Ordinary abelian varieties having small embedding degree

Steven D. Galbraith*, J. McKee and P. Valença

Mathematics Department, Royal Holloway University of London,
Egham, Surrey TW20 0EX, UK.
Steven.Galbraith,James.McKee,P.Valenca@rhul.ac.uk

Abstract. Miyaji, Nakabayashi and Takano (MNT) gave families of group orders of ordinary elliptic curves with embedding degree suitable for pairing applications. In this paper we generalise their results by giving families corresponding to non-prime group orders. We also consider the case of ordinary abelian varieties of dimension 2. We give families of group orders with embedding degrees 5, 10 and 12.

1 Introduction

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ and suppose that

$$\#E(\mathbb{F}_q) = n = hr\,,$$

where r is the largest prime divisor of n. (For cases of interest, h will be 'small'.) Define the *embedding degree* to be the smallest positive integer k such that

$$r \mid q^k - 1\,.$$

In other words, k is minimal such that $r \mid \Phi_k(q)$ where $\Phi_k(x)$ is the k-th cyclotomic polynomial (see Section VI.3 of Lang [11]). The Weil pairing is a function

$$e : E[r] \times E[r] \to \mu_r \subset \mathbb{F}_{q^k}^*$$

where μ_r is the set of r-th roots of unity in $\mathbb{F}_{q^k}^*$.

Currently one of the most active areas in elliptic curve cryptography is the use of the Weil and Tate pairings to construct cryptographic protocols. A fundamental problem in this area is to construct elliptic curves E such that the embedding degree k is of a suitable size.

One popular solution to the problem is to use supersingular curves. In characteristic two there are curves which allow $k = 4$, while in characteristic three there are curves which allow $k = 6$. Efficient implementations using these curves have been developed [2, 7, 10]. There are, however, some unfortunate problems with this approach. First, there are only a small number of suitable group orders available. Second, due to Coppersmith's index calculus method for discrete

* This author thanks the Nuffield foundation grant NUFF NAL-02 for support.

logarithms in finite fields of low characteristic, the field sizes should be larger than those used in the case of large prime characteristic.

Hence it is attractive to use ordinary (i.e., non-supersingular) curves. This is made possible by the important paper of Miyaji, Nakabayashi and Takano [12]. They give families of group orders of ordinary curves with embedding degrees 3, 4 and 6.

In this paper we extend the methods of Miyaji, Nakabayashi and Takano (MNT) in two directions. First, we obtain a larger class of families by incorporating cofactors into the analysis. This idea has also been used by Scott and Barreto [15], although they do not give explicit families.

The second direction taken in the paper is to consider abelian varieties of dimension two. Supersingular abelian varieties have already been proposed for pairing-based cryptography [9, 13]. For example, one can obtain embedding degree 12 from a supersingular abelian surface in characteristic two. We give heuristics which suggest that suitable ordinary abelian surfaces exist. We describe our search for families and give some results. One interesting observation is that the embedding degree 12 cases in characteristic two can also be realised using ordinary abelian varieties.

2 The original MNT results

Miyaji, Nakabayashi and Takano [12] presented explicit families of group orders of ordinary elliptic curves with embedding degree $3, 4$ and 6. More precisely, they gave polynomials $q(l)$ and $t(l)$ in $\mathbb{Z}[l]$ such that the polynomial $n(l) = q(l)+1-t(l)$ divides the polynomial $\Phi_k(q(l))$. Hence, for any integer value l such that $q = q(l)$ is a prime (or prime power) and such that $|t(l)| \leq 2\sqrt{q}$, there is an elliptic curve E over $\mathbb{F}_q$ with $n(l)$ points and embedding degree k. The families they obtained are presented in Table 1.

k	$q(l)$	$t(l)$	$n(l)$
3	$12l^2 - 1$	$-1 \pm 6l$	$12l^2 \pm 6l + 1$
4	$l^2 + l + 1$	$-l, l + 1$	$l^2 + 2l + 2, l^2 + 1$
6	$4l^2 + 1$	$1 \pm 2l$	$4l^2 \pm 2l + 1$

Table 1. MNT families

In each case, $q(l)$ is a quadratic polynomial in l that (heuristically) represents $\theta(\sqrt{X}/\log X)$ prime powers below X. We refer to such families as *quadratic families*. Note the requirement on the heuristic density of prime powers represented by $q(l)$: quadratic polynomials such as $-l^2 + 17$, $6(l^2 + l + 1)$, or $2l^2$ would not satisfy this condition (the last of these (provably!) represents infinitely many prime powers, but with the wrong density), whereas $q(l) = l^2$ would be fine if it arose.

3 Generalisation to cofactors

The MNT results in the previous section cover the cases where $n = \#E(\mathbb{F}_q)$ satisfies $n \mid \Phi_k(q)$. This is most relevant cryptographically for the case where n is prime. However, in cryptography we are also interested in cases where the group order is 'nearly prime', i.e., when $n = \#E(\mathbb{F}_q) = hr$ where $h > 1$ is small, and r is a prime. We then require merely that $r \mid \Phi_k(q)$, and call h the *cofactor*. In fact we do not mind if r itself is a small multiple of a prime, and we can therefore insist that $\gcd(h, \Phi_k(q)) = 1$, else we could reduce to a case with smaller h. We define λ by the equation $\Phi_k(q) = \lambda r$.

Some earlier work on cofactors appears in [15], but they do not give explicit families. Here we generalise the MNT argument to allow for cofactors, indicating how all curves with prescribed cofactor and embedding degree may be found. Other generalisations of the MNT approach have been given in [3, 6].

3.1 The details in the case $k = 6$

We require $\lambda r = \Phi_6(q) = q^2 - q + 1$. Applying the same idea as in [12], we observe that

$$n(h(q+1+t) - \lambda) = h(q+1-t)(q+1+t) - hr\lambda = h(3q - t^2). \qquad (1)$$

Dividing by qh gives

$$\frac{n}{q}\big((q+1+t) - \lambda/h\big) = 3 - \frac{t^2}{q}$$

and Hasse's bound for the number of points yields

$$-4/3 < (q+1+t) - \lambda/h < 3\,,$$

for $q > 64$. (Hasse's bound readily yields $q/n < 4/3$ for large enough q, which with $3 - t^2/q \geq -1$ yields the lower bound. For the upper bound, suppose instead that $(q/n)(3 - t^2/q) \geq 3$. With $n = q + 1 - t$ this gives $t^2 - 3t + 3 \leq 0$, which has no real solutions.)

Define $w = \lfloor \lambda/h \rfloor$ and $\epsilon = \lambda/h - w$ so that $\lambda = (w + \epsilon)h$. We may assume that $\epsilon > 0$ since if $h \mid \lambda$ then $n = hr \mid \Phi_6(q)$ and we are in the original MNT case. Furthermore, we may assume that $\gcd(h, \lambda) = 1$ or else we reduce to a case with smaller h.

We have

$$-4/3 + \epsilon < q + 1 + t - w < 3 + \epsilon < 4$$

and so $v := q + 1 + t - w \in \{-1, 0, 1, 2, 3\}$.

Now substitute into equation (1) to obtain the quadratic

$$t^2 - t(v - \epsilon) + (q+1)(v - \epsilon) - 3q.$$

The solutions to this equation are

$$t = \frac{v - \epsilon \pm \sqrt{\sigma(q,\epsilon)}}{2}$$

where

$$\sigma(q,\epsilon) = (v-\epsilon)^2 + 12q - 4(q+1)(v-\epsilon).$$

Since we want t to be an integer it follows that $\sqrt{\sigma(q,\epsilon)}$ must be of the form $a \pm \epsilon$ for some integer a.

This equation alone does not provide much information, so we consider each possible value for v separately. Writing $\epsilon = \frac{u}{h}$ with u, h co-prime and fixing $v \in \{-1, 0, 1, 2, 3\}$ gives the formulae presented in Table 2. In fact when $v = -1$, and $h \geq 2$, we have that $h\epsilon$ is a positive integer, and hence that

$$r \leq h\epsilon r = (t^2 - 4q) + t - 1 \leq t - 1 = O(\sqrt{q}),$$

which is uninteresting, so we omit this from future discussion.

v	$h^2\sigma(q, u/h)$
-1	$4h(4h+u)q + u^2 + 6uh + 5h^2$
0	$4h(3h+u)q + u^2 + 4uh$
1	$4h(2h+u)q + u^2 + 2uh - 3h^2$
2	$4h(h+u)q + u^2 - 4h^2$
3	$4uhq + u^2 - 2uh - 3h^2$

Table 2. $\sigma(q, u/h)$, fixing v.

Recall that we want $h^2\sigma(q, u/h)$ to be an integer square, say x^2. It is helpful to write $h^2\sigma(q, u/h)$ as $M(u,h) + N(u,h)q$. Our condition that $h^2\sigma(q, u/h) = x^2$ then gives rise to the requirement that $M(u,h)$ be a quadratic residue modulo $N(u,h)$. The pairs (M, N) are listed in Table 3.

v	$M(u,h)$	$N(u,h)$
0	$u^2 + 4uh$	$4h(3h+u)$
1	$u^2 + 2uh - 3h^2$	$4h(2h+u)$
2	$u^2 - 4h^2$	$4h(h+u)$
3	$u^2 - 2uh - 3h^2$	$4uh$

Table 3. Values of $M(u,h)$ and $N(u,h)$.

We now consider particular values for h in turn.

3.2 Curves with cofactor $h = 2$

The case of cofactor $h = 2$ is the simplest case. The group order of such a curve is $\#E(\mathbb{F}_q) = 2r$ where $r \mid (q^2 - q + 1)$. If $2r \mid (q^2 - q + 1)$ then this case is covered by Miyaji *et al.* So we assume that $2r \nmid (q^2 - q + 1)$. In this case $u = 1$ and $\epsilon = 1/2$.

The first stage is to deduce which values for v are permissible. Substituting $(u, h) = (1, 2)$ into table 3 gives the following analysis.

v = 0 : We obtain $x^2 \equiv 9 \pmod{8 \cdot 7}$ and so $x = \pm 3 + 14l$. Now, the equation $x^2 = h^2\sigma(q, 1/2) = 9 + 56q$ implies that

$$q = \frac{l(\pm 3 + 7l)}{2}.$$

One can deduce the corresponding values of t from the formula $t = (hv - u \pm x)/(2h)$ and obtain

$$t = \frac{1 \pm 7l}{2} \text{ or } t = -1 \pm \frac{7l}{2}.$$

Since the expression for q splits in $\mathbb{Q}[l]$ this case is not useful for producing large prime values for q. In fact, the only possible choices are $l = 2$ which gives $(q, t) = (17, -8)$ with group order $2 \cdot 13$ and $l = 3$, which gives $(q, t) = (3^3, -10)$ with group order $2 \cdot 19$.

v = 1 : This case yields no solutions since $x^2 \equiv -7 \pmod{8 \cdot 5}$ is insoluble.

v = 2 : The condition in this case is $x^2 \equiv -15 \pmod{8 \cdot 3}$ and so $x = 3 + 6l$, From $9(1 + 2l)^2 = 24q - 15$ we deduce that $q = (3l^2 + 3l + 2)/2$, which is irreducible in $\mathbb{Q}[l]$.

The full parameterised family is

$$q = \frac{3l^2 + 3l + 2}{2}$$
$$t = \frac{3 + 3l}{2} \text{ or } t = \frac{-3l}{2}.$$

v = 3 : The congruence is $x^2 \equiv -15 \pmod 8$ which implies $x = 1 + 2l$ and $q = (l^2 + l + 4)/2$. Again this is irreducible in $\mathbb{Q}[l]$.

The full parameterised family is

$$q = \frac{l^2 + l + 4}{2}$$
$$t = \frac{3 + l}{2} \text{ or } t = 1 - \frac{l}{2}.$$

We have therefore produced two quadratic families of ordinary elliptic curves with cofactor 2 and embedding degree 6. Since we wish for t to be an integer, and for q to represent prime powers, we can place certain congruence conditions on l in each case. When this is done, q and t are expressed as polynomials in $\mathbb{Z}[l]$, and these are the (q, t) pairs presented in the tables below.

Using similar analysis for cofactors up to 5, and some MAGMA [5] code, we get the following theorem.

Theorem 1. *The only quadratic families of elliptic curves that have embedding degree 3, 4, or 6, and cofactor h in the range $2 \leq h \leq 5$ are those given by tables 4, 5 and 6. (Note that the parameter l may be chosen to be positive or negative.)*

h	q	t
2	$8l^2 + 2l + 1$	$-2l$
	$56l^2 + 6l - 1$	$-14l - 2$
	$56l^2 + 22l + 1$	$-14l - 4$
3	$12l^2 + 8l + 3$	$2l + 1$
4	$16l^2 + 6l + 3$	$-2l$
	$48l^2 + 30l + 5$	$6l + 2$
	$112l^2 + 26l + 1$	$-14l - 2$
	$112l^2 + 58l + 7$	$-14l - 4$
5	$20l^2 + 12l + 5$	$2l + 1$
	$140l^2 + 64l + 7$	$14l + 3$
	$140l^2 + 104l + 19$	$14l + 5$
	$260l^2 + 44l + 1$	$-26l - 3$
	$260l^2 + 164l + 25$	$-26l - 9$
	$380l^2 + 112l + 7$	$-38l - 7$
	$380l^2 + 192l + 23$	$-38l - 11$

Table 4. Valid pairs (q, t) corresponding to $k = 3$ and $2 \leq h \leq 5$

These families cover all the examples found by Scott and Barreto in [15]. For $k = 6$, $h = 4$ and '$d = 13$' (in the notation of their paper) they produced a strikingly large number of examples. These ones come from our families $q(l) = 208l^2+30l+1$ and $q(l) = 208l^2+126l+19$, the first of which is particularly lucky in generating (q, t) pairs for which the construction of a corresponding curve via Complex Multiplication works well.

Selecting one of these pairs (q, t), it is possible to construct an elliptic curve $E/\mathbb{F}_q$ with $q + 1 - t$ points by using Complex Multiplication (see, for example, [4] and [18]). We outline the preparatory details here.

Associated with an elliptic curve is the quantity $t^2 - 4q$ which is negative. Write

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

where $D > 0$ is either of the form $4d$ or d with d square-free. Since $Dy^2 \equiv -t^2 \equiv 0, 3 \pmod 4$, $D = 4d$ when t is even and $D = d$ when t is odd.

Miyaji *et al* noted that, substituting t and q with the formulae they obtained, the problem corresponded to solving a general Pell equation. Similarly, given q and t as polynomials in l (as in tables 4, 5 or 6), the RHS in (2) is now a polynomial in l with degree exactly 2 and (2) can be rewritten as

$$x^2 - sdy^2 = m\,. \tag{3}$$

h	q	t
2	$8l^2+6l+3$	$-2l$
3	$12l^2+2l+3$	$2l+1$
	$12l^2+10l+5$	$-2l$
	$60l^2+14l+1$	$-10l-1$
	$60l^2+26l+3$	$-10l-2$
	$60l^2+34l+5$	$10l+3$
	$60l^2+46l+9$	$10l+4$
4	$16l^2+14l+7$	$-2l$
	$80l^2+38l+5$	$-10l-2$
	$80l^2+58l+11$	$10l+4$
	$208l^2+54l+3$	$-26l-4$
	$208l^2+106l+13$	$26l+6$
5	$20l^2+2l+5$	$2l+1$
	$20l^2+18l+9$	$-2l$
	$260l^2+74l+5$	$-26l-4$
	$260l^2+126l+15$	$26l+6$
	$260l^2+134l+17$	$-26l-7$
	$260l^2+186l+33$	$26l+9$
	$340l^2+46l+1$	$-34l-3$
	$340l^2+114l+9$	$34l+5$
	$340l^2+226l+37$	$-34l-12$
	$340l^2+294l+63$	$34l+14$

Table 5. Valid pairs (q,t) corresponding to $k=4$ and $2 \leq h \leq 5$

h	q	t
2	$8l^2+6l+3$	$2l+2$
	$24l^2+6l+1$	$-6l$
3	$12l^2+4l+3$	$-2l+1$
	$84l^2+16l+1$	$-14l-1$
	$84l^2+128l+49$	$14l+11$
4	$16l^2+10l+5$	$2l+2$
	$112l^2+54l+7$	$14l+4$
	$112l^2+86l+17$	$14l+6$
	$208l^2+30l+1$	$-26l-2$
	$208l^2+126l+19$	$-26l-8$
5	$20l^2+8l+5$	$-2l+1$
	$60l^2+36l+7$	$6l+3$
	$140l^2+36l+3$	$-14l-1$
	$140l^2+76l+11$	$-14l-3$
	$260l^2+96l+9$	$26l+5$
	$260l^2+216l+45$	$26l+11$
	$380l^2+188l+23$	$38l+9$
	$380l^2+268l+47$	$38l+13$

Table 6. Valid pairs (q,t) corresponding to $k=6$ and $2 \leq h \leq 5$

After solving this Pell-type equation, one can construct the curve via Complex Multiplication in the usual way.

4 Heuristics

In this section we give heuristic arguments which predict the number of ordinary abelian varieties of dimension two over $\mathbb{F}_q$ with $q \leq M$ with moderate embedding degree. To explain and motivate our methods we first discuss the elliptic curve case.

4.1 Heuristics in the elliptic curve case

Let k be a positive integer. Consider the set

$$S = \{(q, n) \in \mathbb{R}^2 : 1 \leq q \leq M, |q + 1 - n| \leq 2\sqrt{q}\}$$

whose volume is roughly $\frac{8}{3}M\sqrt{M}$. Hence we expect that $\#(\mathbb{Z}^2 \cap S)$ is also roughly $\frac{8}{3}M\sqrt{M}$.

Now consider the set

$$S' = \{(q, n) \in \mathbb{Z}^2 \cap S : n \mid \Phi_k(q)\}.$$

This set contains the pairs $(q, \#E(\mathbb{F}_q))$ as above which have embedding degree dividing k, but for the moment we do not restrict to prime power values of q.

Let us make the reasonable assumption that we expect $n \mid \Phi_k(q)$ with probability $\theta(1/n)$. (The number of solutions to $\Phi_k(x) \equiv 0 \pmod{n}$ behaves erratically as n varies, but some recent work of Scourfield [16] shows that it is on average constant.) Now, approximating $n \approx M$ we deduce that the number of points in S' is roughly $\theta(1/M)$ times the number of points in $\mathbb{Z}^2 \cap S$.

This heuristic is supported perfectly by the results in the elliptic curve case. There we find that (apart from a finite number of exceptional cases) the values q are quadratic in a parameter l, and each such q yields two possible group orders n. Thus there are of order $\sqrt{M}$ numbers of points in S', corresponding to $\theta(\sqrt{M})$ possibilities for l. Note that the quadratic families in question are not exactly those tabulated earlier: when $k = 3$ (respectively 6) the relevant $q(l)$ is $3l^2 - 1$ (respectively $l^2 + 1$). Considerations of prime-powerness led to the modified families in table 1. Of course one expects only $\theta(\sqrt{M}/\log M)$ elements of S' for which q is a prime power.

Some related work to the above is the result of Balasubramanian and Koblitz [1] which implies that there are $O(\sqrt{M}(\log M)^9(\log\log M)^2)$ isogeny classes of elliptic curves over $\mathbb{F}_p$ with $M/2 \leq p \leq M$, $\#E(\mathbb{F}_p) = r$ prime, and $r \mid (p^k - 1)$ for some $k \leq (\log p)^2$.

4.2 Heuristics in the abelian surface case

Let A be an abelian variety of dimension 2 over $\mathbb{F}_q$. The characteristic polynomial of the Frobenius endomorphism is $P(T) = T^4 + a_1T^3 + a_2T^2 + qa_1T + q^2$ and the coefficients a_1 and a_2 satisfy certain bounds. Then $n = \#A(\mathbb{F}_q) = P(1) = q^2 + a_1q + a_2 + a_1 + 1$ and it is known that $(\sqrt{q}-1)^4 < n < (\sqrt{q}+1)^4$. If A is ordinary, then we get more precise bounds $|a_1| < 4\sqrt{q}$ and $-2q + 2|a_1|\sqrt{q} < a_2 < a_1^2/4 + 2q$ (see Rück [14]). Since $n \approx q^2$ we generally choose k so that $\varphi(k) \geq 4$.

Motivated by the elliptic curve case, we define

$$S = \{(q, n) : 1 \leq q \leq M, |n - q^2| < 4q\sqrt{q}\}.$$

The volume of S is about $3M^{5/2}$. Similarly, define

$$S' = \{(q, n) \in \mathbb{Z}^2 \cap S : n \mid \Phi_k(q)\}.$$

As before, we assume that the values $\Phi_k(q)$ are on average evenly distributed modulo n. Since $n \approx M^2$ there is therefore a $\theta(1/M^2)$ probability that $n \mid \Phi_k(q)$. It follows that the number of points in S' is $\theta(\sqrt{M})$.

The fact that the heuristic in the dimension 2 case gives results similar to the elliptic curve case means it is reasonable to hope that families could be obtained with q a quadratic polynomial in some parameter.

5 An alternative approach to the MNT method

The powerful arguments of Miyaji, Nakabayashi and Takano for elliptic curves do not seem to extend to higher dimensions. We shall now take an alternative approach, that although weaker does readily extend, and which will allow us to find infinite families for abelian varieties of dimension 2. In this section we introduce the ideas in the more familiar elliptic curve setting, and recover all the MNT families, before moving to dimension 2.

If we seek families with embedding degree k (3, 4, or 6) where $q(l)$ is a quadratic polynomial in l, then we are looking for

$$\Phi_k(q(l)) = n_1(l)n_2(l)\,,$$

where $n_1(l)$ and $n_2(l)$ are quadratic polynomials.

Ignoring any constraints on the leading coefficients, let us characterise those quadratic polynomials $q(l)$ with rational coefficients for which $\Phi_k(q(l))$ splits over the rationals as a product of two quadratic polynomials. We give this for general k, as we shall wish to consider $k = 5$, 8, 10, or 12 for the dimension 2 work.

Lemma 1. *Let $q(l)$ be a quadratic polynomial in l, with rational coefficients, and let ζ_k be a primitive complex k-th root of unity. Then $\Phi_k(q(l))$ splits over the rationals as a product of two irreducible polynomials of degree $\varphi(k)$ (Euler's totient function) precisely when the equation*

$$q(z) = \zeta_k$$

has a solution in $\mathbb{Q}(\zeta_k)$. *Otherwise,* $\Phi_k(q(l))$ *is irreducible over* $\mathbb{Q}$, *of degree* $2\varphi(k)$.

Proof. Let θ be any root of $\Phi_k(q(z)) = 0$. Then $q(\theta) = \omega_k$ is a primitive k-th root of unity, and $\omega_k \in \mathbb{Q}(\theta)$, and hence θ has degree a multiple of $\varphi(k)$ over $\mathbb{Q}$. Moreover we see that θ has degree $\varphi(k)$ precisely when $\theta \in \mathbb{Q}(\omega_k)$, and otherwise has degree $2\varphi(k)$. Finally we note that $\theta \in \mathbb{Q}(\omega_k)$ precisely when $q(z) = \omega_k$ has a solution in $\mathbb{Q}(\omega_k)$, and by Galois conjugation this occurs precisely when $q(z) = \zeta_k$ has a solution in $\mathbb{Q}(\zeta_k)$. □

The MNT families naturally fit into this picture:

- $k = 3$, $q(l) = 12l^2 - 1$. Here $q(1/3 + \zeta_3/6) = \zeta_3$.
- $k = 4$, $q(l) = l^2 + l + 1$. Here $q(\zeta_4) = \zeta_4$.
- $k = 6$, $q(l) = 4l^2 + 1$. Here $q(\zeta_6/2) = \zeta_6$.

Of course more is required than just the solubility of $q(z) = \zeta_k$, but this equation gives us a means of attack for the dimension 2 case. For example it immediately shows that no quadratic families exist for the case $k = 8$. Another alternative is simply to expand out the equation $\Phi_k(q(l)) = n_1(l)n_2(l)$ and attempt to solve the resulting Diophantine system. This is explored further in [19].

One can use this idea to find quickly all quadratic families (up to a linear change of variables; and most of these families will involve cofactors) $q(l) = al^2 + bl + c$ with integer coefficients and embedding degree $k = 3$, 4, or 6, for any fixed a. For example, consider $k = 6$. We seek $q(z) = \zeta_6$ with $z \in \mathbb{Q}(\zeta_6)$. Writing $2az + b = A + B\zeta_6$, this leads to two quadratic equations:

$$B(2A + B) = 4a\,,$$

$$A^2 - B^2 = b^2 - 4ac\,.$$

Noting that A and B must be integers, the first equation gives a finite set of possibilities for A and B (for fixed a), and for each of these one can test the solvability of the second equation.

6 Dimension 2: the general strategy

Given the heuristics above, we now seek families in dimension 2 that are parameterised by quadratic polynomials. For convenience we specialise Lemma 1 to the cases that are now of interest:

Lemma 2. *Let* $k = 5$, *8, 10, or 12, and let* ζ_k *be a primitive complex* k*-th root of unity. Let* $q(l)$ *be a quadratic polynomial in* l *with rational coefficients. Then* $\Phi_k(q(l))$ *splits over the rationals as a product of two irreducible quartic polynomials precisely when the equation*

$$q(z) = \zeta_k$$

has a solution in $\mathbb{Q}(\zeta_k)$. *Otherwise,* $\Phi_k(q(l))$ *is an irreducible octic over* $\mathbb{Q}$.

To apply this Lemma, we suppose that $az^2 + bz + c = \zeta_k$ for some rational numbers a, b, c, and some $z \in \mathbb{Q}(\zeta_k)$. Completing the square, and clearing denominators of all rational numbers (including those appearing in z) we get an equation of the shape

$$a_1 w^2 + b_1 = c_1 \zeta_k \,,$$

where a_1, b_1, $c_1 \in \mathbb{Z}$, and $w \in \mathbb{Z}[\zeta_k]$. Then since a_1 divides $c_1\zeta_k - b_1$, we must have that a_1 divides both c_1 and b_1, so we are reduced to

$$w^2 + b_2 = c_2 \zeta_k \,,$$

where b_2, $c_2 \in \mathbb{Z}$ and $w \in \mathbb{Z}[\zeta_k]$.

Writing

$$w = A + B\zeta_k + C\zeta_k^2 + D\zeta_k^3 \,,$$

with A, B, C, $D \in \mathbb{Z}$, expanding w^2 and equating coefficients of powers of ζ, we get (from the ζ^2 and ζ^3 coefficients) two homogeneous quadratics in four integer variables A, B, C, D that must vanish simultaneously.

Eliminating any one of the four variables (by computing a resultant), we get a homogeneous quartic in three variables. (In fact, by careful choice of the variable to be eliminated, we can produce a homogeneous cubic.) In each case this defines an elliptic curve (there is always a solution corresponding to $a = c = 0$). By studying the set of points on this elliptic curve, we learn about possible quadratic families of dimension 2 abelian varieties with embedding degree k.

Not every point on the elliptic curve gives rise to a quadratic family. The process of converting a point on the elliptic curve to a quadratic $q(l)$ may fail for any of the following reasons:

1. there may be points on the elliptic curve that do not lift back to points on both of the quadratic forms in A, B, C, D;
2. a solution $w = A + B\zeta_k + C\zeta_k^2 + D\zeta_k^3$ may yield $w^2 \in \mathbb{Q}$, in which case the 'quadratic' polynomial $q(l)$ is in fact linear, in which case $\Phi_k(q(l))$ does not split;
3. we need $-b_2$ to be a square modulo c_2 if we are to find suitable integers a, b, c (and note that if $-b_2$ *is* a square modulo c_2 then we may have more than one square-root to consider);
4. even if all goes well and we find a quadratic $q(l)$ with $\Phi_k(q(l))$ splitting, there may be no values of l for which $q(l)$ is a prime power.

The examples below will illustrate how one can patch things up if the two factors of $\Phi_k(q(l))$ do not have the same leading coefficient.

Given any $q(l) = al^2 + bl + c$ with integer coefficients such that $\Phi_k(q(l))$ splits, the same is true if we perform any $\mathbb{Z}$-linear change of variables $l \mapsto rl + s$. We regard $q_1(l)$ and $q_2(l)$ as equivalent if we can transform one into the other in this way (note that this does *not* define an equivalence relation, as we do not insist that our transformation is invertible over $\mathbb{Z}$). As remarked above in point 3, a single point on the elliptic curve may give rise to more than one inequivalent $q(l) = al^2 + bl + c$ with the same leading coefficient a. We may suppose, by scaling if necessary, that $\gcd(a, b)^2$ does not divide a, and then by translating and/or changing the sign of l we can insist that $0 \leq b \leq |a|$.

7 Dimension 2: the details

7.1 $k = 8$

With notation as in the previous section, the two equations that must be satisfied by integer variables A, B, C, D are

$$2AD + 2BC = 0\,, \tag{4}$$

and

$$2AC + B^2 - D^2 = 0\,. \tag{5}$$

Since A (or C) appears only to the first degree, we choose to eliminate A to give

$$2BC^2 + B^2D - D^3 = 0\,.$$

Putting $X = -2D$, $Y = 4C$, $Z = B$, we get the Weierstrass equation for an elliptic curve

$$Y^2Z = X^3 - 4XZ^2\,.$$

This curve has rank 0, and just four points: $(0:0:1)$, $(2:0:1)$, $(-2:0:1)$, and $(0:1:0)$. We consider each of these points in turn, and produce a contradiction in each case.

The point $(0:0:1)$ corresponds to $(B:C:D) = (1:0:0)$, but then we cannot solve equation (5) for A.

All other points lead to $w^2 \in \mathbb{Q}$, so that $q(l)$ is linear rather than quadratic.

We have established

Theorem 2. *There is no quadratic polynomial $q(l) = al^2 + bl + c$ with a, b, $c \in \mathbb{Q}$ and $a \neq 0$ such that $\Phi_8(q(l))$ splits into two quartic factors. Hence there is no quadratic family of ordinary abelian varieties of dimension 2 and embedding degree 8.*

The experience of the elliptic curve case, and the heuristic analysis above, make this result surprising. We expect of the order of $\sqrt{M}/\log M$ suitable pairs (q, n) for the field order and group order with $q \leq M$, but we can prove that none of these fit into quadratic families. Similarly in the cases below, where we do find families, we cannot say that these families cover all possible pairs (q, n).

7.2 $k = 12$

The relevant equations for A, B, C, D are now

$$2AD + 2BC + 2CD = 0\,, \tag{6}$$

and

$$2AC + B^2 + C^2 + 2BD = 0\,. \tag{7}$$

Eliminating A gives the elliptic curve defined by

$$C^3 + 3AC^2 + (2A^2 - B^2)C + AB^2 = 0\,.$$

Putting $X = -6C$, $Y = 6B$, $Z = A - C$ we get

$$ZY^2 = X^3 - 7X^2Z + 12XZ^2 .$$

This elliptic curve has rank 0, and torsion group of order 8, with torsion points $(0:1:0)$, $(0:0:1)$, $(6:6:1)$, $(2:-2:1)$, $(4:0:1)$, $(3:0:1)$, $(6:-6:1)$, $(2:2:1)$.

$(X:Y:Z) = (0:1:0)$ Here $(A:B:C) = (0:1:0)$, and equation (7) gives $(A:B:C:D) = (0:2:0:-1)$, so w is an integer multiple of $2\zeta_{12} - \zeta_{12}^3$, leading to $a = 0$, and $q(l)$ linear.

$(X:Y:X) = (0:0:1)$ Here $(A:B:C) = (1:0:0)$, and equation (6) gives $(A:B:C:D) = (1:0:0:0)$, so w is an integer square, again leading to $a = 0$.

$(X:Y:Z) = (4:0:1)$ Here $(A:B:C) = (1:0:-2)$, and equation (6) gives $(A:B:C:D) = (1:0:-2:0)$, so w is an integer multiple of $1 - 2\zeta_{12}^2$, leading to $a = 0$.

$(X:Y:Z) = (3:0:1)$ Here $(A:B:C) = (1:0:-1)$, but we cannot solve equation (7) for D.

$(X:Y:Z) = (2:-2:1)$ Here $(A:B:C) = (2:-1:-1)$, and equation (6) gives $(A:B:C:D) = (2:-1:-1:-1)$, so w is an integer multiple of $2 - \zeta_{12} - \zeta_{12}^2 - \zeta_{12}^3$, $b_2 = 0$, and c_2 is an integer multiple of -6.

Arguing as in the previous case, we have $a = 6t^2$, $c = 6s^2$, $b = 12st$, and after a linear change of variable we have

$$q(l) = 6l^2 .$$

This can never equal a prime power.

Since negating a point on the curve corresponds to replacing ζ_{12} by $-\zeta_{12}$, another primitive 12th root of unity, the point $(2:2:1)$ merely repeats this family.

Similarly the remaining two points reduce to a single case.

$(X:Y:Z) = (6:6:1)$ Here $(A:B:C) = (0:1:-1)$, and equation (6) gives $(A:B:C:D) = (0:1:-1:-1)$, so w is an integer multiple of $\zeta_{12} - \zeta_{12}^2 - \zeta_{12}^3$, $b_2 = 0$, and c_2 is an integer multiple of -2.

Since $-\zeta_{12}$ is also a primitive 12-th root, we may restrict to $a > 0$ without loss, and then a must be twice a rational square; say $a = 2t^2$. Then $8t^2c = b^2$, so c is also twice a square; say $c = 2s^2$. Then $b = 4st$.

Thus the most general quadratic $q(l)$ that serves for this case is

$$q(l) = 2(tl + s)^2 \,,$$

where t and s are rational numbers, with $t \neq 0$. Up to a linear change of variable, we have just one family, with $q(l) = 2l^2$. This is only of interest when $l = 2^m$ is a power of 2, giving $q = 2^{2m+1}$, $n = 4l^4 \pm 4l^3 + 2l^2 \pm 2l + 1$. Writing $n = q^2 + a_1(q+1) + a_2 + 1$ with $a_1 = \pm\sqrt{2q}$ and $a_2 = q$, we see that this includes the known supersingular case in characteristic 2 with embedding degree 12 (see [9]). Nudging a_1 and a_2, we can find ordinary abelian varieties with $a_1 = \pm 2l + 1$ and $a_2 = 4l^2 + 1$.

Note that the family $q(l) = 2l^2$ is not a quadratic family, since l must be restricted to powers of 2. Heuristically, most cases are not covered by this family.

Theorem 3. *There are no quadratic families of ordinary abelian varieties of dimension 2 and embedding degree 12. For any m there are abelian varieties of dimension 2 and embedding degree 12 over the field with $q = 2^{2m+1}$ elements, with $q^2 \pm \sqrt{2q}(q+1) + q + 1$ points, including both supersingular and ordinary cases. The parameters for the ordinary case are*

$$n = q^2 \pm \sqrt{2q}(q+1) + q + 1 \,, \quad a_1 = \pm\sqrt{2q} + 1 \,, \quad a_2 = 2q + 1 \,.$$

7.3 $k = 5$

The relevant equations for A, B, C, D are now

$$2AD + 2BC - 2BD - C^2 = 0 \,, \tag{8}$$

and

$$2AC + B^2 - C^2 - 2BD = 0 \,. \tag{9}$$

Eliminating D gives the elliptic curve defined by

$$2A^2C + AB^2 - 2ABC - AC^2 - B^3 + 2B^2C = 0 \,.$$

First treat the case A=0. If also $B = 0$, then $(A : B : C : D) = (0 : 0 : 0 : 1)$, $w = \zeta_5^3$, and we find the infinite family $q(l) = l^2$.

This (at last!) really is a quadratic family: any prime (power) l will make $q(l)$ a prime power. We then have $n(l) = l^4 \pm l^3 + l^2 \pm l + 1$. It includes a supersingular family, with $a_1 = \pm\sqrt{q}$ and $a_2 = q$, but also includes ordinary varieties, for example with $a_1 = \sqrt{q} - 1$ and $a_2 = 2q + 1$.

If instead (still in the case $A = 0$) $B = 2C \neq 0$, then $(A : B : C : D) = (0 : 8 : 4 : 3)$, and we find that (up to a linear change of variables) $q(l) = -10l^2 - 5l - 2$: this cannot represent prime powers, being always negative.

Now, by scaling, we may set A=1. Making the change of variables

$$t = -2T = -2(1 - B)/C \,, \quad s = (4T^2 + 2T^3)C - 1 - 2T - 2T^2 \,,$$

gives a birational transformation to the curve

$$E:\ s^2 = t^3 - 2t^2 - 2t + 1\,.$$

The map is not defined when $C = 0$, so we need to consider this case separately: we find that either $(A : B : C : D) = (1 : 0 : 0 : 0)$ or $(A : B : C : D) = (2 : 2 : 0 : 1)$. The former gives $q(l)$ linear; the latter gives the family $q(l) = 5l^2$, which can only give a prime power if l is a power of 5. We get a family, but exponential rather than quadratic.

Any remaining infinite families correspond to rational points on E. Now E has rank 1, and a torsion subgroup of order 2. A set of generators for the group is

$$\{P = (-1, 0), Q = (0, 1)\}\,.$$

We can try a few points on this curve, transform back to values for $(A : B : C : D)$, and see whether we can pick up any new families.

For example, the point $(s, t) = (5/8, 1/4)$ gives $(A : B : C : D) = (1 : 4 : 24 : -64)$, and this leads to $q(l) = 1010l^2 + 485l + 59$ or $q(l) = 1010l^2 + 525l + 69$.

For the first of these possibilities, unfortunately, $\Phi_5(q(l))$ splits as a product of two quartics whose leading coefficients are in the ratio of $101^2 : 4^2$, and we cannot tolerate a fractional cofactor of $101/4$. In this example, we can patch things up via the transformation $l \mapsto 101l - 62$, giving a quadratic family (with cofactor $h = 4$)

$$q(l) = 10303010l^2 - 12600255l + 3852429\,.$$

The second possibility, $q(l) = 1010l^2 + 525l + 69$ is more pleasant, giving us immediately a quadratic family, with cofactor $h = 404$. This is recorded in table 7, along with other families found from small-height points.

7.4 k=10

The case $k = 10$ is essentially the same as $k = 5$, via the transformation $\zeta_5 \mapsto -\zeta_{10}$. Any $q(l)$ is replaced by $-q(l)$. So, for example, the useless $q(l) = -10l^2 - 5l - 2$ can be replaced by $q(l) = 10l^2 + 5l + 2$. This gives a quadratic family with cofactor $h = 4$.

One should not get the impression from these carefully selected examples that all points on the elliptic curve give rise to a family for one of $k = 5$ or $k = 10$. As in the case $k = 12$ we find that many points on the curve are useless.

Summing up for embedding degrees 5 and 10, we have the following theorem.

Theorem 4. *For $k = 5$ and $k = 10$ there exist quadratic families of ordinary dimension 2 abelian varieties that have embedding degree k. These include those given in table 7. Any others correspond to points on a rank one elliptic curve, as detailed above.*

k	h	q	a_1	a_2
5	1	l^2	$-\|l\|+1$	-1
			$l-1$	$2l^2+1$
	404	$1010l^2+525l+69$	$-20l-5$	$505l^2+255l+32$
			$-20l-4$	$-505l^2-270l-38$
			$-20l-6$	$1515l^2+780l+102$
10	4	$10l^2+5l+2$	-1	$5l^2+5l+2$
			0	$-5l^2-1$
			-2	$15l^2+10l+5$
			1	$-15l^2-5l-4$
	11	$11l^2+10l+3$	l	$2l+1$
			$l+1$	$-11l^2-8l-3$
			$l-1$	$11l^2+12l+5$
			$l-2$	$22l^2+22l+9$
	11	$55l^2+40l+8$	$15l+4$	$165l^2+110l+20$

Table 7. Some quadratic families for embedding degrees $k=5$ and $k=10$. As before, l may take positive or negative values, except for the first example where the sign is constrained by the lower bound on a_2.

References

1. R. Balasubramanian and N. Koblitz, The improbability that an elliptic curve has sub-exponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm, *J. Crypt.*, **11** (1998) 141–145.
2. P.S.L.M. Barreto, H. Y. Kim, B. Lynn and M. Scott, Efficient implementation of pairing-based cryptosystems, in M. Yung (ed.), CRYPTO 2002, Springer LNCS 2442 (2002) 354–368.
3. P. S. L. M. Barreto, B. Lynn, M. Scott, On the Selection of Pairing-Friendly Groups, in M. Matsui and R. Zuccherato (eds.), SAC 2003, Springer LNCS 3006 (2004) 17–25.
4. I.F. Blake, G. Seroussi and N.P. Smart, *Elliptic curves in cryptography*, Cambridge (2000).
5. W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comp.*, **24** (1997) 235–265.
6. F. Brezing and A. Weng, Elliptic curves suitable for pairing based cryptography, to appear in *Designs, Codes and Cryptography*.
7. I. Duursma and H.-S. Lee, Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$, in C.S. Laih (ed.) ASIACRYPT 2003, Springer LNCS 2894 (2003) 111–123.
8. G. Frey and H.-G. Rück, A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves, Math. Comp., **52** (1994) 865–874.
9. S. D. Galbraith, Supersingular curves in cryptography, in C. Boyd (ed.) ASIACRYPT 2001, Springer LNCS 2248 (2001) 495–513.
10. S. D. Galbraith, K. Harrison and D. Soldera, Implementing the Tate pairing, in C. Fieker and D. Kohel (eds.), ANTS-V, Springer LNCS 2369 (2002) 324–337.
11. S. Lang, *Algebra*, (3rd ed.), Addison-Wesley (1993).
12. A. Miyaji, M. Nakabayashi and S. Takano, New explicit conditions of elliptic curve traces for FR-reduction, IEICE Trans. Fundamentals, E84, (2001) 1234–1243.

13. K. Rubin and A. Silverberg, Supersingular abelian varieties in cryptology, in M. Yung (ed.), CRYPTO 2002, Springer LNCS 2442 (2002) 336–353.
14. H.-G. Rück, Abelian surfaces and Jacobian varieties over finite fields, Compositio Math. **76** (1990), 351–366.
15. M. Scott and P. S. L. M. Barreto, Generating more MNT elliptic curves, Cryptology ePrint archive 2004/058 (2004).
16. E. Scourfield, personal communication.
17. J. H. Silverman, *The arithmetic of elliptic curves*, Springer GTM 106 (1986).
18. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer GTM 151 (1994).
19. P. Valença, PhD thesis, Royal Holloway University of London, in preparation.