On prime-order elliptic curves with embedding degrees $k = 3, 4$ and 6

Koray Karabina and Edlyn Teske

Dept. of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1,
kkarabina@uwaterloo.ca, eteske@uwaterloo.ca

Abstract. We further analyze the solutions to the Diophantine equations from which prime-order elliptic curves of embedding degrees $k = 3, 4$ or 6 (MNT curves) may be obtained. We give an explicit algorithm to generate such curves. We derive a heuristic lower bound for the number $E(z)$ of MNT curves with $k = 6$ and discriminant $D \leq z$, and compare this lower bound with experimental data.

Keywords: Elliptic curves, pairing-based cryptosystems, embedding degree, MNT curves.

1 Introduction

For an elliptic curve E defined over a finite field $\mathbb{F}_q$, let $\#E(\mathbb{F}_q) = n = hr$ be the number of $\mathbb{F}_q$-rational points on E, where r is the largest prime divisor of n, and $\gcd(r, q) = 1$. The set of all points of order r in $E(\bar{\mathbb{F}}_q)$ forms a subgroup of $E(\mathbb{F}_q)$ denoted by $E[r]$. For such an integer r, a bilinear map can be defined from a pair of r-torsion points of E to the group μ_r of rth roots of unity in $\bar{\mathbb{F}}_q$, by

$$e_r : E[r] \times E[r] \mapsto \mu_r.$$

In fact, the multiplicative group μ_r in the above mapping lies in the extension field $\mathbb{F}_{q^k}$ where k is the least positive integer satisfying $k \geq 2$ and $q^k \equiv 1 \pmod{r}$. The above mapping is called the *Weil pairing*, and the integer k is called the *embedding degree* of E.

Pairings such as the Weil pairing (other proposed pairings include the Tate pairing, the Eta pairing [2], or the Ate pairing [8]) are used in many cryptographic applications such as identity based encryption [4], one-round 3-party key agreement protocols [9], and short signature schemes [3]. The computation of pairings requires arithmetic in the finite field $\mathbb{F}_{q^k}$. Therefore, k should be small for the efficiency of the application. On the other hand, the discrete logarithm problem (DLP) in the order-r subgroup of $E(\mathbb{F}_q)$ can be reduced to the DLP in $\mathbb{F}_{q^k}$ [14]. Therefore, k must also be sufficiently large so that the DLP in $\mathbb{F}_{q^k}$ is computationally hard enough for the desired security. In particular, it is reasonable to ask for parameters q, r and k so that the DLP in $E(\mathbb{F}_q)$, and the

DLP in $\mathbb{F}_{q^k}$ have approximately the same difficulty. Given the best algorithms known and today's computer technology to attack discrete logarithms in elliptic curve groups and in finite field groups, the 80-bit security level can be satisfied by choosing $r \approx 2^{160}$, and $q^k \approx 2^{1024}$. If $E/\mathbb{F}_q$ is of prime order, then $r \approx q$, and thus the 80-bit security level can be achieved if $q \approx 2^{170}$ and $k = 6$.

Now, Miyaji, Nakabayashi, and Takano [15] gave a characterization of prime-order elliptic curves with embedding degree $k = 3, 4$ and 6, in terms of necessary and sufficient conditions on the pair (q, t) where $t = q + 1 - \#E(\mathbb{F}_q)$, the *trace* of E over $\mathbb{F}_q$. Such elliptic curves, if ordinary (i.e., when $\gcd(q, t) = 1$), are nowadays commonly called *MNT curves*.

The only known method to construct MNT curves is to compute suitable integers q and t such that there exists an ordinary elliptic curve $E/\mathbb{F}_q$ of prime order and embedding degree k, and to then use the Complex Multiplication method (or CM method) [1] to find the equation of the curve E over $\mathbb{F}_q$. In fact, all methods known so far to construct ordinary elliptic curves of any order and small embedding degree use the CM method; see [5] for a comprehensive survey. A central equation in this context is the *CM equation*

$$4q - t^2 = DY^2 \tag{1}$$

where D is a positive integer and $Y \in \mathbb{Z}$. If D is square-free, we call D the *Complex Multiplication discriminant* (or *CM discriminant*, or briefly discriminant) of E. Given current algorithms and computing power, the CM method is practical if $D < 10^{10}$ (see [5] for a discussion of this bound).

From (1) Miyaji, Nakabayashi, and Takano [15] derived Pell-type equations, which we subsequently call *MNT equations* (see Section 2). For a fixed embedding degree $k \in \{3, 4, 6\}$ and CM discriminant D, solving the corresponding MNT equation leads to candidate parameters (q, t) for prime-order elliptic curves $E/\mathbb{F}_q$ of trace $t = q+1-\#E(\mathbb{F}_q)$, embedding degree k and discriminant D. As, by nature of generalized Pell equations, the solutions of an MNT equation (if sorted by bitsize and enumerated) grow exponentially, MNT curves are very rare. In fact, Luca and Shparlinski [12] gave a heuristic argument that for any upper bound z, there exists only a finite number of MNT curves with discriminant $D \leq z$, regardless of the field size. On the other hand, specific sample curves of cryptographic interest have been found, such as MNT curves of 160-bit, 192-bit, or 256-bit prime order ([18, 21]).

Contribution of this paper. First, we further analyze the solutions of the MNT equations and establish that the MNT curves of embedding degree 6 are given through the solutions in one of the two (if any) solution classes of the MNT equation (Section 3). Based on this analysis we give a complete algorithm (in the appendix) to calculate such solutions that lead to potentially prime-order elliptic curves; we could not find such an explicit algorithm anywhere in the literature. We also point out a one-to-one correspondence between MNT curves of embedding degree 4 and MNT curves of embedding degree 6 (Proposition 1).

Second, building on the work by Luca and Shparlinski [12] who gave a heuristic upper bound on the expected number $E(z)$ of MNT curves with embedding degree 6 and bounded discriminant $D \le z$, we provide a heuristic lower bound for $E(z)$ (Section 4.2). Specifically, we show that for large enough z we have $E(z) \ge 0.49\frac{\sqrt{z}}{(\ln z)^2}$, which nicely complements the Luca-Shparlinski result that $E(z) \ll z/(\log z)^2$ and corrects the guess [12, p. 559] that $E(z) \le z^{o(1)}$. Here and throughout, $\log z$ denotes the natural logarithm of z.

Finally, we give numerical data on $E(z)$ over finite fields of bounded characteristic, and compare those data with our new lower bound (Section 4.3). At least for this experimentally verifyable range, our lower bound, once corrected by a constant factor, seems to quite well capture the number of MNT curves of discriminant $D \le z$.

Acknowledgements. The authors thank Florian Luca and Igor Shparlinski for their feedback on an earlier version of this paper, which helped us to improve the statement and proof of Theorem 3.

2 MNT curves and their Pell equations

The Miyaji-Nakabayashi-Takano characterization [15] of MNT curves is summarized in the following theorem.

Theorem 1. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve defined over a finite field $\mathbb{F}_q$. Let $n = \#E(\mathbb{F}_q)$ be a prime and k the embedding degree of E.*

1. *Suppose $q > 64$. Then $k = 3$ if and only if $q = 12l^2 - 1$ and $t = -1 \pm 6l$ for some $l \in \mathbb{Z}$.*
2. *Suppose $q > 36$. Then $k = 4$ if and only if $q = l^2 + l + 1$ and $t = -l, l + 1$ for some $l \in \mathbb{Z}$.*
3. *Suppose $q > 64$. Then $k = 6$ if and only if $q = 4l^2 + 1$ and $t = 1 \pm 2l$ for some $l \in \mathbb{Z}$.*

Note that for each elliptic curve characterized by Theorem 1 we have exactly two representations. For example ($k = 4$), if $t = -l$ and $q = l^2 + l + 1$ for some integer l, we can also write $l' = -l - 1$ and $t = l' + 1$ and $q = l'^2 + l' + 1$. (See also Proposition 4.)

The characterization from Theorem 1 implies a one-to-one correspondence between MNT curves with embedding degree $k = 4$ and MNT curves with embedding degree $k = 6$.

Proposition 1. *Let $n > 64$ and $q > 64$ be primes. Then n and q represent an elliptic curve $E_6/\mathbb{F}_q$ with embedding degree $k = 6$ and $\#E_6(\mathbb{F}_q) = n$ if and only if n and q represent an elliptic curve $E_4/\mathbb{F}_n$ with embedding degree $k = 4$ and $\#E_4(F_n) = q$.*

Proof. Let $n > 64$ and $q > 64$ represent an elliptic curve $E_6/\mathbb{F}_q$ with $k = 6$ and $\#E_6(\mathbb{F}_q) = n = q + 1 - t$. By Hasse's theorem we have $t^2 \le 4q$. Now,

$$\begin{aligned} t^2 \le 4q &\Leftrightarrow t^2 \le 4(t - 1 + n) \\ &\Leftrightarrow (t-2)^2 \le 4n. \end{aligned} \tag{2}$$

Let $n' = q$, $q' = n$, and $t' = q' + 1 - n'$. Then $t' = 2 - t$, and by (2), t' satisfies the Hasse bound with $q' = n$. So let E_4 be an elliptic curve over $\mathbb{F}_{q'}$ with n' points. Now, by Theorem 1(3) $q = 4l^2 + 1$ for some integer l. If $t = 1 - 2l$, then $q' = q + 1 - t = (2l)^2 + 2l + 1$ and $t' = 2l + 1$, and thus by (2) of Theorem 1, $E_4/\mathbb{F}_{q'}$ has embedding degree $k' = 4$. Replacing l by $-l$ in the last sentence settles the other case, $t = 1 + 2l$.

To prove the converse, let n, q be primes greater than 64 representing an elliptic curve $E_4/\mathbb{F}_q$ with embedding degree $k = 4$ and n points, and let $t = q + 1 - n$. Then by Theorem 1(2) $t = l + 1$ or $t = -l$ for some $l \in \mathbb{Z}$. Since both n, q are odd primes, t must be odd. Thus, l is even if $t = l + 1$, and l is odd if $t = -l$. In the first case, $l = 2m$ and $t = 1 + 2m$ for some integer m, while in the second case, we can write $l = 2(-m) - 1$ and $t = 1 + 2m$ for some $m \in \mathbb{Z}$. We now proceed just as in the first part (starting after (2)).

Now, let us parametrize MNT curves by $(q(l), t(l))$ where $q(l)$ and $t(l)$ are as in Theorem 1. Then, after some elementary manipulation of the corresponding CM equations $4q(l) - t(l)^2 = DY^2$, one can obtain generalized Pell equations which we call the *MNT equations*. In particular:

1. The MNT equation for $k = 3$ is $X^2 - 3DY^2 = 24$, where $t(l) = 6l - 1$ and $X = 6l + 3$, or $t(l) = -6l - 1$ and $X = 6l - 3$.
2. The MNT equation for $k = 4$ is $X^2 - 3DY^2 = -8$, where $t(l) = -l$ and $X = 3l + 2$, or $t(l) = l + 1$ and $X = 3l + 1$.
3. The MNT equation for $k = 6$ is $X^2 - 3DY^2 = -8$. where $t(l) = 2l + 1$ and $X = 6l - 1$, or $t(l) = -2l + 1$ and $X = 6l + 1$.

The *MNT method* then consists of the following: Fix k. Choose $D < 10^{10}$. Solve the MNT equation to (hopefully) find pairs (q, t) such that q is a prime power and of the desired bitlength, and $q + 1 - t$ is prime. Finally, use the CM method to construct the actual curve.

3 Solving the MNT equations

For solving the MNT equations, we need some facts from the theory of Pell equations and continued fractions. We refer to Mollin's book [16] for more details.

Let $m \in \mathbb{Z}$, $D \in \mathbb{N}$ and D not a perfect square. Then a generalized Pell equation can be given as follows

$$X^2 - DY^2 = m. \tag{3}$$

If $x \in \mathbb{Z}, y \in \mathbb{Z}$ and $x^2 - Dy^2 = m$ then we use both (x, y) and $x + y\sqrt{D}$ to refer to a solution of (3), since $x + y\sqrt{D}$ is an element in the quadratic field $\mathbb{Q}(\sqrt{D})$ with norm $x^2 - Dy^2 = m$. Let $\alpha = x + y\sqrt{D}$ be a solution to (3). If gcd(x, y)=1 then α is called a *primitive solution*. Two primitive solutions $\alpha_1 = x_1 + y_1\sqrt{D}$ and $\alpha_2 = x_2 + y_2\sqrt{D}$ belong to the same *class* of solutions if there is a solution $\beta = u + v\sqrt{D}$ of $X^2 - DY^2 = 1$ such that $\alpha_1 = \beta\alpha_2$. Now, if $\alpha = x + y\sqrt{D}$ then let α' denote the *conjugate* of α, that is, $\alpha' = x - y\sqrt{D}$.

If a primitive solution and its conjugate are in the same class then the class is called *ambiguous.* If $\alpha = x + y\sqrt{D}$ is a solution of (3) for which y is the least positive value in its class then α is called the *fundamental solution* in its class. Note that if the class is not ambiguous then the fundamental solution is determined uniquely. If the class is ambiguous then adding the condition $x \geq 0$ defines the fundamental solution uniquely. Finally, if $\alpha = x + y\sqrt{D}$ is a solution of (3) for which y is the least positive value and x is nonnegative in its class then α is called the *minimal solution* in its class, and it is determined uniquely. If (x, y) is a minimal solution to $X^2 - DY^2 = m$, and (u, v) is a minimal solution to $U^2 - DV^2 = 1$ then all primitive solutions (x_j, y_j) in the class of (x, y) are generated as follows:

$$x_j + y_j\sqrt{D} = \pm(x + y\sqrt{D})(u + v\sqrt{D})^j, \text{where } j \in \mathbb{Z}. \tag{4}$$

The following proposition determines whether the given two solutions of a Pell-type equation are in the same class.

Proposition 2 ([16], Proposition 6.2.1). *Let $x_1 + y_1\sqrt{D}$ and $x_2 + y_2\sqrt{D}$ be primitive solutions of $X^2 - DY^2 = m$. They are in the same class if and only if both*

$$(x_1x_2 - y_1y_2D)/m \in \mathbb{Z} \quad \text{and} \quad (y_1x_2 - x_1y_2)/m \in \mathbb{Z}. \tag{5}$$

Consequently, there are only finitely many classes of primitive solutions of $X^2 - DY^2 = m$.

Next, we show that under certain circumstances Pell-type equations cannot have elements from an ambiguous class as solutions. We will use this result in Section 3.1.

Lemma 1. *Let $m \in \mathbb{Z}$, $m \equiv 0 \pmod 4$, and let D be an odd positive integer, not a perfect square. Then, the set of solutions to $X^2 - DY^2 = m$ does not contain any ambiguous class.*

Proof. Suppose that there is an ambiguous class of solutions. Then there exists a primitive solution $\alpha = x + y\sqrt{D}$ such that α and α' are in the same class. Since m is even and D is odd and $\gcd(x, y) = 1$, y must be odd. By Proposition 2, $(x^2 + y^2D)/m = (m + 2y^2D)/m$ must be an integer. In particular, $2y^2D/m$ is an integer. But this is a contradiction since $4|m$ while y and D are odd.

If $\alpha = (x, y)$ is any solution in a given solution class of $X^2 - DY^2 = m$ then it is known ([17], Theorem 4.2) that there exists an integer P_0 which satisfies $-|m|/2 < P_0 \leq |m|/2$ and

$$P_0 + \sqrt{D} = (x + y\sqrt{D})(s + t\sqrt{D}) \tag{6}$$

for some unique element $s + t\sqrt{D}$. In this case $\alpha = (x, y)$ is said to *belong* to the element P_0.

Remark 1. If α belongs to P_0 and the class containing α is not ambigious, then $\alpha' = (x, -y)$ belongs to $-P_0$. This can be seen by conjugating (6) and then multiplying it by -1, which gives $-P_0 + \sqrt{D} = (x - y\sqrt{D})(-s + t\sqrt{D})$.

3.1 Embedding degree $k = 6$

In this section we analyze the MNT equation for the case $k = 6$: $X^2 - 3DY^2 = -8$. We let $D' = 3D$ and for future reference rewrite the equation as

$$X^2 - D'Y^2 = -8. \tag{7}$$

We will show that for finding all computable MNT curves with $k = 6$ the following applies:

1. D' should be fixed such that $0 < D' < 3 \cdot 10^{10}$ and $D'/3$ is squarefree. – This is required for the CM method.
2. $D' \equiv 9 \pmod{24}$ and -2 is a square modulo D' (Proposition 3).
3. If there is a solution to $X^2 - D'Y^2 = -8$ then it is enough to find, if it exists, only one minimal solution, say (x_0, y_0) (Theorem 2, Proposition 4).
4. Let (u, v) be a minimal solution to $U^2 - D'V^2 = 1$ and $(x_j, y_j) = \pm(x_0, y_0)(u, v)^j$ the set of all solutions in the same class as (x, y). Then it is enough to consider only one of the solutions (x_j, y_j) and $-(x_j, y_j)$ (Proposition 4).

Proposition 3. *Assume $E/\mathbb{F}_q$ $(q > 64)$ is an MNT curve with embedding degree $k = 6$ and CM discriminant D that is constructible with the MNT method. Let $D' = 3D$. Then (7) must have only primitive solutions. Further, $D' \equiv 9 \pmod{24}$, and -2 must be a square modulo D'.*

Proof. If there exists $E/\mathbb{F}_q$ with $k = 6$ then by Theorem 1(3) there exists some integer l satisfying $4q - t^2 = 12l^2 \pm 4l + 3$. As the CM equation (1) needs to hold, this implies $4l(3l \pm 1) + 3 = DY^2$, and so $DY^2 \equiv 3 \pmod 8$. Hence, $D \equiv 3 \pmod 8$, and $D' \equiv 9 \pmod{24}$. Now, let (x, y) be a solution of (7) with $\gcd(x, y) = d > 1$ and let $x = dx'$, $y = dy'$. Since $d^2(x'^2 - D'y'^2) = -8$ and D' is odd, we must have $d = 2$. Then $x'^2 - D'y'^2 = -2$ and thus $x'^2 - y'^2 \equiv 6 \pmod 8$. But this congruence has no integer solutions, and so any solution of (7) must be primitive. Finally, reducing (7) modulo D' proves that -2 must be a square modulo D'.

By Proposition 3, the MNT curves with $k = 6$ can only be obtained through the primitive solutions of the equation

$$X^2 - D'Y^2 = -8, \quad \text{where } D' \equiv 9 \pmod{24}. \tag{8}$$

Lemma 2. *If (x, y) is a primitive solution to (8), then x and y must both be odd.*

Proof. First note that D' is odd. Thus, if y is even then x must be even, and is (x, y) is not primitive. So y must be odd. Suppose now that y is odd and x is even. But then $4 \mid D'$, a contradiction.

Remark 2. For any solution (x, y) of (7) with x odd we must have $x \equiv \pm 1 \pmod 6$. (Reducing (7) modulo 3 yields $x^2 \equiv 1 \pmod 3$.)

Theorem 2. *Equation (8) either does not have any solution or it has exactly two classes of solutions. In particular, if α is a solution of (8) then α and its conjugate α' represent the two solution classes.*

Proof. If (8) does not have any solution then we are done. Therefore, we shall assume that α is a solution belonging to some class, say P_0. Then, by Lemma 1 and Remark 1, α' is a solution belonging to $-P_0$. If these are the only two solution classes then we are done. So assume that there are more than two solution classes. Now, by the choice of P_0 we have $P_0^2 - D' \equiv 0 \pmod 8$, and $-4 < P_0 \leq 4$. Thus, since $D' \equiv 1 \pmod 8$, the only possible values for P_0 which represent the different classes of solutions are $P_0 = \pm 1, \pm 3$. So let $\alpha, \alpha', \beta, \beta'$ correspond to the P_0 values $1, -1, 3, -3$, respectively.

Since α is a solution belonging to class $P_0 = 1$ we can write for some integers s_1, t_1 that

$$1 + \sqrt{D'} = \alpha(s_1 + t_1\sqrt{D'}), \tag{9}$$

and thus by conjugation (see Remark 1)

$$1 - \sqrt{D'} = \alpha'(s_1 - t_1\sqrt{D'}). \tag{10}$$

Now, let $D' \equiv 1 \pmod 8$ and let $\alpha = x + y\sqrt{D'}$. Consider the quadratic field $\mathbb{Q}(\sqrt{D'})$, and its ring of integers R. The prime ideal generated by 2 factors in R as

$$2R = \langle 2, \frac{1+\sqrt{D'}}{2}\rangle\langle 2, \frac{1-\sqrt{D'}}{2}\rangle \tag{11}$$

([13, Theorem 25]). Note that $\alpha/2$ and $\alpha'/2$ are both algebraic integers in $Q(\sqrt{D'})$ since, by Lemma 2, x and y have the same parity. Also the principal ideals generated by $\alpha/2$ and $\alpha'/2$ are prime ideals since both have norm 2 in $\mathbb{Q}(\sqrt{D'})$. Therefore, (9) and (10) give the inclusion $\langle 2, \frac{1+\sqrt{D'}}{2}\rangle \subseteq \langle\frac{\alpha}{2}\rangle$ and $\langle 2, \frac{1-\sqrt{D'}}{2}\rangle \subseteq \langle\frac{\alpha'}{2}\rangle$, respectively. In fact, we even have equality in both inclusions since all four ideals are nonzero prime ideals, that is,

$$\langle\frac{\alpha}{2}\rangle = \langle 2, \frac{1+\sqrt{D'}}{2}\rangle \qquad \text{and} \qquad \langle\frac{\alpha'}{2}\rangle = \langle 2, \frac{1-\sqrt{D'}}{2}\rangle.$$

We now apply a similar reasoning to β and β'. Since β is a solution belonging to class $P_0 = 3$ there exist integers s_2 and t_2 such that

$$3 + \sqrt{D'} = \beta(s_2 + t_2\sqrt{D'}),$$

that is,

$$2 - \frac{1-\sqrt{D'}}{2} = \frac{\beta}{2}(s_2 + t_2\sqrt{D'}),$$

and using $\frac{\beta}{2} \cdot \frac{\beta'}{2} = -2$ we obtain

$$\frac{1-\sqrt{D'}}{2} = -\frac{\beta}{2}(\frac{\beta'}{2} + s_2 + t_2\sqrt{D'}).$$

Consequently, $\langle 2, \frac{1-\sqrt{D'}}{2}\rangle \subseteq \langle \frac{\beta}{2}\rangle$, and similarly, also $\langle 2, \frac{1+\sqrt{D'}}{2}\rangle \subseteq \langle \frac{\beta'}{2}\rangle$. Again, all four ideals are nonzero prime ideals so that we have indeed equality in both inclusions. Therefore,

$$\langle 2, \frac{1+\sqrt{D'}}{2}\rangle = \langle \frac{\alpha}{2}\rangle = \langle \frac{\beta'}{2}\rangle \tag{12}$$

and

$$\langle 2, \frac{1-\sqrt{D'}}{2}\rangle = \langle \frac{\alpha'}{2}\rangle = \langle \frac{\beta}{2}\rangle. \tag{13}$$

It follows from (12) that

$$1+\sqrt{D'} = \beta'(\frac{s_3 + t_3\sqrt{D'}}{2}) \tag{14}$$

for some integers s_3, t_3 of the same parity. In fact, s_3 and t_3 must be odd since α and β' belong to different solution classes. Similarly, it follows from (13) that

$$3+\sqrt{D'} = \alpha'(\frac{s_4 + t_4\sqrt{D'}}{2}) \tag{15}$$

for some odd integers s_4 and t_4. Now write $D' = 8n+1$ for some integer n. If n is odd, then we multiply (14) with its conjugate to obtain $s_3^2 - t_3^2 D' = 4n$. So $s_3^2 - t_3^2 \equiv 4 \pmod 8$, which does not have any solution for odd values of (s_3, t_3). If n is even, then multiplying (15) with its conjugate gives $s_4^2 - t_4^2 D' = 4(n-1)$, that is, $s_4^2 - t_4^2 \equiv 4 \pmod 8$ which does not have any solution for odd values of (s_4, t_4). Consequently, the assumption that there are more than two solution classes was wrong. This completes the proof.

Proposition 4. *Assume (8) has a solution, and let S and S' denote the two solution classes. Let $\mathcal{E}$ and $\mathcal{E}'$ denote the sets of elliptic curves of embedding degree 6 that correspond to the solutions in S and S', respectively, using the correspondence from Section 2: if $(x,y) \in S$ (or S') and $x \equiv 1 \pmod 6$, let $l = (x-1)/6$ and E_x be the elliptic curve over $\mathbb{F}_q$ with trace t where $q = 4l^2+1$ and $t = 1+2l$, while if $(x,y) \in S$ (or S') and $x \equiv -1 \pmod 6$, let $l = (x+1)/6$ and E_x be the elliptic curve over $\mathbb{F}_q$ with trace t where $q = 4l^2+1$ and $t = 1-2l$. Then $\mathcal{E} = \mathcal{E}'$.*

Proof. Let $E/\mathbb{F}_q \in \mathcal{E}$ with trace t, and $\#E(\mathbb{F}_q) = n$. Then there exists a pair $(x,y) \in S$ such that $x \equiv \pm 1 \pmod 6$. Suppose first that $x \equiv 1 \pmod 6$, and $l = (x-1)/6$. Then $q = 4l^2+1$, $t = 1-2l$ and $n = 4l^2+2l+1$. Now let $(x', y') = (-x, y)$. Since the set of solutions to (8) does not contain any ambiguous class (Lemma 1), we have $(x', y') \in S'$. Further, $x' \equiv -1 \pmod 6$. Now let $l' = (x'+1)/6$, and $q' = 4l'^2+1$, $t' = 1+2l'$, $n' = 4l'^2+2l'+1$. Let

$E'_x \in \mathcal{E}'$ be the corresponding elliptic curve over $\mathbb{F}'_q$ with trace t' and n' points. Since $l' = -l$ and thus $q' = q$, $t' = t$ and $n' = n$, we have (up to isogenies) $E_{x'} = E$. The analogous reasoning applies for the case $x \equiv -q \pmod 6$. Thus, $\mathcal{E} \subset \mathcal{E}'$. The converse follows with the same argument.

Summing up, we showed that MNT curves with $k = 6$ are completely characterized through certain primitive solutions of the corresponding MNT equation, $X^2 - 3DY^2 = -8$. Moreover, we showed that this MNT equation either has no primitive solutions or has exactly two solution classes. In the latter case, we proved that the two solution classes lead to the same set of elliptic curves and so it is enough to consider only one of the two solution classes. Also, we gave some necessary conditions on D for the existence of solutions to the MNT equation.

3.2 Embedding degree $k = 4$

The case of MNT curves with embedding degree $k = 4$ is completely covered by combining the above analysis for the $k = 6$ case with the explicit one-to-one correspondence of Proposition 1 between the MNT curves with embedding degree $k = 6$ and those with $k = 4$.

3.3 Embedding degree $k = 3$

The analysis of this case is similar to the case $k = 6$. First, we let $D' = 3D$ and rewrite the CM equation for $k = 3$ as

$$X^2 - D'Y^2 = 24.$$

Below, we summarize the results from our analysis [10].

1. D' should be fixed such that $0 < D' < 3 \cdot 10^{10}$ and $D'/3$ is squarefree.
2. $D' \equiv 57 \pmod{72}$ and 6 is a square modulo D'.
3. If there is a solution to $X^2 - D'Y^2 = 24$ then it is enough to find, if it exists, only one minimal solution, say (x_0, y_0).
4. Let (u, v) be a minimal solution to $U^2 - D'V^2 = 1$. Let $(x_j, y_j) = \pm(x_0, y_0)(u, v)^j$ be the set of all solutions in the same class as (x, y). It is enough to consider only one of the solutions (x_j, y_j) and $-(x_j, y_j)$.

4 Frequency of MNT curves

In this section we give estimates for the number of (isogeny classes of) MNT curves of bounded CM discriminant. In our discussion, we focus on the case $k = 6$. Following Luca and Shparlinski [12], we define $E(z)$ to be the expected total number of all isogeny classes of MNT curves (over all finite fields) with embedding degree 6 and CM discriminant $D \leq z$. Luca and Shparlinski [12] gave heuristic upper bounds on $E(z)$ which we recall in Section 4.1, while in Section 4.2 we will give a (new) heuristic lower bound.

4.1 The Luca-Shparlinski upper bounds

Recall from Sections 2 and 3.1 that in order to find MNT curve parameters with $k = 6$ (for a particular D), one needs to first find a minimal solution (x, y) of (8) as well as the minimal solution, say (u, v), of $U^2 - 3DV^2 = 1$. Then the solutions (x_j, y_j) $(j \in \mathbb{Z})$ in the same class as (x, y) would lead to an integer $l_j = (x_j \pm 1)/6$ (see Lemma 2 and Remark 2). Finally, one checks if $q_j := 4l_j^2 + 1$ and $n_j := q_j \mp 2l_j$ (cf. Theorem 1(3)) satisfy the primality conditions.

Luca and Shparlinski [12] define, for a fixed discrininant D, $N(D)$ as the expected total number of $j \in \mathbb{Z}$ for which q_j is a prime power and n_j is a prime. Then

$$E(z) = \sum_{\substack{D \leq z \\ D \text{ squarefree}}} N(D) \ .$$

Under the assumption that the primality properties of q_j and n_j are ruled by the prime number theorem (meaning that q_j and n_j are prime with probabilities $1/\log q_j$ and $1/\log n_j$, respectively), Luca and Shparlinski show that $N(D) \ll 1/(\log D)^2$. They conclude that $E(z) \ll z/(\log z)^2$. Further, Luca and Shparlinski suggest a stronger upper bound for $E(z)$ which relies on the conjecture (see [11, p.185]) that there exists a set $\mathcal{D}$ of nonsquare positive integers that has asymptotic density 1 and such that $\lim_{D \in \mathcal{D}} \frac{\log\log(u+v\sqrt{3D})}{\log\sqrt{D}} = 1$. Using this conjecture, Luca and Shparlinski argue that $N(D) \leq 1/(D^{1+o(1)})$ for $D \in \mathcal{D}$, and suggest that $E(z) \leq z^{o(1)}$. We will see below (Theorem 3) that this does not hold.

4.2 A lower bound

In this section we give a lower bound for $E(z)$. For this we are going to restrict ourselves to solutions of the MNT equation $X^2 - 3DY^2 = -8$ with $Y = 1$.

Theorem 3. *Assume that the primality properties of $4l^2 + 1$ and $4l^2 \pm 2l + 1$, where $l \in \mathbb{N}$ and such that $(6l \pm 1)^2 = 3D - 8$ for some odd squarefree integer D, are captured by the prime number theorem. Then there exists an integer z_0 such that*

$$E(z) \geq 0.49 \frac{\sqrt{z}}{(\log z)^2} \tag{16}$$

for every $z \geq z_0$.

Proof. Let $\mathcal{F}(z)$ denote the set of odd and squarefree integers $D \in [3, z]$ such that $3D - 8$ is a perfect square, and let $F(z) = \#\mathcal{F}(z)$. For $D \in \mathcal{F}(z)$, let $x_D (> 0)$ such that $x_D^2 = 3D - 8$, and let $l_D \in \mathbb{N}$ such that $x_D = 6l_D + 1$ or $x_D = 6l_D - 1$. Denote $q_D = 4l_D^2 + 1$, and $n_D = 4l_D^2 + 2l_D + 1$ if $x_D = 6l_D + 1$ or $n_D = 4l_D^2 - 2l_D + 1$ otherwise.

An easy calculation shows that if $D \leq z$, then $q_D \leq z/2$ and $n_D \leq 3z/4$. As we assume that the primality properties of both q_D and n_D are captured by the prime number theorem, and since for $z > 17$, the number $\pi(z)$ of primes $\leq z$ satisfies $\pi(z) > z/\log z$, we have

$$\begin{aligned}&\mathrm{Prob}(q_D \text{ and } n_D \text{ prime} \mid q_D = 4l^2+1, n_D = 4l^2 \pm 2l + 1, \text{ where}\\ &\qquad\qquad l \geq 1 \text{ and } (6l \pm 1)^2 = 3D - 8 \text{ for some squarefree } D \leq z)\\ &\quad > \tfrac{1}{\log(z/2)} \cdot \tfrac{1}{\log(3z/4)} > \tfrac{1}{(\log z)^2}.\end{aligned}$$

Now, by Section 2, the number $G(z)$ of pairs (q_D, n_D) $(D \in \mathcal{F}(z))$ where both q_D and n_D are prime constitutes a lower bound for $E(z)$. Thus,

$$E(z) \;\geq\; G(z) \;\geq\; F(z) \cdot \frac{1}{(\log z)^2}. \tag{17}$$

To find a lower bound for $F(z)$, first note that $3D - 8$ is a perfect square and D is odd and squarefree, if and only if $D = 12l^2 \pm 4l + 3$ is squarefree (by putting $3D - 8 = (6l \pm 1)^2$). Let $f_+(l) = 12l^2 + 4l + 3$, and $\mathcal{F}_+(z) = \{D \in [5, z] \ : D = f_+(l) \text{ squarefree}\}$. As $f_+(l)$ is irreducible over $\mathbb{Z}[l]$, there are $\sim c_{f_+}L$ positive integers $l \leq L$ such that $f_+(l)$ is squarefree, where c_{f_+} is a positive constant ([19, Theorem A], [6, Theorem 1]). Now, $5 \leq D = f_+(l) \leq z$ if and only if $1 \leq l \leq \sqrt{\frac{z}{12} - \frac{2}{9}} - \frac{1}{6} =: L_+$. Thus, for each $\varepsilon > 0$ there exists an integer Z_+ such that $(c_{f_+} - \varepsilon)L_+ < \#\mathcal{F}_+(z) < (c_{f_+} + \varepsilon)L_+$ for all $z \geq Z_+$. Doing the analogous with $f_-(l) := 12l^2 - 4l + 3$, and $\mathcal{F}_-(z) := \{D \in [5, z] \ : D = f_-(l) \text{ squarefree}\}$ and $L_- := \sqrt{\frac{z}{12} - \frac{2}{9}} + \frac{1}{6}$ we find that there exists a positive constant c_{f_-} such that for each $\varepsilon > 0$ there exists an integer Z_- such that $(c_{f_-} - \varepsilon)L_- < \#\mathcal{F}_-(z) < (c_{f_-} + \varepsilon)L_-$ for all $z \geq Z_-$. Thus, since $\mathcal{F}(z) = \mathcal{F}_+(z) \cup \mathcal{F}_-(z) \cup \{3\}$ (disjoint), we obtain

$$F(z) > (c_{f_+} + c_{f_-} - 2\varepsilon)\sqrt{z/12} \tag{18}$$

for all $z \geq z_0 := \max\{Z_+, Z_-\}$. Now, $c_{f_+} = \prod_{p \text{ prime}} \left(1 - w_{f_+}(p)/p^2\right)$ where $w_{f_+}(p)$ denotes the number of integers $a \in [1, p^2]$ for which $f_+(a) \equiv 0 \pmod{p^2}$ ([19, 6]), and the same holds for c_{f_-} with f_+ replaced by f_- throughout. It can be readily seen that $w_{f_+}(3) = w_{f_-}(3) = 1$ and $w_{f_+}(p), w_{f_-}(p) \in \{0, 2\}$ otherwise. Further, the polynomial $ax^2 + bx + c$ has two solutions modulo p^2 if and only if a is invertible modulo p^2 and $b^2 - 4ac$ is a square modulo p^2. Thus, $f_+(l) \equiv 0 \pmod{p^2}$ $(p > 3)$ has two solutions modulo p^2 if and only if -128 is a quadratic residue modulo p^2. This is the case if and only if $\left(\frac{-2}{p}\right) = 1$, which holds if and only if $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$. The same reasoning applies to $f_-(l)$. Consequently,

$$c_{f_+} = c_{f_-} = \frac{8}{9} \cdot \prod_{p \text{ prime}, \, p \equiv 1,3 \pmod 8} \left(1 - 2/p^2\right).$$

Now, $\prod_{p \text{ prime}, \, p \leq 10000, \, p \equiv 1,3 \pmod 8} \left(1 - 2/p^2\right) > 0.858146$, while the tail can be lower bounded as

$$\prod_{p \text{ prime}, p > 10000} \left(1 - 2/p^2\right) \geq \prod_{s > 10000} \left(1 - 4/s^2\right) = \frac{9999 \cdot 10000}{10001 \cdot 10002} > 0.9996.$$

Hence, $c_{f_\pm} > 0.858146 \cdot 0.9996 > 0.8578$. Combined with (18), using $\varepsilon = 0.0008$, this yields $F(z) > 0.857\sqrt{z/3}$ for all $z \geq z_0$. Used along with (17), this completes the proof.

Remark 3. The above lower bound on $E(z)$ can be increased by a constant factor if also solutions to the MNT equation $X^2 - 3DY^2 = -8$ with $Y > 1$ are considered. In fact, for each odd Y such that $X^2 \equiv 3Y^2 - 8 \pmod{6Y^2}$ is solvable, a lower bound for the number $F_Y(z)$ of odd and squarefree integers $D \in [3, z]$ such that $3Y^2D - 8$ is a perfect square, can be derived in exactly the same way as for $Y = 1$. The corresponding polynomials $f_{Y,\pm}(l)$ are given as $f_{Y,\pm}(l) = 12Y^2l^2 \pm 4sl + (s^2+8)/(3Y^2)$, where $s^2 \equiv 3Y^2 - 8 \pmod{6Y^2}$. They all have (polynomial) discriminant -128, and thus the corresponding c_f-values will differ only by those factors that involve primes $p|Y$. In particular, including the cases $Y = 3, 9$ will raise our lower bound by a factor of $(1 + 1/3 + 1/9)$.

4.3 Experimental results on $E(z)$

Using the computational algebra system MAGMA [7] we implemented an algorithm to calculate, for given bitsize N and upper discriminant bound z, all (isogeny classes of) MNT elliptic curves of embedding degree 6 and discriminant $D \leq z$ over a finite field q where $q - 1$ is an N-bit prime.

As discussed in Section 3, only those squarefree D such that for $D' = 3D$ we have $D' \equiv 9 \pmod{24}$ and $\left(\frac{-2}{D'}\right) = 1$ need to be considered.

For any such $D \leq z$, our algorithm (Algorithm 3 of the appendix) first calls a Pell equation solver to compute minimal solutions (x, y) and (u, v) to (7) and to the equation $u^2 - 3Dv^2 = 1$, respectively. This Pell equation solver is Algorithm 1 (of the appendix) if $3D > 64$ and Algorithm 2 (of the appendix) if $3D < 64$; both algorithms are taken from Robertson [20]. The minimal solutions (x, y) and (u, v) are used to compute, one by one, all primitive solutions to (7). For each such primitive solution, it is checked if it yields values for q and n such that q is a prime power and of the desired bitsize, and n is prime.

Using Algorithm 3, we first conducted a series of experiments to check the quality of our lower bound on $E(z)$ (Theorem 3).

Let $E_B(z)$ denote the number of (isogeny classes of) MNT elliptic curves with embedding degree $k = 6$ and CM discriminant $D \leq z$ over finite fields $\mathbb{F}_q$ with $q < 2^B$. Then $E_B(z) \leq E(z)$ for all B, and $E(z) = \lim_{B\to\infty} E_B(z)$.

We computed $E_B(z)$ for selected values of B, by running Algorithm 3 with input N, for all $1 \leq N \leq B$. Table 4.3 shows the ratios of $E_B(z)$ and the lower bound (16) for $z = 2^i$, $z \leq 2^{25}$ and $B = 160, 300, 500, 700, 1000$.

Let $R(B, z) = E_B(z)/(0.49\frac{\sqrt{z}}{(\log z)^2})$. As we would expect, $R(B, z)$ is increasing for fixed z as B increases. For the smallest values of B, we also see that $R(B, z)$ is essentially decreasing (for fixed B) as z increases. In fact, we expect that $\lim_{z\to\infty} R(B, z) = 0$ for any fixed value of B, as if $X^2 - DY^2 = -8$, then the resulting field size $q(\leq 2^B)$ is of the order of magnitude of $\sqrt{D}$, which implies that $E_B(z)$ remains constant for large enough z. On the other hand, for larger

Table 1. Ratios $R(B,z)$ of $E_B(z)$ and the lower bound (16) for $E(z)$. Here $E_B(z)$ denotes the number of MNT curves with $k = 6$ and $D \leq z$ over $\mathbb{F}_q$ with $q < 2^B$.

	$R(B,z) = E_B(z)/(0.49\frac{\sqrt{z}}{(\log z)^2})$, where $z = 2^i$.							
i	$B = 25$	$B = 50$	$B = 100$	$B = 160$	$B = 300$	$B = 500$	$B = 700$	$B = 1000$
10	30.64	30.64	30.64	33.70	33.70	33.70	33.70	33.70
11	31.45	34.08	34.08	36.70	36.70	36.70	36.70	36.70
12	26.47	28.68	28.68	30.88	30.88	30.88	30.88	30.88
13	23.80	25.63	25.63	27.46	27.46	27.46	27.46	27.46
14	24.02	27.02	27.02	30.02	30.02	30.02	30.02	30.02
15	23.15	26.81	26.81	30.46	30.46	30.46	30.46	30.46
16	21.57	25.49	26.47	29.41	29.41	29.41	29.41	29.41
17	20.35	24.26	26.61	29.74	29.74	29.74	29.74	29.74
18	19.23	23.57	25.43	27.92	27.92	27.92	27.92	27.92
19	18.57	23.46	25.42	27.86	28.35	28.35	28.35	28.35
20	16.85	21.83	24.51	26.81	27.19	27.19	27.57	27.57
21	15.22	21.20	23.58	25.67	26.87	27.47	28.06	28.06
22	14.83	22.01	26.64	28.73	29.66	30.12	30.81	30.81
23	14.32	22.74	27.40	29.72	30.62	30.98	32.05	32.41
24	13.65	24.12	28.54	30.88	32.12	32.67	33.64	34.05
25	13.11	24.54	29.30	31.52	32.79	33.32	34.17	34.48

fixed values of B and in particular along the down-ward diagonal, $R(B,z)$ seems somewhat more stable (around 30, although there is an increase towards the very end). It is tempting to conclude from this that the lower bound (16) for $E(z)$ has indeed the right order of magnitude, and possibly is just off by a factor of around 30. So, let us try to estimate the number of (isogeny classes of) *computable* MNT elliptic curves of embedding degree 6. That is, put $z_0 = 10^{10} (\approx 2^{33})$, and let's boldly assume that $E(z) = 30 \cdot (0.49\frac{\sqrt{z}}{(\log z)^2})$. Then $E(z_0) \approx 30 \cdot 92.4 = 2772$. For comparison, we found that $E_{2^{25}}(2^{10}) = 10, E_{2^{1000}}(2^{10}) = 11, E_{2^{25}}(2^{24}) = 124$ and $E_{2^{1000}}(2^{25}) = 326$.

As prime-order elliptic curves over fields of bitsize $155 - 170$ approximately match the security level of SKIPJACK (i.e., the 80-bit symmetric key security level), we found it of interest to calculate the number of (isogeny classes of) MNT elliptic curves over $155 - 170$-bit fields. But the smallest discriminant for which we found an MNT curve in the desired bit range has 21 bits, with the next two such MNT curves appearing for 24-bit discriminants. These data certainly do not allow for a meaningful extrapolation to $z = 10^{10}$.

5 Conclusion

Our analysis in this paper brought us closer to the true nature of the function $E(z)$, the number of prime-order elliptic curves over finite fields with embedding degree $k = 6$ (MNT curves) and discriminant $D \leq z$. However, it would be nice to be able to estimate the number of MNT curves of bounded discrimant *and* given bit-size. Our experimental data for the cryptographically interesting range are too limited to encourage any predictions.

References

1. A.O.L. Atkin and F. Morain, *Elliptic curves and primality proving*, Mathematics of Computation **61** (1993), 29–68.
2. P.S.L.M. Barreto, S. Galbraith, C. O'hEigeartaigh, and M. Scott, *Efficient pairing computation on supersingular abelian varieties*, Designs, Codes and Cryptography **42** (2007), 239–271.
3. H. Shacham D. Boneh, B. Lynn, *Short signatures from the Weil pairing*, Advances in Cryptology- ASIACRYPT 2001, Lecture Notes in Computer Science **2248** (2001), Springer, 514–532.
4. M. Franklin D. Boneh, *Identity based encryption from the Weil pairing*, Advances in Cryptology- CRYPTO 2004, Lecture Notes in Computer Science **3152** (2004), Springer, 41–55.
5. D. Freeman, M. Scott, and E. Teske, *A taxonomy of pairing-friendly elliptic curves*, Cryptology ePrint Archive Report 2006/372, 2006, http://eprint.iacr.org/2006/372/.
6. A. Granville, *ABC allows us to count squarefrees*, International Mathematical Research Notices **19** (1998), 991–1009.
7. Computational Algebra Group, *The Magma computational algebra system for algebra, number theory and geometry*, School of Mathematics and Statistics, University of Sydney, http://magma.maths.usyd.edu.au/magma.
8. F. Hess, N. Smart, and F. Vercauteren, *The Eta pairing revisited*, IEEE Transactions on Information Theory **52** (2006), 4595–4602.
9. A. Joux, *A one round protocol for tripartite Diffie-Hellman*, Proc. of ANTS IV, Lecture Notes in Computer Science **1838** (2000), Springer, 383–394.
10. K.Karabina, *On prime-order elliptic curves with embedding degrees 3,4 and 6*, Master's thesis, University of Waterloo, 2006, Available at: http://uwspace.uwaterloo.ca/handle/10012/2671.
11. H. W. Jr. Lenstra, *Solving the Pell equation*, Not. Amer. Math. Soc. 49, (2002), 182–192.
12. F. Luca and I. E. Shparlinski, *Elliptic curves with low embedding degree*, Journal of Cryptology **19** (2006), 553–562.
13. D. A. Marcus, *Number fields*, Springer-Verlag, New York, 1977.
14. A. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory **39** (1993), 1639–1646.
15. 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.
16. R. A. Mollin, *Fundamental number theory with applications*, CRC Press, Boca Raton, New York, 1998.
17. ———, *Simple continued fraction solutions for Diophantine equations*, Expositiones Mathematicae **19** (2001), no. 1, 55–73.
18. D. Page, N .P. Smart, and F. Vercauteren, *A comparison of MNT curves and supersingular curves*, Applicable Algebra in Engineering, Communication and Computing **17** (2006), 379–392.
19. G. Ricci, *Ricerche aritmetiche sui polinomi*, Rend. Circ. Mat. Palermo **57** (1933), 433–475.
20. J. P. Robertson, *Solving the generalized Pell equation $x^2 - dy^2 = n$*, 2004, Available at: http://hometown.aol.com/jpr2718/.
21. M. Scott and P.S.L.M. Barreto, *Generating more MNT elliptic curves*, Designs, Codes and Cryptography **38** (2006), 209–217.

Appendix: Algorithms

We present two Pell equation solver algorithms: Algorithms 1 and 2; and one algorithm for finding suitable MNT curve parameters for embedding degree $k = 6$: Algorithm 3. Our reference for the first two algorithms is Robertson's paper [20]. Algorithm 3 uses these two algorithms and the facts developed in this paper.

Algorithm 1 Pell Equation Solver

Input: $D \in \mathbb{Z}$, $m \in \mathbb{Z}\backslash\{0\} : D > m^2$, D is not a perfect square

Output: all minimal positive solutions $(x, y) : \; x^2 - Dy^2 = m$

```
$B_{-1} \leftarrow 0$, $G_{-1} \leftarrow 1$
$P_0 \leftarrow 0$, $Q_0 \leftarrow 1$, $a_0 \leftarrow \lfloor\sqrt{D}\rfloor$, $B_0 \leftarrow 1$, $G_0 \leftarrow a_0$
$i \leftarrow 0$
repeat
  $i \leftarrow i + 1$
  $P_i \leftarrow a_{i-1}Q_{i-1} - P_{i-1}$
  $Q_i \leftarrow (D - P_i^2)/Q_{i-1}$
  $a_i \leftarrow \lfloor(P_i + \sqrt{D})/Q_i\rfloor$
  $B_i \leftarrow a_i B_{i-1} + B_{i-2}$
  $G_i \leftarrow a_i G_{i-1} + G_{i-2}$
until $Q_i = 1$ and $i \equiv 0 \pmod 2$
$s \leftarrow 0$
for $0 \leq j \leq i - 1$ do
  if $G_j^2 - DB_j^2 = m/f^2$ for some $f > 0$ then
    Output: $(fG_j, fB_j)$
    $s \leftarrow 1$
  end if
end for
if $s == 0$ then
  Output: No solutions exist
end if
```

Algorithm 2 Pell Equation Solver 2

Input: $D \in \mathbb{Z}$, $m \in \mathbb{Z}\backslash\{0\} : D \leq m^2$, D is not a perfect square

Output: all fundamental solutions $(x, y) :\ x^2 - Dy^2 = m$

```
Find a minimal solution $(u, v)$ to $U^2 - DV^2 = 1$ using Algorithm 1 with inputs $D$, 1.
if $m > 0$ then
    $L_1 \leftarrow 0$, $L_2 \leftarrow \sqrt{m(u-1)/(2D)}$
else
    $L_1 \leftarrow \sqrt{(-m)/D}$, $L_2 \leftarrow \sqrt{(-m)(v+1)/(2D)}$
end if
for $L_1 \leq y \leq L_2$ do
    if $m + Dy^2$ is a square then
        $x \leftarrow \sqrt{m + Dy^2}$
        if $(x, y)$ and $(-x, y)$ are not in the same class then
            Output: $(x, y), (-x, y)$
        else
            Output: $(x, y)$
        end if
    end if
end for
```

Algorithm 3 Elliptic curve parameters, embedding degree $k = 6$

Input: N, z

Output: EC parameters (q, n, D) where $q-1$ is an N-bit prime, $q^6 \equiv 1 \pmod{n}$ but $q^i \not\equiv 1 \pmod{n}$ for $1 \leq i \leq 5$, and $D \leq z$ (where $4q - t^2 = DY^2$)

.

```
for $0 < D' \leq 3z$, $D'/3$ squarefree, $D' \equiv 9 \pmod{24}$, $-2$ is a square modulo $D'$ do
  if $D' > 64$ then
    find a minimal solution, $(x_0, y_0)$, to $X^2 - D'Y^2 = -8$ by using Algorithm 1 with input $D'$, $-8$.
  else
    find a minimal solution, $(x_0, y_0)$, to $X^2 - D'Y^2 = -8$ by using Algorithm 2 with input $D'$, $-8$.
  end if
  find a minimal solution, $(u, v)$, to $U^2 - D'V^2 = 1$ by using Algorithm 1 with input $D'$, 1.
  $x \leftarrow x_0$, $y \leftarrow y_0$
  if $x \equiv \pm 1 \pmod{6}$ then
    while $|x| \leq 2^{\lceil N/2 \rceil}$ do
      $l \leftarrow (x \mp 1)/6$
      if $(N-3)/2 \leq \log_2 l < (N-2)/2$ then
        $q \leftarrow 4l^2 + 1$, $n \leftarrow 4l^2 \mp 2l + 1$
        if $q$ and $n$ are primes then
          Output $(q, n, D'/3)$
        end if
      end if
      $\widetilde{x} \leftarrow x$
      $x \leftarrow xu + yvD'$
      $y \leftarrow \widetilde{x}v + uy$
    end while
  end if
  $x \leftarrow x_0u - y_0vD'$, $y \leftarrow uy_0 - x_0v$
  if $x \equiv \pm 1 \pmod{6}$ then
    while $|x| \leq 2^{\lceil N/2 \rceil}$ do
      $l \leftarrow (x \mp 1)/6$
      if $(N-3)/2 \leq \log_2 l < (N-2)/2$ then
        $q \leftarrow 4l^2 + 1$, $n \leftarrow 4l^2 \mp 2l + 1$
        if $q$ and $n$ are primes then
          Output $(q, n, D'/3)$
        end if
      end if
      $\widetilde{x} \leftarrow x$
      $x \leftarrow xu - yvD'$
      $y \leftarrow uy - \widetilde{x}v$
    end while
  end if
end for
```