Constructing Families of Pairing-Friendly Elliptic Curves

David Freeman
Information Theory Research
HP Laboratories Palo Alto
HPL-2005-155
August 24, 2005*

cryptography, pairings, elliptic curves, embedding degree

We present a general method for constructing families of elliptic curves with prescribed embedding degree and prime order. We demonstrate this method by constructing curves of embedding degree $k = 10$, a value which has not previously appeared in the literature, and we show that our method applies to existing constructions for $k = 3$, 4, 6, and 12. We give evidence that our method is unlikely to produce infinite families of curves for embedding degrees $k > 12$.

* Internal Accession Date Only
Approved for External Publication

CONSTRUCTING FAMILIES OF PAIRING-FRIENDLY ELLIPTIC CURVES.

DAVID FREEMAN

Abstract. We present a general method for constructing families of elliptic curves with prescribed embedding degree and prime order. We demonstrate this method by constructing curves of embedding degree $k = 10$, a value which has not previously appeared in the literature, and we show that our method applies to existing constructions for $k = 3, 4, 6$, and 12. We give evidence that our method is unlikely to produce infinite families of curves for embedding degrees $k > 12$.

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 [10], identity-based encryption [4], and short digital signatures [5].

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 [13] showed that a supersingular 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 [14] have given a complete characterization of ordinary elliptic curves of prime order and embedding degree 3, 4, or 6. There is a general construction, originally due to Cocks and Pinch [7], 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 have focused on reducing the ratio $\rho = \log r / \log q$; the best current results are by Brezing and Weng [6], which achieve

$\rho \approx 5/4$ for $k = 8$ or $k = 24$, and $\rho \approx (k+2)/(k-1)$ for prime k. Barreto and Naehrig [1] give a construction for $k = 12$ with $\rho \approx 1$, which allows for curves with prime order.

The focus of this paper is the construction of elliptic curves with prime order and prescribed embedding degree. In Section 2 we present a generalized method for constructing such curves, and give conditions for when this method will give us infinite families of elliptic curves. Our method is based on the Complex Multiplication method of curve construction [15], and makes use of properties of real quadratic fields and quadratic extensions of rings $\mathbb{Z}_{p^i}$. In Section 3 we show how this method can be used to construct curves with embedding degree $k = 10$; such curves have not, to our knowledge, previously appeared in the literature. We also demonstrate that our method is a rephrasing of existing constructions for $k = 3, 4, 6$, and 12.

In Section 4, we show that for $k > 6$, our method is not likely to give additional infinite families of elliptic curves with prime degree. Elliptic curves constructed by our method correspond to certain integral points on a curve of the form $Dy^2 = f(x)$, and for $k > 6$ the degree of $f(x)$ is usually at least 4. Thus by Siegel's theorem $Dy^2 = f(x)$ has a finite number of solutions, so the construction generates only finitely many elliptic curves. We note, however, that exceptions to this general result exist for $k = 10$ or 12, and we ask in Section 5 if such exceptions can be constructed in a systematic fashion.

1.1. **Acknowledgments.** Research for this paper was conducted during a summer internship at HP Labs, Palo Alto. I thank Vinay Deolalikar for suggesting this problem and for providing advice and support along the way. I also thank Gadiel Seroussi for bringing me to HP and for supporting my research.

2. A general method for constructing pairing-friendly elliptic curves

In this section, we provide a general method for constructing elliptic curves of a given embedding degree k. We parameterize the number of points on the curve an the size of the field of definition by polynomials $n(x)$ and $q(x)$. For each set of good parameters $n(x_0), q(x_0)$ we use of the Complex Multiplication method of curve construction, and we give a criterion for when there will exist infinite families of such good parameters. To prove existence of these infinite families, we use properties of real quadratic fields and of quadratic extensions of rings $\mathbb{Z}_{p^i}$; the latter is discussed in Section 2.1.

We begin by giving a formal definition of embedding degree.

Definition 2.1. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, 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 $\bar{\mathbb{F}}_q$. 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 in q in advance.

We follow the strategy of Barreto and Naehrig [1] 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 [2, 15] 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, and E has embedding degree at most k.

Proof. We first observe that the given solution allows us to construct the desired elliptic curve via the Complex Multiplication method [2, 15]. Namely, if $H_D(x)$ is the Hilbert polynomial of the quadratic imaginary field $\mathbb{Q}(\sqrt{-D})$, then the equality $t(x_0)^2 + Dy_0^2 = 4q(x_0)$ means that the prime $q(x_0)$ splits into principal prime ideals in $\mathbb{Q}(\sqrt{-D})$, and thus $H_D(x)$ has a root modulo $q(x_0)$. Let j_0 be such a root, and construct an elliptic curve E defined over $\mathbb{F}_{q(x_0)}$ with j-invariant j_0. Then

$$\#E(\mathbb{F}_{q(x_0)}) = q(x_0) + 1 \pm t(x_0).$$

If the sign is negative the curve E has the desired number of points $n(x_0)$, which is prime; if the sign is positive then the quadratic twist E' has the desired number of points. The bottleneck in this construction is computing the Hilbert polynomial $H_D(x)$, whose coefficients will in general be very large. If D (or more precisely, the class number of $\mathbb{Q}(\sqrt{-D})$ is sufficiently small, then $H_D(x)$ can be computed easily, and our construction is efficient.

We now show that a curve with the given number of points over $\mathbb{F}_{q(x_0)}$ (usually) has embedding degree k. Henceforth we suppress x_0 when referring to the specific values of n, q, and t, and use $n(x)$, etc. when referring to the polynomials we have constructed.

By definition, E having embedding degree k means that

$$n \mid q^k - 1, \text{ and } n \nmid q^i - 1 \text{ for } i < k.$$

Since $q = n + t - 1$, this is equivalent to

$$n \mid (t-1)^k - 1, \text{ and } n \nmid (t-1)^i - 1 \text{ for } i < k.$$

Now it is a standard property of cyclotomic polynomials (see [11][§VI.3]) that

$$x^u - 1 = \prod_{v \mid u} \Phi_v(x).$$

We see therefore that E having embedding degree k is equivalent to

$$n \mid \Phi_k(t-1), \text{ and } n \nmid \Phi_i(t-1) \text{ for } i < k.$$

We have chosen the polynomial $n(x)$ to divide $\Phi_k(t(x)-1)$, so n is guaranteed to divide q^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 does not divide $\Phi_i(t-1)$ 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) accordingly, and the same analysis holds.

In practice, to construct an elliptic curve of 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 values of the polynomials $n(x)$ and $q(x)$ are sufficiently randomly distributed, the Prime Number Theorem tells us that we should have to test roughly $\log n(x_0)\log q(x_0)$ values of x near x_0 until we find an x_1 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.

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 of 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 of embedding degree k:

Corollary 2.6. *Suppose (t,n,q) represents a family of curves of 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 choose an appropriate $n(x)$ 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 $Dy^2=f(x)$ defines a hyperelliptic curve of genus at least 1, and in general there will be only a finite number of integral points on such a curve. (See Section 4 for a precise formulation of this result.) Therefore 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 used to

produce curves of embedding degrees 3, 4, and 6, (the MNT curves; see Section 3.2) and curves of embedding degree 10 (see Section 3.1). The idea is as follows: we complete the square to write $Dy^2 = f(x)$ 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 elements of this field of norm 1; 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 of embedding degree k.*

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

$$aD(2y)^2 = (2ax + b)^2 - (b^2 - 4ac).$$

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

$$u^2 - D'v^2 = T.$$

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 $\mathbb{Q}(\sqrt{D'})$ of norm T. Furthermore, this solution satisfies the congruence conditions

$$\begin{aligned} u_0 &\equiv b \pmod{2a} \\ v_0 &\equiv 0 \pmod{2r}. \end{aligned} \tag{2.1}$$

We wish to find an infinite set of solutions (u, v) satisfying the same congruence conditions, for then we can transform such a solution into an integer solution to the original equation. To find such solutions we employ Dirichlet's unit theorem ([16, §1.7]), which tells us that the 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 number $\alpha_0 + \beta_0\sqrt{D'}$ is called the *fundamental unit* of the real quadratic field $\mathbb{Q}(\sqrt{D'})$.

In Section 2.1 below, we will examine quadratic extensions of the integers modulo prime powers, and show in Proposition 2.11 that we can compute an integer $m \approx 2a$ such we can write $(\alpha_0 + \beta_0\sqrt{D})^m$ as $\alpha_1 + \beta_1\sqrt{D}$ for integers α_1, β_1, with

$$\begin{aligned} \alpha_1 &\equiv 1 \pmod{2a}, \\ \beta_1 &\equiv 0 \pmod{2a}. \end{aligned} \tag{2.2}$$

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

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

We claim that (u, v) satisfy the congruence conditions (2.1). To see this, let $\alpha_n + \beta_n\sqrt{D'} = (\alpha_1 + \beta_1\sqrt{D'})^n$. The conditions (2.2) impliy that $\alpha_n \equiv 1 \pmod{2a}$ and

$\beta_n \equiv 0 \pmod{2a}$. Combining this observation with the formulas

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

we see that $u \equiv u_0 \equiv b \pmod{2a}$ and $v \equiv v_0 \pmod{2a}$. In addition, $v_0 \equiv 0 \pmod{2r}$ 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 (2.1). Any integer n gives such a solution, so by setting $x = (u-b)/2a$ and $y = v/2r$ for 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 construction (t, n, q) satisfy conditions (1), (2), (3), so we conclude that (t, n, q) represents a family of curves of embedding degree k. □

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* discriminant D. If $f(x)$ is in fact an integer times a square, then we still get a family of curves, but for only a single D. This is the method used to construct curves for $k = 12$ (see Section 3.3).

Proposition 2.8. *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 $f(x) = Dg(x)^2$ for some square-free positive integer D and some polynomial $g(x)$. Then (t, n, q) represents a family of curves of embedding degree k.*

Proof. Under these hypotheses, the equation $Dy^2 = f(x)$ is satisfied by $(x, g(x))$ for any x, so condition (4) of Definition 2.5 is satisfied for the integer D. □

2.1. **Quadratic extensions of $\mathbb{Z}_{p^r}$.** In the proof of Theorem 2.7 we wished to compute an element $\alpha_1 + \beta_1\sqrt{D'}$ of a real quadratic field $\mathbb{Q}(\sqrt{D'})$ such that α_1 and β_1 satisfied certain congruence conditions. To show that this number can be easily computed from a fundamental unit of $\mathbb{Q}(\sqrt{D'})$, we analyze quadratic extensions of $\mathbb{Z}_{p^r}$, the integers modulo p^r, for various prime powers p^r.

Lemma 2.9. *Let p^r be a power of an odd prime, and let D be a square-free integer. Let R be the ring*

$$\frac{\mathbb{Z}_{p^r}[x]}{(x^2 - D)},$$

and denote its group of units by R^*. Define the norm map $N\colon R \to \mathbb{Z}_{p^r}$ by $N(a + bx) = a^2 - Db^2$, and let N^* be the restriction of N to R^*. If p does not divide D, then N^* maps R^* surjectively onto $\mathbb{Z}_{p^r}^*$, and the size of the kernel is

$$\#\ker N^* = p^{r-1}\left(p - \left(\tfrac{D}{p}\right)\right).$$

If p divides D, then N^* maps R^* surjectively onto $(\mathbb{Z}_{p^r}^*)^2$, and $\#\ker N^* = 2p^r$.

Proof. It is easy to check that N is a homomorphism under multiplication. Now suppose $\theta \in R^*$. Then there is a $\chi \in R$ such that $\chi\theta = 1$, so $N(\chi)N(\theta) = 1$, and $N(\theta) \in \mathbb{Z}_{p^r}^*$. Conversely, if $\theta = a + bx \in R$ and $N(\theta) \in \mathbb{Z}_{p^r}^*$, then $\chi = (a - bx)/N(\theta)$ satisfies $\chi\theta = 1$, so $\theta \in R^*$. We conclude that $\theta \in R^*$ if and only if $N(\theta) \in \mathbb{Z}_{p^r}^*$.

Since $N(a) = a^2$ for $a \in \mathbb{Z}_{p^r}$, it is clear that every square in $\mathbb{Z}_{p^r}^*$ is in the image of N^*. We now consider three possible cases:

- If p divides D then $(\mathbb{Z}_{p^r}^*)^2$ is the entire image, since $N(a+bx) \equiv a^2 \pmod{p}$, and an integer is a square mod p^r if and only if it is a square mod p.
- If $(\frac{D}{p}) = 1$, we set $D = d^2$, and let $\theta = a+(a-1)d^{-1}x$. Then $N(\theta) = 2a-1$, so for any $t \in \mathbb{Z}_{p^r}^*$, setting $a = (t+1)/2$ gives an element $\theta \in R^*$ of norm t, so N^* surjects onto $\mathbb{Z}_{p^r}^*$.
- If $(\frac{D}{p}) = -1$, we wish to show that non-squares of $\mathbb{Z}_{p^r}^*$ are also in the image of N^*. It suffices to show that there is a single $\theta \in R^*$ for which $N(\theta)$ is not a square, since $N(a\theta) = a^2 N(\theta)$. Note that as b takes on all values in $\mathbb{Z}_{p^r}^*$, $-Db^2$ takes on the values of all squares or all non-squares, depending on whether -1 is a square mod p. We consider the two subcases separately:
  (1) If $(\frac{-1}{p}) = 1$ then $N(x) = -D$, which is not a square.
  (2) If $(\frac{-1}{p}) = -1$, then $-Db^2$ is a square for all b. Find an integer c such that c and $c+1$ are nonzero mod p, with c is a square and $c+1$ a non-square mod p; this is always possible since 1 is a square mod p. Now considering c mod p^r, let $b = \sqrt{\frac{c}{-D}} \pmod{p^r}$. Then $N(1+bx) = 1+c$ is a non-square in $\mathbb{Z}_{p^r}^*$.

  We conclude that N^* maps R^* surjectively onto $\mathbb{Z}_{p^r}^*$.

Now that we have determined the image of N^*, we may compute the size of the kernel of N^* by counting the number of elements of R^* and using the formula

$$\#\ker N^* = \frac{\#R^*}{\#\operatorname{im} N^*}.$$

To count the elements of R^*, we count the number of non-invertible elements of R. We have shown above that if $\theta = a + bx$, then $\theta \in R \setminus R^*$ if and only if $N(\theta) \in \mathbb{Z}_{p^r} \setminus \mathbb{Z}_{p^r}^* = p\mathbb{Z}_{p^r}$; i.e. $a^2 \equiv Db^2 \pmod{p\mathbb{Z}_{p^r}}$. There are three cases:

- $(\frac{D}{p}) = -1$: In this case, $a^2 \equiv Db^2 \pmod{p\mathbb{Z}_{p^r}}$ if and only if $a, b \in p\mathbb{Z}_{p^r}$. Thus $\#(R \setminus R^*) = (p^{r-1})^2$.
- $(\frac{D}{p}) = 0$: In this case, a must be in $p\mathbb{Z}_{p^r}$, and b can be any element of $\mathbb{Z}_{p^r}$. Thus $\#(R \setminus R^*) = (p^r)(p^{r-1})$.
- $(\frac{D}{p}) = 1$: In this case, for any a there are two possible values of b modulo $p\mathbb{Z}_{p^r}$, except when $a \in p\mathbb{Z}_{p^r}$, when there is one possible value. Thus $\#(R \setminus R^*) = (p^r - p^{r-1})(2p^{r-1}) - (p^{r-1})^2$.

In each case, we have

$$\#(R \setminus R^*) = p^{2r-2}\left(p + (\tfrac{D}{p})(p-1)\right).$$

Since $\#R = p^{2r}$, we conclude that

$$\#R^* = p^{2r-2}(p-1)(p-(\tfrac{D}{p})),$$

and therefore, since $\mathbb{Z}_{p^r}^*$ has $p^{r-1}(p-1)$ elements, half of which are squares, we have

$$\#\ker N^* = \begin{cases} p^{r-1}\left(p - (\frac{D}{p})\right) & \text{if } p \nmid D \\ 2p^r & \text{if } p \mid D. \end{cases}$$

□

When $p = 2$ the result is slightly different, and depends on the equivalence class of D modulo 8.

Lemma 2.10. *Let p^r be a power of 2, and let D be a square-free integer. Let R, N, and N^* be defined as in Lemma 2.9. The size of the kernel of N^* is*

$$\#\ker N^* = \begin{cases} 2^{r+2} & \text{if } D \equiv 0 \pmod 8 \\ 2^{r+1} & \text{if } D \equiv 2,3,4,6,7 \pmod 8 \\ 2^r & \text{if } D \equiv 1,5 \pmod 8. \end{cases}$$

Proof. As in the case of odd p, N is a homomorphism and $\theta \in R^*$ if and only if $N(\theta) \in \mathbb{Z}_{2^r}^*$. To determine the image of N^*, it suffices to determine its image mod 8, since $t \in Z_{2^r}$ is a square if and only if $t \equiv 1 \mod 8\mathbb{Z}_{2^r}$. Thus we have

$$\#\operatorname{im} N = (\#8\mathbb{Z}_{2^r})(\#\operatorname{im}(N^* \bmod 8)).$$

If D is even, then the possible values of $N(a+bx)$ mod 8 are $\{1, 1-D\}$, which is a single value if $D \equiv 0 \pmod 8$ and two values if $D \equiv 2,4,6 \pmod 8$. In addition, $a + bx \in R^*$ if and only if $a \in Z_{2^r}^*$, so $\#R^* = 2^{2r-1}$.

If D is odd, then the possible values of $N(a+bx)$ mod 8 are $\{1, 4-D, 1-4D, -D\}$. If $D \equiv 1,5 \pmod 8$ then this set contains all four values of $\mathbb{Z}_8^*$, and if $D \equiv 3,7 \pmod 8$ it contains only two. In addition, $a + bx \in R^*$ if and only if exactly one of a, b is odd, so $\#R^* = 2^{2r-1}$ in this case as well.

We use the formula $\#\ker N^* = \#R^*/\#\operatorname{im} N^*$ to get the stated result:

D mod 8	$\#R^*$	$\#\operatorname{im} N^*$	$\#\ker N^*$
0	2^{2r-1}	2^{r-3}	2^{r+2}
2, 3, 4, 6, 7	2^{2r-1}	$2 \cdot 2^{r-3}$	2^{r+1}
1, 5	2^{2r-1}	$4 \cdot 2^{r-3}$	2^r

□

Given a quadratic extension R of $\mathbb{Z}_{p^i}$, Lemmas 2.9 and 2.10 tell us the size of the kernel of the norm map. This kernel is a multiplicative subgroup, so raising any element of norm 1 to the size of the kernel will give us 1 in R. Combining different prime powers via the Chinese Remainder Theorem allows us to get 1 modulo any integer.

Proposition 2.11. *Let D be a square-free positive integer, and let $\alpha_0, \beta_0 \in \mathbb{Z}$ such that $\alpha_0^2 - D\beta_0^2 = 1$. For any positive integer n, there is an integer $m \approx n$ such that we can write $(\alpha_0 + \beta_0\sqrt{D})^m$ as $\alpha_1 + \beta_1\sqrt{D}$ for integers α_1, β_1, with*

$$\begin{aligned} \alpha_1 &\equiv 1 \pmod n, \\ \beta_1 &\equiv 0 \pmod n. \end{aligned}$$

Proof. Let p^r be a prime power dividing n, and let $R = Z_{p^r}[x]/(x^2 - D)$. Considering α_0 and β_0 modulo p^r gives an element $\theta \in R^*$ that is in the kernel of the norm map N^* defined in Lemma 2.9. We may then use Lemma 2.9 (or Lemma 2.10 if $p = 2$) to compute $m_p = \#\ker N^*$. Then $m_p \approx p^r$ and $\theta^{m_p} = 1$ in R. If we write $\alpha_p + \beta_p\sqrt{D} = (\alpha_0 + \beta_0\sqrt{D})^{m_p}$, then $\alpha_p \equiv 1 \pmod{p^r}$ and $\beta_p \equiv 0 \pmod{p^r}$. If we compute m_p for each p dividing n and let $m = \prod m_p$, then by the Chinese Remainder Theorem m satisfies the conditions of the statement. □

3. Examples of elliptic curve families

In this section we give explicit examples of how the general method of Section 2 can be used to construct families of elliptic curves of prime order with specified embedding degrees. We first construct curves with embedding degree 10; such

curves have not (to our knowledge) appeared previously in the literature. We then show how our method gives interpretations of the MNT construction of curves of embedding degrees 3, 4, and 6 [14], and of the Barreto-Naehrig construction of curves of embedding degree 12 [1].

3.1. **Elliptic curves with embedding degree 10.** If we wish to apply Theorem 2.7 to find an infinite family of curves, we require $f(x)$ to be quadratic. If $\varphi(k) = 2$ (i.e. $k = 3, 4$, or 6) and $t(x)$ is linear then this condition is trivial; otherwise we must choose $t(x)$ such that the high-degree terms of $(t(x) - 2)^2$ cancel out those of $n(x)$. It turns out that this is possible when $k = 10$.

For k such that $\varphi(k) = 4$, Galbraith, McKee, and Valença [9] find all of the quadratic polynomials $u(x)$ such that the degree-8 polynomial $\Phi_k(u(x))$ splits into a product of two quartics. For $k = 10$ there is an infinite family of such $u(x)$, parameterized by the rational points of an elliptic curve. It turns out that one of the $t(x)$ that Galbraith, et al give as an example produces a quadratic $f(x)$, and from this $t(x)$ we may thus compute (t, n, x) that represents a family of curves of embedding degree 10.

Theorem 3.1. *Fix a positive square-free integer D such that $15D$ is not a square. Define $t(x)$, $n(x)$, and $q(x)$ by*

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

Let $15D = D'r^2$, where D' is square-free. If the equation $u^2 - D'v^2 = -20$ has a solution with $u \equiv 5 \pmod{15}$ and $v \equiv 0 \pmod{r}$, then (t, n, q) represents a family of curves of embedding degree 10.

Proof. We must verify that conditions (1)-(4) of Definition 2.5 are satisfied. It is easy to check that $n(x) = q(x) + 1 - t(x)$ (1), and that $n(x)$ and $q(x)$ are irreducible (2). Recall that $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$. Then we have

$$\begin{aligned} (3.1)\quad \Phi_{10}(t(x) - 1) = \\ (25x^4 + 25x^3 + 15x^2 + 5x + 1)(400x^4 + 400x^3 + 240x^2 + 60 + 11), \end{aligned}$$

so $n(x)$ satisfies condition (3).

Condition (4) requires an infinite number of integer solutions to $Dy^2 = f(x)$, where D is a square-free integer not equal to 15 and $f(x) = 4q(x) - t(x)^2$. The key observation is that for this choice of t and n,

$$f(x) = 4q(x) - t(x)^2 = 15x^2 + 10x + 3.$$

If we call this expression $f(x)$, we wish to solve $Dy^2 = f(x)$. Multiplying by 15 and completing the square gives

$$D'(ry)^2 = (15x + 5)^2 + 20.$$

Integer solutions to this equation correspond to integer solutions to $u^2 - D'v^2 = -20$ with $u \equiv 5 \pmod{15}$ and $v \equiv 0 \pmod{r}$. By Theorem 2.7, if one such solution exists then an infinite number exist, so (t, n, q) represents a family of curves of embedding degree 10. □

Computations with PARI indicate that for a fixed D the solutions to $Dy^2 = f(x)$ grow very fast, and it is unlikely that we will find a solution where x is of a reasonable size and $q(x)$ is prime. We computed solutions (x, y) for $D = 2$, 3, and 7 (note that an integer solution to $u^2 - 15Dv^2 = -20$ implies $D \equiv 2$ or 3 (mod 5)), and did not find any such solution with $q(x)$ a prime of less than 100 decimal digits. Thus to compute examples of curves of embedding degree 10, we must take a different tack. Namely, we choose values of x and compute $q(x)$; if $q(x)$ is prime we take D to be the non-square factors of $f(x)$. If the class number of D is sufficiently small, we can compute an elliptic curve over $\mathbb{F}_{q(x)}$ with $n(x)$ points. We illustrate this method with a small example. We refer the reader to [2, Chapter VII] for a full description of the Complex Multiplication method of curve construction.

Example 3.2. Let $t(x)$, $n(x)$, and $q(x)$ as in Theorem 3.1. For $x = 4$ we have $t = 183$, $n = 8261$, and $q = 8443$, a prime number. Then $f(x) = 4q - t^2 = 283$. We check that $n \mid q^{10} - 1$ and $n \nmid q^i - 1$ for $i < 10$, so an elliptic curve over $\mathbb{F}_q$ with n points does indeed have embedding degree 10. We now construct such a curve via the CM method.

The class number of $\mathbb{Q}(\sqrt{-283})$ is 3, and the Hilbert polynomial (as computed by Ben Lynn [12]) is

$$H_D(x) = x^3 + 896113233868328017920000x^2 + 90839236535446929408000000x + 2013718431569553653760000000000.$$

This polynomial has roots $\{1129, 5237, 7723\}$ mod q. Taking the first listed root to be the j-invariant of our elliptic curve, we compute the curve

$$E : y^2 = x^3 + 6278x + 1371$$

defined over $\mathbb{F}_q$ with j-invariant 1129. Then $\#E(\mathbb{F}_q) = q + 1 \pm t$; selecting a point $P = (1, 4943)$, we find that $nP \neq O$. Thus the quadratic twist of E has the desired number of points. We twist E by $c = 2$ (a non-square mod q) to get

$$E' : y^2 = x^3 + 8226x + 2525.$$

This curve has the desired number of points, as can be easily checked by computing that $Q = (3, 4565)$ has order n.

Unfortunately, using this method to compute curves of cryptographic size ($q \approx 2^{160}$) seems to be out of reach of current computational power. For such q the corresponding CM discriminant D dividing $f(x)$ would have around 80 bits, and the class number is expected to have roughly 40 bits. The bottleneck comes in computing Hilbert polynomials of quadratic imaginary fields, and the state of the art appears to be when the class number is around 8 bits (see [12]).

The table below lists some possible field sizes $q(x)$, group orders $n(x)$, and discriminants D for curves of embedding degree 10 when the field size is at most 32 bits.

x	$q(x)$	$\lceil \log_2 q(x) \rceil$	$n(x)$	D	class no. of $\mathbb{Q}(\sqrt{-D})$
4	8443	14	$11 \cdot 751$	283	3
10	277603	19	$11 \cdot 31 \cdot 811$	1603	6
16	1747363	21	$11 \cdot 158611$	4003	13
-20	3809803	22	$11 \cdot 31 \cdot 11161$	5803	10
22	6134923	23	$31 \cdot 197741$	7483	10
52	186373723	28	$571 \cdot 326351$	41083	22
-68	526788523	29	$41 \cdot 12847381$	68683	45
-80	1011359203	30	$4391 \cdot 230311$	95203	45
-92	1771725883	31	$191 \cdot 9275611$	126043	28
-110	3627276403	32	$38611 \cdot 93941$	180403	60

We note that for about half of these curves (4 of 10), the ratio $\rho = \log q / \log r$, where r is the largest prime dividing $\#E(\mathbb{F}_q)$, is less than 4/3. Current methods for constructing elliptic curves over prime fields achieve only $\rho \approx 2$, so our curves, if they could be constructed over prime fields of cryptographic size, would represent a significant improvement.

3.2. **MNT elliptic curves.** Theorem 2.7 also allows us to rephrase the results of Miyaji, Nakabayashi, and Takano [14], who showed how to construct ordinary elliptic curves with embedding degrees 3, 4, and 6. Their theorem is as follows:

Theorem 3.3 ([14])**.** *Let E be an ordinary elliptic curve over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = n = q+1-t$ is prime. Then the following table lists all the possibilities for embedding degree $k = 3, 4, 6$:*

k	$t(x)$	$n(x)$	$q(x)$
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	$1 \pm 2x$	$4x^2 \mp 2x + 1$	$4x^2 + 1$

Since $\varphi(k) = 2$ for these k, any linear $t(x)$ will give a CM equation $Dy^2 = f(x)$ with $f(x) = 4q(x) - t(x)^2$ quadratic. If the equation $Dy^2 = f(x)$ has one solution, then by Theorem 2.7 (t, n, q) represents a family of curves of embedding degree k. Miyaji, et al. arrive at their stronger result by using the fact that $n(x)$ must be prime to show that $t(x)$ must be one of the specific forms described in their theorem.

3.3. **Elliptic curves with embedding degree 12.** Finally, we note that the Barreto-Naehrig construction of curves of embedding degree $k = 12$ [1] falls under the case of Proposition 2.8. 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

$$f(x) = 4n(x) - (t(x) - 2)^2 = 3(6x^2 + 4x + 1)^2.$$

We may thus apply Proposition 2.8 to conclude that (t, n, q) represents a family of curves of embedding degree 12.

4. Higher embedding degrees

In this section, we show that for most k, the method of Theorem 2.2 is unlikely to produce infinite families of curves of embedding degree k and prime order. We start by using Siegel's Theorem on integral points on curves to give a condition for when the CM equation $Dy^2 = f(x)$ will have only a finite number of integer solutions. We then analyze the degrees of the polynomials involved in the construction to show that most cases of our construction will satisfy this condition.

As in Section 2, we fix k and consider triples of polynomials $(t(x), n(x), q(x)) \in \mathbb{Z}[x]^3$ such that:

(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.

Let $f(x) = 4q(x) - t(x)^2$. Recall that if $Dy^2 = f(x)$ has infinitely many integer solutions for some positive square-free integer D, then we say that (t, n, q) represents a family of curves of embedding degree k. In this case, a solution (x_0, y_0) to $Dy^2 = f(x)$ with $q(x_0)$ prime gives an elliptic curve over the field $\mathbb{F}_{q(x_0)}$ with $n(x_0)$ points.

Theorem 2.7 tells us that if we choose (t, n, q) such that $f(x)$ is quadratic, then we are likely to find an infinite family of curves. The following proposition gives a partial converse; namely, if the degree of $f(x)$ is at least 3, then we are unlikely to find an infinite family of curves.

Proposition 4.1. *Let (t, n, q) be polynomials with integer coefficients satisfying conditions (1), (2), and (3), 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 of embedding degree k.*

Proof. Let $d = \deg f(x)$, and let $g = \lfloor (d-1)/2 \rfloor$. If $f(x)$ is square-free (i.e. has no double roots), then the equation $y^2 = D^{-1} f(x)$ defines a smooth affine plane curve of genus g (cf. [17, Example II.2.5.1 and Exercise II.14]). By Siegel's Theorem (cf. [17, Theorem IX.4.3] and [8, §I.2]), for $g \geq 1$, such curves have a finite number of integral points, and thus (t, n, q) cannot represent a family of elliptic curves of embedding degree k. □

In the remainder of this section, we give evidence that in general the degree of $f(x)$ is large, and thus by Proposition 4.1 we are unlikely to find an infinite family of curves. We start by showing that the degree of $n(x)$ must be a multiple of $\varphi(k)$, where φ is the Euler phi function, and thus for $k > 6$ Proposition 4.1 is likely to apply.

Lemma 4.2. *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 $\varphi(k)$.*

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 $\deg n(x)$. □

From this lemma and Proposition 4.1, we see that if $\varphi(k) > 2$, then the only way to generate an infinite family of curves is to choose $n(x)$ and $t(x)$ such that $f(x)$ is either quadratic (as in the $k = 10$ case of Section 3.1) or has a square factor (as

in the $k = 12$ case of Section 3.3. This will be difficult in general, as the condition $n(x) \mid \Phi_k(t(x) - 1)$ constrains our choices of n.

In addition, while the degree of $n(x)$ is likely to be large, the Hasse bound $|t| \leq 2\sqrt{q}$ restricts the possible degree of $t(x)$.

Lemma 4.3. *Suppose (t, n, q) represents a family of curves of embedding degree k for some k and D. Then*

$$\deg t(x) \leq \frac{1}{2} \deg n(x).$$

Proof. Suppose $\deg t(x) > \frac{1}{2} \deg n(x)$. Then since $f(x) = 4n(x) - (t(x) - 2)^2$, $\deg f(x) = 2 \deg t(x)$, and furthermore, the leading coefficient of $f(x)$ is negative. Thus $f(x) < 0$ for all but finitely many x. Since $D > 0$, $Dy^2 = f(x)$ can only have a solution when $f(x) \geq 0$, so the equation must have finitely many solutions, contradicting property (4) of Definition 2.5. □

Combining all of these results, we see that in most cases for a given k there will be only one possible value of $\deg t(x)$.

Proposition 4.4. *Let (t, n, q) be polynomials with integer coefficients satisfying conditions (1), (2), and (3), and suppose $\varphi(k) > 2$. If (t, n, q) represents a family of curves of embedding degree k and $f(x) = 4q(x) - t(x)^2$ is square-free, then*

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

Proof. By Lemma 4.3, $\deg t(x) \leq \frac{1}{2} \deg n(x)$. If the degree of $t(x)$ is strictly less than that of $n(x)$, then since $f(x) = 4n(x) - (t(x) - 2)^2$, the degrees of $f(x)$ and $n(x)$ are equal. By Lemma 4.2, $\deg n(x)$ is a multiple of $\varphi(k)$, so $\deg n(x) > 2$. By Proposition 4.1, if $f(x)$ is square-free than (t, n, q) cannot represent a family of curves. We conclude that $\deg t(x) = \frac{1}{2} \deg n(x)$. Furthermore, since $n(x) = q(x) + 1 - t(x)$, we see that $\deg n(x) = \deg q(x)$. □

As an immediate corollary, we see that if $k > 6$ (so $\varphi(k) > 2$) then choosing a linear t will not in general give us an infinite family of curves, whereas if $k > 12$ (so $\varphi(k) > 4$) then choosing a quadratic t will not in general give us an infinite family of curves. Thus for higher embedding degrees we will have to choose t of large degree such that $\phi_k(t(x) - 1)$ is not irreducible. Galbraith, McKee, and Valença [9] observe that this is hard even for quadratic t, and as the degree increases the problem will only become more difficult.

5. Conclusion and Open Questions

We have seen in Section 2 that the current methods in the literature for constructing families of elliptic curves of prime order and prescribed embedding degree can all be subsumed under a generalized method. In Section 3 we showed how the method can be used to construct curves of embedding degree 10, which have not previously appeared, and to rephrase the existing results for embedding degrees $3, 4, 6$, and 12.

In Section 4 we showed that our method can only produce an infinite family of curves if a certain polynomial $f(x)$ is either quadratic or has a square factor. These conditions have been achieved for $k = 10$ and 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 of embedding degree greater than 12 depends on our ability to construct such polynomials, and is thus the most important pressing open question.

Open Question 5.1. *Given an integer k such that $\varphi(k) > 2$, do there exist polynomials $t(x)$ and $n(x)$ such that*

- *$n(x)$ is an irreducible factor of $\Phi_k(t(x)-1)$, where Φ_k is the kth cyclotomic polynomial, and*
- *$f(x) = 4n(x) - (t(x)-2)^2$ is either quadratic or has a square factor.*

If we can choose t and n such that $f(x)$ is quadratic or a square, then we may apply Theorem 2.7 or Proposition 2.8, respectively, to look for infinite families of curves with embedding degree k. However, if $f(x) = g(x)^2 h(x)$ where $h(x)$ is square-free, the process becomes more complicated. In fact, if $\deg h(x) \geq 3$, then under the rational change of variables $y' = yg(x)$, the CM equation $Dy^2 = f(x)$ becomes $Dy'^2 = h(x)$, and by Siegel's theorem the latter can only have infinitely many integral solutions if $\deg h(x) \leq 2$. However, even if $h(x)$ is quadratic, we still do not know of a method for finding infinitely many solutions, as the method of Theorem 2.7, using Dirichlet's unit theorem for real quadratic fields and our analysis of quadratic extensions of $\mathbb{Z}_{p^i}$, does not seem to apply in this case. We thus pose finding solutions to equations of this form as our second open question.

Open Question 5.2. *Given a single solution in the integers to the equation $Dy^2 = g(x)^2 h(x)$, where g, h are polynomials with integer coefficients and h is square-free, find an infinite number of solutions.*

References

[1] P.S.L.M. Barreto, M. Naehrig, "Pairing-friendly elliptic curves of prime order," Cryptology ePrint Archive, report 2005/133 (2005), available at `http://eprint.iacr.org/2005/133`.

[2] I. Blake, G. Seroussi, N. Smart, *Elliptic Curves in Cryptography*, LMS Lecture Note Series **265**, Cambridge University Press, 1999.

[3] I. Blake, G. Seroussi, N. Smart, eds., *Advances in Elliptic Curve Cryptography*, LMS Lecture Note Series **317**, Cambridge Unviersity Press, 2005.

[4] D. Boneh, M. Franklin, "Identity based encryption from the Weil pairing," in *CRYPTO '01*, ed. J. Kilian, Springer LNCS **2139** (2001), 213-229.

[5] D. Boneh, B. Lynn, H. Shacham, "Short signatures from the Weil pairing," in *ASIACRYPT '01*, ed. C. Boyd, Springer LNCS **2248** (2001), 514-532.

[6] F. Brezing, A. Weng, "Elliptic curves suitable for pairing based cryptography," Cryptology ePrint Archive, report 2003/143 (2003), available at `http://eprint.iacr.org/2003/143`.

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

[8] G. Cornell, J. Silverman, eds., *Arithmetic Geometry,* Springer, New York 1986.

[9] S. Galbraith, J. McKee, P. Valença, "Ordinary abelian varieties having small embedding degree," Cryptology ePrint Archive, report 2004/365 (2004), available at `http://eprint.iacr.org/2004/365`.

[10] A. Joux, "A one round protocol for tripartite Diffie-Hellman," in *ANTS-4*, ed. W. Bosma, Springer LNCS **1838** (2000), 385-394.

[11] S. Lang, *Algebra*, Revised 3rd ed., Springer GTM **211**, 2002.

[12] B. Lynn, "Hilbert Polynomials," available online at `http://rooster.stanford.edu/~ben/hilbert`.

[13] 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.

[14] 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.
[15] F. Morain, "Building cyclic elliptic curves modulo large primes," in *EUROCRYPT '91*, ed. D. W. Davies, Springer LNCS **547** (1991) 328-336.
[16] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin 1999.
[17] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer GTM **106**, 1986.

Hewlett-Packard Laboratories
E-mail address: dfreeman@math.berkeley.edu