

Constructing Pairing-Friendly Elliptic Curves

Peter Manohar, Xingyou Song

November 29, 2015

Abstract

The goal of this report is to....

Contents

1	Introduction	1
2	Motivations and Applications	7
3	Constructing Pairing-Friendly Curves	7

1 Introduction

In this section, we shall define key concepts needed for our report. We will prove some of the more important results, and cite a source otherwise.

1.1 Elliptic Curves

For our project, we shall define an elliptic curve to be a curve of the form:

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

where A and B are elements of some field \mathbb{F} , with $\text{char}(\mathbb{F}) \neq 2, 3$. The curve E is nonsingular if $\frac{\partial F}{\partial x}$ and $\frac{\partial F}{\partial y}$ are not simultaneously 0 for all points on E . It follows that E is nonsingular $\iff x^3 + Ax + B$ has distinct roots. Through Vieta's formulas, E has distinct roots $\iff ((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -(4A^3 + 27B^2)$ is nonzero. Therefore, we shall also require that the discriminant of E ,

$$\Delta = -16(4A^3 + 27B^2) \tag{2}$$

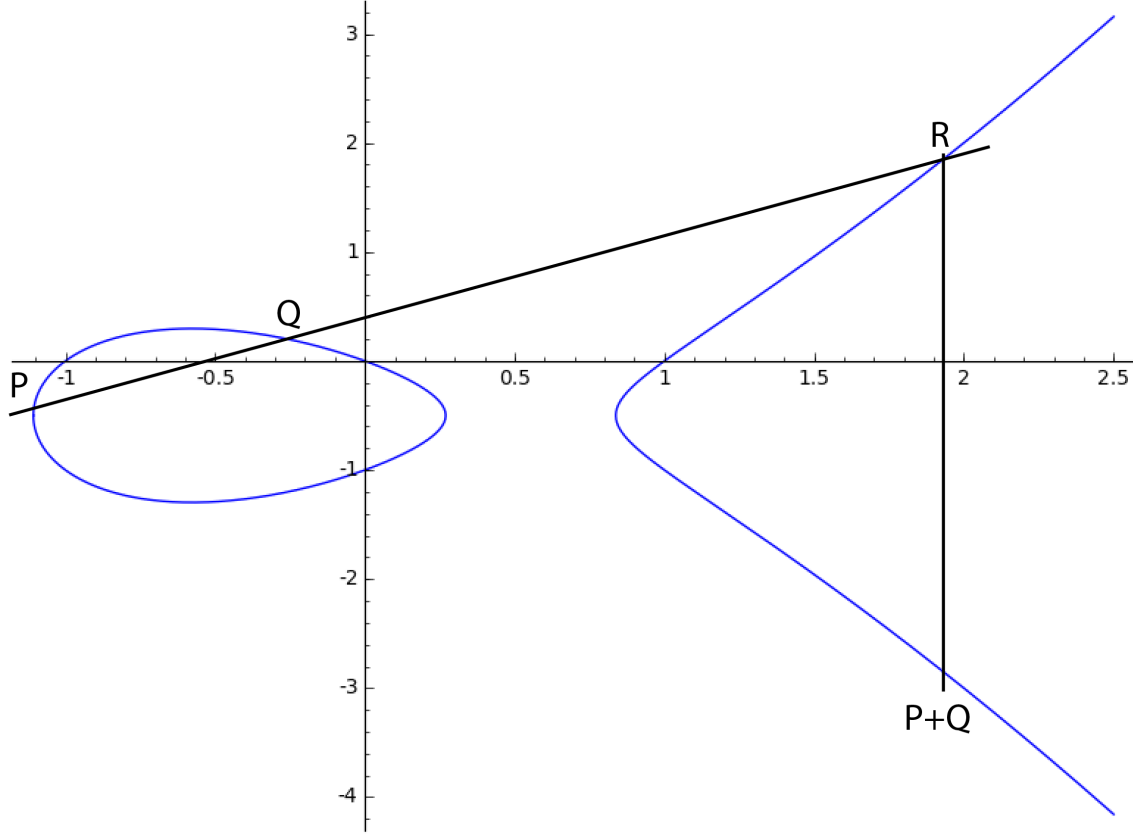
is nonzero. The j-invariant of E is defined by:

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

1.2 Group Law

The points on an elliptic curve form an additive abelian group. We shall define the group law geometrically.

Let $P = (x_p, y_p), Q = (x_q, y_q)$. A line through P and Q intersects E at a third point, $R = (x_r, y_r)$. We define $P + Q := (x_r, -y_r)$. Pictorially, this looks like



The group law can also be defined in terms of algebraic formulas, which can be found in [1].

1.3 Notation

- \mathbb{F} is a field
- $\overline{\mathbb{F}}$ is the algebraic closure of \mathbb{F}
- \mathbb{F}_p is a field with p elements, where p is prime
- $E(\mathbb{F}) = \{\mathbb{F} \times \mathbb{F} \mid E(x, y) = 0\}$
- ϕ is an isogeny (or endomorphism)
- ϕ_p is the Frobenius endomorphism
- $[n]$ is the multiplication by n map

1.4 Isogenies

An isogeny of two elliptic curves E_1 and E_2 defined over a field \mathbb{F} is a nonconstant morphism $\phi : E_1 \rightarrow E_2$, where ϕ is a group homomorphism from $E_1(\overline{\mathbb{F}}) \rightarrow E_2(\overline{\mathbb{F}})$.

E_1 and E_2 are isomorphic if $\exists \phi_1 : E_1 \rightarrow E_2$ and $\phi_2 : E_2 \rightarrow E_1$, isogenies, such that $\phi_2 \circ \phi_1 = \text{Identity}$.

1.4.1 Separable and Inseparable Isogenies

Any isogeny ϕ can be expressed as $\phi(x, y) = (\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$, where $u, v, s, t \in \mathbb{F}[x]$, and $\gcd(u, v) = \gcd(s, t) = 1$. [3] An isogeny is separable if $(\frac{u}{v})' \neq 0$, and is inseparable otherwise. The degree of an isogeny is defined as $\deg(\phi) := \max(\deg(u), \deg(v))$. [3] For any separable isogeny ϕ , $\deg(\phi) = |\ker \phi|$.

1.4.2 Dual isogenies

Theorem 1 *Let $\phi : E_1 \rightarrow E_2$ be an isogeny. Then \exists a unique $\hat{\phi} : E_2 \rightarrow E_1$ such that $\hat{\phi} \circ \phi = [n]$, where $n = \deg(\phi)$.*

The proof of this can be found in either [1] or [3]. Furthermore, for any two isogenies ϕ_1 and ϕ_2 , $\widehat{\phi_1 + \phi_2} = \hat{\phi}_1 + \hat{\phi}_2$.

1.5 Endomorphisms

An endomorphism is an isogeny from E to itself. The endomorphisms of E form a ring, where addition is addition of functions and multiplication is function composition.

1.5.1 Examples

The map $[n] : E \rightarrow E$, where $[n]P = P + P + \dots + P$ (n times) is an endomorphism.

If E is defined over \mathbb{F}_p , the Frobenius map $\phi_p : E \rightarrow E$ defined by $\phi_p(x, y) := (x^p, y^p)$ is an (inseparable) endomorphism.

1.5.2 Trace of an Endomorphism

Theorem 2 *For any endomorphism ϕ , $\phi + \hat{\phi} = 1 + \deg(\phi) - \deg(1 - \phi)$, where we can regard the RHS as an endomorphism by the map $n \mapsto [n]$.*

Proof: As endomorphisms,

$$\begin{aligned} [\deg(1 - \phi)] &= \widehat{(1 - \phi)}(1 - \phi) = (\hat{1} - \hat{\phi})(1 - \phi) = (1 - \hat{\phi})(1 - \phi) \\ &= 1 - \hat{\phi} - \phi + \hat{\phi} \circ \phi = 1 - \hat{\phi} - \phi + [\deg(\phi)] \\ \implies \phi + \hat{\phi} &= 1 + [\deg(\phi)] - [\deg(1 - \phi)] \end{aligned}$$

□

By the above theorem, we can now define $\text{trace}(\phi) := \phi + \hat{\phi}$.

Theorem 3 $\#E(\mathbb{F}_p) = p + 1 - t$, where $t = \text{trace}(\phi_p)$

Proof: The fixed field of ϕ_p is \mathbb{F}_p , and $1 - \phi_p$ is separable (see [3]). Therefore, $\ker(1 - \phi_p) = \#E(\mathbb{F}_p)$. It is clear that $\deg(\phi_p) = p$ by definition ($u(x) = x^p$ and $v(x) = 1$). We have that

$$\begin{aligned} \ker(1 - \phi_p) &= \deg(1 - \phi_p) = 1 + \deg(\phi_p) - \text{trace}(\phi_p) = p + 1 - t \\ \implies \#E(\mathbb{F}_p) &= p + 1 - t \end{aligned}$$

□

Theorem 4 *If K is a field of characteristic 0 or does not divide m , then $E[m] \simeq Z_m \oplus Z_m$.*

The proof of this is mainly using the fundamental theorem of abelian groups, and analyzing the decomposition of the torsion group (TODO?)

1.6 j-invariant

Theorem 5 *Two elliptic curves $E_1(\mathbb{F})$ and $E_2(\mathbb{F})$ are isomorphic over $\overline{\mathbb{F}} \iff j(E_1) = j(E_2)$. Furthermore, $\forall j_0 \in \overline{\mathbb{F}}, \exists$ an elliptic curve $E(\mathbb{F})$ such that $j(E) = j_0$.*

The proof requires some lengthy algebraic manipulation, which can be found in [1]. As a consequence of the proof, for any $j \in \overline{\mathbb{F}}$, we can define an canonical elliptic curve E associated with this j-invariant. We see that

$$\begin{aligned} E : y^2 &= x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j} \text{ if } j \neq 0, 1728 \\ E : y^2 &= x^3 + 1 \text{ if } j = 0 \\ E : y^2 &= x^3 + x \text{ if } j = 1728 \end{aligned} \tag{4}$$

1.6.1 Example

$E_1(\mathbb{F})$ and $E_2(\mathbb{F})$ can be isomorphic over $\overline{\mathbb{F}}$, but not over \mathbb{F} . As an example, consider the curves $E_1 : y^2 = x^3 - 25x$, $E_2 : y^2 = x^3 - 4x$ have $j = 1728$. $\#E_1(\mathbb{Q}) = \infty$ because we can just take an infinite group with generator $(-4, 6)$ but $\#E_2(\mathbb{Q}) < \infty$ because the only points on it $\infty, (2, 0), (-2, 0), (0, 0)$ form a finite abelian group.

The transformation $(x, y) \rightarrow (\mu^2 x, \mu^3 y)$, $\mu = \frac{\sqrt{10}}{2}$ establishes an isomorphism over $\mathbb{Q}(\sqrt{10})$, but no such isomorphism exists over \mathbb{Q} .

From this example, we can see that we do not necessarily need the full closure $\overline{\mathbb{F}}$; we only needed $d \in \mathbb{F}$ such that $d = \mu^2$, which in this case was $\mathbb{Q}(\sqrt{10})$, which gives rise to the idea of quadratic twists.

1.7 Twists

Two curves $E_1(\mathbb{F})$ and $E_2(\mathbb{F})$ are *twists* if they are isomorphic over $\overline{\mathbb{F}}$ but not over \mathbb{F} .

1.7.1 Quadratic Twists

In particular, we are interested in quadratic twists. If $E : y^2 = x^3 + Ax + B$ is an elliptic curve defined over \mathbb{F} , and $d \in \mathbb{F}$ is a nonsquare, then we define the *quadratic twist* of E as $\tilde{E} : y^2 = x^3 + d^2Ax + d^3B$.

Theorem 6 *If $E : y^2 = x^3 + Ax + B$ is an elliptic curve over \mathbb{F}_p with $\#E(\mathbb{F}_p) = p+1-t$, then $\#\tilde{E}(\mathbb{F}_p) = p+1+t$*

Proof: Let $\left(\frac{\cdot}{p}\right)$ be the legendre symbol mod p . For any $x \in \mathbb{F}_p$, we see that $1 + \left(\frac{x^3 + Ax + B}{p}\right) = \#$ of points on E with x-coordinate x . Therefore,

$$\#E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + Ax + B}{p}\right)\right) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{p}\right)$$

Since \mathbb{F}_p is a field, $\forall x \in \mathbb{F}_p, \exists x' \in \mathbb{F}_p$ such that $dx' = x$. Therefore, for $\tilde{E}(\mathbb{F}_p)$, we have that

$$\begin{aligned} \#\tilde{E}(\mathbb{F}_p) &= 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{(dx)^3 + A(dx) + B}{p}\right)\right) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{d^3(x^3 + Ax + B)}{p}\right) \\ &= p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{d}{p}\right) \left(\frac{d^2}{p}\right) \left(\frac{x^3 + Ax + B}{p}\right) = p + 1 - \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{p}\right) \end{aligned}$$

□

1.8 The Complex Lattice

Theorem 7 *Let ω_1, ω_2 be linearly independent points in C . Then define the lattice*

$$L = Z\omega_1 + Z\omega_2$$

Then there exists an elliptic curve that is isomorphic to C/L .

Define $G_k(L) = \sum_{\omega \in L} \omega^{-k}$. Then define the Weierstrass $\wp(z)$ function as follows:

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right) \quad (5)$$

Then this function can easily be shown, by applications of complex analysis, to be convergent and meromorphic, as well as periodic. Then the derivative $\wp'(z)$ is

$$\wp'(z) = -2 \sum_{\omega \in L} \frac{1}{(z - \omega)^2} \quad (6)$$

Now we have a isomorphism from the additive group on C/L to the the group of elliptic points on $E(C)$, by the map

$$z \rightarrow (\wp(z), \wp'(z)), \quad 0 \rightarrow O$$

with E being defined as

$$E : y^2 = 4x^3 - g_2x - g_3 \quad (7)$$

where $g_2 = 60_4, g_3 = 140G_6$. Note that the periodicity will give:

$$(\wp(z_1), \wp'(z_1)) \oplus (\wp(z_2), \wp'(z_2)) = (\wp(z_1 + z_2), \wp'(z_1 + z_2)) \quad (8)$$

which gives rise to the corresponding group law on elliptic curves.

Now we relate the j -invariant on curves to the j -function of a complex lattice. First, let rescale our lattice L to $Z\tau + Z$ where $\tau = \frac{w_1}{w_2}$. First, define $q = e^{2\pi i\tau}$. Then the j -invariant related to the lattice parameter is

$$j(\tau) = 1728 \frac{g_2^3}{g_3^3 - 27g_2^2} \quad (9)$$

The proof of all of this we won't go into detail in this paper, but this gives rise to the relationship between the complex lattice and isogenies, mainly integer endomorphisms $[m]$ give rise to $z \rightarrow mz$, and for multiplication by a complex number c , we have $z \rightarrow cz$, which will induce an endomorphism on the corresponding elliptic curve.

For curves defined on a field K , there is a homomorphism $K \rightarrow C$ if we linearly map the finite basis elements of K , $\alpha_1, \dots, \alpha_n$ respectively to any algebraically independent set of elements in C , τ_1, \dots, τ_n , so we can regard $E(K)$ as a curve in C .

1.8.1 Using Quadratic Lattices

Consider the case when our lattice $L = O_D$ for some discriminant D , where the basis elements will be $[1, \frac{1+\sqrt{D}}{2}]$ or $[1, \sqrt{D}]$ depending on whether D is $\{1\}, \{2, 3\} \pmod{4}$ respectively, which are quadratic integer fields.

Then define the Hilbert Class polynomial $H_D \in Z[X]$ that is the minimal polynomial that contains the $j(L)$ as a root. There are many ways to calculate this, but we won't get to that in this paper. Thus, we can define an elliptic curve based on a square free discriminant D .

1.9 Pairings

Then the Weil-Pairing e_r is defined as a bilinear map,

$$e_r : E[r] \times E[r] \rightarrow \mu_r \quad (10)$$

where μ_r is the set of primitive roots of unity in \bar{K} , i.e. $\mu_r = \{x | x^r = 1\}$. In other words, instead of working with the r -torsion group of $E(K)$, we may work with the much simpler objects in the extension field of K .

Then we may define the embedding degree to be the degree of the extension field $K(\mu_r)$, or in other words, $[K(\mu_r) : K]$. It is shown that then, if k is the embedding degree with respect to r , then k is the smallest integer such that r divides $q^k - 1$.

2 Motivations and Applications

2.1 Discrete Log Problem

In the discrete log problem, we are given any group G , with a base generator element P , with a ciphertext Q , where the problem involves finding k such that $P^k = Q$ in G .

For elliptic curves, this becomes using a base point P with degree N as a generator, in a finite field F_p , which will create a cyclic group. However, note that by the theorem of finite abelian groups, this cyclic group will be isomorphic to a direct sum of cyclic groups based on the prime factorization of N

2.1.1 Pohlig-Hellman Attack

For an element P , assume it has order N in the group G . Then the prime factorization of N , is important to the adversary; i.e. if

$$N = \prod_i q_i^{e_i}$$

then if we need to find k such that $P^k = Q$, then all we need to do is find k in its base q_1, q_2, \dots expansions and then construct k using the Chinese Remainder Method. We can do so on each q_i by successively iteration. Thus the difficulty of attacking this problem relies on the largest prime dividing N .

This implies that we will need to find elliptic curves that have large-prime order torsion groups.

3 Constructing Pairing-Friendly Curves

3.1 Complex Multiplication Method

Input: p , a prime, and N a positive integer

Output: An elliptic curve $E(\mathbb{F}_p)$ where $\#E(\mathbb{F}_p) = N$

$t := p + 1 - N$;

$D =$ square free part of $t^2 - 4p$;

$H_D(x) =$ Hilbert class polynomial

Pick $j \in \mathbb{F}_p$ such that $H_D(j) = 0$ Compute E according to (4).

if $\#E(\mathbb{F}_p) = N$ **then**

 | **return** E

else

 | **return** quadratic twist of E

end

Input: p , a prime, and N a positive integer, k embedding degree
Output: An elliptic curve $E(\mathbb{F}_p)$ where $\#E(\mathbb{F}_p) = N$
 $t := p + 1 - N$;
 Find r such that $r|N$ and the order of q in mod r is k
 $D =$ square free part of $t^2 - 4p$;
 $H_D(x) =$ Hilbert class polynomial
 Pick $j \in \mathbb{F}_p$ such that $H_D(j) = 0$ Compute E according to (4).
if $\#E(\mathbb{F}_p) = N$ **then**
 | **return** E
else
 | **return** quadratic twist of E
end

The above algorithm will always succeed provided that such a curve E exists and D is not too large. A slight subtlety arises if $j = 0$ or $j = 1728$. If $j = 0$, then there are 6 classes of curves, corresponding to sextic twists of E by $1, \zeta, \zeta^2, \dots, \zeta^5$, for ζ a primitive root of unity in \mathbb{F}_p . If $j = 1728$, then there are 4 classes of curves, corresponding to quartic twists of E by $1, \zeta, \dots, \zeta^3$, for ζ a primitive root of unity in \mathbb{F}_p . If a curve E exists, then one of these curves will satisfy the conditions of the algorithm. TODO
 NEED SOURCE

Rationale for this algorithm:

References

[1]. silverman [2]. washington [3]. mit