COMPUTING THE ENDOMORPHISM TYPE OF ORDINARY ELLIPTIC CURVES OVER FINITE FIELDS WITH KANT V4

M. HENNINGSEN

Technische Universität Berlin, Institut für Mathematik,
Straße des 17. Juni 136, 10623 Berlin, Germany
E-mail: hennings@math.tu-berlin.de

Elliptic curve cryptography has received more and more attention from the security industry over the past years. Although some types of special curves have been successfully attacked, carefully chosen curves over prime fields, or over $\mathbb{F}_{2^m}$ with prime exponent m, seem to be intractable, and one cannot do much better than the Pollard-ρ algorithm for generic discrete logarithm problems. Other approaches are the Deuring lifting theorem [2] or the construction of isogenies between elliptic curves. Both attempts require explicit knowledge of the endomorphism ring of the original elliptic curve at some point. The basic ideas for computing the endomorphism type of ordinary elliptic curves over prime fields are outlined in this paper, and the computation of an example using the computer algebra system KANT V4 is presented.

1 Endomorphism Rings over Elliptic Curves

Since we consider prime fields with $p \geq 5$, we may assume that an elliptic curve E over $k = \mathbb{F}_p$ is given as a short Weierstrass model

$$E : y^2 = x^3 + Ax + B. \tag{1}$$

Let O denote the point at infinity and $E(k)$ the group of points (X, Y) satisfying (1).

An isogeny between two elliptic curves E_1 and E_2 is a rational map $\varphi : E_1 \to E_2$ over k with $\varphi(O) = O$. Two elliptic curves are called isogenous if there exists an isogeny between them. Isogenies are either constant or surjective [9]. Further every isogeny φ of elliptic curves respects the group structure of their points, thus φ is a homomorphism. The endomorphism ring $End(E)$ of an elliptic curve E is the set of all isogenies $\varphi : E \longrightarrow E$ which are defined over $\bar{k}$.

The j-invariant of an elliptic curve $E : Y^2 = X^3 + AX + B$ can be calculated easily via

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}. \tag{2}$$

An important fact is that two elliptic curves defined over k are isomorphic if they have the same j-invariant.

We denote by π the Frobenius endomorphism

$$\pi : (x, y) \mapsto (x^p, y^p)$$

on an elliptic curve E/k. Being a zero of its characteristic polynomial, it satisfies the following relation

$$0 = X^2 - tX + p, \tag{3}$$

where t is the trace of π. If the t is divisible by p, $End(E)$ is a quaternion algebra and E is called super singular; otherwise E is called ordinary and $End(E)$ is isomorphic to $\mathbb{Z}$ or to an order in an imaginary quadratic number field [2]. In this paper we consider ordinary curves on prime fields.

Definition 1 *For $n \geq -1$ the nth division polynomial $\psi_n \in k[X, Y]$ of an elliptic curve $E : y^2 = x^3 + Ax + B$ over k of characteristic $\neq 2, 3$ is defined as follows:*

- $\psi_{-1}(X, Y) = -1$,
- $\psi_0(X, Y) = 0$,
- $\psi_1(X, Y) = 1$,
- $\psi_2(X, Y) = 2Y$,
- $\psi_3(X, Y) = 3X^4 + 6AX^2 + 12BX - A^2$,
- $\psi_4(X, Y) = 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3)$,
- $\psi_{2n+1}(X, Y) = \psi_{n+2}(X, Y)\psi_n^3(X, Y) - \psi_{n+1}^3(X, Y)\psi_{n-1}(X, Y)$ *for* $n \geq 2$,
- $\psi_{2n}(X, Y) = \frac{\psi_n(X,Y)}{2Y}(\psi_{n+2}(X, Y)\psi_{n-1}^2(X, Y) - \psi_{n-2}(X, Y)\psi_{n+1}^2(X, Y))$ *for* $n \geq 3$.

Remark 2 *We observe that with the relation of $E : Y^2 = X^3 + AX + B$ each ψ_{2n+1} can be reduced to polynomials in X for $n \in \mathbb{N}$. Each ψ_{2n} can be reduced to a polynomial in X multiplied by Y.*

Another special type of endomorphism of E is the multiplication by n:

$$\begin{aligned} [n] : \quad E \quad &\longrightarrow E \\ (x, y) \ &\mapsto \ (x_n, y_n) = \Big(x - \tfrac{(\psi_{n-1}\cdot\psi_{n+1})(x,y)}{\psi_n^2(x,y)}, \\ &\qquad \tfrac{(\psi_{n+2}\cdot\psi_{n-1}^2 - \psi_{n-2}\cdot\psi_{n+1}^2)(x,y)}{4y\cdot\psi_n^3(x,y)}\Big) \end{aligned} \tag{4}$$

The map $[n]$ can be identified with $n \in \mathcal{O}_E$ where $\mathcal{O}_E \cong End(E)$ is either $\mathbb{Z}$ or an order in an imaginary quadratic field. The points of the subgroup

$$E[l] := \{P = (X, Y) \mid l \cdot P = O\} \tag{5}$$

in $E(k)$ are called the l-torsion points of E.

For a more detailed description of isogenies of elliptic curves see for example the books of Silverman [9] or Lang [5]. Here we just need the fact that any isogeny factors into a power of the Frobenius endomorphism and a separable isogeny. The degree of a separable isogeny $\varphi : E_1 \longrightarrow E_2$ is equal to the number of points in the subgroup $\ker(\varphi)$ [9]. A separable isogeny of degree d is called a d-isogeny.

2 The Endomorphism Type

The Frobenius endomorphism π is defined in any endomorphism ring of an elliptic curve, thus $\mathbb{Z}[\pi] \subseteq \mathcal{O}_E$. Let $\mathcal{O}_K$ be the maximal order in $K = \mathbb{Z}[\pi] \otimes \mathbb{Q}$ with discriminant D_K. Since

$$\mathbb{Z}[\pi] \subseteq \mathcal{O}_E \subseteq \mathcal{O}_K, \tag{6}$$

we know that $End(E) = \mathbb{Z}$ if $\pi \in \mathbb{Z}$, therefore we assume that $\pi \notin \mathbb{Z}$ in the following.

Any order $\mathcal{O} \subseteq \mathcal{O}_K$ has a positive integer c called the conductor of $\mathcal{O}$ in $\mathcal{O}_K$ characterized by

$$\mathcal{O} = \mathbb{Z} \oplus c \cdot \mathcal{O}_K. \tag{7}$$

Note that the conductor c is equal to the index $[\mathcal{O}_K : \mathcal{O}]$.

The order $\mathbb{Z}[\pi] \subseteq \mathcal{O}_K$ has discriminant $d = t^2 - 4p$ and conductor $m = \sqrt{d/D_K}$. There exists an $a \in \mathbb{Z}$ such that

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{\pi - a}{m}\right]. \tag{8}$$

The value of a is determined by $a^2 - ta + p \equiv 0 \bmod m^2$ and $2a \equiv t \bmod m$. A simple calculation shows that we can choose $a = t/2$ if $D_K \equiv 0 \bmod 4$ and $a = (t + m)/2$ if $D_K \equiv 1 \bmod 4$.

2.1 $l \neq 2$

Let $\mathcal{O}_E$ be the order in $\mathcal{O}_K$ isomorphic to $End(E)$. For all primes $l \in \mathbb{P}$ dividing m, we need to find the biggest $n = l^r$ such that $(\pi - a)$ is still the zero map on $\mathcal{O}_E/n\mathcal{O}_E$. Note that l is coprime to p since $l \mid (t^2 - 4p)$ and

$0 < t < p$. For this to occur, there must be an $\alpha \in End(E)$ such that $(\pi - a) = n\alpha$, which is equivalent to $E[n] \subseteq \ker(\pi - a)$.

To do this, we search for the largest possible exponent r. Since ψ_n generates the ideal $E[n] - \{O\}$ we have $(\psi_n) = n\mathcal{O}_E$. Therefore we calculate $(\pi - a)$ modulo ψ_{l^r} starting with $r = 1$. The ring of polynomials

$$k[X, Y]/(\psi_n(X, Y), Y^2 - X^3 - AX - B) \tag{9}$$

reduces to a ring of polynomials in one variable X only.

With (4), we calculate the X- coordinate of $a \cdot P$ for a point $P = (X, Y)$ on E

$$[a](X) = X - \frac{(\psi_{a-1} \cdot \psi_{a+1})(X)}{\psi_a^2(X)}. \tag{10}$$

The Frobenius endomorphism for the X- coordinate is defined by $\pi_x(X) = X^p$. Therefore we calculate

$$\begin{aligned} h_r(X) &\equiv \psi_a^2(X)(\pi_x - a_x)(X) \bmod \psi_{l^r}(X) \\ &\equiv (X^p - X)\psi_a^2(X) + \psi_{a+1}\psi_{a-1}(X) \bmod \psi_{l^r}(X) \end{aligned} \tag{11}$$

Note that we can take $\tilde{a} \equiv a \bmod l^r$ instead of a in the calculation above.

If $h_r(X) = 0$, we increase the parameter r step by step until $h_r(X) \neq 0$ or until r exceeds the exponent of l in the conductor of $\mathbb{Z}[\pi]$. Then we have found the exponent r of the prime l in the index $[\mathcal{O}_E : \mathbb{Z}[\pi]]$.

Problems can arise if $n = l^r$ gets too large, since ψ_n is of degree $O(n^2)$. For small l but large exponent r the following method is very useful. If there are large prime divisors of the conductor m of $\mathbb{Z}[\pi]$ one should use another idea shown by Kohel [4] involving the class group of the endomorphism ring $\mathcal{O}_E$.

2.2 $l = 2$

For $l = 2$ we have the problem of dealing with $\psi_{2^r}(X, Y)$, which cannot be reduced to a polynomial in X (Remark 2). Therefore in this case we use a different method for calculating the index $[\mathcal{O}_E : \mathbb{Z}[\pi]]$ described by Kohel [4]. The algorithm outlined here is based on the following theorem and can thus be used for arbitrary primes $l \neq 2$ as well.

Given that $\mathbb{Z}[\pi] \subseteq \mathcal{O}_E \subseteq \mathcal{O}_K$, by an l-isogeny $\varphi : E \longrightarrow E'$ up we mean that for $End(E') \cong \mathcal{O}_{E'}$

$$[\mathcal{O}_K : \mathcal{O}_E] = l \cdot [\mathcal{O}_K : \mathcal{O}_{E'}]. \tag{12}$$

An l-isogeny down describes the opposite situation

$$[\mathcal{O}_K : \mathcal{O}_{E'}] = l \cdot [\mathcal{O}_K : \mathcal{O}_E]. \tag{13}$$

Theorem 3 (Number of Isogenies [3,4]) *Let E/k be an ordinary elliptic curve having endomorphism ring $\mathcal{O}$ where $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ and D its discriminant. Let l be a prime number and $(\frac{D}{l})$ the Legendre symbol.*

1. *If $l \nmid [\mathcal{O}_K : \mathcal{O}]$ then the number of l-isogenies of elliptic curves not isomorphic to E with endomorphism ring equal to $\mathcal{O}$ is $1 + (\frac{D}{l})$.*
2. *If $l \mid [\mathcal{O}_K : \mathcal{O}]$ then there is one l-isogeny up to an elliptic curve having a smaller conductor than E.*
3. *If $l \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ then there are no l-isogenies down to elliptic curves with bigger conductor than E.*
4. *If $l \mid [\mathcal{O}_K : \mathcal{O}]$ and $l \mid [\mathcal{O} : \mathbb{Z}[\pi]]$ then the number of l-isogenies down is l.*
5. *If $l \mid [\mathcal{O}_K : \mathcal{O}]$ and $l \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ then the number of l-isogenies down is $l - (\frac{D}{l})$.*

Therefore we have to find sequences of l-isogenies to other elliptic curves. The j-invariants $j(E)$ of these elliptic curves can be computed via modular equations or polynomials $\Phi_l(X, Y) \in \mathbb{Z}[X, Y]$ [5,10,4,6]. The most important property for us is that the j-invariants of elliptic curves l-isogenous to an elliptic curve E are roots of

$$\Phi_l(X, j(E)) = 0. \tag{14}$$

The algorithm is described here for $l = 2$ only because the coefficients of the modular polynomial get very large, but the method can be used for other primes as well. We assume that $l = 2$ divides the conductor m of $\mathbb{Z}[\pi]$. First we compute the j-invariant of the elliptic curve E and the modular polynomial.

$$\begin{aligned}\Phi_2(X, Y) = {} & Y^3 + (-X^2 + 1488X - 162000)Y^2 \\ & +(1488X^2 + 40773375X + 8748000000)Y \\ & +X^3 - 162000X^2 + 8748000000X - 157464000000000\end{aligned} \tag{15}$$

In the next step we factor $\Phi_2(X, j(E))$, which is of degree $l + 1 = 3$. If there is only one root $j(E')$, the isogeny to the elliptic curve E' is going up and we know that $l = 2$ does not divide the index $[\mathcal{O}_E : \mathbb{Z}[\pi]]$. If $\Phi_2(X, j(E))$ factors completely, $l = 2$ divides $[\mathcal{O}_E : \mathbb{Z}[\pi]]$ at least once.

Setting $E_0 = E$ and $E_1 = E'$ we then construct sequences of $j(E_r)$ with $j(E_{r+1})$ a root of $\Phi_2(X, j(E_r))$ until we find an r such that $\Phi_2(X, j(E_r))$ has exactly one root or until r exceeds the exponent of $l = 2$ in m.

Since we might pick an isogeny that is going up (if we are in case 2. of Theorem 3) or staying on the same level (if we are in case 1.), we have to take two probes of sequences with two distinct $j(E_1)$ in the beginning.

If r exceeds the exponent of $l = 2$ in the conductor m of $\mathbb{Z}[\pi]$ in both cases, we conclude that l does not divide $[\mathcal{O}_K : \mathcal{O}_E]$. Otherwise the smaller r is the exponent of l in $[\mathcal{O}_E : \mathbb{Z}[\pi]]$.

Algorithm 1 (Calculation of the exponent of $l = 2$ in the index $[\mathcal{O}_E : \mathbb{Z}[\pi]]$ if $l = 2$ divides the conductor of $\mathbb{Z}[\pi]$)
Input: *E elliptic curve over the finite field $\mathbb{F}_p$, k exponent of $l = 2$ in the conductor m of $\mathbb{Z}[\pi]$*
Output: *$r \in \mathbb{N}$ such that $2^r \mid [\mathcal{O}_E : \mathbb{Z}[\pi]]$ and $2^{r+1} \nmid [\mathcal{O}_E : \mathbb{Z}[\pi]]$*

1 *Set*

$$\Phi_2(X,Y) := Y^3 + (-X^2 + 1488X - 162000)Y^2 + (1488X^2 + 40773375X + 8748000000)Y + X^3 - 162000X^2 + 8748000000X - 157464000000000$$

For $i = 1, 2$ do steps 2 to 12.

2 *Set stop := false; $j(E_0) := j(E)$; and $r_i := 0$;*

3 *Factor $\phi(X) := \Phi_2(X, j(E_0))$.*

if $\phi(X)$ has exactly one root **then**

4 *return 0;*

else

5 *Set $j(E_{1_i})$:= (i^{th} root of $\phi(X)$); #This assures that $j(E_{1_1}) \neq j(E_{1_2})$*

6 *Set prev := $j(E_0)$;*

7 *Set $r_i := r_i + 1$;*

fi;

repeat

8 *Factor $\phi(X) := \Phi_2(X, j(E_{r_i}))$.*

if $\phi(X)$ has exactly one root **then**

9 *Set stop := true;*

else

10 *Set $j(E_{r_i+1})$:= (root of $\phi(X)$ which is $\neq$ prev);*

11 *Set prev* $:= j(E_{r_i})$;

12 *Set* $r_i := r_i + 1$;

fi;

until $r_i > k$ *or stop;*

if $r_1 > k$ and $r_2 > k$ **then**

13 *return* k; # *case 1. of Theorem 3*

else

14 *return Minimum*(r_1, r_2);

fi;

2.3 Complete algorithm

In the following we present the complete algorithm for determining the conductor c of the endomorphism ring of an elliptic curve $E : Y^2 = X^3 + AX + B$ over a finite field k of characteristic $\neq 2, 3$.

Algorithm 2 (Calculation of the conductor of the endomorphism ring)
Input: *E elliptic curve over finite field k*
Output: $c \in \mathbb{N}$ *such that* $End(E) \cong \mathcal{O}_E = \mathbb{Z} + c \cdot \mathcal{O}_K$

1 *Calculate the trace t of the Frobenius endomorphism, for example with the SEA-algorithm* [7,8].

2 *Calculate the discriminant* D_K *of the maximal order* $\mathcal{O}_K \supseteq \mathcal{O}_E \cong End(E)$.

3 *Set the discriminant of the order* $\mathbb{Z}[\pi]$ *to* $d := t^2 - 4p$ *via the Frobenius endomorphism* π *of* E.

4 *Set* $m := \sqrt{d/D_K}$; *and* $a := t/2$ *if* $D_K \bmod 4 \equiv 0$ *or* $a := (t + m)/2$ *if* $D_K \bmod 4 \equiv 1$;

5 *Set* $j := 1$; $c := 1$; *and factorize* m.

if $2|m$ **then**

6 *Compute the exponent* r *of* 2 *in* $[\mathcal{O}_E : \mathbb{Z}[\pi]]$ *with Algorithm 1.*

7 *Set* $c := c * 2^r$;

fi;

if no odd primes divide m **then**

8 *return* c;

fi;

repeat

9 *Set* $l :=$ *(jth odd prime dividing* m*);* $\tilde{a} := a \bmod l$;
$k :=$ *(exponent of* l *in* m*) and* $r := 0$;

repeat

10 $r := r + 1$;

11 *Compute:*

$$h(X) \equiv (X^p - X) \cdot \psi_{\tilde{a}}^2(X) + \psi_{\tilde{a}+1} \cdot \psi_{\tilde{a}-1}(X) \bmod \psi_{l^r}(X)$$

if $h(X) \neq 0$ **then**

12 *Set* $r := r - 1$; *and stop:=true;*

fi;

until $r = k$ *or stop;*

13 $c := c * l^r$; # c *is the index* $[\mathcal{O}_E : \mathbb{Z}[\pi]]$.

14 $j := j + 1$;

until $l =$ *maximal odd prime dividing* m*;*

15 $c := m/c$; # *We are looking for* $[\mathcal{O}_K : \mathcal{O}_E]$

16 *return* c;

3 Computations with KANT V4

The following sample computations are done with the programming shell KASH of the computer algebra system KANT V4 [a].

Let $p = 27717762618429664442479579697218415549196462369 1$ and

$$E : Y^2 = X^3 + AX + B$$

over $k = \mathbb{F}_p$ with $A = 272541518603739663048376297783171386047488081741$ and $B = 155915327533246157338971654070259643256587149 9$. First we initialize the elliptic curve in KASH, and set the preliminaries of Algorithm 2.

[a] You can obtain the KANT V4 [1]- package at:
ftp://ftp.math.tu-berlin.de/pub/algebra/Kant/Kash/

```
kash> p:=27717762618429664442479579697218415549196462369 1;;
kash> A:=27254151860373966304837629778317138604748808174 1;;
kash> B:=15591532753324615733897165407025964325658714 99;;
kash> E:=EccInit(p,A,B);;
kash> t:=Trace(E);
-51582832225621049808412
kash> d:=t^2-4*p;
-11060497161567700082324164330065186933859525330 20
kash> D:=Disc(OrderMaximal(x^2-d));
-34137336918418827414580754105139465845245448 55
kash> m:=IntRoot(d/D,2);
18
kash> a:=(t+m)/2;
-25791416112810524904197
```

Next we factor m and since $m = (2 \cdot 3^2)$ we calculate the division polynomials up to the 9th polynomial.

```
kash> fac:=Factor(m);
[ [ 2, 1 ], [ 3, 2 ] ]
kash> DP:=EccDivisionPolys(E,9);;
```

We now do the calculation for $l = 2$.

```
kash> Zy:=PolyAlg(Zx);
Univariate Polynomial Ring in y over Univariate Polynomial Ring
in x over Integer Ring
kash>   PHI_2:=Poly(Zy,List([ [ 1 ], [ -1, 1488, -162000 ],
>   [ 1488, 40773375, 8748000000 ],
>   [ 1, -162000, 8748000000, -157464000000000 ] ] ,
>   x->Poly(Zx,x)));
y^3 + (-x^2 + 1488*x - 162000)*y^2 + (1488*x^2 + 40773375*x + 8\
748000000)*y + x^3 - 162000*x^2 + 8748000000*x - 157464000000000
kash> jinv:=EccJInv(E);
603681299467986064109010100930130264402626659 43
kash> phi:=Eval(PHI_2,jinv);
x^3 + 24600108708053728728741720806772571177842033633 9*x^2 + 15\
560335799662549095819111662059674254829349791 4*x + 254370737584\
915898614371952293314118463679262623
kash> fac:=Factor(phi);
[ [ x + 135762359057552848562112296440686912015063305923, 1 ],
```

```
[ x + 188365304178092657449871881545799381460179438904, 1 ],
[ x + 199051050029188425700228827053423573795142215203, 1 ] ]
```

Since $\phi = \Phi_2(X, J(E))$ factors completely, we conclude that there is at least one 2-isogeny down to an elliptic curve E' thus

$$[\mathcal{O}_K : \mathcal{O}_{E'}] = 2 \cdot [\mathcal{O}_K : \mathcal{O}_E], \tag{16}$$

and therefore 2 does not divide the conductor c of $\mathcal{O}_E$.

Calculating $h_1(X)$ and $h_2(X)$ of Eq. (11), we find that $h_1(X) = 0$ and $h_2(X) \neq 0$ for $l = 3$ which means that $(\pi - a)$ is zero on $\mathcal{O}_E/3\mathcal{O}_E$ but not on $\mathcal{O}_E/9\mathcal{O}_E$ thus the conductor c of $\mathcal{O}_E$ is equal to 3.

References

1. M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, K. Wildanger, KANT V4, J. Symb. Comp. Vol. 24 **3**, 267-283 (1997).
2. M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hamburg **14**, 197-272 (1941).
3. S.D. Galbraith, *Constructing Isogenies between Elliptic Curves over Finite Fields*, LMS J. Comput. Math. **2**, 118-138 (1999).
4. D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, Berkeley PhD thesis, 1996.
5. S. Lang, *Elliptic Functions*, Springer, New York (1973).
6. F. Morain, *Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques*, J. Théorie des Nombres de Bordeaux **7**, 219-254 (1995).
7. V. Müller, *Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei*, Saarbrücken PhD thesis, 1995.
8. R. Schoof, *Counting points on elliptic curves over finite fields*, J. Théorie des Nombres de Bordeaux **7**, 219-254 (1995).
9. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York (1986).
10. J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York (1994).