Elliptic Curves for Pairing Applications

Angela Murphy and Noel Fitzpatrick

School Of Mathematical Sciences,
Dublin City University,
Dublin 9, Ireland.

angela.murphy@dcu.ie
noelfitz@redbrick.dcu.ie

September 2, 2005

Abstract

In this paper we address the question of representing the discriminant of an imaginary quadratic field with respect to the basis of a cyclotomic field. This representation allows us to parameterize new families of ordinary elliptic curves over finite prime fields suitable for pairing applications. In particular these curves have small discriminants greater than four and arbitrary embedding degree. Computational results are presented which support the theoretical findings.

Keywords: Pairing Based Cryptosystem, Elliptic Curves.

1 Introduction

In Miyaji, Nakabayashi and Takano's seminal article [10] on elliptic curves of prime order, explicit conditions were given to obtain families of group orders with embedding degree $k \leq 6$. Scott and Barreto [13] provided an alternative derivation of their results and extended them to allow for the generation of curves with near prime order (for large discriminants with $k \leq 6$). The idea of incorporating cofactors in the analysis allowed Galbraith, McKee and Valença [8] to obtain a large class of families corresponding to prime and non-prime group orders.

A measure of the suitability of an elliptic curve for pairing based cryptography is provided by the ratio $\rho = log(q)/log(l)$; i.e. the ratio between the bit length of the finite field $\mathbb{F}_q$ and the order l of the subgroup with embedding degree k. Two methods, in particular have been proposed to construct curves with arbitrary k. Barreto, Lynn and Scott [3] and Dupont, Enge and Morain [7] independently proposed different parameterizations of (q, l) for constructing curves over finite prime fields with arbitrary k. For both methods, the ratio ρ was up to 2 and discriminants greater than 8 bits were used. Since the security depends on l, the use of such curves in existing protocols will often result in an increase in the size of the cipher-texts or signatures generated.

Alternative methods adopting an algebraic strategy may generate curves with ρ closer to one. Such techniques include the families of curves by Barreto, Lynn and Scott [3] and by Brezing and Weng [6]. The latter authors achieve a ratio of $\rho = 5/4$ with embedding degree $k = 8$ or $k = 24$. By extending the work of Galbraith et al [8], Barreto and Naehrig [4] presented an efficient algorithm to construct elliptic curves of prime order with embedding degree $k = 12$ over a prime field and $\rho \approx 1$.

In [4] it was shown that the ability to handle large complex multiplication discriminants may have a positive influence on the minimization of ρ. In this paper we adopt and extend the Brezing and Weng method by finding suitable representations for discriminants greater than 4.

The paper is organized as follows: We first state and prove a number of results on the proper containment of quadratic fields in cyclotomic fields. We then describe how to represent elements of these quadratic fields with respect to the canonical basis of a cyclotomic field, particularly when the imaginary quadratic field is not isomorphic to a cyclotomic field. Following this we give an overview of Brezing and Weng's method [6] for generating elliptic curves with small embedding degrees with our own adaptations. We then give some numerical examples.

2 Constructing a Basis for Quadratic fields contained in Cyclotomic Fields

We begin by showing the containment of quadratic fields within a given cyclotomic field.

Lemma: 2.1 If ζ_n is a primitive n^{th} root of unity and $8|n$ then $\mathbb{Q}(\zeta_n)$ contains $\sqrt{2}, \sqrt{-2}$ and has subfields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$.

Proof: As 8 divides n; $\mathbb{Q}(\zeta_n)$ contains primitive eight and fourth roots of unity denoted by ζ_8 and $\zeta_4 = i = \sqrt{-1}$ respectively. Then $(1+i)^2 = 1 + 2i + i^2 = 2i$ and so $2 = -i(1+i)^2$. Therefore;

$$\begin{aligned} \sqrt{2} &= \sqrt{-i}(1+i) \\ &= \zeta_4\zeta_8(1+\zeta_4) \end{aligned}$$

$$\begin{aligned} \sqrt{-2} &= \sqrt{i}(1+i) \\ &= \zeta_8(1+\zeta_4) \end{aligned}$$

As the field contains $\sqrt{2}, \sqrt{-2}$, it is trivial to form a basis for $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{2})$.

QED

Lemma: 2.2 Let $p > 2$ be a prime. Let ζ_p be a primitive p^{th} root of unity and $\mathbb{Q}(\zeta_p)$ the p^{th} cyclotomic field. If;

$$p \equiv 1 \pmod 4; \text{then } \sqrt{p} \in \mathbb{Q}(\zeta_p) \text{ and } \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$$

$$p \equiv 3 \pmod 4; \text{then } \sqrt{-p} \in \mathbb{Q}(\zeta_p) \text{ and } \mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_p)$$

Proof: This proof is taken from [9]. The Galois group of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ is cyclic of order $p-1$. This number is even so there is precisely one subgroup of index two. Corresponding to that subgroup is a unique quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$.

Suppose $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_p)$. Any prime q that ramifies in $\mathbb{Q}(\sqrt{d})$ must also ramify in $\mathbb{Q}(\zeta_p)$. Since p is the only prime that ramifies in $\mathbb{Q}(\zeta_p)$, the discriminant of the ring of integers in $\mathbb{Q}(\sqrt{d})$ must be divisible only by p. This discriminant is either $4d$ or d. Since p is odd, the discriminant must be d and so $d \equiv 1 \pmod 4$. Thus $d = \pm p$ with the sign determined by the congruence $\pm p \equiv 1 \pmod 4$. .

QED

Note: It is trivial to show that if $4 \mid n$ and $p \mid n$ for p an odd prime. Then $\sqrt{-p}, \sqrt{p}$ are both contained in $\mathbb{Q}(\zeta_n)$. As $4 \mid n$ implies that $\sqrt{-1} = \zeta_4$ is an element of $\mathbb{Q}(\zeta_n)$.

Lemma: 2.3 Let ζ_n be a primitive n^{th} root of unity. Then $\mathbb{Q}(\zeta_n)$ is the n^{th} cyclotomic field. Let d be a square free postivie integer. Then;

- If $2 \not| d$, $4 \not| n$ and $d|n$ then $\sqrt{d} \in \mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_n)$ if $d \equiv 1 \pmod 4$ or $\sqrt{-d} \in \mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\sqrt{-d}) \subset \mathbb{Q}(\zeta_n)$ if $d \equiv 3 \pmod 4$
- If $4|n$ and $d|n$ but $2 \not| d$ then $\sqrt{d}, \sqrt{-d} \in \mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{-d}) \subset \mathbb{Q}(\zeta_n)$.
- If $8|n$ and $d|n$ then; $\sqrt{d}, \sqrt{-d} \in \mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{-d}) \subset \mathbb{Q}(\zeta_n)$.

Proof: Suppose $d = p_1p_2...p_r$ is the prime factorization of d. As $d|n$ then $p_i|n$ for $1 \leq i \leq r$ and so $\mathbb{Q}(\zeta_{p_i}) \subset \mathbb{Q}(\zeta_n)$. Hence, $\sqrt{p_i}$ or $\sqrt{-p_i}$ is contained in $\mathbb{Q}(\zeta_n)$ with the sign depending on which congruence class p_i is equivalent to in $\mathbb{Z}/ < 4\mathbb{Z} >^*$. Suppose the r primes dividing d are reordered so that $p_1, p_2, ..., p_s$ are all congruent to $3 \pmod 4$ and the primes $p_{s+1}, p_{s+2}, ..., p_r$ are congruent to $1 \pmod 4$. Then it is easy to see that $\sqrt{p_{s+1}p_{s+2}...p_r} = \prod_{i=s+1}^{r} \sqrt{p_i}$ is contained in $\mathbb{Q}(\zeta_n)$.

It remains to show that $\sqrt{-p_1p_2...p_s}$ is contained in $\mathbb{Q}(\zeta_n)$ if $d \equiv 3 \pmod 4$ and $\sqrt{p_1p_2...p_s}$ is contained in $\mathbb{Q}(\zeta_n)$ if $d \equiv 1 \pmod 4$. If $d \equiv 3 \pmod 4$ then s must be odd as $3^s \equiv 3 \pmod 4$ if s is odd, similarly if $d \equiv 1 \pmod 4$ then s must be even.

Hence as $\sqrt{-p_i} \in \mathbb{Q}(\zeta_n)$ it follows that $\sqrt{(-1)^s p_1p_2...p_s}$ is contained in $\mathbb{Q}(\zeta_n)$. If $d \equiv 3 \pmod 4$, s must be odd and so $\sqrt{-p_1p_2...p_s}$ is contained in $\mathbb{Q}(\zeta_n)$. If $d \equiv 1 \pmod 4$, s must be even and so $\sqrt{p_1p_2...p_s}$ is contained in $\mathbb{Q}(\zeta_n)$. Once it has been shown that $\sqrt{d}$ or $\sqrt{-d}$ are contained in $\mathbb{Q}(\zeta_n)$, it is a simple matter to construct an explicit basis for the required subfields with elements in $\mathbb{Q}(\zeta_n)$. This completes the proof of part 1 of the lemma.

Part two is trivial as $4|n$ implies that $\sqrt{-1} = i \in \mathbb{Q}(\zeta_n)$ and so if $\sqrt{d}$ or $\sqrt{-d}$ $\in \mathbb{Q}(\zeta_n)$ then they are both elements of $\mathbb{Q}(\zeta_n)$. Again it is simple to construct an explicit basis for the required subfields.

Part three can easily be proved using the first lemma. This lemma states that $\sqrt{-2}$ and $\sqrt{2}$ are both contained in $\mathbb{Q}(\zeta_n)$ if $8|n$. The first part of the current lemma shows that $\sqrt{d/2}$ or $\sqrt{-d/2}$ (*recall that* d *is squarefree*) are elements of $\mathbb{Q}(\zeta_n)$ and so $\sqrt{d}$ and $\sqrt{-d}$ are both elements of $\mathbb{Q}(\zeta_n)$. Once again we can construct an explicit basis for the required subfields.

QED

2.1 Constructing an Explicit Basis

The simplest case to work with is where you wish to construct a basis for $\mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{-p})$ in $\mathbb{Q}(\zeta_p)$. In order to do this is it useful to view $\mathbb{Q}(\zeta_p)$ as the polynomial ring $\mathbb{Q}[x] \mod$ the ideal generated by $\Phi_p(x)$ (Note: $\Phi_p(x)$ *is the* p^{th} *cyclotomic polynomial*) i.e $\mathbb{Q}[x]/(\Phi(x))$. Consider the following [11] for p an odd prime and ζ_p a primitive p^{th} root of unity:

$$p = (-1)^{(p-1)/2} \prod_{j=1}^{(p-1)/2} (\zeta_p^j - \zeta_p^{-j})^2 \tag{1}$$

Taking square roots of both sides we find

$$\sqrt{p} = \prod_{j=1}^{(p-1)/2} (\zeta_p^j - \zeta_p^{-j}) \tag{2}$$

or

$$\sqrt{-p} = \prod_{j=1}^{(p-1)/2} (\zeta_p^j - \zeta_p^{-j}) \tag{3}$$

depending on whether $p \equiv 1$ or $3 \pmod 4$. In $\mathbb{Q}[x]/(\Phi_p(x))$ we have $\phi(p)$ possible p^{th} primitive roots of unity to choose from. Taking any one of these we can construct a polynomial representation for $\sqrt{p}$ or $\sqrt{-p}$ in $\mathbb{Q}[x]/(\Phi_p(x))$.

This method can then be generalized to represent any square root which satisfies the conditions in the previous lemmas.

2.2 Examples

2.2.1 Representing $\sqrt{-7}$ in $\mathbb{Q}(\zeta_{28})$

From the relation (1) we have

$$\sqrt{-7} = \prod_{j=1}^{3}(\zeta_7^j - \zeta_7^{-j})$$

As x is a primitive 28^{th} root of unity in $\mathbb{Q}[x]/(\Phi_{28}(x))$ then x^4 is a primitive 7^{th} root of unity. Hence

$$\sqrt{-7} = \prod_{j=1}^{3}((x^4)^j - (x^4)^{-j})$$

Compute this polynomial mod $\Phi_{28}(x)$ to give

$$\sqrt{-7} = -2x^8 - 2x^4 + 2x^2 - 1$$

in $\mathbb{Q}[x]/(\Phi_{28}(x))$.

2.2.2 Representing $\sqrt{-2}$ in $\mathbb{Q}(\zeta_{24})$

As x is a primitive 24^{th} root of unity in $M = \mathbb{Q}[x]/(\Phi_{24}(x))$ then x^6 and x^3 are primitive 4^{th} and 8^{th} roots of unity respectively. Hence in M we can represent $\sqrt{-2}$ as

$$\begin{aligned} \sqrt{-2} &= \zeta_8(1+\zeta_4) \\ &= x^3(1+x^6) \bmod \Phi_{24}(x) \\ &\equiv -x^5 - x^3 + x \bmod \Phi_{24}(x) \end{aligned}$$

2.2.3 Representing $\sqrt{-5}$ in $\mathbb{Q}(\zeta_{40})$.

From the relation (1) we have

$$\sqrt{5} = \prod_{j=1}^{2}(\zeta_5^j - \zeta_5^{-j})$$

As x is a primitive 40^{th} root of unity in $\mathbb{Q}[x]/(\Phi_{40}(x))$ then x^8 is a primitive 5^{th} root of unity. Hence

$$\sqrt{5} = \prod_{j=1}^{2}((x^8)^j - (x^8)^{-j})$$

Compute the product of this polynomial with x^{10} (as x^{10} is a primitive 4^{th} root of unity) mod $\Phi_{40}(x)$ we have

$$\sqrt{-5} = -2x^{14} + x^{10} - 2x^6$$

in $\mathbb{Q}[x]/(\Phi_{40}(x))$.

2.2.4 Representing $\sqrt{-15}$ in $\mathbb{Q}(\zeta_{30})$

As x is a primitive 30^{th} root of unity then x^{10} and x^6 give primitive 3^{rd} and 5^{th} roots of unity respectively in $\mathbb{Q}[x]/(\Phi_{30}(x))$. Using (1) we then have:

$$\sqrt{5} = \prod_{j=1}^{2}((x^6)^j - (x^6)^{-j}) \tag{4}$$

$$\sqrt{-3} = 2x^{10} - 1 \tag{5}$$

$$\tag{6}$$

Taking the product of these and reducing mod $\Phi_{30}(x)$ gives a representation of $\sqrt{-15}$ in $\mathbb{Q}[x]/(\Phi_{30}(x))$ as follows:

$$\sqrt{-15} = -2x^7 + 2x^5 - 4x^4 + 2x^3 - 2x^2 - 4x + 3$$

2.3 Algorithm For Constructing Basis

INPUT: A positive integer $n > 3$ and a square free integer d.
OUTPUT: A polynomial representation R of $\sqrt{d}$ in $\mathbb{Q}[x]/(\Phi_n(x))$ or failure if $\mathbb{Q}(\zeta_n)$ does not contain $\sqrt{d}$.

1. Set $R = 1$.
2. **TEST INPUT**
   - Test if $d \mid n$. If not, stop and report failure. Else continue.
   - Test if $2 \mid d$. If so and $8 \nmid n$ stop and return failure. Else continue.
   - Test if $d < 0$. If so check that $d \equiv 3 \pmod 4$ or $4 \mid n$. If not, stop and return failure. Else continue.
   - Test if $d > 0$. If so check that $d \equiv 1 \pmod 4$ or $4 \mid n$. If not, stop and return failure. Else continue.
3. Factorize $d = p_1 p_2 .... p_r$
4. For $i = 1$ to r :
   (a) if $(p_i \neq 2)$
      - Construct a p_i^{th} root of unity. Let $\theta = x^{n/p_i}$.
      - Construct a polynomial representation of $\sqrt{\pm p_i}$, $P_i(y)$, where y is assumed to be a p_i^{th} root of unity using relation (1).
      - Multiply R by $P_i(\theta)$.

   (b) else
      - Construct an eight and fourth root of unity $\zeta_4 = x^{n/4}$, $\zeta_8 = x^{n/8}$.
      - Multiply R by $\zeta_n \zeta_8 (1 + \zeta_4)$.
5. (Correct Sign).
   - If $d < 0$ and $d \equiv 1 \pmod 4$. Multiply R by $\zeta_4 = x^{n/4}$.
   - If $d > 0$ and $d \equiv 3 \pmod 4$. Multiply R by $\zeta_4 = x^{n/4}$.
   - If $2 \mid d$. Then:
     - If $d < 0$ and $(d/2) \equiv 1 \pmod 4$. Multiply R by $\zeta_4 = x^{n/4}$.
     - If $d > 0$ and $(d/2) \equiv 3 \pmod 4$. Multiply R by $\zeta_4 = x^{n/4}$.
6. Return R.

3 Overview

Let E be an elliptic curve over the finite field $\mathbb{F}_q$ (note: $q = p^1$ where p is a prime) and let $\#E(\mathbb{F}_q) = hl$ where l is the largest prime dividing $\#E(\mathbb{F}_q)$ such that $l \nmid (q-1)$. Then $\#E(\mathbb{F}_q) = hl = q+1-t$; where t is the trace of Frobenius. This implies that $q \equiv t - 1 \pmod l$. The embedding degree of $E(\mathbb{F}_q)$ is defined to be the least positive integer k such that l divides $q^k - 1$. This is equivalent to the following condition observed by Cocks and Pinch [5]: $t - 1 \equiv \zeta_k \pmod l$; where ζ_k is a primitive k^{th} root of unity. For a given k our goal is to construct an elliptic curve E over $\mathbb{F}_q$ such that $E(\mathbb{F}_q)$ has embedding degree k with respect to a prime l and the ratio $\rho = log(q)/log(l)$ is as close to 1 as possible.

We now describe how to construct the Frobenius element (denoted by π) of an elliptic curve with the desired properties. The general methodology used here is the same as that of [6]. Our contribution is the algorithm in section 2.3. This algorithm allows us to use arbitrary imaginary quadratic fields contained in some cyclotomic field. Brezing and Weng used imaginary quadratic fields which were isomorphic to cyclotomic fields i.e. $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_4)$. In both of these cases it is trivial to find a basis for the imaginary quadratic field. Although their theory acknowledges that the imaginary quadratic field does not have to be a cyclotomic field, they do not explain how to work examples in the case where the quadratic field is not isomorphic to a cyclotomic field.

Let $g(x)$ be some primitive k^{th} root of unity in $M = \mathbb{Q}[x]/(\Phi_n(x))$ or more generally $M = \mathbb{Q}(\zeta_n, \sqrt{-D})$ where $-D$, for $D > 0$ is the discriminant of an imaginary quadratic field, ζ_n a primitive n^{th} root of unity and $k \mid n$. Let $h(x)$ be a polynomial which represents $\sqrt{-D}$ or $\sqrt{-D/4}$ in M depending on whether $-D \equiv 1 \pmod 4$ or $-D \equiv 0 \pmod 4$ respectively. We refer the reader to section 2.2 for detailed examples on how to construct $h(x)$. Suppose also that $g(x)$ and $h(x)$ lie in $\mathbb{Z}[x]$. Construct the polynomials $a(x)$, $b(x)$ and $p(x)$ with conditions satisfied as in [6]:

$$\begin{aligned} a(x) &:= g(x) + 1 \\ b(x) &:= (a(x) - 2)h(x) \\ p(x) &:= \frac{1}{4}(a(x)^2 + \frac{b(x)^2}{D}) \end{aligned}$$

Note that $a(x)$ represents the trace of Frobenius. We then try to find primes l and p such that $l = \Phi_n(x_1)$ and $p = p(x_1)$ where $x_1 \equiv x_0 \pmod D$. If we can find such primes, then we can find an elliptic curve E with order $\#E(\mathbb{F}_q)$ divisible by l with embedding degree k. As we know such a curve will have complex multiplication by the order

$$\mathcal{O} = \mathbb{Z}[\pi(x_1)] = \mathbb{Z}[\frac{a(x_1) \pm \frac{b(x_1)}{D}\sqrt{-D}}{2}]$$

To see why this is the case consider the values of

$$\#E(\mathbb{F}_{p(x_1)}) = N_{\mathbb{Q}(\sqrt{-D})/\mathbb{Q}}(\pi(x_1) - 1)$$

and

$$p(x_1) = \pi(x_1)\bar{\pi}(x_1)$$

where $\pi(x) = \frac{a(x) - \frac{b(x)}{D}\sqrt{-D}}{2}$. Reduced modulo l the first equation yields

$$\begin{aligned} N_{\mathbb{Q}(\sqrt{-D})/\mathbb{Q}}(\pi(x_1) - 1) &= \frac{(a(x_1) - 2)^2 + \frac{b(x)^2}{D}}{4} \\ &\equiv \frac{(\zeta_k - 1)^2 - (\zeta_k - 1)^2}{4} \pmod l \\ &\equiv 0 \pmod l \end{aligned}$$

while the second equation becomes

$$\pi(x_1)\bar{\pi}(x_1) = \frac{1}{4}(a(x_1)^2 + \frac{b(x_1)^2}{D}) \equiv \frac{(\zeta_k + 1)^2 - (\zeta_k - 1)^2}{4} \equiv \zeta_k \pmod l$$

4 Numerical Results

This section contains examples of the possible numerical results which can be achieved using our method. The listed examples are in no way exhaustive. Most parameters have extremely dense solutions sets, meaning that for a given $-D, k$ and n the possible values for x_1 which give suitable output are quite numerous and easily found. Examples of this include the parameters $(-D, k, n) = (-7, 14, 14,), (-15, 15, 15)$. Other parameters give very sparse solution sets. For $(-D, k, n) = (-7, 28, 56)$ the first solution gives a 377 bit prime l. This may be due to the higher degree of $\Phi_n(x)$ leading to fewer representable primes of suitable size. More work is needed to improve this situation, perhaps consideration of a more general polynomial family for the representation of l.

The numerical results were computed using a C++ program making use of the LiDIA [2] and GMP [1] libraries. Michael Scott's complex multiplication implementation [12] was used to generate the final curves which are given in the tables below by $E : y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{F}_q$ $(q = p(x_1)^1)$.

4.1 Tabulated Summary Of Results

$\phi(k)$	k	$-D$	n	Actual ρ	Bound ρ	$log_2(l)$	$log_2(q)$
4	10	-20	40	1.732	1.750	187	324
4	10	-15	30	1.737	1.750	160	272
6	7	-7	7	1.650	1.666	160	264
6	14	-7	14	1.654	1.666	162	268
8	15	-15	15	1.725	1.750	160	276
8	24	-8	24	1.475	1.500	160	236
10	11	-11	22	1.775	1.800	169	300
10	22	-11	44	1.793	1.800	237	425
12	28	-7	56	1.493	1.500	377	563
12	28	-7	28	1.820	1.833	234	426

4.2 $\phi(k) = 4$

k	10
-D	-20
n	40
$\Phi_n(x)$	$x^{16} - x^{12} + x^8 - x^4 + 1$
g(x)	$-x^{12} + x^8 - x^4 + 1$
h(x)	$-2x^{14} + x^{10} - 2x^6$
x_1	3196
l	118497265990650143638940886913063255688422174813106568961(187 bits)
q	2691656114049822988376675914574795422806785455749627181432 9796276308782360965160815950571330669569(324 bits)
ρ	1.73262
A	2
B	25575441317520594647996278509327595814781177583607486825447 55542022504589304559812663114754842137
$\#E(\mathbb{F}_q)$	269165611404982298837667591457479542280678545574962718154655 42359371237908912671854899838150479104
h	227149216612491653871749738083825253649664

k	10
-D	-15
n	30
$\Phi_n(x)$	$x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$
g(x)	x^3
h(x)	$2x^7 - 2x^5 - 4x^4 - 2x^3 - 2x^2 + 4x + 3$
x_1	-1028669
l	1253732242268690674049383020671966019699064954321 (160 bits)
q	39612061054789106390969804068289066415604050183196 3430185626838652064692433391635091 (272 bits)
ρ	1.7375
A	2
B	384776587942284046569417998917012451962737988852464805 945105201423467817793288117568
$\#E(\mathbb{F}_q)$	39612061054789106390969804068289066415604050183 1963430185626838653153188731457177400
h	315953117574045294258870823811369400

4.3 $\phi(k) = 6$

k	7
-D	-7
n	7
$\Phi_n(x)$	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
g(x)	x
h(x)	$-2x^4 - 2x^2 - 2x - 1$
x_1	-100667465
l	1040722131042824291503998495039735508885676564761(160 bits)
q	15268391681519532829942582276850914805033533358709195412419252889296190850361031 (264 bits)
ρ	1.65
A	6904773185115407288774998350780739098916655907628522574186610383491054693339853
B	13251658526834614301595330074142879828332779599503131865585960266801828161187012
$\#E(\mathbb{F}_q)$	15268391681519532829942582276850914805033533358709195412419252889296190951028496
h	14670958967904622570631039861136

k	14
-D	-7
n	14
$\Phi_n(x)$	$x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$
g(x)	x
h(x)	$-2x^4 - 2x^2 + 2x - 1$
x_1	133004537
l	5536033773959257978391961177327958068345407274793(162 bits)
q	247495046145227616682894072671426466574818509920143212768914007106237443263422969(268 bits)
ρ	1.65432
A	11
B	71285808459422779938688412730348685273804058581787919610711710083152769312725972
$\#E(\mathbb{F}_q)$	247495046145227616682894072671426466574818509920143212768914007106237443130418432
h	44706202355449906932824497773824

4.4 $\phi(k) = 8$

k	15
-D	-15
n	15
$\Phi_n(x)$	$x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$
g(x)	x^2
h(x)	$-2x^7 + 2x^5 - 4x^4 + 2x^3 - 2x^2 + -4x + 3$
x_1	-1000471
l	1003775220704386773178297083604487423516523566881(160 bits)
q	247495046145227616682894072671426466574818509920143212768914007106237443263422969(276 bits)
ρ	1.725
A	6
B	4029514575351498550139991979767287914867834918099249017754788402239844319671554731 3
$\#E(\mathbb{F}_q)$	671077491930193455092875722166472531788997764352607192748592598661190335507246781 40
h	6685535547084666764287115746301094 0

k	24
-D	-8
n	24
$\Phi_n(x)$	$x^8 - x^4 + 1$
g(x)	x
h(x)	$-x^5 - x^3 + x$
x_1	-985463
l	889452139047835861417980800969216088560624633761 (160 bits)
q	1048563582552305367800197044893830726902849800202982672138417 79302725409(236 bits)
ρ	1.475
A	1
B	1023963806031047812676889009518936467970885870987298707653416 01082901825
$\#E(\mathbb{F}_q)$	1048563582552305367800197044893830726902849800202982672138417 79303710872
h	117888702103161988307352

4.5 $\phi(k) = 10$

k	11
-D	-11
n	22
$\Phi_n(x)$	$x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$
g(x)	x^2
h(x)	$2x^9 + 2x^5 - 2x^4 + 2x^3 + 2x - 1$
x_1	-18658
l	449044374966079776811018938862000399066079697680411 (169 bits)
q	1357441919222352203382074016394474770290194297862981173430741491198729593166465924090047211 (300 bits)
ρ	1.77515
A	-3
B	619390962271619881020563887569843211715485828959953678398832824586309700504136093237616017
$\#E(\mathbb{F}_q)$	1357441919222352203382074016394474770290194297862981173430741491198729593166465910586212775
h	3022957183964038266269047184406033927525

k	22
-D	-11
n	44
$\Phi_n(x)$	$x^{20} - x^{18} + x^{16} - x^{14} + x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$
g(x)	$-x^{16}$
h(x)	$2x^{36} + 2x^{20} + 2x^{16} + 2x^{12} + 2x^4 + 1$
x_1	-3616
l	146072480042839735410839194855815902380834280400918514359230300179430401 (237 bits)
q	45382715071996076852244307042606621548796179757008093618976734645298549353613552077513158958602545660520238745221082532592382511(425 bits)
ρ	1.79325
A	1
B	37840467800420056507144940890276367088595736218617547958652445648078663095915069888648827721118413252917019980177642352154718308
$\#E(\mathbb{F}_q)$	45382715071996076852244307042606621548796179757008093618976734645298550208000782574271143051912222578493258834949276209314951727
h	310686277515698774524080190155394166389785366317894970927

4.6 $\phi(k) = 12$

k	28
-D	-7
n	56
$\Phi_n(x)$	$x^{24} - x^{20} + x^{16} - x^{12} + x^8 - x^4 + 1$
g(x)	x^2
h(x)	$-2x^{32} - 2x^{16} - 2x^8 - 1$
x_1	-52863
l	226800152294323177942420071321155727783101516305369247057567782068436961779089828080279772242398751946572875092481(377 bits)
q	154300371767859141675459960546834345538636866874241707938903498782211428953884334310603399988674621724711560929866065143770675792186501982116511368569268318113064411880 97(563 bits)
ρ	1.49337
A	6
B	158275426407123834728836268767365342556028036103393826303940542770296655515672035567698814841103628468254289626675565978540700897291957185373411407578387113211113447091 3
$\#E(\mathbb{F}_q)$	154300371767859141675459960546834345538636866874241707938903498782211428953884334310603399988674621724711560929866065143770675792186501982116511368569268318113036466913 28
h	6803362793496734775898298507439638553214964764333231308 8

k	28
-D	-7
n	28
$\Phi_n(x)$	$x^{12} - x^{10} + x^8 - x^6 + x^4 - 1x^2 + 1$
g(x)	x^3
h(x)	$-2x^8 - 2x^4 + 2x^2 - 1$
x_1	-724247
l	20827659027425489963756462886247268966068900480293595663855491908821297 (234 bits)
q	1181434009177633862291643211695317654788308498138683722202415825031045302497172549334381829488725773863722769670019609631189372 09 (426 bits)
ρ	1.82051
A	17
B	72794043783606148440980385477445215391850990370190154330885804742240644630649331833197704638020599074688184087825214497695038730
$\#E(\mathbb{F}_q)$	11814340091776338622916432116953176547883084981386837222024158250310453024971725493343818294887257738637227696738185293406155443 2
h	5672428224515979586931610079091374501265707945018575219456

5 Conclusion

We have developed an algorithm to extend the Brezing-Weng method for discriminants $D > 4$. This new approach has enabled us to generate suitable elliptic curve parameters with embedding degree k, which for $\phi(k) > 4$ exhibit an improved ratio relative to published material [3],[7], where the ratio may be up to 2.

5.1 Acknowledgments

We would like to thank Michael Scott for his support and for bringing to our attention his unpublished results for D=7,k=7 and D=8,k=24; and Steven Galbraith for his helpful comments and advice on this paper.

References

[1] GMP: GNU Multiple Precision Arithmetic Library. Version 4.1.4. **http://www.swox.com/gmp/**.

[2] LiDIA: A C++ library for computational number theory. Version 2.1.3. **http://www.informatik.tu-darmstadt.de/TI/LiDIA/**.

[3] P.S.L.M. Barreto, B Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. *Security in Communication Networks*, Vol. 2576 of *Lecture Notes in Computer Science*:263–273, 2002.

[4] P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. Cryptology ePrint Archive, Report 2005/133, 2005. **http://eprint.iacr.org/**.

[5] I.F. Blake, G. Seroussi, and N.P. Smart. *Advances in Ellipitic Curve Cryptography.* Cambridge University Press, 2005.

[6] F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. *Designs, Codes and Cryptography*, to appear.

[7] R. Dupont, A. Enge, and F. Morain. Building curves with arbitrary small MOV degree over finite prime fields. *Journal of Cryptography*, 18(2005),79-89.

[8] S.D. Galbraith, J. McKee, and P. Valenca. Ordinary abelian varieties having small embedding degree. Cryptology ePrint Archive, Report 2004/365, 2004. **http://eprint.iacr.org/**.

[9] G.J. Janusz. *Algebraic Number Fields, Second Edition.* American Mathematical Society, 1991.

[10] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Transactions on Fundamentals*, E84-A(5):1234–1243, 2001.

[11] P. Ribenboim. *Classical Theory of Algebraic Numbers.* Springer, 2001.

[12] M. Scott, 2002. **http://ftp.compapp.dcu.ie/pub/crypto/cm.exe**.

[13] M. Scott and P.S.L.M Barreto. Generating more MNT elliptic curves. Cryptology ePrint Archive, Report 2004/058, 2004. **http://eprint.iacr.org/**.