On Prime-Order Elliptic Curves
with Embedding Degrees 3,4 and 6

by
Koray Karabina

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Master of Mathematics
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 2006

I hereby declare that I am the sole author of this thesis. I authorize the University of Waterloo to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I understand that my thesis may be made electronically available to the public.

Abstract

Bilinear pairings on elliptic curves have many cryptographic applications such as identity based encryption, one-round three-party key agreement protocols, and short signature schemes. The elliptic curves which are suitable for pairing-based cryptography are called *pairing friendly* curves. The prime-order pairing friendly curves with embedding degrees $k = 3, 4$ and 6 were characterized by Miyaji, Nakabayashi and Takano. We study this characterization of MNT curves in details. We present explicit algorithms to obtain suitable curve parameters and to construct the corresponding elliptic curves. We also give a heuristic lower bound for the expected number of isogeny classes of MNT curves. Moreover, the related theoretical findings are compared with our experimental results.

Acknowledgements

I would like to thank my supervisor Edlyn Teske for her invaluable comments and help which motivated me during this work.

I would like to acknowledge Hugh C. Williams for pointing out Proposition 4.7. I thank Igor Shparlinski as I benefited a lot from our discussions.

I also thank my readers Alfred Menezes and David Jao for their thoughtful feedback and advice.

Contents

CHAPTER 1

Introduction

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Also let $\#E(\mathbb{F}_q) = n = hr$ be the number of $\mathbb{F}_q$-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 is defined from the pair of r-torsion points of E to the rth roots of unity in $\bar{\mathbb{F}}_q$ as

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

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. There also exists a similar mapping which is called the Tate pairing. For more details on the properties of these pairings we refer the reader to the book [**3**].

These pairings are used in many cryptographic applications such as identity based encryption [**7**], one-round 3-party key agreement protocols [**15**], and short signature schemes [**6**]. The computation of pairings requires arithmetic in the finite field $\mathbb{F}_{q^k}$. Therefore, k should be a 'small' integer for the efficiency of the application. On the other hand, the discrete logarithm problem in the order-r subgroup of $E(\mathbb{F}_q)$ can be reduced to the discrete logarithm problem in $\mathbb{F}_{q^k}$ [**23**]. Therefore, k must also be 'big' enough to satisfy the security requirements. In other words, it is reasonable to ask for parameters (q, r, k) so that the discrete logarithm problem in $E(\mathbb{F}_q)$, and the discrete logarithm problem in $\mathbb{F}_{q^k}$ have approximately the same difficulty. In particular, given the best algorithms known and today's computer technology to attack discrete logarithms in elliptic curve groups and in finite field groups, 80-bit security level is satisfied by choosing $r \approx 2^{160}$, and $q^k \approx 2^{1024}$.

Miyaji, Nakabayashi, and Takano gave the characterization of prime order elliptic curves with embedding degree $k = 3, 4$ and 6 [**24**]. Barreto and Naehrig, in 2005, constructed an explicit family of prime order elliptic curves with $k = 12$ [**2**]. In 2006, Freeman constructed a family of prime order elliptic curves with $k = 10$ [**10**]. Galbraith, McKee, and Valenca extended the methods of [**24**] to non-prime order elliptic curves and they characterize the families of elliptic curves with embedding degrees $k = 3, 4, 6$, and with cofactors $2 \leq h \leq 5$ [**12**]. Barreto, Lynn, and Scott [**1**] investigated elliptic curve constructions for certain values of k. In particular, they described a construction method for $k = 2^i 3^j p^s$ which can generate curves with $1 < \rho = \log_2 n / \log_2 r \approx 2$. Moreover, Dupont, Enge, Morain [**8**], and Cocks, Pinch [**4**] presented constructions of elliptic curves for arbitrary values of k. In general, their methods are expected to produce elliptic curves with $\rho \approx 2$.

In this work, we concentrate on the characterization of elliptic curves with embedding degrees $k = 3, 4$, and 6, and the detailed analysis of this construction.

In Chapter 2, we give some background and definitions related to finite fields, and elliptic curves. Then, we give details on the MNT characterization theorem. Given the parameters for prime order ordinary elliptic curves with $k = 3, 4$, and 6, Section 2.1 explains the construction of these curves through the complex multiplication method. Section 2.2 presents the results of Luca and Shparlinski [**18**], [**19**] which show that MNT curves are very rare.

As we see in Section 2.1, the construction of elliptic curves is based on solving some particular Pell equations. Therefore, some background on continued fractions and Pell-type equations is provided in Chapter 3.

In Chapter 4, we study the construction of prime order elliptic curves with $k = 6$. First, we provide a detailed analysis of the corresponding Pell equation. A necessary and sufficient condition for the solubility of the Pell-equation is given by Theorem 4.10. Using the sufficiency part of this theorem, we obtain a lower bound for the number of Pell equations having integer solutions. Moreover, we give a lower bound for the expected number of MNT curves. We also present an explicit algorithm to obtain suitable elliptic curve parameters. Outputs of this algorithm are discussed and they are compared with the theoretical findings from [**18**] and from this work.

Chapter 5 is analogous to Chapter 4 and investigates elliptic curves with $k = 3$ and 4.

In Chapter 6 we give some cryptographically interesting examples of prime order elliptic curves.

We conclude by Chapter 7 by giving a brief summary of our work and suggesting some research problems.

CHAPTER 2

Prime-order curves of low embedding degree

We begin by giving some facts on finite fields and elliptic curves. The proofs of the statements relating to finite fields can be found in the book by R. Lidl and H. Niederreiter [**17**]. We refer to Silverman's book [**30**] for more details on elliptic curves.

Let $\mathbb{F}_q$ be a finite field with q elements, and $\mathrm{char}(\mathbb{F}_q) = p$. The set of nth *roots of unity* over $\mathbb{F}_q$ is defined to be

$$\mu_n = \{u \in \overline{\mathbb{F}}_q \ : \ u^n = 1\}$$

where $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$. Let f be a positive degree polynomial with coefficients in $\mathbb{F}_q$. The *splitting field* of f over $\mathbb{F}_q$ is the smallest field containing all the roots of f. For $n \geq 1$ the splitting field of $f(x) = x^n - 1$ over $\mathbb{F}_q$ is called the nth *cyclotomic field* over $\mathbb{F}_q$, and hence obtained as $\mathbb{F}_q(\mu_n)$. If $\gcd(p, n) = 1$ then μ_n is a cyclic group of order n with respect to multiplication in $\mathbb{F}_q(\mu_n)$. In this case, any generator of the cyclic group μ_n is called a *primitive nth root of unity* over $\mathbb{F}_q$.

Let ζ be a primitive nth root of unity over $\mathbb{F}_q$. Then, for $1 \leq s < n$ with $\gcd(s, n) = 1$, ζ^s is also a primitive nth root of unity over $\mathbb{F}_q$ and the polynomial

$$\phi_n(x) = \prod_{\substack{s=1 \\ \gcd(s,n)=1}}^{n} (x - \zeta^s) \tag{2.1}$$

is called the *nth cyclotomic polynomial* over $\mathbb{F}_q$. The cyclotomic field $\mathbb{F}_q(\mu_n)$ is an algebraic extension of $\mathbb{F}_q$. Moreover, if n is coprime to q then the extension degree is $[\mathbb{F}_q(\mu_n) : \mathbb{F}_q] = k$, where k is the least positive integer such that $q^k \equiv 1 \pmod{n}$.

Let $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$. An *elliptic curve* over $\mathbb{F}_q$ is defined by the *Weierstrass equation*

$$E : Y^2 = X^3 + aX + b, \ \ a, b \in \mathbb{F}_q, \ \ 4a^3 + 27b^2 \neq 0,$$

and denoted by $E/\mathbb{F}_q$. The set of *rational points* on $E/\mathbb{F}_q$ is defined by

$$E(\mathbb{F}_q) = \{(x, y) \in (\mathbb{F}_q, \mathbb{F}_q) : y^2 = x^3 + ax + b, a, b \in \mathbb{F}_q\} \cup \{O\}$$

where O is the *point at infinity.* The rational points on an elliptic curve form an abelian group with identity O, under the addition operation defined by the *tangent-chord* method ([**30**], p.55). The cardinality of $E(\mathbb{F}_q)$ is denoted by $\#E(\mathbb{F}_q)$ and is called the *order* of E . The following theorem is due to Hasse:

THEOREM 2.1. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then*

$$(\sqrt{q} - 1)^2 \leq \#E(\mathbb{F}_q) \leq (\sqrt{q} + 1)^2.$$

By Theorem 2.1, $\#E(\mathbb{F}_q) = q+1-t$ for some integer t such that $|t| \leq 2\sqrt{q}$. The integer t is called the *trace* of the elliptic curve E.

Let P be a point in $E(\mathbb{F}_q)$. The *order* of P is the least positive integer r such that $rP = O$. If $P \in E(\mathbb{F}_q)$ has order dividing r then it is called an r-*torsion* point. The set of all r-torsion points in $E(\mathbb{F}_q)$ forms a subgroup in $E(\mathbb{F}_q)$, and it is denoted by $E(\mathbb{F}_q)[r]$.

Elliptic curves are characterized as *supersingular* elliptic curves and *ordinary* (or *non-supersingular*) elliptic curves depending on whether the *endomorphism ring* is non-commutative (i.e., the supersingular case) or commutative (i.e., the ordinary case). If E is defined over a finite field $\mathbb{F}_q$ with $\mathrm{char}(\mathbb{F}_q) = p$ then it is known that E is supersingular if and only if $p \mid t$ where t is the trace of E. The supersingular elliptic curves in Theorem 2.3.(ii) and (iii) are defined over finite fields of characteristic 2 and 3 (see the proof of Theorem 2.3) and there are faster algorithms for *discrete logarithm problem* in fields of small characteristics. For instance, the record for discrete logarithms in fields of characteristic two is in the field $\mathbb{F}_{2^{613}}$ whereas the record for fields of large characteristic is in the field $\mathbb{F}_q$ where $q \approx 2^{448}$ (see [**16**], [**21**], [**32**], [**28**]). We should note that even though these attacks are applicable in finite field groups, elliptic curve groups may still suffer from these attacks since if $E/\mathbb{F}_q$ is an elliptic curve then the group $E(\mathbb{F}_q)$ can be embedded into the multiplicative group of $\mathbb{F}_{q^k}$ for some k via the MOV-*reduction* and FR-*reduction* [**23**], [**11**]. The security of supersingular elliptic curves defined over a finite field $\mathbb{F}_{q_3}$ of characteristic three (with $k = 6$), and the security of ordinary elliptic curves defined over a finite field $\mathbb{F}_{q_p}$ of characteristic p (with $k = 6$) is compared by Page, Smart, and Vercauteren [**28**]. They conclude that $q_3 \approx q_p^{1.7}$ must be satisfied in order to get the same level of security. Moreover, supersingular curves defined over fields of characteristic 3 are compared to ordinary curves [**28**] in terms of efficiency and they are shown to be less efficient in the verification algorithm in BLS signatures [**6**], and in Boneh-Franklin [**7**] encryption. Therefore, we will focus on ordinary elliptic curves because of efficiency and security reasons.

Now, let $\#E(\mathbb{F}_q) = n = hr$ where r is a large prime factor of n and $\gcd(q, r) = 1$. As discussed above, $\mathbb{F}_q(\mu_r) = \mathbb{F}_{q^k}$ where k is the least positive integer satisfying $q^k \equiv 1 \pmod{r}$. The integer k is called the *embedding degree* of E. The elliptic curves with embedding degree $k = 3, 4, 6$ are characterized by Miyaji, Nakabayashi and Takano [**24**]. The authors give the parametrization of such curves in terms of their group orders and traces. The main theorem is given below. The proof we provide here is a combination of proofs given by Miyaji, Nakabayashi and Takano [**24**], and by Menezes [**22**]. It uses the following lemma by Menezes [**22**] .

LEMMA 2.2 ([**22**], Lemma 6.3). *Let n be a prime and let q be an integer such that $n \mid \phi_k(q)$ and $n \nmid k$. Then $n \nmid q^d - 1$ for each $1 \leq d \leq k-1$.*

PROOF. We should first note that in the original statement of this lemma q is taken to be prime. The proof given by Menezes [**22**] also applies to the case when q is an integer as follows:

Let $f(X) = X^k - 1$ and $\mathbb{F}$ be the field of integers modulo n. Note that q is a root of $f(X)$ over $\mathbb{F}$ and also $f(X) = X^k - 1 = \prod_{d|k} \phi_d(X)$ (Theorem 2.45(i), [**17**]). Now, since $n \nmid k$ we have $\gcd(f(X), f'(X)) = 1$ in $\mathbb{F}[X]$ and so $f(X)$ does not have any repeated roots in $\mathbb{F}[X]$. Hence, $n \nmid q^d - 1$ for each d such that $d < k$ and $d \mid k$. Also, $n \nmid q^d - 1$ for $d \in [1, k-1]$ and $d \nmid k$ since otherwise we would have $n \mid q^e - 1$ where $e = \gcd(d, k)$ which is a contradiction as $e \mid k$. □

Theorem 2.3 ([**24**]). *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.*
(i) Suppose $q > 64$. Then $k = 3$ if and only if $q = 12l^2 - 1$ and $t = -1 \pm 6l$ for some $l \in \mathbb{Z}$.
(ii) Suppose $q > 36$. Then $k = 4$ if and only if $q = l^2 + l + 1$ and $t = -l, l + 1$ for some $l \in \mathbb{Z}$.
(iii) Suppose $q > 64$. Then $k = 6$ if and only if $q = 4l^2 + 1$ and $t = 1 \pm 2l$ for some $l \in \mathbb{Z}$.

Proof. (i) Let $q = 12l^2 - 1$ and $t = -1 \pm 6l$. Then $n = q + 1 - t = 12l^2 \mp 6l + 1$ and $q \equiv -1 \pm 6l \pmod{n}$. Since

$$\begin{aligned} q^3 - 1 &= (q-1)(q^2 + q + 1) \\ &\equiv (q-1)((-2 \pm 6l)^2 + (-2 \pm 6l) + 1) \pmod{n} \\ &\equiv 3(q-1)(12l^2 \mp 6l + 1) \pmod{n} \\ &\equiv 0 \pmod{n}, \end{aligned}$$

we get $k \leq 3$. Now, using Lemma 2.2 we conclude that $k = 3$.

Conversely, suppose that $k = 3$. Then, $n \mid q^3 - 1$ and also $n \nmid q - 1$ since $k \neq 1$. Therefore, $n \mid q^2 + q + 1$ and we can write for some integer λ that

$$q^2 + q + 1 = \lambda n. \tag{2.2}$$

Rewriting $q^2 + q + 1 = (q+1)^2 - t^2 + t^2 - q$ in the above equation and using $q + 1 - t = n$, we get

$$\begin{aligned} q - t^2 &= (q+1)^2 - t^2 - \lambda n \\ &= (q + 1 - t)(q + 1 + t) - \lambda n \\ &= n(q + 1 + t - \lambda), \end{aligned} \tag{2.3}$$

and dividing both sides by q results in

$$1 - \frac{t^2}{q} = \frac{n}{q}(q + 1 + t - \lambda). \tag{2.4}$$

By Hasse's Theorem, t satisfies $|t| \leq 2\sqrt{q}$, that is,

$$-3 \leq 1 - \frac{t^2}{q} \leq 1. \tag{2.5}$$

Also, the assumption $q > 64$ in Hasse's Theorem $\frac{(\sqrt{q}-1)^2}{q} < \frac{n}{q} < \frac{(\sqrt{q}+1)^2}{q}$ implies that

$$\frac{49}{64} < \frac{n}{q} < \frac{81}{64}. \tag{2.6}$$

Now, combining (2.4), (2.5) and (2.6) gives that $q + 1 + t - \lambda \in \{-3, -2, -1, 0, 1\}$. We analyse these 5 possibilities. For this, we first rewrite (2.3) as

$$q - t^2 = (q + 1 - t)(q + 1 + t - \lambda) \tag{2.7}$$

Case 1. $q+1+t-\lambda \in \{-3,-1,1\}$:
If $q+1+t-\lambda=-3$ then $t^2+3t-(4q+3)=0$ by (2.7). But, reducing this equation modulo 2 gives that $t^2+t+1 \equiv 0 \pmod 2$, a contradiction. Similarly, the cases $q+1+t-\lambda=-1,1$ give the same contradiction.

Case 2. $q+1+t-\lambda=0$:
By substituting $q+1+t-\lambda=0$ in (2.7) we get $t^2=q$, that is $t=\pm\sqrt{q}$ for $q=p^r$ for some prime p and even integer r. In this case, E is a supersingular elliptic curve.

Case 3. $q+1+t-\lambda=-2$:
By substituting $q+1+t-\lambda=-2$ in (2.7) we get $t^2+2t-(3q+2)=0$. The roots of this equation are given by $t=-1\pm\sqrt{3(q+1)}$. In order to have integer solutions for t we need that q satisfies the relation $q=12l^2-1$ which completes the proof of (i).

(ii) Let $q=l^2+l+1$ and $t=-l,l+1$. Then $n=q+1-t=l^2+2l+2$ if $t=-l$ and $n=q+1-t=l^2+1$ if $t=l+1$. Suppose $t=-l$ and so $q\equiv(-l-1) \pmod n$. Since

$$\begin{aligned} q^4-1 &= (q^2-1)(q^2+1) \\ &\equiv (q^2-1)((-l-1)^2+1) \pmod n \\ &\equiv (q^2-1)(l^2+2l+2) \pmod n \\ &\equiv 0 \pmod n, \end{aligned}$$

we get $k\le 4$. Now, using Lemma 2.2 we conclude that $k=4$. Similarly, $t=l+1$ gives $k=4$.

Now, suppose that $k=4$. Then, $n \mid q^4-1$ and also $n\nmid q^2-1$ since $k\neq 1,2$. Therefore, $n\mid q^2+1$ and we can write for some integer λ that

$$q^2+1=\lambda n. \tag{2.8}$$

Similarly as in the proof of (i), rewriting $q^2+q+1=(q+1)^2-t^2+t^2-q$ in the above equation and using $q+1-t=n$, we get

$$2q-t^2=n(q+1+t-\lambda), \tag{2.9}$$

and dividing both sides by q results in

$$2-\frac{t^2}{q}=\frac{n}{q}(q+1+t-\lambda). \tag{2.10}$$

In the same way as in the proof of (i), using $|t|\le 2\sqrt{q}$ and $\frac{(\sqrt{q}-1)^2}{q}<\frac{n}{q}<\frac{(\sqrt{q}+1)^2}{q}$ with $q>36$ we get $q+1+t-\lambda\in\{-2,-1,0,1,2\}$. We first rewrite (2.9) as

$$2q-t^2=(q+1-t)(q+1+t-\lambda), \tag{2.11}$$

Case 1. $q+1+t-\lambda\in\{-2,-1,2\}$:
If $q+1+t-\lambda=-2$ then t must satisfy $t^2+2t-(4q+2)=0$ by (2.11). The roots of this equation are given by $t=-1\pm\sqrt{4q+3}$. However, for any integer m we have $m^2\equiv 0,1 \pmod 4$. Hence, there are no integer solutions for t. If $q+1+t-\lambda=-1$ then t must satisfy $t^2+2t-(3q+1)=0$. The roots of this equation are given by $t=\frac{-1\pm\sqrt{12q+5}}{2}$. However, for any integer m we have $m^2\equiv 0,1,4,9 \pmod{12}$. Again, there are no integer solutions for t. If $q+1+t-\lambda=2$ then we get $t^2-2t+2=0$ for which there are no integer solutions.

Case 2. $q+1+t-\lambda=0$:
By (2.11), t must satisfy $t^2=2q$, that is $t=\pm\sqrt{2p^r}$ for $p=2$ and an odd integer r. In this case, E is a supersingular elliptic curve.

Case 3. $q+1+t-\lambda=1$:
By substituting $q+1+t-\lambda=1$ in (2.11) we get $t^2-t-(q-1)=0$. The roots of this equation are given by $t=\frac{1\pm\sqrt{4q-3}}{2}$. In order to have integer solutions for t we let $4q-3=m^2$ for some odd integer m, say $m=2l+1$. Then we get $q=l^2+l+1$ and $t=-l,l+1$, as required.

(iii) Let $q=4l^2+1$ and $t=1\pm 2l$. Then $n=q+1-t=4l^2\mp 2l+1$ and so $q\equiv \pm 2l \pmod{n}$. Since

$$\begin{aligned} q^6-1 &= (q^3-1)(q+1)(q^2-q+1) \\ &\equiv (q^3-1)(q+1)(4l^2\mp 2l+1) \pmod{n} \\ &\equiv 0 \pmod{n}, \end{aligned}$$

we get $k\leq 6$. Now, using Lemma 2.2 we conclude that $k=6$.

Now, suppose that $k=6$. Then, $n\mid q^6-1$ and $n\nmid q^3-1$ since $k\neq 3$. Moreover, $n\nmid q+1$ since otherwise we would have $n\mid q^2-1$ and $k\leq 2$. Therefore, $n\mid q^2-q+1$ and we can write for some integer λ that

$$q^2-q+1=\lambda n. \tag{2.12}$$

As in the proof of (i), replacing $q^2+q+1=(q+1)^2-t^2+t^2-q$ in the above equation and using $q+1-t=n$, we get

$$3q-t^2=n(q+1+t-\lambda). \tag{2.13}$$

Since $q>64$, similarly as in the proof of (i), we are left with cases $q+1+t-\lambda\in\{-1,0,1,2,3\}$. Before analyzing these 5 possibilities we rewrite (2.13) as

$$3q-t^2=n(q+1+t-\lambda). \tag{2.14}$$

Case 1. $q+1+t-\lambda\in\{-1,1,3\}$:
Reducing (2.14) modulo 2 gives $t^2+t+1\equiv 0 \pmod{2}$, contradiction.

Case 2. $q+1+t-\lambda=0$:
By (2.14), t must satisfy $t^2=3q$, that is $t=\pm\sqrt{3p^r}$ for $p=3$ and an odd integer r. In this case, E is a supersingular elliptic curve.

Case 3. $q+1+t-\lambda=2$:
By substituting $q+1+t-\lambda=2$ in (2.14) we get $t^2-2t-(q-2)=0$. The roots of this equation are given by $t=1\pm\sqrt{q-1}$. In order to have integer solutions for t we let $q-1=m^2$ for some even integer m, say $m=2l$. Then we get $q=4l^2+1$ and $t=1\pm 2l$, as required. □

1. Constructing elliptic curves with embedding degree $k = 3, 4$ or 6

The prime order ordinary elliptic curves with embedding degree $k = 3, 4$, and 6 are completely classified by Theorem 2.3. For practical applications, the next step is to construct such curves. One way of constructing an elliptic curve $E/\mathbb{F}_q$ with trace t is the *complex multiplication (CM)* method. In this method, given q and t one writes the following *CM equation*

$$4q - t^2 = DV^2 \tag{2.15}$$

where D is the square free part of $4q - t^2$. Then any root of the *Hilbert class polynomial* $H_{-D}(x)$ modulo q gives rise to an elliptic curve $E/\mathbb{F}_q$ which has *complex multiplication* in $\mathbb{Q}(\sqrt{-D})$, and $\#E(\mathbb{F}_q) = q + 1 - t$. The CM method is efficient only for small values of D; in practice, we are restricted to $D \leq 10^{10}$ [**9**]. We refer the reader Chapter 6 and [**3**] for more details on the CM method.

Our ultimate aim is to construct ordinary elliptic curves, $E/\mathbb{F}_q$, with embedding degree $k = 3, 4$ and 6. In cryptographic applications it is desirable for q and n to be prime and also $\log n \approx \log q \approx 160$ for efficiency and security reasons. Note that if one chooses q and t first then the square-free part of $4q - t^2$ is of the order of the magnitude of q. However, handling discriminants of the size $D \approx q \approx 2^{160}$ is simply impossible given today's algorithmic knowledge and computer technology. But if we choose D first then it is almost impossible to solve for q, t, V when simply working with (2.15). Therefore, we need to find a way to keep D under control, or to fix D first, and still be able to find q, t, V. For this reason, following the approach of Miyaji, Nakabayashi and Takano [**24**], we manipulate the CM equations for elliptic curves with embedding degree $k = 3, 4$ and 6.

1.1. CM equation for $k = 3$.

By Theorem 2.3, if E is an ordinary elliptic curve defined over a finite field $\mathbb{F}_q$, q is prime, and $n = \#E(\mathbb{F}_q)$ is prime then E has an embedding degree $k = 3$ if and only if $q = 12l^2 - 1$, and $t = -1 \pm 6l$ for some $l \in \mathbb{Z}$. Note that $t = -1 \pm 6l$ gives $n = q + 1 - t = 12l^2 \mp 6l + 1$.

Case 1. $q = 12l^2 - 1$, $t = -1 + 6l$, $n = 12l^2 - 6l + 1$.
In this case, the CM equation can be written as

$$\begin{aligned} 4q - t^2 = D'V^2 \;\; &\Leftrightarrow \;\; 12l^2 + 12l - 5 = D'V^2 \\ &\Leftrightarrow \;\; (6l + 3)^2 - 3D'V^2 = 24. \end{aligned} \tag{2.16}$$

Case 2. $q = 12l^2 - 1$, $t = -1 - 6l$, $n = 12l^2 + 6l + 1$.
In this case, the CM equation can be written as

$$\begin{aligned} 4q - t^2 = D'V^2 \;\; &\Leftrightarrow \;\; 12l^2 - 12l - 5 = D'V^2 \\ &\Leftrightarrow \;\; (6l - 3)^2 - 3D'V^2 = 24. \end{aligned} \tag{2.17}$$

The above discussion shows that in order to construct an elliptic curve of prime order with embedding degree $k = 3$ we have to find some special pair of solutions to the following Pell equation (see Chapter 3)

$$X^2 - DY^2 = 24, \qquad D > 0, \qquad D \equiv 0 \pmod 3). \tag{2.18}$$

If (x, y) is a solution to (2.18) we have to guarantee that $x \equiv 3 \pmod 6$ and that for $l = (x \pm 3)/6$ we must have $q = 12l^2 - 1$ and $n = 12l^2 \pm 6l + 1$ are primes.

1.2. CM equation for $k = 4$. By Theorem 2.3, if E is an ordinary elliptic curve defined over a finite field $\mathbb{F}_q$, q is prime, and $n = \#E(\mathbb{F}_q)$ is prime then E has an embedding degree $k = 4$ if and only if $q = l^2 + l + 1$, and $t = -l, l + 1$ for some $l \in \mathbb{Z}$. Note that $t = -l$ gives $n = q+1-t = l^2+2l+2$ and $t = l+1$ gives $n = q+1-t = l^2+1$.

Case 1. $q = l^2 + l + 1$, $t = -l$, $n = l^2 + 2l + 2$.
First note that the primality of n requires that $l \equiv 1 \pmod 2$. Therefore, we can replace l by $2l' - 1$ and this gives the parametrization as $q = 4l'^2 - 2l' + 1$, $t = 1 - 2l'$, $n = 4l'^2 + 1$. Now, the CM equation can be written as

$$\begin{aligned} 4q - t^2 = D'V^2 \quad &\Leftrightarrow \quad 12l'^2 - 4l' + 3 = D'V^2 \\ &\Leftrightarrow \quad (6l' - 1)^2 - 3D'V^2 = -8. \end{aligned} \tag{2.19}$$

Finally, since q is prime we must have $l' \not\equiv 1 \pmod 3$.

Case 2. $q = l^2 + l + 1$, $t = l + 1$, $n = l^2 + 1$.
Similarly as in first case, we can replace l by $2l'$ since n is prime and so l is even. Then, the new parametrization is $q = 4l'^2 + 2l' + 1$, $t = 1 + 2l'$, $n = 4l'^2 + 1$, and the CM equation can be written as

$$\begin{aligned} 4q - t^2 = D'V^2 \quad &\Leftrightarrow \quad 12l'^2 + 4l' + 3 = D'V^2 \\ &\Leftrightarrow \quad (6l' + 1)^2 - 3D'V^2 = -8. \end{aligned} \tag{2.20}$$

Similarly as above, the primality of q requires $l' \not\equiv 2 \pmod 3$.

The above discussion shows that in order to construct an elliptic curve of prime order with embedding degree $k = 4$ we have to find some special pair of solutions to the following Pell equation

$$X^2 - DY^2 = -8, \qquad D > 0, \qquad D \equiv 0 \pmod 3. \tag{2.21}$$

If (x, y) is a solution to (2.21) we have to guarantee that $x \equiv \mp 1 \pmod 6$ and that for $l' = (x \pm 1)/6$ we must have $n = 4l'^2 + 1$ and $q = 4l'^2 \mp 2l' + 1$ are primes.

1.3. CM equation for $k = 6$. By Theorem 2.3, if E is an ordinary elliptic curve defined over a finite field $\mathbb{F}_q$, q is prime, and $n = \#E(\mathbb{F}_q)$ is prime then E has an embedding degree $k = 6$ if and only if $q = 4l^2 + 1$, and $t = 1 \pm 2l$ for some $l \in \mathbb{Z}$. Recall that $t = 1 \pm 2l$ gives $n = q + 1 - t = 4l^2 \mp 2l + 1$.

Case 1. $q = 4l^2 + 1$, $t = 1 + 2l$, $n = 4l^2 - 2l + 1$.
In this case, the CM equation can be written as

$$\begin{aligned} 4q - t^2 = D'V^2 \quad &\Leftrightarrow \quad 12l^2 - 4l + 3 = D'V^2 \\ &\Leftrightarrow \quad (6l - 1)^2 - 3D'V^2 = -8. \end{aligned} \tag{2.22}$$

Also note that if $l \equiv 1 \pmod 3$ then $n \equiv 0 \pmod 3$. Therefore, in order to obtain n prime the restriction $l \not\equiv 1 \pmod 3$ is required.

Case 2. $q = 4l^2 + 1$, $t = 1 - 2l$, $n = 4l^2 + 2l + 1$.
In this case, the CM equation can be written as

$$4q - t^2 = D'V^2 \quad \Leftrightarrow \quad 12l^2 + 4l + 3 = D'V^2 \qquad (2.23)$$
$$\Leftrightarrow \quad (6l + 1)^2 - 3D'V^2 = -8.$$

Similarly as above, the primality of n requires $l \not\equiv 2 \pmod 3$.

The above discussion shows that in order to construct an elliptic curve of prime order with embedding degree $k = 6$ we have to find some special pair of solutions to the following Pell equation

$$X^2 - DY^2 = -8, \qquad D > 0, \qquad D \equiv 0 \pmod 3. \qquad (2.24)$$

If (x, y) is a solution to (2.24) then we have to guarantee that $x \equiv -1 \pmod 6$ or $x \equiv 1 \pmod 6$. In the former case, setting $l = (x + 1)/6$, we must have

$$q = 4l^2 + 1 \text{ is prime, and } n = 4l^2 - 2l + 1 \text{ is prime.} \qquad (2.25)$$

In the latter case, setting $l = (x - 1)/6$, we must have

$$q = 4l^2 + 1 \text{ is prime, and } n = 4l^2 + 2l + 1 \text{ is prime.} \qquad (2.26)$$

Remark 2.1. By equations (2.22) and (2.23) it is clear that D in (2.24) must be odd.

The following proposition is new.

Proposition 2.4. *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 Theorem 2.1, we have $t^2 \leq 4q$. Now,

$$t^2 \leq 4q \quad \Leftrightarrow \quad t^2 \leq 4(t - 1 + n)$$
$$\Leftrightarrow \quad (t - 2)^2 \leq 4n. \qquad (2.27)$$

Now, let $n' = q$, $q' = n$, and $t' = q' + 1 - n' = (2 - t)$. By (2.27), t' satisfies the Hasse bound with $q' = n$ so that $E_4/\mathbb{F}_n$ with $\#E_4(F_n) = q$ is well defined. The fact that the corresponding embedding degree $k' = 4$ follows easily from the above derivation of CM equations for $k = 4$ and $k = 6$. The converse part can be proved similarly. □

2. Scarcity of MNT curves

Now, suppose that $E/\mathbb{F}_q$ is an elliptic curve with embedding degree k and $\#E(\mathbb{F}_q) = n = hr = q + 1 - t$ where r is a large prime factor of n. By Theorem 2.1, t must satisfy $|t| \leq 2\sqrt{q}$. Also, it follows from Lemma 2.2 that $r \mid \phi_k(q)$. Luca and Shparlinski [**18**] define $Q_k(x, y, z)$ as the number of prime powers $q \leq x$ for which there exist a prime $r \geq y$ and an integer t satisfying

$$|t| \leq 2\sqrt{q}, \; r \mid q + 1 - t, \; r \mid \phi_k(q),$$

and (2.15) has a solution (D, V) where D is positive, square-free and $D \leq z$. Luca and Shparlinski, in 2005, proved an upper bound for $Q_k(x, y, z)$:

THEOREM 2.5 (Theorem 1, [**18**]). *For any fixed integer k and positive real numbers x, y, and z the following bound holds:*

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

as $x \to \infty$.

Then, in 2006 [**19**], the same authors improved the upper bound in Theorem 2.5 as follows:

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

where $\phi(k)$ is the Euler totient function. Also, based on the results about the distribution of square free integers, and the number of primes in an interval, they gave a heuristic lower bound for $Q_k(x, y, z)$ provided that $y \geq x^{1/2}$ [**19**]:

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

In Theorem 2.5, let $y = x^\alpha$ for some positive real number α and let k be fixed. Also, let $z = O(1)$ since the CM method is only effective for small values of D. Then the number of possible fields $\mathbb{F}_q$ such that $q \leq x$ and $E/\mathbb{F}_q$ with embedding degree k is constructable can be bounded above by $x^{3/2+o(1)-\alpha}$ for large enough x. By the prime number theorem the number of all finite fields $\mathbb{F}_q$ with $q \leq x$ is more than $x/\log x$. So, the density of suitable fields is less than $\frac{x^{3/2+o(1)-\alpha}}{x/\log x} = x^{1/2-\alpha+o(1)} \log x$. In particular, if $y > x^{1/2}$ (that is, $\alpha > 1/2$) then the density goes to zero as $x \to \infty$. Hence, this shows that elliptic curves with a fixed embedding degree k, and with $\rho = \log_2 n / \log_2 r < 2$ are scarce.

Moreover, Luca and Shparlinski [**18**] show that the number of possible constructable prime order elliptic curves given that D has to be bounded with embedding degree $k = 3, 4$ or 6 is bounded above by an absolute constant. For instance, the construction of $E/\mathbb{F}_q$ with $k = 6$ reduces to finding some suitable solutions of (2.24). As we will see in Chapter 3, an infinite class of solutions of (2.24), say (x_j, y_j), can be obtained from a *minimal* solution (x, y) of (2.24). In fact, all solutions can be obtained in this way by using all minimal solutions. However, (x_j, y_j) and D will have to satisfy some extra conditions because of the parametrization of E, $(q(l), t(l))$. Also, the solutions (x_j, y_j) grow exponentially. Combining these facts with heuristic arguments, Luca and Shparlinski define $N(D')$ as the expected total number of prime powers among the numbers of $q_j(l)$ satisfying the additional condition that $n_j(l)$ is also a prime, and they show that

$$N(D') \ll \frac{1}{(\log D')^2}. \tag{2.28}$$

Then they define $E(z)$ as the expected total number of isogeny classes of MNT curves with $k = 6$ and $D' \leq z$, and conclude that

$$E(z) = \sum_{\substack{D' \leq z \\ D' \text{square-free}}} N(D') \ll \sum_{D' \leq z} \frac{1}{(\log D')^2} \ll \frac{z}{(\log z)^2}\ . \tag{2.29}$$

Also, assuming a widely believed conjecture about the size of a *regulator* of a quadratic field holds, Luca and Shparlinski provide a better upper bound for $E(z)$ [**18**]:

$$E(z) \leq z^{1/2+o(1)}. \tag{2.30}$$

We will come back to these bounds in Chapters 4, 5 and compare them with our experimental results.

CHAPTER 3

Continued fractions and Pell-type equations

In this chapter, some background on continued fractions and Pell equations is given. We use Mollin's book [**25**] as our guide. Before proceeding we shall give some preliminaries on quadratic number fields.

Let D be a nonzero square free integer. The *quadratic field* $\mathbb{Q}(\sqrt{D})$ is obtained by adjoining the element $\sqrt{D}$ to $\mathbb{Q}$. If $D > 0$ $(D < 0)$ then $\mathbb{Q}(\sqrt{D})$ is called a *real* (*imaginary*) quadratic field. The elements in $\mathbb{Q}(\sqrt{D})$ are represented by $a+b\sqrt{D}$ where $a, b \in \mathbb{Q}$. Clearly, $\mathbb{Q}(\sqrt{D})$ is a subfield of the complex numbers $\mathbb{C}$. By definition, a complex number is an *algebraic integer* if it is a root of some monic polynomial with coefficients in $\mathbb{Z}$. The set of algebraic integers forms a ring in $\mathbb{C}$, and denoted by $\mathbb{A}$. Then $\mathbb{A} \cap \mathbb{Q}(\sqrt{D})$ is the ring of algebraic integers in $\mathbb{Q}(\sqrt{D})$, and denoted by R.

Theorem 3.1 ([**20**], Corollary 2, p.15). *Let D be a square free integer. The set of algebraic integers in the quadratic field $Q(\sqrt{D})$ is*

$$\{a+b\sqrt{D} : \ a, b \in \mathbb{Z}\} \quad \textit{if } D \equiv 2,\ 3 \pmod 4,$$

$$\{\frac{a+b\sqrt{D}}{2} : \ a, b \in \mathbb{Z},\ a \equiv b \pmod 2\} \quad \textit{if } D \equiv 1 \pmod 4.$$

Let $\alpha = a+b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$. The *norm* map $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{C}$ is defined as $N(a+b\sqrt{D}) = a^2 - Db^2$ and it is easy to check that N is multiplicative. The norm of an element is denoted by $\|\alpha\|$. It is known that α is an algebraic integer if and only if $2a$ and $\|\alpha\|$ are integers. A *unit* in R is an element u such that there exists an element $v \in R$ with $uv = 1$. The set of units is a group under multiplication, and denoted by R^*. The units in R are the elements with norm ± 1.

An *ideal* in R is an additive subgroup $I \subset R$ such that $ra \in I$ for every $r \in R, a \in I$. An ideal $I \subset R$ is called a *principal ideal* if there exists $\alpha \in R$ such that $I = \alpha R = \{\alpha r : r \in R\}$, and denoted by (α). An ideal $P \subset R$ is called *prime ideal* if $\alpha, \beta \in R$ and $\alpha\beta \in P$ implies $\alpha \in P$ or $\beta \in P$. The ideals in R factor uniquely into prime ideals ([**20**], Corollary, p.60). Now, let p be a prime in $\mathbb{Z}$ and $\mathbb{Q}(\sqrt{D}), R$ be as above. Then the factorization of the principal ideal pR in R is given in the following theorem:

Theorem 3.2 ([**20**], Theorem 25, p.74). *If $p \mid D$, then $pR = (p, \sqrt{D})^2$.*

If D is odd, then

$$2R = \begin{cases} (2, 1+\sqrt{D})^2 & \textit{if } D \equiv 3 \pmod 4 \\ (2, \frac{1+\sqrt{D}}{2})(2, \frac{1-\sqrt{D}}{2}) & \textit{if } D \equiv 1 \pmod 8 \\ \textit{prime} & \textit{if } D \equiv 5 \pmod 8. \end{cases}$$

If D is odd, $p \nmid D$, then

$$pR = \begin{cases} (p, m+\sqrt{D})(p, m-\sqrt{D}) & \text{if } D \equiv m^2 \pmod{p} \\ \text{prime} & \text{if } D \text{ is not a square mod } p. \end{cases}$$

1. Continued Fractions

Let $\alpha \in \mathbb{R}$. A *continued fraction* is an expression of the form

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_{l-1} + \cfrac{1}{q_l} \ddots}}}$$

and where $q_0 = \lfloor \alpha \rfloor$, $q_i \in \mathbb{R}^+$ for $i > 0$. If the fraction terminates after some finite terms, say at q_l, then it is called a *finite continued fraction of length l* and denoted by $\langle q_0; q_1, \ldots, q_l \rangle$. Otherwise, it is an *infinite continued fraction* and denoted by $\langle q_0; q_1, \ldots, q_l, \ldots \rangle$. A continued fraction is called *simple* if $q_i \in \mathbb{Z}$ for all $i \geq 0$. An infinite simple continued fraction is called *periodic* if there exist integers $k \geq 0$ and $l \in \mathbb{N}$ such that $q_n = q_{n+l}$ for all integers $n \geq k$. A periodic continued fraction is denoted by

$$\alpha = \langle q_0; q_1, \ldots, q_{k-1}, \overline{q_k, q_{k+1}, \cdots q_{k+l-1}} \rangle.$$

The *period* of α is the smallest $l = l(\alpha)$ with the above property. Finally, if α has a continued fraction expansion $\alpha = \langle q_0; q_1, \ldots, q_l, \ldots \rangle$, then $C_k = \langle q_0; q_1, \ldots, q_k \rangle$ is defined to be the k^{th} convergent of α.

It is known that $\alpha \in \mathbb{Q}$ if and only if α can be written as a finite simple continued fraction. In particular we have a recursive formula for determining any convergent of α, given by the following theorem:

Theorem 3.3 ([**25**], Theorem 5.1.2). *Let $\alpha = \langle q_0; q_1, \ldots, q_l \rangle$ for $l \in \mathbb{N}$ be a finite continued fraction expansion. Define two sequences for an integer $k \geq 0$:*

$$A_{-2} = 0, A_{-1} = 1, A_k = q_k A_{k-1} + A_{k-2},$$

and

$$B_{-2} = 1, B_{-1} = 0, B_k = q_k B_{k-1} + B_{k-2}.$$

Then

$$C_k = A_k / B_k = \frac{q_k A_{k-1} + A_{k-2}}{q_k B_{k-1} + B_{k-2}}$$

is the k^{th} convergent of α.

Similarly, α is an irrational number if and only if it has an infinite simple continued fraction expansion. And, there is a special subset of irrational numbers which are equivalent to having a periodic infinite simple continued fraction expansion. These irrational numbers are called *quadratic irrationals* and defined as follows:

$$\alpha = \frac{P + \sqrt{D}}{Q}$$

where $D \in \mathbb{N}$, D is not a perfect square, $P, Q \in \mathbb{Z}, Q \neq 0$ and $P^2 \equiv D (\text{mod } Q)$ for a suitable choice of a triple (P, Q, D). The continued fraction expansion of a quadratic irrational $\alpha = \frac{P+\sqrt{D}}{Q} = \langle q_0; q_1, \dots, q_k, \dots \rangle$ can be determined by the following recursive relations:

$$\begin{aligned} P_0 &= P, Q_0 = Q, \\ q_k &= \left\lfloor \frac{P_k + \sqrt{D}}{Q_k} \right\rfloor, \\ P_{k+1} &= q_k Q_k - P_k, \\ Q_{k+1} &= \frac{D - P_{k+1}^2}{Q_k}. \end{aligned}$$

Also, the *algebraic conjugate* of α is defined by $\alpha' = \frac{P-\sqrt{D}}{Q}$.

Finally, the integer G_{k-1} for $k \geq -1$ is defined by

$$G_{k-1} = Q_0 A_{k-1} - P_0 B_{k-1} \tag{3.1}$$

where A_{k-1}, B_{k-1} are as in Theorem 3.3. The following relation holds for $k \geq 1$ ([**25**], Theorem 5.3.4, p.246) :

$$G_{k-1}^2 - B_{k-1}^2 D = (-1)^k Q_k Q_0. \tag{3.2}$$

2. Pell Equation

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

$$X^2 - DY^2 = m. \tag{3.3}$$

Note that finding a solution pair (x, y), $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ to (3.3) is equivalent to finding an element $(x + y\sqrt{D}) \in \mathbb{Q}(\sqrt{D})$ with norm m and $x, y \in \mathbb{Z}$. For instance, the set of all integer solutions of

$$X^2 - DY^2 = 1 \tag{3.4}$$

is contained in the set of units of the field $\mathbb{Q}(\sqrt{D})$. Therefore, we use both (x, y) and $(x + y\sqrt{D})$ to refer to a solution of (3.3).

Now, let $\alpha = x + y\sqrt{D}$ be a solution to (3.3). 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 (3.4) such that $\alpha_1 = \beta\alpha_2$. If α_1 and $\alpha_1' = x_1 - y_1\sqrt{D}$ are in the same class then the class is called *ambiguous.* If $\alpha = x+y\sqrt{D}$ is a solution of (3.3) 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 (3.3) 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. We should note that the minimal solution and the fundamental solution in the same class does not have to be the same.

We give some important facts about the solutions of Pell equations.

PROPOSITION 3.4 ([**25**], Proposition 6.2.1). *Two primitive solutions $x_j + y_j\sqrt{D}$ for $j = 1, 2$ of $X^2 - DY^2 = m$ are in the same class if and only if both*

$$(x_1x_2 - y_1y_2D)/m \in \mathbb{Z} \quad \text{and} \quad (y_1x_2 - x_1y_2)/m \in \mathbb{Z}. \tag{3.5}$$

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

THEOREM 3.5 ([**26**], Theorem 4.2). *Let $D \in \mathbb{N}$, not a perfect square, and $m \in \mathbb{Z}$. Then*

$$x + y\sqrt{D}$$

is a primitive solution of

$$X^2 - DY^2 = m$$

if and only if all of the following hold:

(a) There exists an integer P_0 defined by

$$P_0 + \sqrt{D} = (x + y\sqrt{D})(x_1 + y_1\sqrt{D}),$$

for some unique element $x_1 + y_1\sqrt{D}$ with $-|m|/2 < P_0 \leq |m|/2$.

(b) In the simple continued fraction expansion of $\alpha = (P_0 + \sqrt{D})/m$, there is a nonnegative integer t such that $Q_t = 1$. And, in the simple continued fraction expansion of $-\alpha'$, there is a nonnegative integer t' such that $Q_{t'} = 1$.

(c) There exists a nonnegative integer z such that $lz + t - 1$ is odd where $l = l(\alpha)$, $x_0 = G_{lz+t-1}$, and $y_0 = B_{lz+t-1}$. And, there exists a nonnegative integer z' such that $lz' + t' - 1$ is odd where $l = l(\alpha) = l(-\alpha')$, $x_0 = G_{lz'+t'-1}$, and $y_0 = B_{lz'+t'-1}$.

REMARK 3.1. The uniqueness of the element $x_1 + y_1\sqrt{D}$ in part (a) follows from the restriction $-|m|/2 < P_0 \leq |m|/2$. Since $x + y\sqrt{D}$ is a primitive solution we have $\gcd(x, y) = 1$ and so there exist integers r, s such that $xr + ys = 1$. Now, setting $x_1 = s - tx$ and $y_1 = r + ty$ for $t \in \mathbb{Z}$ gives that

$$\begin{aligned}(x + y\sqrt{D})(x_1 + y_1\sqrt{D}) &= (xx_1 + yy_1D) + (xy_1 + yx_1)\sqrt{D} \\ &= xs + yrD - t(x^2 - y^2D) + (xr + ys)\sqrt{D} \\ &= (xs + yrD - tm) + \sqrt{D}.\end{aligned}$$

Hence, restricting $-|m|/2 < P_0 \leq |m|/2$ fixes the value of t and determines $x_1 + y_1\sqrt{D}$ uniquely.

Remark 3.2 ([**25**], Theorem 4.2-(4)). Let $\alpha = x + y\sqrt{D}$ and P_0 be as in Theorem 3.5. Let $\beta = a + b\sqrt{D}$ be in the same class as α. Then, by Proposition 3.4, we have

$$\begin{aligned} xa - ybD &= mU, \\ ya - xb &= mT \end{aligned}$$

for some integers U, V. This implies

$$\begin{aligned} x &= aU + bDT, \\ y &= aT + bU. \end{aligned}$$

Let $a_1 = x_1U + y_1TD$ and $b_1 = y_1U + x_1T$. Then

$$\begin{aligned} (a + b\sqrt{D})(a_1 + b_1\sqrt{D}) &= aa_1 + bb_1D + (ab_1 + a_1b)\sqrt{D} \\ &= x_1(aU + bTD) + y_1(aTD + bUD) + \\ &\quad (y_1(aU + bTD) + x_1(aT + bU))\sqrt{D} \\ &= xx_1 + yy_1D + (xy_1 + x_1y)\sqrt{D} \\ &= P_0 + \sqrt{D}. \end{aligned}$$

The last equality follows from the fact that $(x + y\sqrt{D})(x_1 + y_1\sqrt{D}) = P_0 + \sqrt{D}$. Hence, P_0 is unique in a sense that every solution $\beta = a + b\sqrt{D}$, in the same class as α, has a unique element $(a_1 + b_1\sqrt{D})$ such that $(a + b\sqrt{D})(a_1 + b_1\sqrt{D}) = P_0 + \sqrt{D}$.

As a consequence of the above remark we can give the following definition.

Definition 3.1 ([**25**], Definition 6.2.4). If α is any solution in a given class of (3.3), then α is said to belong to the unique element $-P_0$ where P_0 is determined by Theorem 3.5.

Note that Theorem 3.5 suggests an algorithm to check if there exist solutions to the equation $X^2 - DY^2 = m$. If there is a solution we can also determine the fundamental solution of each class. In fact, each possible class is represented by an element in the set

$$\mathcal{P} = \{P_0 : P_0^2 \equiv D \pmod{|m|},\ -|m|/2 < P_0 \leq |m|/2\} \tag{3.6}$$

by Theorem 3.5 (a). For each $P_0 \in \mathcal{P}$, there may or may not be solutions belonging to P_0. In order to analyze the existence of a solution belonging to the class P_0 we set $\alpha = (P_0 + \sqrt{D})/Q_0$ where $Q_0 = m$. Note that α is a quadratic irrational and it has a periodic infinite simple continued fraction expansion, say with period $l = l(\alpha)$. By Theorem 3.5 (b), we look for a nonnegative integer t such that $Q_t = 1$ in the continued fraction expansion of α. The existence of such a t and the existence of a nonnegative integer z with $lz + t - 1$ is odd guarantees that there is a solution. Now, using that α is periodic with period l, $Q_t = 1$, $lz + t$ is even, and $m = Q_0$, we can write by (3.2) that

$$\begin{aligned} G_{lz+t-1}^2 - B_{lz+t-1}^2D &= (-1)^{lz+t}Q_{lz+t}Q_0 \\ &= Q_tQ_0 \\ &= m. \end{aligned}$$

Hence, $x_0 = G_{lz+t-1}$ and $y_0 = B_{lz+t-1}$ gives a solution to $X^2 - DY^2 = m$ such that (x_0, y_0) belongs to P_0. Finally, choosing t and z as the least positive integers satisfying the above properties gives a minimal solution belonging to P_0.

The algorithm discussed above determines the minimal solutions with their corresponding P_0 values. However, in some circumstances we may not need to know the corresponding P_0 values, but only we may be interested in the list of all minimal solutions. The following algorithm is a variant of the above algorithm and, according to Robertson [**29**], it lists the minimal solutions of each class for $D > m^2$.

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
   $i \leftarrow i + 1$
   $P_i \leftarrow a_{i-1}Q_{i-1} - P_{i-1}$
   $Q_i \leftarrow (D - P_i^2)/Q_{i-1}$
   $a_i \leftarrow \lfloor(P_i + \sqrt{D})/Q_i\rfloor$
   $B_i \leftarrow a_iB_{i-1} + B_{i-2}$
   $G_i \leftarrow a_iG_{i-1} + G_{i-2}$
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
```

We shall note that the sequence $\{Q_i\}$ has the same period as the continued fraction expansion of the quadratic irrational $\alpha = \sqrt{D} = \langle a_0; a_1, \cdots, a_k, \cdots\rangle$, say l. So, the smallest integer i with $Q_i = 1$ and $i \equiv 0 \pmod 2$ has the property that either $i = l$ or $i = 2l$ since $1 = Q_0 = Q_l$.

As we noted above, Algorithm 1 finds minimal solutions when $D > m^2$. The brute-force searching algorithm can be used to find fundamental solutions when $D \leq m^2$ [**29**].

The following two lemmas are new.

LEMMA 3.6. *Let $m > 2$ be an even integer and D 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. Note that since α is a primitive solution and m is even, y must be odd. By Proposition 3.4,

$(x^2+y^2D)/m = (m+2y^2D)/m$ must be an integer. In particular, $2y^2D/m$ is an integer. But this is a contradiction since y and D are odd and $2 < m$ is even. □

Lemma 3.7. *Let $D \in \mathbb{N}$, not a perfect square, and $m \in \mathbb{Z}$ such that $gcd(D, m) = 1$. Two solutions (x, y) and (a, b) of $X^2 - DY^2 = m$ belong to the same $-P_0$ (P_0 as defined in 3.5(a)) if and only if they are in the same class.*

Proof. Suppose first that (x, y) and (a, b) belong to the same $-P_0$. By Theorem 3.5, there exist unique (x_1, y_1) and (a_1, b_1) such that

$$\begin{aligned} x_1 + y_1\sqrt{D} &= \frac{P_0+\sqrt{D}}{x+y\sqrt{D}} \\ &= \frac{P_0x + yD + (P_0y + x)\sqrt{D}}{m} \end{aligned}$$

and

$$\begin{aligned} a_1 + b_1\sqrt{D} &= \frac{P_0+\sqrt{D}}{a+b\sqrt{D}} \\ &= \frac{P_0a + bD + (P_0a + b)\sqrt{D}}{m}. \end{aligned}$$

In particular, we have

$$P_0x + yD \equiv 0 \pmod{m}, \tag{3.7}$$

$$P_0a + bD \equiv 0 \pmod{m}, \tag{3.8}$$

$$P_0y + x \equiv 0 \pmod{m}, \tag{3.9}$$

$$P_0b + a \equiv 0 \pmod{m}. \tag{3.10}$$

Now, multiplying (3.8) by x and (3.9) by $-bD$ and then adding those two together we get

$$P_0(ax - byD) \equiv 0 \pmod{m}. \tag{3.11}$$

Similarly, first multiplying (3.7) by $-b$ and (3.8) by y and then adding those two together we get

$$P_0(ay - bx) \equiv 0 \pmod{m}. \tag{3.12}$$

Note that $\gcd(P_0, m) = 1$ since $P_0^2 \equiv D \pmod{m}$ and $\gcd(D, m) = 1$. Hence, (3.11) and (3.12) give us that $(ax - byD)/m$ and $(ay - bx)/m$ are integers. In other words, (x, y) and (a, b) are in the same class by Proposition 3.4. Remark 3.2 proves the converse part of the theorem. □

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 $U^2 - DV^2 = 1$ by using Algorithm 1 with input $D$, 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
```

CHAPTER 4

The case $k = 6$: $X^2 - DY^2 = -8$

Let q and n be prime integers. Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with embedding degree $k = 6$, and $\#E(\mathbb{F}_q) = n$. It was shown in Section 2.1.3 that constructing E is reduced to finding some suitable solutions to the Pell equation

$$(4.1)\, X^2 - DY^2 = -8, \qquad D > 0, \qquad D \equiv 0 \pmod 3, \qquad D \equiv 1 \pmod 2.$$

Recall from Section 2.1 that for efficiency reasons it is essential to keep D small. Therefore, the general strategy is first fixing a small D and then tracing for suitable solutions to (4.1) using the techniques developed in Chapter 3. However, it is known that this construction method is unlikely to generate curves (see Section 2.2). In this chapter we try to find some necessary conditions on D, and also analyze the solution classes of (4.1) in order to gain some efficiency in searching for suitable elliptic curves. Then we give a searching algorithm and provide some experimental results.

Lemma 4.1. *If (x, y) is a primitive solution to (4.1), (that is gcd$(x, y) = 1$) then x and y must be odd.*

Proof. First note that if y is even then x must be even, that is (x, y) is not primitive. So, it is enough to show that the case: x is even, y is odd is not possible. Suppose to the contrary that x is even and y is odd. Then $4 \mid D$ and we get a contradiction as $D \equiv 1 \pmod 2$. $\square$

Lemma 4.2. *If (4.1) has a primitive solution then $D \equiv 1 \pmod 8$.*

Proof. Let (x, y) be a primitive solution. By Lemma 4.1, x and y must be odd. Now, reducing (4.1) modulo 8 we get $D \equiv 1 \pmod 8$. $\square$

Theorem 4.3. *Equation (4.1) either does not have any solution or it has exactly two classes of solutions. In particular, if α is a solution of (4.1) then α and α' represent the two solution classes.*

Proof. If (4.1) 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 3.6, α' is a solution belonging to $-P_0$. If these are the only two solution classes then we are done. So, we assume that there are more than two solution classes. Note that the possible values for P_0 which represent the different classes of solutions are $P_0 = \pm 1, \pm 3$ since $P_0^2 \equiv D \pmod 8$, $-4 < P_0 \leq 4$ by Theorem 3.5 and $D \equiv 1 \pmod 8$ by Lemma 4.2. Therefore, we can assume without loss of generality that $\alpha, \alpha', \beta, \beta'$ are solutions corresponding to 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, m_1, n_1 that

$$1 + \sqrt{D} = \alpha(m_1 + n_1\sqrt{D}), \tag{4.2}$$

and from which it follows that

$$1 - \sqrt{D} = \alpha'(m_1 - n_1\sqrt{D}). \tag{4.3}$$

Assume first that $D = 8m+1$ with m even and let $\alpha = x+y\sqrt{D}$. Consider the quadratic field $Q(\sqrt{D})$, and its ring of integers R. The prime ideal generated by 2 is factorized in R as follows:

$$2R = (2, \frac{1+\sqrt{D}}{2})(2, \frac{1-\sqrt{D}}{2}). \tag{4.4}$$

Note that $\alpha/2$ and $\alpha'/2$ are both algebraic integers in $Q(\sqrt{D})$ since x and y have the same parity by Lemma 4.1. Also the principal ideals generated by $\alpha/2$ and $\alpha'/2$ are prime ideals since $\|\alpha/2\| = \|\alpha'/2\| = 8/4 = 2$. We can also check that the ideals $(\frac{\alpha}{2})$ and $(\frac{\alpha'}{2})$ are coprime: Let π be a prime dividing both $\alpha/2$ and $\alpha'/2$. Then $\pi \mid \frac{\alpha}{2} + \frac{\alpha'}{2} = x$ and $\pi \mid \frac{\alpha}{2} \cdot \frac{\alpha'}{2} = -2$. Since x is an odd integer there exist integers u and v such that $ux - 2v = 1$, that is $\pi \mid 1$ in R but this is a contradiction since π is a prime, not a unit. Combining this argument with (4.2) and (4.3), it follows from the unique factorization of ideals in R that

$$\begin{aligned} 2R &= (2, \frac{1+\sqrt{D}}{2})(2, \frac{1-\sqrt{D}}{2}) \\ &= (\frac{\alpha}{2})(\frac{\alpha'}{2}) \end{aligned} \tag{4.5}$$

with $(\frac{\alpha}{2}) = (2, \frac{1+\sqrt{D}}{2})$ and $(\frac{\alpha'}{2}) = (2, \frac{1-\sqrt{D}}{2})$.

Now, we apply a similar reasoning to β and β'. Since β is a solution belonging to class $P_0 = -3$ there exist integers m_2 and n_2 such that

$$3 + \sqrt{D} = \beta(m_2 + n_2\sqrt{D}), \tag{4.6}$$

that is,

$$2 - (\frac{1-\sqrt{D}}{2}) = \frac{\beta}{2}(m_2 + n_2\sqrt{D}) \tag{4.7}$$

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

$$\frac{1-\sqrt{D}}{2} = -\frac{\beta}{2}(\frac{\beta}{2} + m_2 + n_2\sqrt{D}). \tag{4.8}$$

Therefore, the inclusion of ideals $(2, \frac{1-\sqrt{D}}{2}) \subseteq (\frac{\beta}{2})$ holds. Similarly, $(2, \frac{1+\sqrt{D}}{2}) \subseteq (\frac{\beta'}{2})$. In fact, the inclusions imply the equality of the ideals since they are all nonzero prime ideals. Hence, the below factorization holds:

$$2R = (2, \frac{1+\sqrt{D}}{2})(2, \frac{1-\sqrt{D}}{2}) = (\frac{\alpha}{2})(\frac{\alpha'}{2}) = (\frac{\beta}{2})(\frac{\beta'}{2}) \tag{4.9}$$

where

$$(2, \frac{1+\sqrt{D}}{2}) = (\frac{\alpha}{2}) = (\frac{\beta'}{2}), \tag{4.10}$$

$$(2, \frac{1-\sqrt{D}}{2}) = (\frac{\alpha'}{2}) = (\frac{\beta}{2}). \tag{4.11}$$

It follows from (4.10) that

$$1 + \sqrt{D} = \beta'(\frac{m_3 + n_3\sqrt{D}}{2}) \tag{4.12}$$

for some integers m_3, n_3 of the same parity. In fact, m_3 and n_3 must be odd since β' is a solution belonging to the class $P_0 = 3$. Also, it follows from (4.10) that

$$\alpha = \beta'(\frac{m_4 + n_4\sqrt{D}}{2}) \tag{4.13}$$

for some integers m_4, n_4 of having the same parity. In fact, m_4 and n_4 must be odd since α and β' belong to different solution classes.

Now combining (4.2), (4.12) and (4.13) together we get

$$m_3 + n_3\sqrt{D} = (m_1 + n_1\sqrt{D})(m_4 + n_4\sqrt{D}), \tag{4.14}$$

and so

$$n_3 = m_1 n_4 + m_4 n_1. \tag{4.15}$$

Recall that n_3, m_4 and n_4 are all odd integers. Hence, we have only two possibility for the parity of integers m_1 and n_1: (m_1 is even and n_1 is odd) or (m_1 is odd and n_1 is even). In both cases, the integer $m_1^2 - n_1^2 D$ is odd. Now, taking the norm of both sides of (4.2)

$$1 - D = \|\alpha\| \left\| m_1 + n_1\sqrt{D} \right\|, \tag{4.16}$$

that is,

$$m_1^2 - n_1^2 D = \left\| m_1 + n_1\sqrt{D} \right\| = m. \tag{4.17}$$

This finally gives a contradiction since m was assumed to be even.

Now, suppose $D = 8m + 1$ and m is odd. It follows from (4.11) that

$$3 + \sqrt{D} = \alpha'(\frac{m_1 + n_1\sqrt{D}}{2}) \tag{4.18}$$

for some integers m_1 and n_1 of having the same parity. In fact, m_1 and n_1 must be odd since α' is a solution belonging to class $P_0 = 1$. By (4.10) and the fact that β and α' belong to different solution classes we get

$$\beta = \alpha'(\frac{m_3 + n_3\sqrt{D}}{2}) \tag{4.19}$$

for some odd integers m_4 and n_4. Combining (4.6), (4.18), and (4.19) gives us

$$m_1 = m_2m_3 + n_2n_3D. \tag{4.20}$$

However, m_1, m_3, n_3 and D are all odd integers and so there can only be two configurations for m_2 and n_2: (m_2 is even and n_2 is odd) or (m_2 is odd and n_2 is even). In both cases, $m_2^2 - n_2^2D$ is odd. Taking the norm of both sides of (4.18) gives

$$9 - D \ = \ \|\alpha\| \left\|m_2 + n_2\sqrt{D}\right\|, \tag{4.21}$$

that is,

$$m_2^2 - n_2^2D = \left\|m_2 + n_2\sqrt{D}\right\| = m - 1 \tag{4.22}$$

is an even integer, contradiction. The proof is complete. □

If (x, y) is a minimal solution to $X^2 - DY^2 = n$, 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) can be generated as follows:

$$x_j + y_j\sqrt{D} = \pm(x + y\sqrt{D})(u + v\sqrt{D})^j, \text{where } j \in \mathbb{Z}. \tag{4.23}$$

It is stated in [**18**] that the sequence $(x_j)_{j\in\mathbb{Z}}$ defined as in (4.23) and belonging to (4.1) is periodic modulo 6 with period at most 2. We could not find a proof anywhere, and we include our own proof for a more general case.

Lemma 4.4. *Let m be a nonzero integer, and let D be a positive integer such that D is not a perfect square and $D \equiv 0 \pmod 3$. Then, the sequence $(x_j)_{j\in\mathbb{Z}}$ defined as in (4.23) and belonging to $X^2 - DY^2 = m$ is periodic modulo 6 with period at most 2.*

Proof. Suppose $j \geq 0$. By expanding (4.23) we can write $x_0 = x, y_0 = y$, $x_{i+1} = x_iu + y_ivD$, and $y_{i+1} = x_iv + y_iu$ for $i \geq 0$. Then, using $u^2 + v^2D = 1 + 2v^2D$ and $2D \equiv 0 \pmod 6$, we get

$$\begin{aligned} x_i &= x_{i-1}u + y_{i-1}vD \\ &= x_{i-2}(u^2 + v^2D) + 2y_{i-2}uvD \\ &\equiv x_{i-2} \pmod 6 \end{aligned}$$

for $i \geq 2$, which proves the result. Similarly, the case when $j < 0$ can be proved. □

Proposition 4.5. *If an ordinary elliptic curve E over a prime field with embedding degree 6 is constructable then (4.1) must have only primitive solutions and the value D in (4.1) must satisfy $D \equiv 9 \pmod{24}$. Also, -2 must be a square modulo D.*

PROOF. If E with $k = 6$ is constructable then there exists some integer l satisfying $12l^2 \pm 4l + 3 = D'V^2$ by (2.22) and (2.23). In other words, $4l(3l \pm 1) + 3 = D'V^2$ holds, and so $D'V^2 \equiv 3 \pmod 8$. Hence,$D' \equiv 3 \pmod 8$ proving that $D \equiv 9 \pmod{24}$ since $D = 3D'$. Now, let (x, y) be a solution of (4.1) with $\gcd(x, y) = d > 1$ and let $x = dx'$, $y = dy'$. Since $d^2(x'^2 - Dy'^2) = -8$ is satisfied we must have $d = 2$. Then $x'^2 - Dy'^2 = -2$ and reducing this equation modulo 8 gives $x'^2 - y'^2 \equiv 6 \pmod 8$. But, the last congruence does not have any integer solutions and so any solution of (4.1) must be primitive. Finally, reducing (4.1) modulo D proves that -2 must be a square modulo D. □

PROPOSITION 4.6. *Let S_α and $S_{\alpha'}$ denote the two solution classes of (4.1) as in Theorem 4.3. Then the set of elliptic curves, say $\mathcal{E}_\alpha$, constructed through S_α and the set of elliptic curves, say $\mathcal{E}_{\alpha'}$, constructed through $S_{\alpha'}$ are identical.*

PROOF. Let $E_\alpha(\mathbb{F}_q) \in \mathcal{E}_\alpha$ with trace t, and $\#E_\alpha(\mathbb{F}_q) = n$. Then there exists a pair (x, y) in S_α such that $x \equiv 1 \pmod 6$ or $x \equiv 5 \pmod 6$. Suppose first that $x \equiv 1 \pmod 6$ and let $x = 6l+1$ for some integer l. Then by Theorem 2.3.(iii) (see also (2.26)) $q = 4l^2+1$, $t = 1-2l$ and $n = 4l^2+2l+1$. Let $(x', y') = (-x, y)$. Then $(x', y') \in S_{\alpha'}$ since (4.1) does not contain any ambiguous class by Lemma 3.6. Now, $x' = 6(-l) - 1$, $x' \equiv 5 \pmod 6$ and (see (2.25)) also $q' = 4(-l)^2 + 1 = q$, $t' = 1 + (-2l) = t, n' = 4(-l)^2 - 2(-l) + 1 = n$. Since (x', y') corresponds to an elliptic curve $E_{\alpha'} \in \mathcal{E}_{\alpha'}$ defined over $\mathbb{F}_{q'}$ with trace t' and $\#E_{\alpha'}(\mathbb{F}_{q'}) = n'$ we find $E_\alpha = E_{\alpha'}$ and $\mathcal{E}_\alpha \subset \mathcal{E}_{\alpha'}$. Conversely, the same argument proves that $\mathcal{E}_{\alpha'} \subset \mathcal{E}_\alpha$. Also, the case when $x \equiv 5 \pmod 6$ is similar as above and hence, $\mathcal{E}_\alpha = \mathcal{E}_{\alpha'}$ □

Before giving the searching algorithm we shall summarize the above results.

- D should be fixed such that $0 < D \leq 10^{10}$, $D/3$ is square free, $D \equiv 9 \pmod{24}$, and -2 is a square modulo D.
- Let (u, v) be a minimal solution to $U^2 - DV^2 = 1$. If there is a solution to $X^2 - DY^2 = -8$ then it is enough to find, if it exists, only one minimal solution, say (x_0, y_0).
- 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 $-(x_j, y_j)$, by the proof of Proposition 4.6
- If $x_0 \not\equiv \pm 1 \pmod 6$ then there do not exist any suitable (i.e., curve generating) solutions (x_j, y_j) for $j \equiv 0 \pmod 2$ by Lemma 4.4, and Section 2.1.3. Similarly, if $x_1 \not\equiv \pm 1 \pmod 6$ then there do not exist any suitable solutions (x_j, y_j) for $j \equiv 1 \pmod 2$.

Algorithm 3 searches through all solutions (x_j, y_j) satisfying $(x_j + y_j\sqrt{D}) = (x + y\sqrt{D})(u + v\sqrt{D})^j$ for $j \geq 0$. Of course, the solutions corresponding to $j < 0$ must also be considered. For simplicity, we haven't included this case in the algorithm.

Algorithm 3 EC parameters with $k = 6$

Input: N, z

Output: EC parameters (q, n, k, D') where q and n are N-bit primes, $k = 6$, and $D' \leq z$ (where $4q - t^2 = D'V^2$)

```
for $0 < D \leq 3z$, $D/3$ square free, $D \equiv 9 \pmod{24}$, $-2$ is a square modulo $D$ do
  if $D > 64$ then
    find a minimal solution, $(x_0, y_0)$, to $X^2 - DY^2 = -8$ by using Algorithm 1 with
    input $D$, $-8$.
  else
    find a minimal solution, $(x_0, y_0)$, to $X^2 - DY^2 = -8$ by using Algorithm 2 with
    input $D$, $-8$.
  end if
  find a minimal solution, $(u, v)$, to $U^2 - DV^2 = 1$ by using Algorithm 1 with input
  $D$, 1.
  $x_1 \leftarrow x_0u + y_0vD$, $y_1 \leftarrow x_0v + y_0u$
  $x \leftarrow x_0$, $y \leftarrow y_0$, $x' \leftarrow x_1$, $y' \leftarrow y_1$
  if $x_0 \equiv \pm 1 \pmod{6}$ then
    while $|x| \leq 2^{\lceil N/2 \rceil}$ do
      $l \leftarrow (x \mp 1)/6$
      if $\lfloor (N - 2 \rfloor)/2 \leq \log_2 l < \lceil (N - 2)/2 \rceil$ then
        $q \leftarrow 4l^2 + 1$, $n \leftarrow 4l^2 \mp 2l + 1$
        if $q$ and $n$ are primes then
          Output $(q, n)$
        end if
      end if
      $\widetilde{x} \leftarrow x$
      $x \leftarrow x(2u^2 - 1) + 2yuvD$
      $y \leftarrow y(2u^2 - 1) + 2\widetilde{x}uv$
    end while
  end if
  if $x_1 \equiv \pm 1 \pmod{6}$ then
    while $|x'| \leq 2^{\lceil N/2 \rceil}$ do
      $l \leftarrow (x' \mp 1)/6$
      if $(N - 2)/2 \leq \log_2 l < \lceil (N - 2)/2 \rceil$ then
        $q \leftarrow 4l^2 + 1$, $n \leftarrow 4l^2 \mp 2l + 1$
        if $q$ and $n$ are primes then
          Output $(q, n)$
        end if
      end if
      $\widetilde{x}' \leftarrow x'$
      $x' \leftarrow x'(2u^2 - 1) + 2y'uvD$
      $y' \leftarrow y'(2u^2 - 1) + 2\widetilde{x}'uv$
    end while
  end if
end for
```

Now, let n and q be primes and define the following sets

$\mathcal{D} = \{D : D/3$ is square free, $D \equiv 9 \pmod{24}, -2$ is a square modulo $D\}$,

$\mathcal{D}[i] = \{D \in \mathcal{D} : \ \ 0 < D \leq 2^i\}$,

$\mathcal{D}_{-8}[i] = \{D \in \mathcal{D}[i] :$ there exist solutions to $X^2 - DY^2 = -8\}$,

$\mathcal{D}_{-8,q,n}[i] = \{(D, (q, n)) : D \in \mathcal{D}_{-8}[i]$ and primes q, n exist through the solutions of $X^2 - DY^2 = -8\}$,

Recall that in Chapter 2 $E(z)$ is defined to be the number of isogeny classes of MNT curves for $k = 6$ and $D' \leq z$ (where $4q - t^2 = D'V^2$). So, in the context of the above definitions we can write $\#\mathcal{D}_{-8,q,n}[i] = E(2^i/3)$.

For a given integer i, we aim to find some approximations for the cardinality of the sets $\mathcal{D}[i], \mathcal{D}_{-8}[i]$ and $\mathcal{D}_{-8,q,n}[i]$.

First we give an asymptotic approximation for $\#\mathcal{D}[i]$. Let $D \in \mathcal{D}$ and let $D = \prod_{s=1}^{w(D)} p_s$ be the prime factorization of D where $p_1 = 3$ and $w(D)$ is the number of distinct prime factors of D. We know that -2 is a square modulo D if and only if -2 is a square modulo p_s for every $s = 1, \ldots, w(D)$. And, -2 is a square modulo p_s if and only if $p_s \equiv 1, 3 \pmod 8$. Moreover, it is known that if $F(z)$ is the set of integers D such that $D \leq z$ and $(1 - \epsilon) \ln \ln D < w(D) < (1 + \epsilon) \ln \ln D$ for every positive ϵ then $F(z)$ has density one, that is, $F(z)/z \to 1$ as $z \to \infty$ ([**13**]). So, choosing ϵ arbitrarily small, we may suppose on average that the number of distinct prime factors of D is $\ln \ln D$. Therefore, the probability that -2 is a square modulo D may be written as $\left(\frac{1}{2}\right)^{\ln \ln D}$. Also, the asymptotic number of square free integers $\leq z$, say $S(z)$, is given by [**27**]

$$S(z) = \frac{6z}{\pi^2} + O(\sqrt{z}). \tag{4.24}$$

The above discussion then leads to the following asymptotic approximation for $\#\mathcal{D}[i]$.

$$\#\mathcal{D}[i] = \frac{1}{24} \cdot \left(\frac{1}{2}\right)^{\ln \ln 2^i} \left(\frac{6(2^i/3)}{\pi^2} + O(2^{i/2})\right),$$

or

$$\#\mathcal{D}[i] = \frac{2^{i - \ln \ln 2^i}}{12\pi^2} + O(2^{i/2 - \ln \ln 2^i}) \tag{4.25}$$

For future reference, we define

$$f(i) = \frac{2^{i - \ln \ln 2^i}}{12\pi^2}. \tag{4.26}$$

The next proposition provides a sufficient condition for $X^2 - DY^2 = -8$ to have a solution and will be helpful to give a lower bound for $\#\mathcal{D}_{-8}[i]$.

Proposition 4.7. *Let D' be a positive, square free integer such that $D' \equiv 1 \pmod 8$, and $D' \equiv 0 \pmod 3$. Let $h_{D'}$ denote the class number of the quadratic field $Q(\sqrt{D'})$. If $h_{D'} = 1$ then $X^2 - D'Y^2 = -8$ has a solution.*

Proof. Let R be the ring of integers of the field $Q(\sqrt{D'})$. By (4.4), the ideal $I = (2, \frac{1+\sqrt{D'}}{2})$ is a prime divisor of the ideal (2) in R. Since $h_{D'} = 1$, there exists $\alpha \in R$ such that $(\alpha) = I$. In particular, $|N(\alpha)| = N(I) = 2$. By Theorem 3.1, $\alpha = \frac{x+y\sqrt{D'}}{2}$ for some x, y such that $x \equiv y \pmod 2$. We claim that $x \equiv y \equiv 1 \pmod 2$ and $N(\alpha) = -2$: If $x \equiv y \equiv 0 \pmod 2$ and $N(\alpha) = 2$ then we would have $a^2 - D'b^2 = 2$ for some integers a, b and reducing this equation modulo 8 gives $a^2 - b^2 \equiv 2 \pmod 8$, contradiction. If $x \equiv y \equiv 0 \pmod 2$ and $N(\alpha) = -2$ then we would have $a^2 - D'b^2 = -2$ for some integers a, and b. Reducing both sides modulo 8 we would get $a^2 - b^2 \equiv 6 \pmod 8$, contradiction. If $x \equiv y \equiv 1 \pmod 2$ and $N(\alpha) = 2$ then we would have $x^2 - D'y^2 = 8$ for some integers x, and y. Reducing this equality modulo 3 we would get $x^2 \equiv 2 \pmod 3$, contradiction. Hence, the only possible case is $\alpha = \frac{x+y\sqrt{D}}{2}$, $x \equiv y \equiv 1 \pmod 2$, and $N(\alpha) = -2$, that is $x^2 - D'y^2 = -8$, as required. □

We should note that according to the Cohen-Lenstra heuristics [**5**], 75.4% of the real quadratic fields $Q(\sqrt{D'})$ with prime D' have class number 1. In fact, if $h_{D'} = 1$ then it is known that $D' = p$ for some prime p, or $D' = 2q$, or $D' = q_1q_2$ for some primes $q, q_1, q_2 \equiv 3 \pmod 4$. And, it is widely believed that similar heuristics hold for all such configurations of D' [**31**]. In particular, we may assume that the set of quadratic fields $Q(\sqrt{D'})$ with $D' = 3q_1$ ($q_1 \equiv 3 \pmod 4$), and $h_{D'} = 1$ has a positive density in the set of all real quadratic fields $Q(\sqrt{D'})$ with $D' \equiv 3q_1$, $q_1 \equiv 3 \pmod 4$.

Therefore, under this assumption, we can conclude that

Theorem 4.8. *Let q represent a prime congruent to 3 modulo 4. Assume that the set of quadratic fields $Q(\sqrt{D'})$ with $D' = 3q$, and $h_{D'} = 1$ has a positive density, say C, in the set of all real quadratic fields $Q(\sqrt{D'})$ with $D' = 3q$. Then a lower bound for $\#\mathcal{D}_{-8}[i]$ can be given as follows*

$$\#\mathcal{D}_{-8}[i] \geq \frac{C}{12}\frac{2^i}{\ln(2^i/3)}. \tag{4.27}$$

Proof. Define $S = \{D : \ D \leq 2^i, \ D = 3q, \ q \neq 3, \ q \equiv 3 \pmod 8\}$. Note that $S \subset D[i]$ and by the prime number theorem, $|S| \approx \frac{1}{4}\frac{2^i/3}{\ln(2^i/3)}$. Hence, by the assumption of the theorem, and by Proposition 4.7 we conclude

$$\#\mathcal{D}_{-8}[i] \geq \frac{C}{4} \cdot \frac{2^i/3}{\ln(2^i/3)}, \tag{4.28}$$

where C is the constant specified in the statement of the theorem. □

For future reference, we define

$$g(i) = \frac{2^i}{\ln(2^i)}. \tag{4.29}$$

The following proposition will help to prove the lower bound (4.27) with the assumption of Theorem 4.8 replaced by another assumption, and using the Cohen-Lenstra heuristics on the class numbers of quadratic fields with prime D'.

PROPOSITION 4.9. *Let p be a prime such that $p \equiv 1 \pmod 8$ and $p \equiv 1 \pmod 3$. Assume that $Q(\sqrt{p})$ has class number $h_p = 1$. Then, at least one of the equations $X^2 - pY^2 = -8$ or $X^2 - pY^2 = 8$ has an integer solution. Moreover, if $X^2 - pY^2 = -8$ is soluble then $X^2 - 9pY^2 = -8$ is also soluble.*

PROOF. The first part of the theorem follows from the proof of Proposition 4.7. Now, assume (x, y) is a solution to $X^2 - pY^2 = -8$. Then $x^2 - y^2 \equiv 1 \pmod 3$ and this is possible only if $y \equiv 0 \pmod 3$. In this case, $(x, y/3)$ is a solution to $X^2 - 9pY^2 = -8$ as required. □

Note that the lower bound in Theorem 4.8 was computed by considering the set $S = \{D : D \leq 2^i, D = 3p, p \neq 3, p \equiv 3 \pmod 8\}$. We can apply a similar argument and prove the lower bound (4.27) by replacing S with $S' = \{D : D \leq 2^i, D = 9p, p \equiv 1 \pmod 3), p \equiv 1 \pmod 8\}$, and by using Cohen-Lenstra heuristics and Proposition 4.9. Of course, we need to replace the assumption of Theorem 4.8 with the assumption that for primes p as in Proposition 4.9, the set of equations $X^2 - pY^2 = -8$ that are soluble has a positive density in the set of equations $X^2 - pY^2 = \pm 8$ that are soluble.

In the proof of Proposition 4.7, the sufficiency condition $h_{D'} = 1$ is used only to guarantee that the ideal $I = (2, \frac{1+\sqrt{D'}}{2})$ is principal. In other words, the existence of a solution to $X^2 - D'Y^2 = -8$ is guaranteed when the ideal $(2, \frac{1+\sqrt{D'}}{2})$ is principal, and say generated by α. In this case, the conjugate of α would generate the ideal $(2, \frac{1-\sqrt{D'}}{2})$, and by Theorem 3.2 the prime factors of the ideal $2R$ would be principal. Conversely, if $\alpha = x + y\sqrt{D'}$ is a solution to $X^2 - D'Y^2 = -8$ then the ideal $(2, \frac{1+\sqrt{D'}}{2})$ is principal and, without loss of generality, generated by $\alpha/2$. Moreover, $(2, \frac{1+\sqrt{D'}}{2})$ is generated by $\alpha'/2$ (see the proof of Theorem 4.3). To summarize, we get the following theorem as a generalization of Proposition 4.7:

THEOREM 4.10. *Let D' be a positive, square free integer such that $D' \equiv 1 \pmod 8$, and $D' \equiv 0 \pmod 3$. Then $X^2 - D'Y^2 = -8$ has an integer solution if and only if the ideal $(2, \frac{1+\sqrt{D'}}{2})$ is principal in the quadratic field $Q(\sqrt{D'})$. Equivalently, $X^2 - D'Y^2 = -8$ has an integer solution if and only if the prime 2 splits as a product of two principal prime ideals in the ring of integers of $Q(\sqrt{D'})$.*

Next, we give a lower bound for $E(z)$. We represent an elliptic curve E, defined over a finite field $\mathbb{F}_q$, with embedding degree k, and $\#E(\mathbb{F}_q) = n$ by a tuple (E, q, n, k, D') where $4q - t^2 = D'V^2$. We restrict $q > 64$, and $n > 64$ to be prime and $k = 6$. Recall from Section 2.1.3 that constructing E is reduced to finding some suitable solutions to

$$X^2 - 3D'Y^2 = -8 \tag{4.30}$$

where $D' > 3$ is a square free integer. For a given D', once a solution (x, y) is found then the parameters are given by

- *Case 1.* $x \equiv 1 \pmod 6$: $q = 4l^2 + 1$, $n = 4l^2 + 2l + 1$ where $l = (x - 1)/6$, or,
- *Case 2.* $x \equiv -1 \pmod 6$: $q = 4l^2 + 1$, $n = 4l^2 - 2l + 1$ where $l = (x + 1)/6$.

REMARK 4.1. Given a solution (x, y) of $X^2 - 3D'Y^2 = -8$ with x is odd we must have $x \equiv 1 \pmod 6$ or $x \equiv -1 \pmod 6$. (If $x \equiv 0 \pmod 3$ then reducing $x^2 - 3D'y^2 = -8$ modulo 3 gives a contradiction.)

Also, an easy counting argument gives the following lemma:

LEMMA 4.11. *Let $s \geq 0$ be an integer and define*

$$\begin{aligned} A_1(s) &= \{a \in \mathbb{Z} : 1 \leq a \leq (2s+1)^2, a \textit{ is perfect square}, a \equiv 1 \pmod 6\}, \\ A_4(s) &= \{a \in \mathbb{Z} : 1 \leq a \leq (2s)^2, a \textit{ is perfect square}, a \equiv 4 \pmod 6\}. \end{aligned}$$

Then $|A_1(s)| = \lceil (2s+1)/3 \rceil$, and $|A_4(s)| = \lceil 2s/3 \rceil$.

Note that the sequence $\{(3D' - 8)\}_{D'}$ runs through all integers congruent to 1 modulo 3 as D' runs through all integers greater than 2. So, by Lemma 4.11, $\{(3D' - 8)\}_{D'}$ where $D' \in [3, (z + 8)/3]$, runs through $\frac{2\sqrt{z}}{3} + O(1)$ many perfect squares in the interval $[1, z]$. That is, if D' is an integer randomly chosen from the interval $[3, (z + 8)/3]$, then the probability that $(3D' - 8)$ is a perfect square can be estimated as $\frac{2\sqrt{z}+O(1)}{3z}$.

Also, recall that the asymptotic number of square free integers $\leq z$, say $S(z)$, is given by $S(z) = 6z/\pi^2 + O(\sqrt{z})$ (see (4.24)). Moreover, we can write that the asymptotic number of square free integers which are odd is at least $S(z)/2$ since every even square free integer, say m, corresponds to an odd square free integer, say $m/2$.

Now, for an integer D', randomly chosen from the interval $[3, (z + 8)/3]$, define $e(D')$ as the event that D' is odd, square free and that $(3D' - 8)$ is a perfect square. Then, using the above discussion, we may argue that the probability assigned to $e(D')$ is

$$P(e(D')) \geq \frac{1}{2} \cdot \frac{6(z/3)/\pi^2 + O(\sqrt{z/3})}{z/3} \cdot \frac{2\sqrt{z} + O(1)}{3z}. \tag{4.31}$$

That is, we may write for some positive constants c_1, and c_2 that

$$\begin{aligned} P(e(D')) &\geq \frac{1}{2} \cdot \left(\frac{6}{\pi^2} - \frac{c_1}{\sqrt{z}} \right) \cdot \left(\frac{2}{3\sqrt{z}} - \frac{c_2}{z} \right) \\ &\geq \frac{1}{2} \cdot \left(\frac{4}{\pi^2\sqrt{z}} - \frac{(18c_2 + 2\pi^2 c_1)}{3\pi^2 z} + \frac{c_1 c_2}{z\sqrt{z}} \right) \\ &\geq \left(\frac{2}{\pi^2\sqrt{z}} - \frac{(9c_2 + \pi^2 c_1)}{3\pi^2 z} \right). \end{aligned} \tag{4.32}$$

Now, suppose D' satisfies the conditions that D' is odd, square free and $(3D' - 8) = x^2$ for some integer x. Then we get a solution, $(x, 1)$, to the Pell equation $X^2 - 3D'Y^2 = -8$. Note that $x > 0$ is odd and also, by Remark 4.1, x must satisfy $x \equiv 1, -1 \pmod 6$. Suppose first that $x \equiv 1 \pmod 6$. Define the following integers $l = (x - 1)/6$, $q = 4l^2 + 1$, $n = 4l^2 + 2l + 1$. That is, $q = \frac{2x^2}{3} - \frac{4x}{3} + \frac{5}{3}$ and $n = \frac{2x^2}{3} - x + \frac{4}{3}$. Note that $q \leq x^2 = 3D' - 8$ and $n \leq x^2 = 3D' - 8$. By the prime number theorem, we may estimate the probability that both q and n are prime as $\frac{1}{(\ln(3D'-8))^2}$. Similarly, this estimation holds when we assume $x \equiv -1 \pmod 6$. So, for an integer D' randomly chosen from an interval $[5, (z+8)/3]$, the probability of obtaining (E, q, n, k, D') is at least

$$\left(\frac{2}{\pi^2\sqrt{z}} - \frac{(9c_2 + \pi^2 c_1)}{3\pi^2 z}\right) \cdot \frac{1}{(\ln(3D' - 8))^2}. \tag{4.33}$$

Summing (4.33) for all D' in $[5, (z+8)/3]$, and defining $c = \frac{(9c_2+\pi^2c_1)}{3\pi^2}$, we get

$$\begin{aligned} E(z) &\geq \cdot \left(\frac{2}{\pi^2\sqrt{z}} - \frac{c}{z}\right) \sum_{D'=5}^{\lfloor (z+8)/3 \rfloor} \frac{1}{(\ln(3D'-8))^2} \\ &\geq \left(\frac{2}{3\pi^2} \cdot \frac{\sqrt{z}}{(\ln z)^2} - \frac{c}{(\ln z)^2}\right). \end{aligned}$$

We can summarize our discussion in the following theorem:

THEOREM 4.12. *Let $E(z)$ denote the expected number of isogeny classes of MNT curves with $k = 6$ and $D' \leq z$. Then, given any $\epsilon > 0$, $E(z)$ satisfies*

$$E(z) \geq \frac{2}{3\pi^2} \cdot \frac{\sqrt{z}}{(\ln z)^2} - \epsilon, \tag{4.34}$$

as $z \longrightarrow \infty$.

For future reference, we define

$$\sigma(z) = \frac{\sqrt{z}}{(\ln z)^2}. \tag{4.35}$$

We have tested the approximation for $\#\mathcal{D}[i]$ (see (4.25)), the lower bound for $\#\mathcal{D}_{-8}[i]$ (see (4.27)), We have also tested the upper and lower bounds for $\#\mathcal{D}_{-8,q,n}[i]$ (see (2.29), (2.30), (4.34) and recall that $E(2^i/3) = \#\mathcal{D}_{-8,q,n}[i]$) in experiments.

In particular, we have run Algorithm 3 with inputs $1 \leq N \leq 300$, and $z = 8/3 \cdot 10^7$. The results are given in Table 1. Note that for some integers i we have $\#\mathcal{D}_{-8}[i] < \#\mathcal{D}_{-8,q,n}[i]$ because for some values of $D \in \mathcal{D}_{-8}[i]$ there correspond more than one suitable prime pair (q, n). We see that the necessary conditions put on D for the existence of a solution to $X^2 - DY^2 = -8$ are not sufficient since $\mathcal{D}[i] \neq \mathcal{D}_{-8}[i]$ in general. The smallest 11 elements, corresponding to $\mathcal{D}[12] \backslash \mathcal{D}_{-8}[12]$, are $\{321, 993, 1257, 1641, 1761, 1929, 2313, 2913, 3201, 3609, 3873\}$. The class numbers of the corresponding quadratic fields are $\{3, 3, 3, 5, 7, 3, 3, 7, 8, 5, 3\}$.

We investigated additive and multiplicative structures of D to find some pattern on the set $\mathcal{D}_{-8}[i]$ (or $\mathcal{D}[i] \backslash \mathcal{D}_{-8}[i]$). In particular, we analyzed the values $D \in \mathcal{D}_{-8}[i]$ modulo some integers. However, all the patterns we found for $D \in \mathcal{D}_{-8}[i]$ to satisfy were already implied by the conditions in $\mathcal{D}$. For instance, $D \not\equiv 5 \pmod{10}$, or $D \not\equiv 7 \pmod{14}$ are implied by the condition that -2 is a square modulo D. On the other hand, one interesting observation appears in the fifth column of Table 1 and that indicates a convergence to a 75% proportion for $\#\mathcal{D}_{-8}[i]/\#\mathcal{D}[i]$. This is not obvious from our theoretical findings (4.25) and (4.27) because $\lim_{i\to\infty} f(i)/g(i) = \infty$. Note that in the proof of the lower bound for $\#\mathcal{D}_{-8}[i]$, only quadratic fields with class number 1 were considered and there still exist values of D such that $Q(\sqrt{D})$ has class number greater than 1 and

$X^2 - DY^2 = -8$ has a solution. For instance, if $D = 561$ then $h_D = 2$ and $(71, 3)$ is a solution to $X^2 - DY^2 = -8$. So, it may be possible to improve the lower bound for $\#\mathcal{D}_{-8}[i]$ by analyzing the fields with class numbers greater than 1, and to use Theorem 4.10 in order to explain the convergence 75%. More precisely, this would be achieved in the following scenario: For a given ideal $(1, 1 + \sqrt{D}/2)$, if $e(D)$ is the event that $(1, 1 + \sqrt{D}/2)$ is principal in $Q(\sqrt{D})$ then there exists a probability function, say $p(e(D), h_D)$ (given D, the probability that $(1, 1 + \sqrt{D}/2)$ is principal), which only depends on the class number of $Q(\sqrt{D})$. For example we already know that $p(e(D), 1) = 1$. This might be possible in general for $h_D > 1$ because it is known that ideals are approximately uniformly distributed among the ideal classes. And, this might not be possible because the uniform distribution is asymptotic in the size of the norm of ideals.

In the sixth and seventh columns of Table 1, $\#\mathcal{D}[i]$ and $\#\mathcal{D}_{-8}[i]$ are compared with $f(i)$ and $g(i)$ (see (4.25), (4.26),and (4.27), (4.29)). The increase in the ratio $\#\mathcal{D}[i]/f(i)$ suggests that there may be a better approximation for $\#\mathcal{D}[i]$ or the discrepancy is swallowed in the big O notation in (4.25). The increase in the ratio $g(i)/\#\mathcal{D}_{-8}[i]$ indicates that $g(i)$ can be improved as we discussed before. Finally, we can see the behaviour of $E(z)$ compared to its upper bound (2.30), and to its lower bound (see (4.34) and (4.35)) in the last two columns of Table 1.

(Note that in our discussion we should omit the last row of the table since it corresponds to a search range such that $3 \leq D \leq 2^{27}$, whereas we run our experiments for $D \leq 8 \cdot 10^7 < 2^{27}$.)

i	$\#\mathcal{D}[i]$	$\#\mathcal{D}_{-8}[i]$	$\#\mathcal{D}_{-8,q,n}[i]$	$\frac{\#\mathcal{D}_{-8}[i]}{\#\mathcal{D}[i]}$	$\frac{1}{10}\frac{\#\mathcal{D}[i]}{f(i)}$	$\frac{1}{5}\frac{g(i)}{\#\mathcal{D}_{-8}[i]}$	$\frac{10\cdot\#\mathcal{D}_{-8,q,n}[i]}{\sqrt{2^i}}$	$\frac{1}{10}\frac{\#\mathcal{D}_{-8,q,n}[i]}{\sigma(2^i)}$
1	0	0	0					
2	0	0	0					
3	0	0	0					
4	0	0	0					
5	0	0	0					
6	2	2	3	1	0.9939	1.5388	3.7500	0.6486
7	2	2	3	1	0.5530	2.6380	2.6516	0.6242
8	7	7	5	1	1.0616	1.3190	3.1250	0.9609
9	12	11	7	0.9166	0.9873	1.4922	3.0935	1.2039
10	25	23	7	0.9200	1.1064	1.2846	2.1875	1.0509
11	44	38	8	0.8636	1.0401	1.4137	1.7677	1.0276
12	85	74	12	0.8706	1.0671	1.3309	1.8750	1.2972
13	165	136	14	0.8242	1.0948	1.3369	1.5467	1.2559
14	322	270	14	0.8385	1.1246	1.2506	1.0937	1.0299
15	619	519	17	0.8384	1.1339	1.2144	0.9391	1.0152
16	1198	977	22	0.8155	1.1475	1.2096	0.8593	1.0569
17	2327	1885	27	0.8100	1.1623	1.1801	0.7457	1.0355
18	4511	3594	32	0.7967	1.1721	1.1692	0.6250	0.9729
19	8783	6915	43	0.7873	1.1846	1.1514	0.5938	1.0300
20	17102	13356	49	0.7810	1.1950	1.1326	0.4785	0.9196
21	33349	25828	65	0.7745	1.2052	1.1156	0.4488	0.9510
22	65090	50115	78	0.7699	1.2147	1.0976	0.3808	0.8856
23	127199	97545	105	0.7669	1.2241	1.0788	0.3625	0.9214
24	248833	189651	147	0.7622	1.2331	1.0635	0.3588	0.9931
25	487218	369882	187	0.7592	1.2419	1.0470	0.3228	0.9693
26	954700	722611	268	0.7569	1.2503	1.0306	0.3271	1.0625
27	1132405	855990	290	0.7560	0.7611	1.6756	0.2503	0.8767

Table 1: $k = 6$; see Algorithm 3 and (4.26), (4.29), (4.35) for definitions of f, g, σ

CHAPTER 5

The cases $k = 3, 4$

The constructability of elliptic curves with embedding degree $k = 6$ was analyzed in Chapter 4 by discussing the set of solutions to the corresponding Pell equation. In this chapter, a similar analysis is given for embedding degrees $k = 3$ and $k = 4$. First we note that the analysis of the case $k = 4$ is exactly the same as the case $k = 6$ by Proposition 2.4. So, we only concentrate on the case $k = 3$.

It was shown in Section 2.1.1 that constructing an elliptic curve E with $k = 3$ is reduced to finding some suitable solutions to

$$X^2 - DY^2 = 24, \qquad D > 0, \qquad D \equiv 0 \pmod 3. \tag{5.1}$$

The analysis of (5.1) was mostly done by Miyaji, Nakabayashi, and Takano [**24**]. The following proposition summarizes their results.

Proposition 5.1. *If an ordinary elliptic curve E over a prime field with embedding degree 3 is constructable then (5.1) must have only primitive solutions and the value D in (5.1) must satisfy $D \equiv 57 \pmod{72}$. Moreover, (5.1) has exactly two classes of solutions and if $\alpha = (x, y)$ is a solution to (5.1) then α and $\alpha' = (x, -y)$ represent the two different solution classes.*

Proof. The proof follows from Lemma 1, Lemma 2 and Proposition 1 of [**24**]. □

The following proposition is analogous to Proposition 4.6.

Proposition 5.2. *Let S_α and $S_{\alpha'}$ denote the two solution classes of (5.1) as in Proposition 5.1. Then the set of elliptic curves, say $\mathcal{E}_\alpha$, constructed through S_α and the set of elliptic curves, say $\mathcal{E}_{\alpha'}$, constructed through $S_{\alpha'}$ are identical.*

Now, let (x, y) be a minimal solution to $X^2 - DY^2 = n$, and let (u, v) be a minimal solution to $U^2 - DV^2 = 1$. Recall that all primitive solutions (x_j, y_j) in the class of (x, y) can be generated as follows:

$$x_j + y_j\sqrt{D} = \pm(x + y\sqrt{D})(u + v\sqrt{D})^j, \text{where } j \in \mathbb{Z}. \tag{5.2}$$

As in Chapter 4, we summarize our discussion and give a searching algorithm for suitable prime order elliptic curve parameters with $k = 3$.

- D should be fixed such that $0 < D \leq 10^{10}$, $D/3$ is square free, $D \equiv 57 \pmod{72}$, Also, 6 must be a square modulo D.

- Let (u, v) be a minimal solution to $U^2 - DV^2 = 1$. If there is a solution to $X^2 - DY^2 = 24$ then it is enough to find, if it exists, only one minimal solution, say (x_0, y_0).
- Let $(x_j, y_j) = \pm(x_0, y_0)(u, v)^j$ be the set of all solutions as in the same class as (x, y). It is enough to consider only one of the solutions (x_j, y_j) and $-(x_j, y_j)$.
- If $x_0 \not\equiv 3 \pmod 6$ then there do not exist any suitable (i.e., curve generating) solutions (x_j, y_j) for $j \equiv 0 \pmod 2$ by Lemma 4.4, and Section 2.1.1. Similarly, if $x_1 \not\equiv 3 \pmod 6$ then there do not exist any suitable solutions (x_j, y_j) for $j \equiv 1 \pmod 2$.

Algorithm 4 EC parameters with $k = 3$

Input: N

Output: EC parameters (q, n, k, D') where q and n are N-bit primes, $k = 3$, and $D' \leq z$ (where $4q - t^2 = D'V^2$)

```
for $0 < D \leq 3z$, $D/3$ square free, $D \equiv 57 \pmod{72}$, 6 is a square modulo $D$ do
  if $D > 576$ then
    find a minimal solution, $(x_0, y_0)$, to $X^2 - DY^2 = -8$ by using Algorithm 1 with input $D$, 24.
  else
    find a minimal solution, $(x_0, y_0)$, to $X^2 - DY^2 = -8$ by using Algorithm 2 with input $D$, 24.
  end if
  find a minimal solution, $(u, v)$, to $U^2 - DV^2 = 1$ by using Algorithm 1 with input $D$, 1.
  $x_1 \leftarrow x_0u + y_0vD$, $y_1 \leftarrow x_0v + y_0u$
  $x \leftarrow x_0$, $y \leftarrow y_0$, $x' \leftarrow x_1$, $y' \leftarrow y_1$
  if $x_0 \equiv 3 \pmod 6$ then
    while $|x| \leq 2^{\lceil N/2 \rceil}$ do
      $l_1 \leftarrow (x-3)/6$, $l_2 \leftarrow (x+3)/6$
      if $\lfloor (N-4 \rfloor)/2 \leq \log_2 l_1, \log_2 l_2 < \lceil (N-3)/2 \rceil$ then
        $q_1 \leftarrow 12l_2^2 - 1$, $n_1 \leftarrow 12l_1^2 - 6l + 1$, $q_2 \leftarrow 12l_2^2 - 1$, $n_2 \leftarrow 12l_2^2 + 6l_2 + 1$
        if $q_1$ and $n_1$ are primes then
          Output $(q_1, n_1)$
        end if
        if $q_2$ and $n_2$ are primes then
          Output $(q_2, n_2)$
        end if
      end if
      $\widetilde{x} \leftarrow x$
      $x \leftarrow x(2u^2 - 1) + 2yuvD$
      $y \leftarrow y(2u^2 - 1) + 2\widetilde{x}uv$
    end while
  end if
  if $x_1 \equiv 3 \pmod 6$ then
    while $|x'| \leq 2^{\lceil N/2 \rceil}$ do
      $l_1 \leftarrow (x'-3)/6$, $l_2 \leftarrow (x'+3)/6$
      if $\lfloor (N-4 \rfloor)/2 \leq \log_2 l_1, \log_2 l_2 < \lceil (N-3)/2 \rceil$ then
        $q_1 \leftarrow 12l_2^2 - 1$, $n_1 \leftarrow 12l_1^2 - 6l + 1$, $q_2 \leftarrow 12l_2^2 - 1$, $n_2 \leftarrow 12l_2^2 + 6l_2 + 1$
        if $q_1$ and $n_1$ are primes then
          Output $(q_1, n_1)$
        end if
        if $q_2$ and $n_2$ are primes then
          Output $(q_2, n_2)$
        end if
      end if
      $\widetilde{x}' \leftarrow x'$
      $x' \leftarrow x'(2u^2 - 1) + 2y'uvD$
      $y' \leftarrow y'(2u^2 - 1) + 2\widetilde{x}'uv$
    end while
  end if
end for
```

Now, let n and q be primes and define the following sets

$\mathcal{D} = \{D : D/3 \text{ is square free, } D \equiv 57 \pmod{72}, 6 \text{ is a square modulo } D\}$,

$\mathcal{D}[i] = \{D \in \mathcal{D} : \ 0 < D \leq 2^i\}$,

$\mathcal{D}_{24}[i] = \{D \in \mathcal{D}[i] : \text{ there exist solutions to } X^2 - DY^2 = 24\}$,

$\mathcal{D}_{24,q,n}[i] = \{(D,(q,n)) : D \in \mathcal{D}_{24}[i]$ and primes q, n exist through the solutions of $X^2 - DY^2 = 24\}$.

As in Chapter 4, defining $E(z)$ to be the number of isogeny classes of MNT curves for $k = 3$ and $D' \leq z$ (where $4q - t^2 = D'V^2$) we have the relation $\#\mathcal{D}_{24,q,n}[i] = E(2^i/3)$.

We proceed similarly as in Chapter 4 and try to find approximations for the cardinality of the sets $\mathcal{D}[i], \mathcal{D}_{24}[i]$ and $\mathcal{D}_{24,q,n}[i]$.

First we consider the set $\mathcal{D}[i]$. Let $D \in \mathcal{D}$ and let $D = \prod_{s=1}^{w(D)} p_s$ be the prime factorization of D where $p_1 = 3$ and $w(D)$ is the number of distinct prime factors of D. We know that 6 is a square modulo D if and only if 6 is a square modulo p_s for every $s = 1, \ldots, w(D)$. Assuming without loss of generality that $p_s > 3$, 6 is a square modulo p_s if and only if the Legendre symbol satisfies $\left(\frac{6}{p_s}\right) = 1$. In other words, we must have $\left(\frac{2}{p_s}\right) = \left(\frac{3}{p_s}\right) = 1$ or $\left(\frac{2}{p_s}\right) = \left(\frac{3}{p_s}\right) = -1$. Using the facts that

$$\left(\frac{2}{p_s}\right) = \begin{cases} 1 & \text{if } p \equiv 1,7 \pmod{8} \\ -1 & \text{if } p \equiv 3,5 \pmod{8}, \end{cases}$$

and

$$\left(\frac{3}{p_s}\right) = \begin{cases} 1 & \text{if } p \equiv 1,11 \pmod{12} \\ -1 & \text{if } p \equiv 5,7 \pmod{12} \end{cases}$$

we can conclude that 6 is a square modulo $p_s > 3$ if and only if $p_s \equiv 1, 5, 19, 23 \pmod{24}$ and 6 is a not a square modulo $p_s > 3$ if and only if $p_s \equiv 7, 11, 13, 17 \pmod{24}$. Now, applying the similar reasoning as in the case for $k = 6$, we obtain the following approximation for $\#\mathcal{D}[i]$ follows as

$$\#\mathcal{D}[i] = \frac{2^{i - \ln\ln 2^i}}{36\pi^2} + O(2^{i/2 - \ln\ln 2^i}). \tag{5.3}$$

For future reference, we define

$$f(i) = \frac{2^{i - \ln\ln 2^i}}{36\pi^2}. \tag{5.4}$$

We will use the following proposition to give a lower bound for $\#\mathcal{D}_{24}[i]$.

PROPOSITION 5.3. *Let D' be an integer such that $D' = 3q$ where q is a prime and $q \equiv 19 \pmod{24}$. Let $h_{D'}$ denote the class number of the quadratic field $Q(\sqrt{D'})$. If $h_{D'} = 1$ then $X^2 - D'Y^2 = 24$ has a solution.*

PROOF. Let R be the ring of integers of the field $Q(\sqrt{D'})$. By Theorem 3.2, the ideal $I = (2, \frac{1+\sqrt{D'}}{2})$ is a prime divisor of the ideal (2) in R, and $J = (3, \sqrt{D'})$ is a prime divisor of the ideal (3) in R. Since $h_{D'} = 1$, there exists $\alpha \in R$ such that $(\alpha) = IJ$. In particular, $|N(\alpha)| = N(IJ) = 6$. By Theorem 3.1, $\alpha = \frac{x+y\sqrt{D'}}{2}$ for some x, y such that $x \equiv y \pmod{2}$. We claim that $x \equiv y \equiv 1 \pmod{2}$ and $N(\alpha) = 6$: If $x \equiv y \equiv 0 \pmod{2}$ and $N(\alpha) = 6$ then we would have $a^2 - D'b^2 = 6$ for some integers a, b and reducing this equation modulo 8 gives $a^2 - b^2 \equiv 6 \pmod{8}$, contradiction. If $x \equiv y \equiv 0 \pmod{2}$ and $N(\alpha) = -6$ then we would have $a^2 - D'b^2 = -6$ for some integers a, and b. Reducing both sides modulo 8 we would get $a^2 - b^2 \equiv 2 \pmod{8}$, contradiction. If $x \equiv y \equiv 1 \pmod{2}$ and $N(\alpha) = -6$ then we would have $x^2 - D'y^2 = -24$ for some integers x, and y. Considering this equality modulo 3 we get $x \equiv 0 \pmod{3}$. Now, let $x = 3s$ for some integer s. Then $(9s^2) - D'y^2 = -24$, and so $6s^2 \equiv 3 \pmod{9}$, contradiction. Hence, the only possible case is $\alpha = \frac{x+y\sqrt{D}}{2}$, $x \equiv y \equiv 1 \pmod{2}$, and $N(\alpha) = 6$, that is $x^2 - D'y^2 = 24$, as required. □

THEOREM 5.4. *Let q represent a prime congruent to 19 modulo 24. Assume that the set of quadratic fields $Q(\sqrt{D'})$ with $D' = 3q$, and $h_{D'} = 1$ has a positive density, say C, in the set of all real quadratic fields $Q(\sqrt{D'})$ with $D' \equiv 3q$. Then a lower bound for $\#\mathcal{D}_{24}[i]$ can be given as follows*

$$\#\mathcal{D}_{24}[i] \geq \frac{C}{36} \cdot \frac{2^i}{\ln(2^i/3)} \tag{5.5}$$

PROOF. Define $S = \{D : \; D \leq 2^i, \; D = 3q, \; q \neq 3, \; q \equiv 19 \pmod{24}\}$. Note that $S \subset D[i]$ and by the prime number theorem, $|S| \approx \frac{1}{12}\frac{2^i/3}{\ln(2^i/3)}$. Hence, by the assumption of the theorem, and by Proposition 5.3 we conclude

$$\#\mathcal{D}_{24}[i] \geq \frac{C}{12} \cdot \frac{2^i/3}{\ln(2^i/3)}$$

where C is the constant specified in the statement of the theorem. □

For future reference, we define

$$g(i) = \frac{2^i}{\ln(2^i)}. \tag{5.6}$$

Analogous to Theorem 4.10, we can give a generalization of Theorem 5.4 as follows:

THEOREM 5.5. *Let D' be an integer such that $D' = 3q$ where q is a prime and $q \equiv 19 \pmod{24}$. Then $X^2 - D'Y^2 = 24$ has an integer solution if and only if the ideal generated by 6 can be written as a product of two principal ideals of both of norm 6 in $Q(\sqrt{D'})$.*

Using similar arguments as in the proof of Theorem 4.12, one can prove the following theorem:

THEOREM 5.6. *Let $E(z)$ denote the expected number of isogeny classes of MNT curves with $k = 3$ and $D' \leq z$. Then, given any $\epsilon > 0$, $E(z)$ satisfies*

$$E(z) \geq \frac{1}{3\pi^2} \cdot \frac{\sqrt{z}}{(\ln z)^2} - \epsilon, \tag{5.7}$$

as $z \longrightarrow \infty$.

For future reference, we define

$$\sigma(z) = \frac{\sqrt{z}}{(\ln z)^2}. \tag{5.8}$$

We have tested the approximation for $\#\mathcal{D}[i]$ (see (5.3)), the lower bound for $\#\mathcal{D}_{24}[i]$ (see (5.5)). We have also tested the upper and lower bounds for $\#\mathcal{D}_{24,q,n}[i]$ (see (2.29), (2.30), (5.7) and recall that $E(2^i/3) = \#\mathcal{D}_{24,q,n}[i])$ in experiments.

The analysis is very similar to the case $k = 6$ in Chapter 4. In particular, we have run Algorithm 4 with inputs $1 \leq N \leq 300$, and $z = 13/3 \cdot 10^7$. The results are given in Table 1. Note that for some integers i we have $\#\mathcal{D}_{24}[i] < \#\mathcal{D}_{24,q,n}[i]$ because for some values of $D \in \mathcal{D}_{24}[i]$ there correspond more than one suitable prime pair (q, n). We see that the necessary conditions put on D for the existence of a solution to $X^2 - DY^2 = 24$ are not sufficient since $\mathcal{D}[i] \neq \mathcal{D}_{24}[i]$ in general. The smallest 7 elements, corresponding to $\mathcal{D}[11] \backslash \mathcal{D}_{24}[11]$, are $\{993, 1641, 1929, 2505, 3585, 3873, 4161\}$. The fifth column of Table 1 indicates a convergence to a constant proportion for $\#\mathcal{D}_{-8}[i]/\#\mathcal{D}[i]$, and this convergence might be explained by Theorem 5.5 (also see the analysis of the case $k = 6$).

In the sixth and seventh columns of Table 1, $\#\mathcal{D}[i]$ and $\#\mathcal{D}_{24}[i]$ are compared with $f(i)$ and $g(i)$ (see (5.3), (5.4),and (5.5), (5.6)). As in the case for $k = 6$, it might be possible to find a better approximation for $\#\mathcal{D}[i]$ and to improve the lower bound $g(i)$. Finally, we can see the behaviour of $E(z)$ compared to its upper bound (2.30), and to its lower bound (see (5.6) and (5.8)) in the last two columns of Table 1.

(Note that in our discussion we should omit the last row of the table since it corresponds to a search range such that $3 \leq D \leq 2^{27}$, whereas we run our experiments for $D \leq 13 \cdot 10^7 < 2^{27}$.)

i	$\#\mathcal{D}[i]$	$\#\mathcal{D}_{24}[i]$	$\#\mathcal{D}_{24,q,n}[i]$	$\frac{\#\mathcal{D}_{24}[i]}{\#\mathcal{D}[i]}$	$\frac{1}{15}\frac{\#\mathcal{D}[i]}{f(i)}$	$\frac{1}{13}\frac{g(i)}{\#\mathcal{D}_{24}[i]}$	$\frac{10\cdot\#\mathcal{D}_{24,q,n}[i]}{\sqrt{2^i}}$	$\frac{1}{7}\frac{\#\mathcal{D}_{24,q,n}[i]}{\sigma(2^i)}$
1	0	0	0					
2	0	0	0					
3	0	0	0					
4	0	0	0					
5	0	0	0					
6	1	1	3	1	0.9939	1.1837	3.7500	0.3815
7	1	1	3	1	0.5530	2.0292	2.6516	0.3672
8	3	3	6	1	0.9099	1.1837	3.7500	0.6782
9	6	5	7	0.8333	0.9873	1.2626	3.0935	0.7081
10	11	9	8	0.8181	0.9736	1.2626	2.5000	0.7065
11	20	16	14	0.8000	0.94562	1.2913	3.0935	1.0579
12	37	30	15	0.8108	0.9290	1.2626	2.3437	0.9538
13	71	58	19	0.8169	0.9422	1.2057	2.0992	1.0026
14	136	107	21	0.7868	0.9500	1.2137	1.6406	0.9087
15	258	212	27	0.8217	0.9452	1.1435	1.4915	0.9484
16	498	405	32	0.8132	0.9540	1.1223	1.2500	0.9043
17	964	796	41	0.8257	0.9630	1.0749	1.1324	0.9249
18	1866	1511	49	0.8097	0.9697	1.0696	0.9570	0.8763
19	3624	2903	64	0.8010	0.9776	1.0548	0.8838	0.9017
20	7058	5619	81	0.7961	0.9864	1.0354	0.7910	0.8942
21	13765	10872	112	0.7898	0.9949	1.0193	0.7733	0.9639
22	26857	21027	148	0.7829	1.0024	1.0062	0.7226	0.9885
23	52484	40732	191	0.7760	1.0101	0.9937	0.6594	0.9859
24	102673	79446	258	0.7737	1.0176	0.9764	0.6298	1.0253
25	201040	154715	330	0.7695	1.0249	0.9627	0.5696	1.0062
26	394039	302129	440	0.7650	1.0344	0.9480	0.5371	1.0261
27	749310	572505	585	0.7640	1.0073	0.9636	0.5049	1.0403

Table 1: $k = 3$; see Algorithm 4 and (5.4), (5.6), (5.8) for definitions of f, g, σ

CHAPTER 6

Cryptographically Interesting Examples

Let the triple $(E/\mathbb{F}_q, n, k)$ represent an elliptic curve E such that E is defined over $\mathbb{F}_q$, $\#E(\mathbb{F}_q) = n = q + 1 - t$, and E has embedding degree k. We give some examples of $(E/\mathbb{F}_q, n, 6)$ where q and n are prime. In the examples given below we choose $q \approx 2^{160}$ because of the current requirements in the cryptographic applications.

Recall from Section 2.1.3 that in order to construct $(E/\mathbb{F}_q, n, 6)$ one should find a solution (x, y) to the equation

$$X^2 - DY^2 = -8, \quad D > 0,\ D' = D/3 \text{ is square free}$$

such that $x = 6l + 1$ or $x = 6l - 1$. If $x = 6l + 1$ we set $l = (x - 1)/6$ and check the primality of $q = 4l^2 + 1$ and $n = 4l^2 + 2l + 1$. If $x = 6l - 1$ we set $l = (x + 1)/6$ and check the primality of $q = 4l^2 + 1$ and $n = 4l^2 - 2l + 1$. Suppose that one of these primality conditions are satisfied for (q, n). Then $(E/\mathbb{F}_q, n, 6)$ with complex multiplication in $\mathbb{Q}(\sqrt{-D'})$ can be constructed as follows: First the Hilbert class polynomial $H_{-D'}(x)$ is computed ([**3**], p.150). Any root of $H_{-D'}(x)$ over $\mathbb{F}_q$, say j, is called the *j-invariant*, and an elliptic curve E with given j-invariant can be obtained by using the following lemma.

Lemma 6.1 ([**3**], Lemma VIII.3, p.153). *Let q be a prime. Then the following hold for elliptic curves over $\mathbb{F}_q$.*
(i) Every element in $\mathbb{F}_q$ is the j-invariant of an elliptic curve over $\mathbb{F}_q$.
(ii) Let $D > 4$ and $j \in \mathbb{F}_q$ with $j \neq 0, 1728$. Then all elliptic curves over $\mathbb{F}_q$ with j-invariant j are given by

$$y^2 = x^3 + 3sc^2x + 2sc^3$$

where $s = j/(1728 - j)$ and c is any element in $\mathbb{F}_q$.
(iii) Suppose E and E' have the same j-invariant j but are not isomorphic over the field $\mathbb{F}_q$. If $j \neq 0$ or 1728, then E' is the quadratic twist of E and if $\#E(\mathbb{F}_q) = q + 1 - t$ then $\#E'(\mathbb{F}_q) = q + 1 + t$.

Moreover, because of the efficiency in the implementations [**14**], we specifically look for elliptic curve equations of the form

$$E/\mathbb{F}_q : y^2 = x^3 - 3x + b, \quad b \in \mathbb{F}_q. \tag{6.1}$$

By Lemma 6.1.(ii), given q, n, D' and j as in Lemma 6.1-(ii), then choosing $c \in \mathbb{F}_q$ such that $3kc^2 = -3$ gives rise to an elliptic curve $E/\mathbb{F}_q$ with curve equation (6.1). Note that $\#E(\mathbb{F}_q) = q + 1 - t$ or $\#E(\mathbb{F}_q) = q + 1 + t$ by Lemma 6.1.(iii). The former case would give us the desired triple $(E/\mathbb{F}_q, n, 6)$ since $n = q + 1 - t$. The algorithm can be given as follows.

Algorithm 5 EC Generation

Input: $(q,\ t,\ D):\ 4q-t^2=(D/3)V^2$

Output: A set of isogenous, non-isomorphic elliptic curves with $\#E(\mathbb{F}_q)=q+1-t$ and curve equation (6.1)

```
$D' \leftarrow D/3$
compute $H_{-D'}(x)$
for each $j : H_{-D'}(j)=0$ in $\mathbb{F}_q$ do
  $s \leftarrow j/(1728-j)$
  if $(-1/s)$ is a square in $\mathbb{F}_q$ then
    $c \leftarrow \sqrt{-1/s}$
    $b \leftarrow 2sc^3$
    $E \leftarrow y^2 = x^3-3x+b$
    if $\#E = q+1-t$ then
      Output: $E$
    end if
  end if
end for
```

Note that given parameters (q,t,D) we may not always be able to find a curve equation of the form (6.1). In general, for given (q,t,D) (where $n=q+1-t, q$ are primes, $4q-t^2=DV^2, q^k \equiv 1 \pmod{n}$, and $D'=D/3$), let R be the the number of distinct roots of $H_{-D'}(x)$ over $\mathbb{F}_q$. Then we may expect that the number of non-isomorphic elliptic curves $(E/\mathbb{F}_q,n,k)$ with curve equation of the form (6.1) is

$$(1/2)(1/2)R. \tag{6.2}$$

The first factor $(1/2)$ is because of the fact that $(-1/s)$ must be a square in $\mathbb{F}_q$, and the second factor $(1/2)$ is because of the fact that the obtained elliptic curve has order either $q+1-t$ or $q+1+t$. Hence, given (q,t), if Algorithm 5 does not succeed to find an elliptic curve then we may need to relax the condition (6.1) and construct other elliptic curves.

Now, we give some examples $(E/\mathbb{F}_q,n,6)$ satisfying (6.1), and $q \approx n \approx 2^{163}$. The parameters q, t, and D in the examples are obtained using Algorithm 3. Note that the parameters already guarantee that the embedding degree is 6. Then the elliptic curves are constructed using Algorithm 5.

Example 6.1. *If $D=3D'=3\cdot 3\cdot 602489$ then for*
$q=6409832084579048520099972164544618793148521015057$*, and*
$n=6409832084579048520099969632780000077765548633973$*, we have*

$$4q-t^2=(3)\cdot(602489)\cdot(326173568658181984415 3)^2.$$

The Hilbert class polynomial $H_{-D'}$ is a 234th degree polynomial and we denote its roots over $\mathbb{F}_q$ by j_i for $1 \le i \le 234$.
1. One triple $(j_1,s_1,c_1):\ s_1=j_1/(1728-j_1),\ 3s_1c_1^2=-3$ can be given as

$$\begin{aligned} j_1 &= 5588945237810751704052174660973282911676679 52084, \\ s_1 &= 6337638885562738737659376147650853771198981874925, \\ c_1 &= 4547195893538903524295645367021365051863034819249 \end{aligned}$$

which leads to the elliptic curve with embedding degree $k = 6$:

$$E_1/\mathbb{F}_q: \ y^2 = x^3 - 3x + 37252723820802899916086535950465074825709723916 16.$$

2. Another triple $(j_2, s_2, c_2): \ s_2 = j_2/(1728 - j_2), \ 3s_2c_2^2 = -3$ can be given as

$$\begin{aligned} j_2 &= 5560874278238032820206557608749608568238909863 64, \\ s_2 &= 20195621803164542288496418015632109762056502688 70, \\ c_2 &= 6405541916102174689219590515151681488684959286604 \end{aligned}$$

which leads to the elliptic curve with embedding degree $k = 6$:

$$E_2/\mathbb{F}_q: \ y^2 = x^3 - 3x + 8580336953747661760763298785874608927123456906.$$

3. Another triple $(j_3, s_3, c_3): \ s_3 = j_3/(1728 - j_3), \ 3s_3c_3^2 = -3$ can be given as

$$\begin{aligned} j_3 &= 7324726030870967548191927668337526414705539137 26, \\ s_3 &= 16280605325454837563694246686286808132076669048 84, \\ c_3 &= 1306765472096623448859897527422769434446815629623 \end{aligned}$$

which leads to the elliptic curve with embedding degree $k = 6$:

$$E_3/\mathbb{F}_q: \ y^2 = x^3 - 3x + 3796301140385801622380177109699079924254889755811.$$

Similarly, we can produce (at most) 234 non-isomorphic triple $(E/\mathbb{F}_q, n, 6)$ satisfying (6.1).

We give a list of parameters for $(E/\mathbb{F}_q, n, 6)$ in Table 1, where $4q - t^2 = 4n - (t-2)^2 = D'V^2$ for some V. The parameters were obtained by running Algorithm 3 exhaustively with inputs $160 \leq N \leq 300$ and $z = 8/3{\cdot}10^7$. The integer n is coded with its hexadecimal representation in the table.

Note that, by Proposition 2.4, each parameter for an isogeny class of elliptic curves with embedding degree $k = 6$ also leads to an isogeny class of elliptic curves with embedding degree $k = 4$. We close this chapter by giving an application of Proposition 2.4.

EXAMPLE 6.2. *If $D = 3D' = 3 \cdot 3 \cdot 602489$ then for*
$q = 640983208457904852009996963278000007776554863397 3$, *and*
$n = 6409832084579048520099972164544618793148521015057$, *we have*

$$4q - t^2 = (3) \cdot (602489) \cdot (326173568658181984415 3)^2.$$

The Hilbert class polynomial $H_{-D'}$ is a 234th degree polynomial and we denote its roots over $\mathbb{F}_q$ by j_i for $1 \leq i \leq 234$.
1. One triple $(j_1, s_1, c_1): \ s_1 = j_1/(1728 - j_1), \ 3s_1c_1^2 = -3$ can be given as

$$\begin{aligned} j_1 &= 2053824867597561027313452699234091194976770950 11, \\ s_1 &= 10300742724147460702270329374610914410240206800 54, \\ c_1 &= 4913131820296422278034456914854176685888512376772 \end{aligned}$$

which leads to the elliptic curve with embedding degree $k = 4$:

$$E_1/\mathbb{F}_q: \ y^2 = x^3 - 3x + 2993400528565252484131025435851646783754072514402.$$

$\log_2(q)$	n	t	D'
161	155FCBA17D27DBF83AF9FD356017E52DC96BA3B93	−1397283740559671498201549	12574563
163	462C2CFB8DAF4B2900F9D0C24FF03527FF496EF75	2531764618715382972381085	1807467
203	72910E9DFC2C47EB63868A3D9A3350AA45CC9DB1D98E38979F5	−3392099969120518114320071409379	1060147
204	D6A9E1C9B05FD8BEBE17E7BB1F2FE140314E9F9AD763E360EDD	−4643214861269453164637057497163	20902979
206	23D95C1E7E1B4C336BF5D823283F1905EB83CD664F6436C345C9	−7589942119653545518047831928199	9877443
224	8EB4FCF5E831AC7AB5918D6AB621AF5A6691BB9C34648F2259467B0D	3876699577473734869516699942644997	496659
226	3AEBF8126FF428B6BE9B3F101636B6DB7BB24DA229ADBB6CD6E335CAB	−9964083456805723098430155805814405	16460547
261	14749107E42C9FB1D262AE514706F39BABD560AC355577B56320985934B2B5C1AB	1539014724578737543627323023405643880571	15496387
263	4AB39EA921C86AEA4EB6C0239014EB4E9E6C7F29DAECE6535390069F5599A34191	2941064251695286479215216871059617419121	17960923
296	CA6E1A83814CC9334C6BAD8A2D4EAED740FA60ECA58583813EED642FE2DA370A54997EABE9	317290385189035493455173766896601332896354905	1695003

Table 1: list of parameters for $k = 6$

CHAPTER 7

Conclusion

In our work, we gave a detailed analysis of prime order elliptic curves with embedding degree $k = 3, 4, 6$ which are so called MNT curves. Finding suitable parameters for such curves is closely related to finding solutions to certain Pell equations. We provided necessary and sufficient conditions for solubility of the equations $X^2 - DY^2 = m$ for $(D, m) = (3D', -8)$, and $(D, m) = (3D', 24)$. In particular, using the sufficency condition, we were able to give a heuristic lower bound for the number of Pell equations which have integer solutions.

We also presented explicit algorithms to obtain MNT curve parameters and to construct these curves. An upper bound for the expected number of isogeny classes of MNT curves $(E(z))$ was known before and we gave a lower bound for $E(z)$. We compared these theoretical findings with experimental results that we obtained by running our algorithms for certain ranges. Our comparisons showed that it is quite possible to find a precise approximation for $E(z)$.

Moreover, we gave a list of new cryptographically interesting elliptic curve parameters.

One possible direction for work would be finding a tight approximation for $E(z)$. Finding necessary and sufficient conditions (depending on D and m) for solubility of a larger family of Pell equations $X^2 - DY^2 = m$ would be another interesting research problem.

Bibliography

[1] P. S. L. M. Barreto, B. Lynn, and M. Scott, *Constructing elliptic curves with prescribed embedding degrees*, SCN'2002, Lecture Notes in Computer Science **2576** (2002), Springer, 263–273.

[2] P. S. L. M. Barreto and M. Naehrig, *Pairing-friendly elliptic curves of prime order*, SAC 2005, Lecture Notes in Computer Science **3897** (2006), 319–331.

[3] I. Blake, G. Seroussi, and N. Smart, *Elliptic curves in cryptography*, Cambridge University Press, Cambridge, 1999.

[4] C. Cocks and R.G.E. Pinch, *Identity-based cryptosystems based on the Weil pairing*, unpublished manuscript, 2001.

[5] H. Cohen and H.W. Lenstra, *Heuristics on class groups of number fields*, In Number Theory, Lecture notes in Mathematics **1068** (1983), Springer–Verlag, 33–62.

[6] 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.

[7] 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.

[8] R. Dupont, A. Enge, and F. Morain, *Building curves with arbitrary small MOV degree over finite prime fields*, Journal of Cryptology **18** (2005), Springer–Verlag, 79–89.

[9] D. Freeman, *Methods for constructing pairing friendly elliptic curves*, 10th Workshop on ECC Fields Institute, 19 Sept 2006, available at `www.cacr.math.uwaterloo.ca/conferences/2006/ecc2006/freeman.pdf`.

[10] ———, *Constructing pairing-friendly elliptic curves with embedding degree 10*, ANTS-VII, Lecture Notes in Computer Science **4076** (2006), Springer, Berlin, 452–465.

[11] G. Frey and H. G. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. **62** (1994), 865–874.

[12] S. Galbraith, J. McKee, and P. Valenca, *Ordinary abelian varieties having small embedding degree*, Proceedings of a workshop on Mathematical Problems and Techniques in Cryptology, CRM Barcelona (2005), 29–45.

[13] G. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Clarendon Press, Oxford, 1968.

[14] IEEE, *Computer society, IEEE standard specifications for public key cryptography*, IEEE Std (2000), 1363–2000.

[15] A. Joux, *A one round protocol for tripartite Diffie-Hellman*, Proc. of ANTS IV, Lecture Notes in Computer Science **1838** (2000), Springer, 383–394.

[16] R. Lercier, *Discrete logarithms in GF(p)*, Posting to NMBRTHRY List (2005), available at `http://www.medicis.polytechnique.fr/~lercier/file/nmbrJL05a.html`.

[17] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge, 1986.

[18] F. Luca and I. E. Shparlinski, *Elliptic curves with low embedding degree*, Journal of Cryptology **19** (2006), 553–562.

[19] ———, *On finite fields for pairing based cryptography*, Preprint (2006), 1–10.

[20] D. A. Marcus, *Number fields*, Springer-Verlag, New York, 1977.

[21] D. Matyukhin, *Discrete logarithm in GF(p)*, Posting to NMBRTHRY List (2006), available at `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0612&L=nmbrthry&T=0&P=2033`.

[22] A. Menezes, *An introduction to pairing-based cryptography*, Notes from lectures given in Santander, Spain, 2005, available at `http://www.cacr.math.uwaterloo.ca/~ajmeneze/publications/pairings.pdf`.

[23] 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.

[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] R. A. Mollin, *Fundamental number theory with applications*, CRC Press, Boca Raton, New York, 1998.

[26] ______, *Simple continued fraction solutions for Diophantine equations*, Expositiones Mathematicae **19** (2001), no. 1, 55–73.

[27] T. Nagell, *Introduction to number theory*, Wiley, New York, 1951.

[28] D. Page, N. Smart, and F. Vercauteren, *A comparison of MNT curves and supersingular curves*, Cryptology ePrint Archive, Report 2004/165 (2004), available at `eprint.iacr.org/2004/165.pdf`.

[29] J. P. Robertson, *Solving the generalized Pell equation $x^2 - dy^2 = n$*, 2004, available at `http://hometown.aol.com/jpr2718/`.

[30] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, Inc., 1986.

[31] H. te Riele and H. Williams, *New computations concerning the Cohen-Lenstra heuristics*, Experiment. Math. 12, iss. 1 (2003), 99–113.

[32] E. Thome, *Computation of discrete logarithms in $GF(2^{607})$*, Advances in Cryptology-ASIACRYPT 2001, Lecture Notes in Computer Science **2248** (2001), Springer, 107–124.