves from [19], and give some heuristic arguments which suggest that this construction may produce only a very limited family of curves once one wants that $\ell = q + 1 - t$ is prime. On the other hand, we give some arguments showing for any fixed $\delta > 0$ one can generate substantially many more curves if only $\log \ell / \log q \ge 1 - \delta$ is desired. Moreover, one can let δ be a slowly decreasing function of q.

Throughout the paper, the implied constants in the symbols 'O', '$\ll$' and '$\gg$', may occasionally, where obvious, depend on the small positive parameters ε and δ and are absolute otherwise (we recall that $U = O(V)$, $U \ll V$ and $V \gg U$ are all three equivalent to the inequality $|U| \le cV$ with some constant $c > 0$).

Acknowledgements. The authors would like to thank Paulo Barreto, Steven Galbraith, James McKee and Alfred Menezes for several enlightening discussions. This paper was written during an enjoyable visit by F. L. to

the Macquarie University in Sydney, Australia; this author wishes to express his thanks to that institution for its hospitality and support. During the preparation of this paper, F. L. was also supported in part by grant SEP-CONACyT 46755 and a Guggenheim Fellowship, and I. S. was supported in part by ARC grant DP0556431.

2 Scarcity of the Pairing Friendly Fields

According to the heuristics given in [13], there are about $x^{1/2+o(1)}$ of prime powers $q \le x$ for which there is an ordinary elliptic curve $\mathcal{E}$ satisfying $\#\mathcal{E}(\mathbb{F}_q) \mid \Phi_k(q)$. We note that these heuristics apply to all curves without any restriction on the arithmetic structure of $\#\mathcal{E}(\mathbb{F}_q)$, or on the size of the discriminant of the field of complex multiplication. It seems that giving a rigorous proof of this result is out of reach nowadays due to our poor knowledge of the distribution of roots of polynomial congruences (see [11] for the limits of what is achievable nowadays). However, in the most important practical case when the cardinality of the curve is required to have a large prime divisor and the complex multiplication discriminant must be small, we are able to prove a comparable upper bound.

Theorem 1. *For any fixed integer k and positive real numbers x, y and z the following bound holds*

$$Q_k(x, y, z) \le x^{3/2+o(1)} y^{-1} z$$

as $x \to \infty$.

Proof. Since $\ell \mid q + 1 - t$ and $\ell \mid \Phi_k(q)$, we also have $\ell \mid \Phi_k(t-1)$. In particular, each such ℓ divides

$$W = \prod_{|t| \le 2x^{1/2}} \Phi_k(t-1).$$

Clearly, $\log W = O(kx^{1/2} \log x)$.

Let $\omega(n)$ denote the number of prime divisors of an integer n. Since $\omega(n)! \le n$, we have

$$\omega(n) = O\left(\frac{\log n}{\log \log n}\right).$$

Thus, there are at most

$$L \le \omega(W) = O(kx^{1/2}) \tag{3}$$

suitable values of ℓ.

For each fixed $\ell \ge y$ we have

$$\ell m = q + 1 - t \tag{4}$$

with some positive integer $m \le M$, where

$$M = \left\lfloor \frac{x + 1 + 2x^{1/2}}{y} \right\rfloor = O(x/y). \tag{5}$$

Using (4), we can express (2) as

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

which has only $(\ell m)^{o(1)} = x^{o(1)}$ integer solutions (r, t), once ℓ, m and s are fixed. Furthermore, the number q is uniquely determined when ℓ, m and t are fixed. Since there are $O(LMz)$ possible triples (ℓ, m, s), we derive

$$Q(x, y, z) \le LMzx^{o(1)},$$

and by (3) and (5) we conclude the proof. □

In particular, if $z = x^{o(1)}$, which is the only practically interesting case anyway, we see that unless $y \le x^{1/2}$ there are very few finite fields suitable for pairing based cryptography. In other words, unless the request of the primality of the cardinality of the curve is relaxed to the request for this cardinality to have a large prime divisor (that is, a prime divisor ℓ with $\log \ell / \log q \ge 1/2$), the suitable fields are very rare.

3 Heuristic on MNT Curves

3.1 General outline

Here, we give some heuristic estimates on the number of elliptic curves which can be produced by the algorithms of [19] designed to produce elliptic curves satisfying the condition (1) with $k = 3, 4, 6$, and the condition (2) for a given value of s.

In general, our arguments are based on a combination of the following observations:

- The algorithm of [19] gives a parametric family of curves whose parameter runs through a solution of a *Pell equation* $u^2 - Dv^2 = a$.
- Consecutive solutions (u_j, v_j) of a Pell equation grow exponentially, as e^{cj} for some constant $c > 0$.
- The probability of a random integer n to be prime is $1/\log n$.
- MNT curves should satisfy two independent primality conditions (on the field size and on the cardinality of the curve).

Putting all these observations together leads to the conclusion that the expected total number of such curves is bounded, by the order of magnitude, by the converging series

$$\sum_{j=1}^{\infty} \frac{1}{(\log e^{cj})^2} = c^{-2} \sum_{j=1}^{\infty} \frac{1}{j^2} = \frac{\pi^2}{6c^2}.$$

This leads to the conclusion that the total number of all MNT curves of prime cardinalities (over all finite possible fields) is bounded by an absolute constant. This certainly does not undermind the practical usability of the algorithms of [19] which seem to produce enough such curves in ranges which are used nowadays (for example, for finite fields F_q, where q is a 160-170 bit prime power).

On the other hand, since the set of numbers with a large prime divisor is denser than the set of primes, similar heuristic arguments also show that the algorithms of [19] should be able to produce sufficiently many curves with a low embedding degree and whose cardinalities have a large prime divisor.

We now implement this heuristics in a more precise (and thus more technically cluttered) form which leads to more specific estimates.

3.2 Prime cardinalities

Since all three algorithms for $k = 3, 4, 6$ can be analyzed along the same lines, we only concentrate on the case $k = 6$. In this case, if successful, the algorithm produces positive integers q and t of the form

$$q = 4m^2 + 1, \qquad t = \pm 2m + 1$$

for some positive integer m, where $u = 6m + 1$ is a solution to the following Pell equation

$$u^2 - 3sv^2 = -8, \qquad u, v \in \mathbb{N}. \tag{6}$$

Assume that $3 \nmid s$. Since 8 is a prime power, it follows from the well-known theory of quadratic fields that if we write $(u_1(s), v_1(s))$ for the smallest positive integer solution of the equation (6) with odd u, then all the positive integer solutions to (6) are of the form $(u_j(s), v_j(s))$, where

$$u_j(s) + v_j(s)\sqrt{3s} = (u_1(s) + v_1(s)\sqrt{3s}) \left(U_0(s) + V_0(s)\sqrt{3s}\right)^j, \qquad j \in \mathbb{Z},$$

where $(U_0(s), V_0(s))$ is the fundamental solution of the Pell equation

$$U^2 - 3sV^2 = 1, \qquad U, V \in \mathbb{N}.$$

We also put

$$m_j(s) = \frac{u_j(s) - 1}{6}.$$

Note that we need that $u_j(s) \equiv 1 \pmod 3$ in order for $m_j(s)$ to be an integer. The sequence $(u_j(s))_{j \geq 1}$ is periodic modulo 6 with period at most 2, so if at least one of $u_1(s)$ and $u_2(s)$ is congruent to 1 (mod 3), then at least every second value of $u_j(s)$, $j = 1, 2, \ldots$, is also be congruent to 1 (mod 3), otherwise none of these numbers can satisfy this congruence.

Using the regular heuristics that the probability of a random integer n to be prime is $1/\log n$ and assuming that the numbers

$$q_j(s) = 4m_j(s)^2 + 1 \qquad \text{and} \qquad \ell_j(s) = q_j(s) + 1 \mp (2m_j(s) + 1)$$

behave like random integers with respect to primality, we see that if we denote by $N(s)$ the expected total number of prime powers among the numbers of the form $q_j(s)$ satisfying the additional condition that $\ell_j(s)$ is also a prime, then we expect that uniformly in s (even if we ignore the fact that solutions with $u_j(s) \not\equiv 1 \pmod 6$ do not lead to integer values of $m_j(s)$), we have

$$\begin{aligned} N(s) \ \ll \ & \sum_{j=0}^{\infty} \frac{1}{\log(4m_j(s)^2 + 1) \log(4m_j(s)^2 + 2m_j(s) + 1)} \\ & + \sum_{j=0}^{\infty} \frac{1}{\log(4m_j(s)^2 + 1) \log(4m_j(s)^2 - 2m_j(s) + 1)}. \end{aligned}$$

Since it is clear that

$$U_0(s) = \sqrt{3sV_0^2(s) + 1} \gg s^{1/2},$$

we easily get that if we write

$$\alpha(s) = U_0(s) + V_0(s)\sqrt{3s} \qquad \text{and} \qquad \beta(s) = u_0(s) + v_0(s)\sqrt{3s}, \tag{7}$$

then

$$m_j(s) = \frac{1}{6}\left(\frac{1}{2}\left(\beta(s)\alpha(s)^j + 8\beta(s)^{-1}\alpha(s)^{-j}\right) - 1\right) \gg s^{j/2}.$$

Thus,

$$N(s) \ll \sum_{j\geq 1} \frac{1}{j^2(\log s)^2} \ll \frac{1}{(\log s)^2}. \tag{8}$$

In the case when $3 \mid s$, say $s = 3s_0$, the same arguments apply and lead to the same bound (8). The only change is that the positive integer solutions to (6) are of the form $(u_j(s), v_j(s))$, where

$$u_j(s) + 3v_j(s)\sqrt{s_0} = (u_1(s) + 3v_1(s)\sqrt{s_0})\,(U_0(s) + 3V_0(s)\sqrt{s_0})^j\,, \qquad j \in \mathbb{Z},$$

where $(U_0(s), V_0(s))$ is the smallest positive solution of the Pell equation

$$U^2 - s_0(3V)^2 = 1, \qquad U, V \in \mathbb{N}.$$

We now see that the bound (8) implies that the expected total number $E(z)$ of all MNT curves with $s \leq z$ is

$$E(z) = \sum_{\substack{s\leq z \\ s \text{ square-free}}} N(s) \ll \sum_{s\leq z} \frac{1}{(\log s)^2} \ll \frac{z}{(\log z)^2}.$$

In fact, more is believed (see, for example, [16]), namely that for most s the number $\alpha(s)$ in (7) is very large. Specifically, it is believed that there exists a set $\mathcal{S}$ of asymptotic density 1 of positive integers such that the relation

$$\lim_{s\in\mathcal{S}} \frac{\log\log \alpha(s)}{\log(\sqrt{s})} = 1$$

holds. In particular, $\alpha(s) \geq \exp(s^{1/2+o(1)})$, and thus

$$N(s) \leq \frac{1}{s^{1/2+o(1)}}$$

when $s \in \mathcal{S}$. Thus, it is quite possible that in fact

$$E(z) \leq z^{1/2+o(1)}.$$

3.3 Cardinalities with a large prime divisor

Similar heuristics apply if we weaken the condition that $\ell_j(s)$ is prime and request only that it has a sufficiently large prime divisor, say $l_j(s) \geq q_j(s)^{1-\delta}$ for some $\delta > 0$.

Since in this case we are likely to get infinitely many isogeny classes of elliptic curves, it is natural to introduce the counting function $E_\delta(x, z)$ for the number of isogeny classes of such elliptic curves with $q_j(s) \leq x$ and $s \leq z$.

Let $\rho(u)$ be the *Dickman function* which is defined for $u \geq 0$ by the difference-differential equation

$$u\rho'(u) + \rho(u-1) = 0, \qquad u > 1, \tag{9}$$

together with the initial condition

$$\rho(u) = 1, \qquad 0 \leq u \leq 1.$$

We recall that the number of positive integers $n \leq X$ such that no prime divisor of n exceeds $X^{1/u}$ is $(1+o(1))\rho(u)X$ for every fixed u (see [24, Corollary 9.3, Chapter III.5] for a much more precise statement). Since $\rho(u) < 1$ for every $u > 1$, we see that for every $\delta \in (0,1)$ there is a positive proportion $1 - \rho(1/(1-\delta)) + o(1)$ of positive integers $n \leq X$ which have a prime divisor $l \geq n^{1-\delta}$.

Let us write $M_\delta(s, x)$ for the expected total number of isogeny classes of the above elliptic curves with $q_j(s) \leq x$ and such that $q_j(s)+1 \mp (2m_j(s)+1)$ has a prime divisor $l_j(s) \geq q_j(s)^{1-\delta}$. We say that s is *admissible* if it is square-free and if the equation (6) has solutions with $u_j(s) \equiv 1 \pmod 6$ (and thus, at least 50% of such solutions).

If s is admissible, then similar heuristics as the one used in Section 3.2 together with the fact that $\log \alpha(s) \ll \sqrt{s} \log s$ and $\log \beta(s) \ll \sqrt{s} \log s$ give that for every $\delta \in (0,1)$ we should have

$$\begin{aligned} M_\delta(s,x) &\gg \left(1 - \rho\left(\frac{1}{1-\delta}\right)\right) \sum_{j=1}^{J(s,x)} \frac{1}{j s^{1/2} \log s} \\ &\gg \left(1 - \rho\left(\frac{1}{1-\delta}\right)\right) \frac{\log J(s,x)}{s^{1/2} \log s}, \end{aligned}$$

where

$$J(s,x) = \left\lfloor \frac{\kappa \log x}{s^{1/2} \log s} \right\rfloor$$

and $\kappa > 0$ is some absolute constant. In particular,

$$M_\delta(s,x) \gg \frac{\log\log x}{s^{1/2}\log s}$$

in the range $s < (\log x)^{2-\varepsilon}$ for any fixed positive ε and δ.

It is natural to assume that there is a positive proportion of admissible values of s. Thus, the expected total number $E_\delta(x,z)$ of isogeny classes of such elliptic curves with $q_j(s) \le x$ and $s \le z$ is

$$E_\delta(x,z) = \sum_{\substack{s \le z \\ s \text{ admissible}}} M_\delta(s,x) \gg \sum_{\substack{s \le z \\ s \text{ admissible}}} \frac{\log\log x}{s^{1/2}\log s} \gg \frac{z^{1/2}\log\log x}{\log z}$$

for every $z < (\log x)^{2-\varepsilon}$.

4 Concluding Remarks

One should certainly be very cautious when applying heuristic arguments of the type used in Section 3. In particular, upper bounds of the type $o(1)$ on quantities which take integer values (see (8), for example) look especially dubious. So, we withdraw from making any binding conclusions. However, we believe that overall, the arguments Section 3 give some indication about the power and limitation of the algorithms from [19]. We also hope that some ideas of this paper can be used for evaluating some other similar constructions.

Since

$$\rho(u) = 1 - \log u, \qquad 1 \le u \le 2,$$

one can expect that for a sufficiently small δ the implied constant in the lower bound (5) is proportional to

$$\log\left(\frac{1}{1-\delta}\right) \sim \delta.$$

In particular, one can take δ to be a slowly decreasing function of s, which would correspond to "almost prime" cardinalities.

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange and K. Nguyen, *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.

[3] P. S. L. M. Barreto, B. Lynn and M. Scott, 'Elliptic curves with prescribed embedding degrees', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **3006** (2003), 17–25.

[4] P. S. L. M. Barreto, B. Lynn and M. Scott, 'Efficient implementation of pairing-based cryptosystems', *J. Cryptology*, **17** (2004), 297–319.

[5] P. S. L. M. Barreto and M. Naehrig, 'Pairing-friendly elliptic curves of prime order', *Selected Areas in Cryptography, SAC'2005*, Springer-Verlag, Berlin, (to appear).

[6] I. Blake, G. Seroussi and N. Smart, *Elliptic curves in cryptography*, London Math. Soc., Lecture Note Series, **265**, Cambridge Univ. Press, 1999.

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

[8] D. Boneh and M. Franklin, 'Identity-based encryption from the Weil pairing', *SIAM J. Comp.*, **32** (2003), 586–615.

[9] D. Boneh, B. Lynn and H. Shacham, 'Short signatures from the Weil pairing', *J. Cryptology*, **17** (2004), 297–319.

[10] F. Brezing and A. Weng, 'Elliptic curves suitable for pairing based cryptography', *Designs, Codes and Cryptography*, **37** (2005), 133–141.

[11] W. Duke, J. B. Friedlander and H. Iwaniec, 'Equidistribution of roots of a quadratic congruence to prime moduli', *Annals of Math.*, **141** (1995), 423–441.

[12] R. Dupont, A. Enge and A. Morain, 'Building curves with arbitrary small MOV degree over finite prime fields', *J. Cryptology*, **18** (2005), 79–89.

[13] 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.

[14] A. Joux, 'A one round protocol for tripartite Diffie–Hellman', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1838** (2000), 385–393.

[15] A. Joux, 'The Weil and Tate pairings as building blocks for public key cryptosystems', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2369** (2002), 20–32.

[16] H. W. Lenstra Jr., 'Solving the Pell equation', *Notices Amer. Math. Soc.*, **49** (2002), 182–192.

[17] F. Luca, D. J. Mireles and I. E. Shparlinski, 'MOV attack in various subgroups on elliptic curves', *Illinois J. Math.*, **48** (2004), 1041–1052.

[18] 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.

[19] 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.

[20] K. Rubin and A. Silverberg, 'Supersingular abelian varieties in cryptology', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2442** (2002) 336–353.

[21] R. Sakai, K. Ohgishi and M. Kasahara, 'Cryptosystems based on pairing', *Proc. of SCIS'2000*, Okinawa, Japan, 2000.

[22] M. Scott and P. S. L. M. Barreto, 'Generating more MNT elliptic curves,' *Designs, Codes and Cryptography*, to appear.

[23] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.

[24] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Univ. Press, Cambridge, UK, 1995.

[25] E. R. Verheul, 'Evidence that XTR is more secure than supersingular elliptic curve cryptosystems', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2045** (2001), 195–210.