Elliptic curves over finite fields and the Weil pairing

Jerome T. Dimabayao [†]

[†] jdimabayao@math.upd.edu.ph

Division Polynomials

Start with variables A and B. Define $\psi_m \in \mathbb{Z}[x, y, A, B]$ by

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \text{ for } m \geq 2 \\
\psi_{2m} &= (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), \text{ for } m \geq 3.
\end{aligned}$$

We call ψ_m the m**th division polynomial**.

Fact:

1. $\psi_{2m+1} \in \mathbb{Z}[x, y^2, A, B]$
2. $\psi_{2m} \in 2y\mathbb{Z}[x, y^2, A, B]$

Torsion Points of E

Let $E : y^2 = x^3 + Ax + B$, where $A, B \in K$.

Then

1. $\psi_{2m+1} \in \mathbb{Z}[x, A, B]$
2. $\psi_{2m} \in 2y\mathbb{Z}[x, A, B]$
3. The roots ψ_{2m+1} are the x-coordinates of points in $E[2m+1]$ (except $\mathcal{O}$)
4. For $m > 1$, the roots $y^{-1}\psi_{2m}$ are the x-coordinates of points in $E[2m]$ (except $E[2]$)
5. If $P = (x, y) \in E(K)$, then

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)} \right),$$

where

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$$
$$\omega_n = (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2).$$

The Weil pairing

Let E be an elliptic curve over K and let n be a positive integer. Assume that the characteristic of K does not divide n. Then there exists a pairing

$$e_n : E[n] \times E[n] \to \mu_n,$$

that satisfies the following properties:

1. e_n is bilinear in each variable. This means that

   $$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

   and

   $$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

   for all $S, S_1, S_2, T, T_1, T_2 \in E[n]$.
2. e_n is nondegenerate in each variable. This means that
   - if $e_n(S, T) = 1$ for all $T \in E[n]$ then $S = \mathcal{O}$, and
   - if $e_n(S, T) = 1$ for all $S \in E[n]$ then $T = \mathcal{O}$.

The Weil pairing (cont.)

Let E be an elliptic curve over K and let n be a positive integer. Assume that the characteristic of K does not divide n. Then there exists a pairing

$$e_n : E[n] \times E[n] \to \mu_n,$$

that satisfies the following properties:

3. $e_n(T,T) = 1$ for all $T \in E[n]$.
4. $e_n(T,S) = e_n(S,T)^{-1}$ for all $S,T \in E[n]$.
5. $e_n(\sigma S, \sigma T) = \sigma(e_n(S,T))$ for all automorphisms σ of $\overline{K}$ such that σ is the identity map on the coefficients of E.
6. $e_n(u(S), u(T)) = e_n(S,T)^{\deg(u)}$ for all (separable) endomorphisms u of E.

Elliptic curves over finite fields

Let $q = p^e$, where p is an odd prime and $e \geq 1$.
Let $E/\mathbb{F}_q$ be an elliptic curve and $a = q + 1 - \#E(\mathbb{F}_q)$.

Theorem (Hasse-Weil)

$$|a| \leq 2\sqrt{q}.$$

Theorem

The Frobenius endomorphism ϕ_q satisfies the equation

$$\phi_q^2 - [a]\phi_q + [q] = 0.$$

Moreover, a is the unique integer such that

$$a \equiv \mathrm{Trace}((\phi_q)_m) \pmod{m}$$

for all m coprime to p.

The polynomial $X^2 - aX + q$ is called the *characteristic polynomial of the Frobenius*. The integer a is called the *trace of Frobenius*.

Baby steps-giant steps

Goal: Find order of a point $P \in E(\mathbb{F}_q)$.
Let $P \in E(\mathbb{F}_q)$.
Baby steps: Compute $Q := [q+1]P$. Compute $[j]P$ for $j = 0, 1, \ldots, m := \lceil q^{1/4} \rceil$.
Giant steps: Compute $R := [2m]P$, then compute

$$Q + [k]R, \text{ for } k = -m, -(m-1), \ldots, m-1, m$$

until there is a match $Q + [k]R = \pm[j]P$, for some j.
Then $[M]P = \mathcal{O}$, where $M = q + 1 + 2mk \mp j$.
Let $p_1, \ldots, p_r$ be the distinct prime divisors of M.
(*) Compute $[M/p_i]P$ for all i.
If $[M/p_i]P = \mathcal{O}$ for some i, then replace M with M/p_i and repeat (*).
Otherwise, M is the order of P.

Schoof's method

Assume $p > 3$ and

$$E : y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{F}_p.$$

Recall that $\#E(\mathbb{F}_p) = p + 1 - a$ with $|a| \leq 2\sqrt{p}$.
Idea: Compute a modulo small primes $\ell_1, \ldots, \ell_r$ such that $\prod_{j=1}^r \ell_j > 4\sqrt{p}$. We can determine a, and hence $\#E(\mathbb{F}_p)$, using the Chinese remainder theorem.

1. Computation of $a \pmod 2$:
   We have

$$\begin{aligned} a \equiv 1 \pmod 2 &\iff x^3 + a_4 x + a_6 \text{ is irreducible} \pmod p \\ &\iff \gcd(x^3 + a_4 x + a_6, x^p - 1) = 1 \end{aligned}$$

Schoof's method (cont.)

2 Computation of $a \pmod{\ell}$, with ℓ odd:
For $P = (x_1, y_1) \in E[\ell](\overline{\mathbb{F}_p})$, we have

$$\phi_p^2(P) + [p_\ell]P = [a_\ell]\phi_p(P),$$

with $a_\ell \equiv a \pmod{\ell}, p_\ell \equiv p \pmod{\ell}$, and $0 \leq a_\ell < \ell, |p_\ell| < \ell/2$.
If P has order ℓ then P is a solution of the following system of equations

$$E(x, y) = y^2 - (x^3 + a_4 x + a_6) = 0, \quad \psi_\ell(x) = 0.$$

Thus

$$(x^{p^2}, y^{p^2}) + [p_\ell](x, y) = [a_\ell](x^p, y^p) \pmod{E(x, y), \psi_\ell(x)}. \quad (1)$$

To compute a_ℓ, try all $b \in \{0, 1, \ldots, \ell - 1\}$ until we find the unique value b such that (1) holds.

An Example:

Consider $E : y^2 = f(x) = x^3 + 2x + 1$ over $\mathbb{F}_{19}$.
What is $a \pmod 2$?
We have $x^{19} \equiv x^2 + 13x + 14 \pmod{f(x)}$.
Then

$$\gcd(x^{19} - x, f(x)) = \gcd(x^2 + 12x + 14, f(x)) = 1.$$

So $E(\mathbb{F}_{19})$ has no point of order 2.
Thus $a \equiv 1 \pmod 2$.

An Example (cont.):

Consider $E : y^2 = f(x) = x^3 + 2x + 1$ over $\mathbb{F}_{19}$.
What is $a \pmod 5$?
We have $19 \equiv -1 \pmod 5$.

- Let

$$(x', y') = (x^{19^2}, y^{19^2}) + [-1](x, y) = (x^{19^2}, y^{19^2}) + (x, -y),$$

  for $(x, y) \in E[5]$.
  Note $x' = \left(\frac{f(x)(f(x)^{180}+1)}{x^{361}-x}\right)^2 - x^{361} - x$.

- Find $j \in \{0, 1, 2, 3, 4\}$ such that

$$(x', y') = [j](x^{19}, y^{19}) =: (x_j^p, y_j^p).$$

  We can find j subject to the condition $x' - x_j^{19} \equiv 0 \pmod{\psi_5}$.
  Here,

$$\psi_5 = 5x^{12} + 10x^{10} + 17x^8 + 5x^7 + x^6 + 9x^5 + 12x^4 + 2x^3 + 5x^2 + 8x + 8.$$

$$x_2^{19} = \left(\frac{3x^{38} + 2}{2y^{19}}\right)^2 - 2x^{19}.$$

An Example: (cont.)

It can be shown that $x' - x^{19} \not\equiv 0 \pmod{\psi_5}$, but

$$x' = \left(\frac{f(x)(f(x)^{180}+1)}{x^{361}-x}\right)^2 - x^{361} - x \equiv \left(\frac{3x^{38}+2}{2y^{19}}\right)^2 - 2x^{19} = x_2^{19} \pmod{\psi_5}.$$

Thus, $a \equiv \pm 2 \pmod{5}$.

- To determine the sign, look at y-coordinates. It turns out that

$$(y' + y_2^{19})/y \equiv 0 \pmod{\psi_3}.$$

That is, $(x', y') = (x_2^{19}, -y_2^{19}) = [-2](x^{19}, y^{19})$.

So $a \equiv -2 \pmod{5}$.

An Example (cont.)

Consider $E : y^2 = f(x) = x^3 + 2x + 1$ over $\mathbb{F}_{19}$.
We have

$$\psi_3(x) = 3x^4 + 12x^2 + 12x - 4.$$

Note that

$$\psi_3(8) = 0 \pmod{19}.$$

The point $(8, 4) \in E(\mathbb{F}_{19})$ has order 3.
Thus

$$19 + 1 - a = \#E(\mathbb{F}_{19}) \equiv 0 \pmod{3}.$$

So $a \equiv 2 \pmod 3$.
We have

$$a \equiv 1 \pmod{2}, \quad a \equiv 2 \pmod{3}, a \equiv 3 \pmod{5}.$$

Thus, $a \equiv 23 \pmod{30}$.
Since $|a| < 2\sqrt{19} < 9$, we have $a = -7$. Thus

$$\#E(\mathbb{F}_{19}) = 19 + 1 - a = 27.$$

Schoof algorithm (Given: $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$)

Start with a set of primes $S = \{2, 3, \ldots, L\}$ ($p \notin S$) such that $\prod_{\ell \in S} \ell > 4\sqrt{p}$. To compute a_ℓ for odd $\ell \in S$, do:

(a) Let $p_\ell \equiv p \pmod{\ell}$ with $|p_\ell| \leq \ell/2$.

(b) Compute the x-coordinate x' of

$$(x', y') = (x^{p^2}, y^{p^2}) + [p_\ell](x, y) \pmod{\psi_\ell}.$$

(c) For $j = 1, 2, \ldots, (\ell - 1)/2$, do:

- (i) Compute x-coordinate x_j of $(x_j, y_j) = [j](x, y)$.
- (ii) If $x' - x_j^p \equiv 0 \pmod{\psi_\ell}$, go to (iii). Otherwise, try next j in (c). If all values $1 \leq j \leq (\ell - 1)/2$ have been tried, go to step (d).
- (iii) Compute y' and y_j. If $(y' - y_j^p)/y \equiv 0 \pmod{\psi_\ell}$, then $a \equiv j \pmod{\ell}$. If not, then $a \equiv -j \pmod{\ell}$.

(d) If all j with $1 \leq j \leq (\ell - 1)/2$ have been tried without success, let $w^2 \equiv p \pmod{\ell}$. If w does not exist, then $a \equiv 0 \pmod{\ell}$.

(e) If $\gcd(\text{numerator}(x^p - x_w), \psi_\ell) = 1$, then $a \equiv 0 \pmod{\ell}$. Otherwise compute $\gcd(\text{numerator}(y^p - y_w)/y, \psi_\ell)$. If gcd is not 1, then $a \equiv 2w \pmod{\ell}$. Otherwise, $a \equiv -2w \pmod{\ell}$.

Constructing the Weil pairing

Divisors

Let E be an elliptic curve over K.

1. A *divisor D on E* is an element of the free abelian group $\mathrm{Div}(E)$ generated by symbols $[P]$, where $P \in E(\overline{K})$; that is,

$$D = \sum_{P \in E} n_P[P], \quad n_P \in \mathbb{Z}, n_P = 0, \text{ for all but finitely many } P.$$

2. The *degree* of a divisor $D = \sum_{P \in E} n_P[P]$ is

$$\deg(D) = \sum_{P \in E} n_P.$$

3. Fact: The divisors of degree 0 form a subgroup $\mathrm{Div}^0(E)$ of $\mathrm{Div}(E)$.

Divisors

Let E be an elliptic curve over K. Let $\overline{K}(E)$ denote the function field of E.

4. For $P \in E(\overline{K})$, there is a function u_P, the *uniformizer at* P such that

$$u_P(P) = 0 \text{ and every } f \in \overline{K}(E) \text{ can be written as } f = u_P^r g.$$

   The *order of* f *at* P is $r =: \mathrm{ord}_P(f)$.
   $\mathrm{ord}_P(f) > 0$ means P is a zero of f
   $\mathrm{ord}_P(f) < 0$ means P is a pole of f

5. For $f \in \overline{K}(E)$ ($f \not\equiv 0$), the *divisor of* f is

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f)[P] \in \mathrm{Div}(E).$$

Divisors

Let E be an elliptic curve over K. Let $\overline{K}(E)$ denote the function field of E.

6. $f \in \overline{K}(E)$ has only finitely many zeros and poles.
7. $\deg(\mathrm{div}(f)) = 0$
8. $\mathrm{div}(f) = 0$ if and only if f is constant.
9. A divisor $D \in \mathrm{Div}(E)$ is called *principal* if $D = \mathrm{div}(f)$ for some f.
10. $D_1, D_2 \in \mathrm{Div}(E)$ are said to be *linearly equivalent*, written $D_1 \sim D_2$, if
$$D_1 - D_2 = \mathrm{div}(f), \text{ for some } f.$$
11. $\mathrm{Pic}(E) = \mathrm{Div}(E)/(\text{principal divisors})$;
$\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/(\text{principal divisors})$

Riemann-Roch

Definition

A divisor $D = \sum_{P \in E} a_P[P]$ is said to be positive (written "$D \geq 0$") if $a_P \geq 0$ for all $P \in E$.
Let $D \in \mathrm{Div}(E)$. Define

$$\mathcal{L}(D) := \{f \in \overline{K}(E)^* : \mathrm{div}(f) + D \geq 0\} \cup \{0\}.$$

Note that $\dim_{\overline{K}} \mathcal{L}(D) < \infty$.

Remarks:

- $\mathcal{L}(0) = \overline{K}$.
- $D_1 \sim D_2$ implies $\mathcal{L}(D_1) = \mathcal{L}(D_2)$.

Riemann-Roch Theorem

$$\dim_{\overline{K}} \mathcal{L}(D) = \deg(D),$$

for all divisors $D \in \mathrm{Div}(E)$ with $\deg D \geq 0$.

Consequences

Corollary

Let $P, Q \in E$. Then $(P) \sim (Q)$ if and only $P = Q$.

Proposition

Let E/K be an elliptic curve.

a For every $D \in \mathrm{Div}^0(E)$, there exists a unique $P \in E$ such that $D \sim (P) - (\mathcal{O})$.
Define $\sigma : \mathrm{Div}^0(E) \to E$ to be the map that sends D to its associated P.

b The map σ is surjective.

c Let $D_1, D_2 \in \mathrm{Div}^0(E)$. Then

$$\sigma(D_1) = \sigma(D_2) \quad \text{if and only if} \quad D_1 \sim D_2.$$

Proposition (cont.)

d Thus σ induces a bijection of sets (also denoted by σ),

$$\sigma : \mathrm{Pic}^0(E) \to E,$$

with inverse given by

$$\kappa : E \to \mathrm{Pic}^0(E), \quad P \mapsto (\text{divisor class of } (P) - (\mathcal{O})).$$

(e) If E is given by a Weierstrass equation then the "geometric group law" on E and the "algebraic group law" on $\mathrm{Pic}^0(E)$ using σ are the same.

Corollary

Let $D = \sum_{P \in E} n_P[P] \in \mathrm{Div}(E)$. Then D is a principal divisor if and only if $\sum_{P \in E} n_P = 0$ and $\sum_{P \in E} [n_P]P = \mathcal{O}$.

Weil pairing construction

Let E/K be an elliptic curve. Assume that $\mathrm{char}(K) \nmid n$.
Let $T \in E[n]$. Then there is a function f such that

$$\mathrm{div}(f) = n(T) - n(\mathcal{O}).$$

Similarly, if we let $T' \in E$ with $[n]T' = T$, then there is a function g such that

$$\mathrm{div}(g) = \sum_{R \in E[n]} (T' + R) - (R).$$

Then

$$\mathrm{div}(f \circ [n]) = \mathrm{div}(g^n).$$

After scaling, we may suppose $f \circ [n] = g^n$.
If $S \in E[n]$, then for any $X \in E$,

$$g(X+S)^n = f([n]X + [n]S) = f([n]X) = g(X)^n.$$

We now define $e_n : E[n] \times E[n] \to \mu_n$ by

$$e_n(S,T) := \frac{g(X+S)}{g(X)}.$$