Title
Constructing pairing-friendly elliptic curves with embedding degree 10

Journal
ALGORITHMIC NUMBER THEORY, PROCEEDINGS, 4076

ISSN
0302-9743

Author
Freeman, D

Publication Date
2006

Peer reviewed

Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10.

David Freeman

University of California, Berkeley
dfreeman@math.berkeley.edu

Abstract. We present a general framework for constructing families of elliptic curves of prime order with prescribed embedding degree. We demonstrate this method by constructing curves with embedding degree $k = 10$, which solves an open problem posed by Boneh, Lynn, and Shacham [6]. We show that our framework incorporates existing constructions for $k = 3$, 4, 6, and 12, and we give evidence that the method is unlikely to produce infinite families of curves with embedding degree $k > 12$.

1 Introduction

A cryptographic pairing is a bilinear map between two groups in which the discrete logarithm problem is hard. In recent years, such pairings have been applied to a host of previously unsolved problems in cryptography, the most important of which are one-round three-way key exchange [13], identity-based encryption [5], and short digital signatures [6].

The cryptographic pairings used to construct these systems in practice are based on the Weil and Tate pairings on elliptic curves over finite fields. These pairings are bilinear maps from an elliptic curve group $E(\mathbb{F}_q)$ to the multiplicative group of some extension field $\mathbb{F}_{q^k}$. The parameter k is called the *embedding degree* of the elliptic curve. The pairing is considered to be secure if taking discrete logarithms in the groups $E(\mathbb{F}_q)$ and $\mathbb{F}_{q^k}^*$ are both computationally infeasible.

For optimal performance, the parameters q and k should be chosen so that the two discrete logarithm problems are of approximately equal difficulty when using the best known algorithms, and the order of the group $\#E(\mathbb{F}_q)$ should have a large prime factor r. For example, a pairing is considered secure against today's best attacks when $r \sim 2^{160}$ and $k \sim$ 6-10, depending on the application. In order to vary the security level or adapt to future improvements in discrete log technology, we would like to have a supply of elliptic curves at our disposal for arbitrary q and k.

Many researchers have examined the problem of constructing elliptic curves with prescribed embedding degree. Menezes, Okamoto, and Vanstone [16] showed that a supersingular elliptic curve must have embedding degree $k \leq 6$, and furthermore $k \leq 3$ in characteristic not equal to 2 or 3. Miyaji, Nakabayashi, and

Takano [17] have given a complete characterization of ordinary elliptic curves of prime order with embedding degree $k = 3$, 4, or 6, while Barreto and Naehrig [2] give a construction for curves of prime order with $k = 12$. There is a general construction, originally due to Cocks and Pinch [8], for curves of arbitrary embedding degree k, but in this construction the sizes of the field $\mathbb{F}_q$ and the subgroup of prime order r are related by $q \approx r^2$, which leads to inefficient implementation. Recent efforts (cf. [7], [10]) have focused on reducing the ratio $\rho = \log q / \log r$ for arbitrary k, but no additional examples have been found with ρ small enough to allow for curves of prime order.

The focus of this paper is the construction of ordinary elliptic curves of prime order with prescribed embedding degree. In Section 2 we present a general framework for constructing such curves and give conditions under which this method will give us infinite families of elliptic curves. The method is based on the Complex Multiplication method of curve construction [19] and is implicit in the constructions of several other researchers. Our contribution is to gather all of the relevant results in one place and to define terminology that makes it apparent that these various constructions are all instances of the same general method.

Our main contribution appears in Section 3, where we show how the method of Section 2 can be used to construct curves with embedding degree $k = 10$. We give examples of such curves over fields of cryptographic size, solving an open problem posed by Boneh, Lynn, and Shacham [6].

In Section 4 we show how the existing constructions of elliptic curves of prime order with embedding degree $k = 3$, 4, 6, or 12 can be explained via the framework of Section 2. In Section 5, we show that for $k > 6$, our method is not likely to give additional infinite families of elliptic curves with the specified embedding degree. We note, however, that examples of such families exist for $k = 10$ and $k = 12$, and we ask in Section 6 if such examples can be constructed in a systematic fashion.

Acknowledgments

Research for this paper was conducted during a summer internship at Hewlett-Packard Laboratories, Palo Alto. I thank Vinay Deolalikar for suggesting this topic and for providing advice and support along the way. I also thank Gadiel Seroussi for bringing me to HP and for supporting my research.

I thank Paulo Barreto, Steven Galbraith, Ed Schaefer, and Mike Scott for their valuable feedback on earlier versions of this paper. I am especially indebted to Mike Scott, who used the method presented in Section 3 to compute examples of elliptic curves of cryptographic size with embedding degree 10. Two of these curves now appear in this paper as Examples 3.5 and 3.6.

2 A Framework for Constructing Pairing-Friendly Elliptic Curves

In this section we describe a general framework for constructing elliptic curves of a given embedding degree k. This framework is implicit in the constructions of Miyaji, Nakabayashi, and Takano [17]; Barreto, Lynn, and Scott [1]; Cocks and Pinch [8] (as explained in [4]); and Brezing and Weng [7]. After stating the relevant results, we define terminology that will allow us to show that these constructions are all specific cases of the same general method.

To construct our elliptic curves, we parameterize the number of points on the curve and the size of the field of definition by polynomials $n(x)$ and $q(x)$, respectively. For each x_0 that gives prime values for $n(x_0)$ and $q(x_0)$, we can use the Complex Multiplication method to construct an elliptic curve with the desired properties. The main result of this section is Theorem 2.7, which gives a criterion for the existence of infinite families of such good parameters.

We begin by giving a formal definition of embedding degree.

Definition 2.1. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, and let n be a prime dividing $\#E(\mathbb{F}_q)$. The embedding degree of E with respect to n is the smallest integer k such that n divides $q^k - 1$.*

Equivalently, k is the smallest integer such that $\mathbb{F}_{q^k}$ contains μ_n, the group of nth roots of unity in $\overline{\mathbb{F}}_q$. We often ignore n when stating the embedding degree, as it is usually clear from the context.

If we fix a target embedding degree k, we wish to solve the following problem: find a prime (power) q and an elliptic curve E defined over $\mathbb{F}_q$ such that $n = \#E(\mathbb{F}_q)$ is prime and E has embedding degree k. Furthermore, since we may wish to construct curves over fields of different sizes, we would like to be able to specify (approximately) the number of bits of q in advance.

We follow the strategy of Barreto and Naehrig [2] in parameterizing the trace of the curves to be constructed. Namely, we choose some polynomial $t(x)$, which will be the trace of Frobenius for our hypothetical curve, and construct polynomials $q(x)$ and $n(x)$ that are possible orders of the prime field and the elliptic curve group, respectively. More precisely, if $q(x_0)$ is prime for some x_0, we can use the Complex Multiplication method [3], [19] to construct an elliptic curve over $\mathbb{F}_{q(x_0)}$ with $n(x_0)$ points and embedding degree k.

Theorem 2.2. *Fix a positive integer k, and let $\Phi_k(x)$ be the kth cyclotomic polynomial. Let $t(x)$ be a polynomial with integer coefficients, let $n(x)$ be an irreducible factor of $\Phi_k(t(x) - 1)$, and let $q(x) = n(x) + t(x) - 1$. Let $f(x) = 4q(x) - t(x)^2$. Fix a positive square-free integer D, and suppose (x_0, y_0) is an integer solution to the equation $Dy^2 = f(x)$ for which*

1. *$q(x_0)$ is prime, and*
2. *$n(x_0)$ is prime.*

If D is sufficiently small, then there is an efficient algorithm to construct an elliptic curve E defined over $\mathbb{F}_{q(x_0)}$ such that $E(\mathbb{F}_{q(x_0)})$ has prime order $n(x_0)$ and E has embedding degree at most k.

Proof. By hypothesis, we have a solution (x_0, y_0) to the equation $Dy^2 = f(x)$ for which $q(x_0)$ is prime. If D is sufficiently small then the construction of an elliptic curve E over $\mathbb{F}_{q(x_0)}$ with $\#E(\mathbb{F}_{q(x_0)}) = n(x_0)$ is standard via the Complex Multiplication method; see [3] or [19] for details. Since $n(x_0)$ is prime, $E(\mathbb{F}_{q(x_0)})$ has prime order, and it remains only to show that E has embedding degree at most k. Barreto, Lynn, and Scott [1, Lemma 1] show that E having embedding degree k is equivalent to $n(x_0)$ dividing $\Phi_k(t(x_0) - 1)$ and $n(x_0)$ not dividing $\Phi_i(t(x_i) - 1)$ for $i < k$. Since we have chosen the polynomial $n(x)$ to divide $\Phi_k(t(x)-1)$, $n(x_0)$ is guaranteed to divide $q(x_0)^k - 1$, and the embedding degree of E is thus at most k. □

Remark 2.3. The fact that $n(x)$ does not divide $\Phi_i(t(x) - 1)$ as polynomials for $i < k$ does not guarantee that $n(x_0)$ does not divide $\Phi_i(t(x_0) - 1)$ as integers for some $i < k$. However, this latter case will be rare in practice, and thus the embedding degree of a curve constructed via the method of Theorem 2.2 will usually be k.

Remark 2.4. If we wish to construct curves whose orders are not necessarily prime but merely have a large prime factor, we may relax condition (2) of the theorem accordingly, and the same analysis holds.

In practice, to construct an elliptic curve with embedding degree k one chooses polynomials $t(x)$, $n(x)$, and $q(x)$ satisfying the conditions of Theorem 2.2 and tests various values of x until $n(x)$ and $q(x)$ are prime. If the distributions of the values of the polynomials $n(x)$ and $q(x)$ are sufficiently random, the Prime Number Theorem tells us that we should have to test roughly $\log n(x_1) \log q(x_1)$ values of x near x_1 until we find an x_0 that gives a prime value for both polynomials. Since the distribution of prime values of polynomials is not well understood in general, it will be hard to prove theorems that explicitly construct infinite families of elliptic curves of prime order. Rather, we will be slightly less ambitious and search for polynomials as in Theorem 2.2 that will give us the desired elliptic curves whenever the polynomials take on prime values. We incorporate this approach into the following definition.

Definition 2.5. *Let $t(x)$, $n(x)$, and $q(x)$ be polynomials with integer coefficients. For a given positive integer k and positive square-free integer D, the triple (t, n, q) represents a family of curves with embedding degree k if the following conditions are satisfied:*

1. *$n(x) = q(x) + 1 - t(x)$.*
2. *$n(x)$ and $q(x)$ are irreducible.*
3. *$n(x)$ divides $\Phi_k(t(x) - 1)$, where Φ_k is the kth cyclotomic polynomial.*
4. *The equation $Dy^2 = 4q(x) - t(x)^2$ has infinitely many integer solutions (x, y).*

Defining a family of curves in this way gives us a simple criterion for constructing elliptic curves with embedding degree k. This criterion is implicit in the Barreto-Naehrig construction of curves with $k = 12$ and $D = 3$ [2].

Corollary 2.6. *Suppose (t, n, q) represents a family of curves with embedding degree k for some D. Then for each x_0 such that $n(x_0)$ and $q(x_0)$ are both prime, there is an elliptic curve E defined over $\mathbb{F}_{q(x_0)}$ such that $\#E(\mathbb{F}_{q(x_0)})$ is prime, and E has embedding degree at most k.*

In practice, for any $t(x)$ we can easily find $n(x)$ and $q(x)$ satisfying conditions (1), (2), and (3) of Definition 2.5; the difficulty arises in choosing the polynomials so that $Dy^2 = 4q(x) - t(x)^2$ has infinitely many integer solutions. In general, if $f(x)$ is a square-free polynomial of degree at least 3, then there will be only a finite number of integer solutions to the equation $Dy^2 = f(x)$ (cf. Proposition 2.10). Thus we conclude that (t, n, q) can represent a family of curves only if $f(x)$ has some kind of special form.

We now show that if $f(x)$ is quadratic, then one integral solution to the equation $Dy^2 = f(x)$ will give us infinitely many solutions. This is the technique that Miyaji, et al. [17] use to produce curves with embedding degree 3, 4, or 6, and we will use the same technique in Section 3 to construct curves with embedding degree 10. The idea is as follows: we complete the square to write the equation $Dy^2 = f(x)$ as $u^2 - D'v^2 = T$ for some constant T, and observe that (u, v) is a solution to this equation if and only if $u + v\sqrt{D'}$ has norm T in the real quadratic field $\mathbb{Q}(\sqrt{D'})$. By Dirichlet's unit theorem, there is a one-dimensional set of norm-one integral elements of this field; multiplying each of these units by our element of norm T gives an infinite family of elements of norm T. We then show that a certain fraction of these elements can be converted back to solutions of the original equation.

Theorem 2.7. *Fix an integer $k > 0$, and choose polynomials $t(x)$, $n(x)$, $q(x) \in \mathbb{Z}[x]$ satisfying conditions (1), (2), and (3) of Definition 2.5. Let $f(x) = 4q(x) - t(x)^2$. Suppose $f(x) = ax^2 + bx + c$, with $a, b, c \in \mathbb{Z}$, $a > 0$, and $b^2 - 4ac \neq 0$. Let D be a square-free integer such that aD is not a square. If the equation $Dy^2 = f(x)$ has a solution (x_0, y_0) in the integers, then (t, n, q) represents a family of curves with embedding degree k.*

Proof. Completing the square in the equation $Dy^2 = f(x)$ and multiplying by $4a$ gives

$$aD(2y)^2 = (2ax + b)^2 - (b^2 - 4ac). \tag{2.1}$$

If we write $aD = D'r^2$ with D' square-free and make the substitutions $u = 2ax + b$, $v = 2ry$, $T = b^2 - 4ac$, the equation becomes

$$u^2 - D'v^2 = T. \tag{2.2}$$

Note that since aD is not a square, we have $D' > 1$.

Under the above substitution, a solution (x_0, y_0) to the original equation $Dy^2 = f(x)$ gives an element $u_0 + v_0\sqrt{D'}$ of the real quadratic field $\mathbb{Q}(\sqrt{D'})$ with norm T. Furthermore, this solution satisfies the congruence conditions

$$\begin{aligned} u_0 &\equiv b \pmod{2a} \\ v_0 &\equiv 0 \pmod{2r}. \end{aligned} \tag{2.3}$$

We wish to find an infinite set of solutions (u, v) satisfying the same congruence conditions, for we can transform such a solution into an integer solution to the original equation. To find such solutions we employ Dirichlet's unit theorem [20, §1.7], which tells us that the integer solutions to the equation $\alpha^2 - D'\beta^2 = 1$ are in one-to-one correspondence with the real numbers $\alpha+\beta\sqrt{D'} = \pm(\alpha_0+\beta_0\sqrt{D'})^n$ for some fixed (α_0, β_0) and any integer n. The real number $\alpha_0 + \beta_0\sqrt{D'}$ is either a fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{D'})$ or (if the norm of the fundamental unit is -1) the square of a fundamental unit.

Reducing the coefficients of $\alpha_0 + \beta_0\sqrt{D'}$ modulo $2a$ gives an element $z = \bar{\alpha}_0 + \bar{\beta}_0\bar{x}$ of the ring

$$R = \frac{\mathbb{Z}[x]}{(2a, x^2 - D')}. \tag{2.4}$$

Furthermore, since $(\alpha_0 + \beta_0\sqrt{D'})(\alpha_0 - \beta_0\sqrt{D'}) = 1$, z is invertible in R, i.e. $z \in R^*$. Since R^* is a finite group of size less than $4a^2$, there is an integer $m < 4a^2$ such that $z^m = 1$ in R^*.[1] Lifting back up to the full ring $\mathbb{Z}[\sqrt{D'}]$, we see that $(\alpha_0 + \beta_0\sqrt{D'})^m = \alpha_1 + \beta_1\sqrt{D'}$ for integers α_1, β_1 satisfying

$$\begin{aligned} \alpha_1 &\equiv 1 \pmod{2a}, \\ \beta_1 &\equiv 0 \pmod{2a}. \end{aligned} \tag{2.5}$$

Now for any integer n we can compute integers (u, v) such that

$$u + v\sqrt{D'} = (u_0 + v_0\sqrt{D'})(\alpha_1 + \beta_1\sqrt{D'})^n. \tag{2.6}$$

We claim that (u, v) satisfy the congruence conditions (2.3). To see this, let $\alpha_n+\beta_n\sqrt{D'} = (\alpha_1+\beta_1\sqrt{D'})^n$. The conditions (2.5) imply that $\alpha_n \equiv 1 \pmod{2a}$ and $\beta_n \equiv 0 \pmod{2a}$. Combining this observation with the formulas

$$\begin{aligned} u &= \alpha_n u_0 + \beta_n v_0 D' \\ v &= \alpha_n v_0 + \beta_n u_0, \end{aligned} \tag{2.7}$$

we see that $u \equiv u_0 \equiv b \pmod{2a}$ and $v \equiv v_0 \pmod{2a}$. Furthermore, $v_0 \equiv 0 \pmod{2r}$ and $2r$ divides $2a$ (since $aD = D'r^2$ and D is square-free), so we conclude that $v \equiv 0 \pmod{2r}$.

The new solution (u, v) thus satisfies the congruence conditions (2.3). Any integer n gives such a solution, so by setting $x = (u - b)/2a$ and $y = v/2r$ for

[1] In fact, since z is an element of the norm-one subgroup of R^*, m is bounded above by $2^s a$, where s is the number of distinct primes dividing $2a$. A more detailed study of the group R^* appears in an earlier draft of this paper [11].

each such (u, v), we have generated an infinite number of integer solutions to the equation $Dy^2 = f(x)$. This is condition (4) of Definition 2.5; by hypothesis (t, n, q) satisfy conditions (1), (2), and (3), so we conclude that (t, n, q) represents a family of curves with embedding degree k. □

Remark 2.8. More generally, we may find an infinite family of curves in the case where $f(x) = g(x)^2 h(x)$, with $h(x)$ quadratic. Specifically, if we let $y = y'g(x)$, then given one integral solution (x, y') to the equation $Dy'^2 = h(x)$ we may use the method of Theorem 2.7 to find an infinite number of solutions. However, we currently know of no examples for which $f(x)$ is of this form.

Theorem 2.7 tells us that if $f(x)$ is quadratic and square-free, we may get a family of curves of the prescribed embedding degree for *each* D. If $f(x)$ is instead a linear function times a square, then we may still get a family of curves, but for only a single D. This is the method that Barreto and Naehrig [2] use to construct curves with $k = 12$ (see Section 4.2).

Proposition 2.9. *Fix an integer $k > 0$, and let $n(x)$, $t(x)$, and $q(x)$ be polynomials in $\mathbb{Z}[x]$ satisfying conditions (1), (2), and (3) of Definition 2.5. Let $f(x) = 4q(x) - t(x)^2$, and suppose $f(x) = (Ax + D)g(x)^2$ for some positive integer D and some polynomial $g(x)$. Then (t, n, q) represents a family of curves with embedding degree k.*

Proof. For any integer v, we set $x = ADv^2 + 2Dv$ and let $y = (Av + 1)g(x)$. An easy computation shows that (x, y) is a solution to the equation $Dy^2 = f(x)$, so if D is square-free then condition (4) is satisfied for the integer D. If D is not square-free then we may absorb its square factors into y, and condition (4) is satisfied for the largest square-free factor D' of D. □

We conclude this section with a partial converse to Theorem 2.7; namely, if the degree of $f(x)$ is at least 3, then we are unlikely to find an infinite family of curves.

Proposition 2.10. *Let (t, n, q) be polynomials with integer coefficients satisfying conditions (1), (2), and (3) of Definition 2.5, and let $f(x) = 4q(x) - t(x)^2$. Suppose $f(x)$ is square-free and* $\deg f(x) \geq 3$. *Then (t, n, q) does not represent a family of elliptic curves with embedding degree k.*

Proof. Since $f(x)$ is square-free (i.e. has no double roots) and has degree at least 3, the equation $Dy^2 = f(x)$ defines a smooth affine plane curve of genus $g \geq 1$. By Siegel's Theorem (cf. [23, Theorem IX.4.3] and [9, §I.2]) such curves have a finite number of integral points, so condition (4) is not satisfied. □

3 Elliptic Curves with Embedding Degree 10.

In this section, we use the method of Section 2, and Theorem 2.7 in particular, to construct elliptic curves of prime order with embedding degree 10. Our key

observation is that since the hypotheses of Theorem 2.7 require $f(x) = 4n(x) - (t(x) - 2)^2$ to be quadratic, we should choose $n(x)$ and $t(x)$ in such a way that the high-degree terms of $t(x)^2$ cancel out those of $4n(x)$; in particular, the degree of $t(x)$ must be half the degree of $n(x)$. We have discovered that for $k = 10$ there is a choice of $n(x)$ and $t(x)$ such that this is possible. The resulting construction of elliptic curves with embedding degree 10 solves an open problem posed by Boneh, Lynn, and Shacham [6, §4.5].

We begin by recalling that to construct a curve with embedding degree k, we must choose the number of points $n(x)$ and the trace $t(x)$ such that $n(x)$ is an irreducible factor of $\Phi_k(t(x) - 1)$, where Φ_k is the kth cyclotomic polynomial. If $k = 10$ and $t(x)$ is linear then $\Phi_k(t(x) - 1)$ is an irreducible quartic polynomial, so there is no hope of $f(x) = 4n(x) - (t(x) - 2)^2$ being quadratic. If $k = 10$ and $t(x)$ is quadratic, Galbraith, McKee, and Valença [12] show that in this case $\Phi_k(t(x)-1)$ either is irreducible of degree 8 or factors into two irreducible quartic polynomials. They then show that there is an infinite set of $t(x)$ such that the latter occurs, and that these $t(x)$ are parameterized by the rational points of a certain elliptic curve. By experimenting with some of the examples given by Galbraith, et al., we discovered that $t(x) = 10x^2 + 5x + 3$ leads to a quadratic $f(x)$.

Theorem 3.1. *Fix a positive square-free integer D relatively prime to 15. Define $t(x)$, $n(x)$, and $q(x)$ by*

$$\begin{aligned} t(x) &= 10x^2 + 5x + 3 \\ n(x) &= 25x^4 + 25x^3 + 15x^2 + 5x + 1 \\ q(x) &= 25x^4 + 25x^3 + 25x^2 + 10x + 3. \end{aligned}$$

If the equation $u^2 - 15Dv^2 = -20$ has a solution with $u \equiv 5 \pmod{15}$, then (t, n, q) represents a family of curves with embedding degree 10.

Proof. It is easy to verify that conditions (1)-(3) of Definition 2.5 hold. Condition (4) requires an infinite number of integer solutions to $Dy^2 = f(x)$, where $f(x) = 4q(x) - t(x)^2$. The key observation is that for this choice of t and n,

$$f(x) = 4q(x) - t(x)^2 = 15x^2 + 10x + 3. \tag{3.1}$$

Multiplying by 15 and completing the square transforms the equation we wish to solve into

$$D'y^2 = (15x + 5)^2 + 20, \tag{3.2}$$

where $D' = 15D$. Integer solutions to this equation correspond to integer solutions to $u^2 - D'v^2 = -20$ with $u \equiv 5 \pmod{15}$. By Theorem 2.7, if one such solution exists then an infinite number exist, so (t, n, q) represents a family of curves with embedding degree 10. □

To use the above result to construct curves with embedding degree 10, we choose a D and search for solutions to the equation $u^2 - 15Dv^2 = -20$ that give prime values for q and n. The following lemma, proposed by Mike Scott, speeds up this process by restricting the values of D that we can use.

Lemma 3.2. *Let $q(x)$ be as in Theorem 3.1. If (x, y) is an integer solution to $Dy^2 = 15x^2 + 10x + 3$ such that $q(x)$ is prime, then $D \equiv 43$ or $67 \pmod{120}$.*

Proof. If $x \equiv 0$ or $2 \pmod 3$ then $q(x)$ is divisible by 3, while if x is odd then $q(x)$ is even. Thus if $q(x)$ is prime, then $x \equiv 4 \pmod 6$.

To deduce the stated congruence for D, we consider the equation $Dy^2 = 15x^2 + 10x + 3$ modulo 3, 5, and 8. To begin, we have $Dy^2 \equiv x \equiv 1 \pmod 3$, so $D \equiv 1 \pmod 3$. Next, we have $Dy^2 \equiv 3 \pmod 5$, so $y^2 \equiv 1$ or $4 \pmod 5$ and $D \equiv 2$ or $3 \pmod 5$. Finally, since x is even we see that $Dy^2 = 3 \pmod 8$, and thus $y^2 \equiv 1 \pmod 8$ and $D \equiv 3 \pmod 8$. Combining these results via the Chinese remainder theorem, we conclude that $D \equiv 43$ or $67 \pmod{120}$. □

After reading an earlier draft of this paper [11], Mike Scott used Theorem 3.1 and Lemma 3.2 to find examples of elliptic curves with embedding degree 10 via the following algorithm.

Algorithm 3.3 *Let (t, n, q) be as in Theorem 3.1. The following algorithm takes inputs* `MaxD`*,* `MinBits`*, and* `MaxBits`*, and outputs pairs (D, x) such that $D <$* `MaxD`*, the number of bits in $q(x)$ is between* `MinBits` *and* `MaxBits`*, and (D, x) satisfy the conditions of Corollary 2.6 with $k = 10$.*

1. *Set D to be a positive integer such that $D \equiv 43$ or $67 \pmod{120}$ and $15D$ is square-free.*
2. *Use the Continued Fraction algorithm [21] to compute a fundamental unit γ of the ring of integers in $\mathbb{Q}(\sqrt{15D})$. Let $\delta = \gamma^2$ if γ has norm -1, $\delta = \gamma$ otherwise.*
3. *Use the algorithm of Lagrange, Matthews [15], and Mollin [18] to find fundamental solutions (u, v) to the equation $u^2 - 15Dv^2 = -20$. (See also [21].)*
4. *For each fundamental solution (u, v) found in (3):*
   (a) *If $\log_2 u >$ (`MaxBits` $+ 11)/4$, go to the next fundamental solution.*
   (b) *If $u \equiv \pm 5 \pmod{15}$ and $\log_2 u >$ (`MinBits` $+ 11)/4$, then:*
      i. *Let $x = (-5 \pm u)/15$.*
      ii. *If $q(x)$ and $n(x)$ are prime, output (D, x).*
   (c) *Multiply $u + v\sqrt{15D}$ by δ to get a new u, and return to step (a).*
5. *Increase D. If $D <$* `MaxD`*, return to step (1); otherwise terminate.*

Remark 3.4. The bounds on $\log_2 u$ in Step 4 can be explained as follows: since $q(x) = 25x^4 + O(x^3)$ and $x = (-5 \pm u)/15$, $q(x)$ grows roughly like $u^4/2025$. We conclude that $\log_2 q(x) \approx 4 \log_2 u - 11$, so we require u in the algorithm to satisfy

$$\frac{\texttt{MinBits} + 11}{4} < \log_2 u < \frac{\texttt{MaxBits} + 11}{4}.$$

In our construction of Algorithm 3.3, the specific parameters of Theorem 3.1 have allowed us to simplify the procedure described in the proof of Theorem 2.7. The requirement that $15D$ be square-free implies that $r = 1$, and the fact that $b = 10$ is even allows us to remove the factors of 2 in the congruence moduli of equations (2.3). Thus in Step 4 we need only to find (u, v) with $u^2 - 15Dv^2 = -20$

and $u \equiv \pm 5 \pmod{15}$. Given this requirement, we see that the only restriction on the unit $\delta = \alpha + \beta\sqrt{15D}$ in Step 4c is that $\alpha \neq 0 \pmod 3$, which must be true since $\alpha^2 - 15D\beta^2 = 1$. Thus our choice of $\delta = \gamma$ or γ^2 will always give new solutions (u, v) with $u \equiv \pm 5 \pmod{15}$; i.e. the parameter m of Theorem 2.7 is equal to 1.

In practice the fundamental unit γ computed in Step 2 will usually be very large, in which case we may skip Step 4c altogether. For example, computations with PARI indicate that when $D \approx 10^9$, γ has at least 100 bits 99.5% of the time and at least 200 bits 98.9% of the time.

Scott ran Algorithm 3.3 with inputs $\texttt{MaxD} = 2 \cdot 10^9$, $\texttt{MinBits} = 148$, and $\texttt{MaxBits} = 512$. For each (D, x) output by the algorithm, one may then use the Complex Multiplication method (cf. [3], [19]) to construct an elliptic curve over $\mathbb{F}_{q(x)}$ whose number of points is $n(x)$. By Theorem 2.2 this curve has embedding degree at most 10, and in practice we find that the embedding degree is exactly 10. Below are two examples of elliptic curves that Scott constructed in this manner.

Example 3.5. (A 234-bit curve.) Running Algorithm 3.3 with $D = 1227652867$ produces the following example. Let q, n, A, B be as follows:

$$\begin{aligned} q &= 18211650803969472064493264347375950045934254696657090420726230043203803 \\ n &= 18211650803969472064493264347375949776033155743952030750450033782306651 \\ A &= -3 \\ B &= 15748668094913401184777964473522859086900831274922948973320684995903275. \end{aligned}$$

Then q and n are 234-bit prime numbers such that the curve $y^2 = x^3 + Ax + B$ defined over $\mathbb{F}_q$ has n points. Since $n \mid q^{10} - 1$ and $n \nmid q^i - 1$ for $i < 10$, this curve has embedding degree 10.

Example 3.6. (A 252-bit curve.) Running Algorithm 3.3 with $D = 1039452307$ produces the following example. Let q, n, A, B be as follows:

$$\begin{aligned} q &= 64623109973488169622031249105052520826733388469664312016352626944028254616 43 \\ n &= 64623109973488169622031249105052520825125618461566285955627764593062921012 61 \\ A &= -3 \\ B &= 49465381666402513742746288202696941442491817760131548632880862120768085281 41. \end{aligned}$$

Then q and n are 252-bit prime numbers such that the curve $y^2 = x^3 + Ax + B$ defined over $\mathbb{F}_q$ has n points. Since $n \mid q^{10} - 1$ and $n \nmid q^i - 1$ for $i < 10$, this curve has embedding degree 10.

Ideally, the bit size of curves with embedding degree 10 should be chosen so that the discrete logarithm in the finite field $\mathbb{F}_{q^{10}}$ is approximately of the same difficulty as the discrete logarithm problem on an elliptic curve of prime order over $\mathbb{F}_q$. Using the best known discrete logarithm algorithms, this happens when q has between 220 and 250 bits [3]. The curves in Examples 3.5 and 3.6 have

been selected so that their bit sizes are close to this range and their complex multiplication discriminants D are not much larger than 10^9. The equation for a curve with this size D can be computed in about a week on today's fastest PCs.

In practice, it appears that curves with small embedding degree, prime order, and small complex multiplication discriminant D are quite rare. Luca and Shparlinski [14] come to this conclusion for curves with embedding degree 3, 4, or 6 (the so-called MNT curves) through a heuristic analysis of the MNT construction. Since our construction of curves with embedding degree 10 is similar to the MNT construction (cf. Section 4.1), a similar analysis should hold for our $k = 10$ curves. The experimental evidence supports this reasoning: Scott's execution of Algorithm 3.3 with $\texttt{MaxD} = 2 \cdot 10^9$ found only 23 curves with prime orders between 148 and 512 bits [22].

If we relax the condition on $n(x)$ in step 4(b)ii of Algorithm 3.3 and write $n = kr$ with r a large prime and k a small cofactor, then we may find a larger number of suitable curves. Scott also ran this version of the algorithm and found 101 curves with r between 148 and 512 bits, k at most 16 bits, and $D < 2 \cdot 10^9$ [22].

4 Elliptic Curve Families with Small Embedding Degree

In this section we show how the existing constructions of ordinary elliptic curves of prime order with embedding degree 3, 4, or 6 [17] or embedding degree 12 [2] can be explained via the framework of Section 2. The former uses Theorem 2.7, while the latter employs Proposition 2.9.

4.1 MNT Elliptic Curves

Miyaji, Nakabayashi, and Takano [17] have classified all ordinary elliptic curves of prime order with embedding degree 3, 4, and 6. Their theorem is as follows:

Theorem 4.1 ([17]). *Let E be an ordinary elliptic curve over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = n = q + 1 - t$ is prime and E has embedding degree $k = 3, 4,$ or 6. Then there exists an integer x such that t, n, and q are of the form specified in the following table:*

k	t	n	q
3	$-1 \pm 6x$	$12x^2 \mp 6x + 1$	$12x^2 - 1$
4	$-x$ *or* $x + 1$	$x^2 + 2x + 2$ *or* $x^2 + 1$	$x^2 + x + 1$
6	$1 \pm 2x$	$4x^2 \mp 2x + 1$	$4x^2 + 1$

This theorem fits into the framework of Section 2 as follows. To find an infinite family of curves via Theorem 2.7, we require $f(x)$ to be quadratic. Since $\deg \Phi_k(x) = 2$ for $k = 3$, 4, or 6, if we let $t(x)$ be any linear polynomial and $n(x)$ be the (irreducible) quadratic $\Phi_k(t(x) - 1)$ (with any constant factor divided out), then $f(x) = 4n(x) - (t(x) - 2)^2$ is quadratic. If $q(x) = n(x) + t(x) - 1$ is also irreducible and the equation $Dy^2 = f(x)$ has one solution, then (t, n, q)

satisfy the hypotheses of Theorem 2.7 and thus represent a family of curves with embedding degree k. Miyaji, et al. arrive at their stronger result by using the fact that $\#E(\mathbb{F}_q)$ is prime to show that any values of t, n, and q that give rise to such a curve must be of the specified form.

4.2 Elliptic Curves with Embedding Degree 12

Finally, we note that the Barreto-Naehrig construction [2] of curves with embedding degree 12 falls under the case of Proposition 2.9. Specifically, if $t(x) = 6x^2+1$, then $\Phi_{12}(t(x)-1) = n(x)n(-x)$, where $n(x) = 36x^4+36x^3+18x^2+6x+1$, and

$$f(x) = 4n(x) - (t(x)-2)^2 = 3(6x^2+4x+1)^2. \tag{4.1}$$

Since $q(x) = 36x^4 + 36x^3 + 12x^2 + 6x + 1$ is also irreducible, Proposition 2.9 tells us that if we set $D = 3$, then (t, n, q) represents a family of curves with embedding degree 12.

5 Higher Embedding Degrees

To construct families of elliptic curves with prescribed embedding degree, the method of Section 2 requires us to find an infinite number of integer solutions to an equation of the form $Dy^2 = f(x)$. In this section, we give evidence that in general the degree of $f(x)$ is large, and thus by Proposition 2.10 we are unlikely to find an infinite family of curves. We begin with a lemma that restricts the possible degrees of the polynomial $n(x)$; the lemma generalizes a result of Galbraith, et al. [12, Lemma 1].

Lemma 5.1. *Fix k, let $t(x)$ be a polynomial, and let $n(x)$ be an irreducible factor of $\Phi_k(t(x)-1)$. Then the degree of n is a multiple of $\varphi(k)$, where φ is the Euler phi function.*

Proof. Suppose $t(x)$ has degree d, so $\deg \Phi_k(t(x)-1) = d\varphi(k)$. Let θ be a root of $n(x)$, and let $\omega = t(\theta) - 1$. Then $\Phi_k(\omega) = 0$, so ω is a primitive kth root of unity. We thus have the inclusion of fields $\mathbb{Q}(\theta) \supset \mathbb{Q}(\omega) \supset \mathbb{Q}$. Since $[\mathbb{Q}(\theta) : \mathbb{Q}] = \deg n(x)$ and $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(k)$, we conclude that $\varphi(k)$ divides $\deg n(x)$. □

The key observation that allowed us to construct families of elliptic curves with embedding degree 10 was that if $f(x)$ is quadratic and $n(x)$ has degree greater than 2, then the polynomial $t(x)$ must be chosen so that the high degree terms of $t(x)^2$ cancel out those of $4n(x)$. The following proposition shows that this is in fact the only way to construct such families.

Proposition 5.2. *Suppose (t, n, q) represents a family of curves with embedding degree k, and suppose further that $f(x) = 4n(x) - (t(x)-2)^2$ is square-free. If $\varphi(k) \geq 4$, then*

$$\deg t(x) = \frac{1}{2}\deg n(x) = \frac{1}{2}\deg q(x). \tag{5.1}$$

Furthermore, if a is the leading coefficient of $t(x)$, then $a^2/4$ is the leading coefficient of $n(x)$ and $q(x)$.

Proof. Since $\varphi(k) \geq 4$, by Lemma 5.1 $\deg n(x) \geq 4$, and since $f(x)$ is square-free, by Proposition 2.10 $\deg f(x) \leq 2$. Since $f(x) = 4n(x) - (t(x) - 2)^2$, we conclude that $\deg t(x) = \frac{1}{2} \deg n(x)$, and since $n(x) = q(x) + 1 - t(x)$, we see that $\deg n(x) = \deg q(x)$. The observation about the leading coefficients follows immediately. □

As an immediate corollary, we see that if $k > 6$ (so $\varphi(k) \geq 4$) then choosing a linear $t(x)$ will not in general give us an infinite family of curves, whereas if $k > 12$ (so $\varphi(k) \geq 6$) then choosing a quadratic $t(x)$ will not in general give us an infinite family of curves.

Proposition 5.2 tells us that for embedding degrees k with $\varphi(k) \geq 4$, to find an infinite family of curves we will have to choose $t(x_0)$ of degree at least 2 such that $\phi_k(t(x) - 1)$ is not irreducible. Galbraith, McKee, and Valença [12] observe that this is hard even for quadratic $t(x)$, and as the degree increases the problem will only become more difficult. An alternative would be to choose t and n such that $f(x)$ has a square factor; this appears to be just as difficult, but has not been studied in depth.

6 Conclusion

We have seen in Section 2 that the current methods for constructing families of elliptic curves of prime order with prescribed embedding degree can all be subsumed under a general framework. In Section 3 we showed how this framework can be used to construct curves with embedding degree 10 and we gave examples of such curves, which have not previously appeared in the literature. In Section 4 we showed how this framework incorporates the existing constructions for embedding degrees $3, 4, 6$, and 12.

In Section 5 we showed that our method can only produce an infinite family of curves if a certain polynomial $f(x)$ either is quadratic or has a square factor. These two conditions have been achieved for $k = 10$ and $k = 12$, respectively, but these two examples appear to be special cases, and in general we have not found a way to achieve either of these two conditions. The success of our method in producing curves with embedding degree greater than 12 depends on our ability to control the behavior of $f(x)$, which leads to the following important open problem.

Problem 6.1. Given an integer k such that $\varphi(k) \geq 4$, find polynomials $t(x)$ and $n(x)$ such that

1. $n(x)$ is an irreducible factor of $\Phi_k(t(x) - 1)$, where Φ_k is the kth cyclotomic polynomial, and
2. $f(x) = 4n(x) - (t(x) - 2)^2$ is either quadratic or of the form $g(x)^2 h(x)$, with $\deg h(x) \leq 2$.

References

1. P.S.L.M. Barreto, B. Lynn, M. Scott, "Constructing elliptic curves with prescribed embedding degrees," in *SCN 2002*, ed. S. Cimato, C. Galdi, G. Persiano, Springer LNCS **2576** (2003) 257-267.
2. P.S.L.M. Barreto, M. Naehrig, "Pairing-friendly elliptic curves of prime order," in *SAC 2005*, ed. B. Preneel, S. Tavares, Springer LNCS **3897** (2006) 319-331.
3. I. Blake, G. Seroussi, N. Smart, *Elliptic Curves in Cryptography*, LMS Lecture Note Series **265**, Cambridge University Press, 1999.
4. I. Blake, G. Seroussi, N. Smart, eds., *Advances in Elliptic Curve Cryptography*, LMS Lecture Note Series **317**, Cambridge Unviersity Press, 2005.
5. D. Boneh, M. Franklin, "Identity based encryption from the Weil pairing," in *CRYPTO '01*, ed. J. Kilian, Springer LNCS **2139** (2001), 213-229.
6. D. Boneh, B. Lynn, H. Shacham, "Short signatures from the Weil pairing," in *ASIACRYPT '01*, ed. C. Boyd, Springer LNCS **2248** (2001), 514-532.
7. F. Brezing, A. Weng, "Elliptic curves suitable for pairing based cryptography," *Designs, Codes, and Cryptography* **37** (2005) 133-141.
8. C. Cocks, R.G.E. Pinch, "Identity-based cryptosystems based on the Weil pairing," unpublished manuscript, 2001.
9. G. Cornell, J. Silverman, eds., *Arithmetic Geometry,* Springer, New York 1986.
10. S. Cui, P. Duan, C.W. Chan, "A new method of building more non-supersingular elliptic curves," in *ISH 2005*, ed. O. Gervasi et al., Springer LNCS **3481** (2005), 657-664.
11. D. Freeman, "Constructing families of pairing-friendly elliptic curves," Hewlett-Packard Laboratories technical report HPL-2005-155 (2005), available at `http://www.hpl.hp.com/techreports/2005/HPL-2005-155.html`.
12. S. Galbraith, J. McKee, P. Valença, "Ordinary abelian varieties having small embedding degree," in *Proceedings of a Workshop on Mathematical Problems and Techniques in Cryptology,* ed. R. Cramer, T. Okamoto, CRM Barcelona (2005) 29-45.
13. A. Joux, "A one round protocol for tripartite Diffie-Hellman," in *ANTS-IV*, ed. W. Bosma, Springer LNCS **1838** (2000), 385-394.
14. F. Luca, I. Shparlinski, "Elliptic curves with low embedding degree," preprint, available at `http://eprint.iacr.org/2005/363`.
15. K. Matthews, "The diophantine equation $x^2?Dy^2 = N$, $D > 1$, in integers," *Expositiones Mathematicae* **18** (2000), 323-331.
16. A. Menezes, T. Okamoto, S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transactions on Information Theory* **39** (1993), 1639-1646.
17. A. Miyaji, M. Nakabayashi, S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Transactions on Fundamentals* **E84-A(5)** (2001), 1234-1243.
18. R. Mollin, *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, 1998.
19. F. Morain, "Building cyclic elliptic curves modulo large primes," in *EUROCRYPT '91*, ed. D. W. Davies, Springer LNCS **547** (1991) 328-336.
20. J. Neukirch, *Algebraic Number Theory*, Springer, Berlin 1999.
21. J. Robertson, "Solving the generalized Pell equation," unpublished manuscript (2004), available at `http://hometown.aol.com/jpr2718/pell.pdf`.
22. M. Scott, personal communication, 7 November 2005.
23. J. Silverman, *The Arithmetic of Elliptic Curves*, Springer GTM **106**, 1986.