Introduction to elliptic curves and an application to cryptography

Justin Wu

December 2019

1 Introduction

In this paper, we introduce the basic theory of elliptic curves, and look at an application of the Weil pairing to cryptography. The goal will be to provide a high level overview, and so many technical unenlightening proofs will be omitted. Throughout this paper, K and $\bar{K}$ will denote a field and it's algebraic closure, and $G_{\bar{K}/K}$ the galois group. Curves are smooth projective varieties of dimension 1, $K(E)$ and $\bar{K}(E)$ denote the function fields for an arbitrary variety E over K and $\bar{K}$ respectively.

2 Preliminaries

Definition 1. *The divisor group of a curve $Div(C)$, is the free abelian group generated by the points of C i.e. all formal finite $\mathbb{Z}$ linear combinations of points of C. Divisors are denoted $D = \sum_{P \in C} n_P(P)$.*

Definition 2. *The degree of D is defined by $degD = \sum_{P \in C} n_P$. The divisors of degree 0 is the subgroup of $Div(C)$ denoted $Div^0(C)$.*

$G_{\bar{K}/K}$ naturally acts on $Div(C)$ and $Div^0(C)$ by

$$D^\sigma = \sum_{P \in C} n_P(P^\sigma)$$

Definition 3. *D is defined over K if $D^\sigma = D$ $\forall \sigma \in G_{\bar{K}/K}$. We denote the group of divisors defined over K as $Div_K(C)$ and similarily $Div^0_K(C)$.*

Definition 4. *Let $f \in \bar{K}(C)^*$. Then we define*

$$div(f) = \sum_{P \in C} ord_P(f)(P)$$

See Hartshorne I.6.5 for a proof that there are only finitely many points where f has a pole or zero. We define $D \in Div(C)$ to be principle if $D = div(f)$

for some $f \in \bar{K}(C)*$. Divisors D_1 and D_2 are linearly equivalent, written $D_1 \sim D_2$ if $D_1 - D_2$ is principal. The Picard group of C, denoted $Pic(C)$ is the quotient of $Div(C)$ by its subgroup of principal divisors (easy exercise: prove that the collection of principal divisors is indeed a subgroup).

Theorem 1. *$deg(div(f)) = 0$.*

Proof. See Hartshorne II.6.10. □

A divisor $D = \sum n_P(P)$ is positive if $n_P \geq 0 \ \forall P \in C$. We write $D_1 \geq D_2$ to mean that $D_1 - D_2$ is positive.

Definition 5. *Let $D \in Div(C)$. Define*

$$L(D) = \{f \in \bar{K}(C)* : div(f) \geq -D\} \cup \{0\}$$

This is a finite dimensional $\bar{K}$ vector space, and we denote $\ell(D) = dim_{\bar{K}} L(D)$.

Theorem 2. *We have the following.*
(a) If $deg(D) < 0$, then $L(D) = \{0\}$ and $\ell(D) = 0$
(b) L(D) is a finite-dimensional $\bar{K}$ vector space.
(c) If $D_1 \sim D_2$, then $L(D_1) \cong L(D_2)$.
(a) and (c) are easy exercises left to the reader, and (b) follows from Hartshorne, II.5.19.

Theorem 3. *(Riemann-Roch) Let C be a smooth curve and let K_C be a canonical divisor on C. Then there is an integer $g \geq 0$, called the genus of C, such that for every divisor $D \in Div(C)$,*

$$\ell(D) - \ell(K_C - D) = deg(D) - g + 1$$

We do not concern ourselves with the details of what a canonical divisor is, and the proof. For a proof, see Hartshorne IV.1 or Lang, An Introduction to algebraic and abelian functions.

3 Basic theory of elliptic curves

3.1 Elliptic Curves

The most natural definition of an elliptic curve is a genus 1 curve with a distinguished point (denoted O). This definition is equivalent to a plane cubic, and can be written in a Weierstrass form.

Theorem. *There exist functions $x, y \in K(E)$ such that the map*

$$\phi : E \to \mathbb{P}^2$$

$$\phi = [x, y, 1]$$

such that $\phi(O) = [0, 1, 0]$ and is an isomorphism of E/K onto a curve

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with $a_1 \dots a_6 \in K$.

The proof involves the Riemann-Roch theorem and is omitted.

If we assume K has characteristic $p \geq 5$, then substitutions of variables allows us to reduce the Weierstrauss form to the Weierstrauss normal form $y^2 = x^3 + ax + b$ (See Silverman, Arithmetic of Elliptic Curves for a proof). Note that we typically are only interested in nonsingular curves, which is true if and only if the discriminant $4a^3 + 27b^2 \neq 0$.

3.2 Group structure

The reader is likely familiar with the group structure on an elliptic curve where given two points P, Q, $P + Q$ is defined as the point obtained from drawing a line through P and Q (tangent line if $P = Q$) which intersects E at R, and the third intersection with E of the line going through R and O is defined as the sum $P + Q$. However, this group structure can be framed algebraically with the Picard group:

Theorem 4. *There exists a map $\sigma : Div^0(E) \to E$ as follows: For every degree-0 divisor $D \in D^0(E)$, we define σD as the unique point $P \in E$ satisfying $D \sim (P) - (O)$.*

(a) This point exists and is unique

(b) σ is surjective

(c) $\sigma(D_1) = \sigma D_2$ if and only if $D_1 \sim D_2$. Therefore σ induces a bijection of sets between $Pic^0(E)$ and E.

(d) The geometric group law on E and this algebraic group law induced by the inverse map $P \to$ divisor class of $(P) - (O)$ are the same.

Theorem 5. *$D = div(f)$ for some $f \in \bar{K}(E)*$ if and only if $deg(D) = 0$ and the evaluation of the formal sum with the group structure on E gives O.*

Definition 6. *An Isogeny of elliptic curves is a morphism $\phi : E_1 \to E_2$ with $\phi(O_{E_1}) = O_{E_2}$.*

Note: In general, morphisms of curves are constant or surjective (see Hartshorne II.6.8) for a proof. Therefore all isogenies are either trivial or surjective.

Definition 7. *Let $[m]$ denote the multiplication by m isogeny $E \to E$ (exercise: verify that this is an isogeny).*

Definition 8. *An isogeny ϕ of elliptic curves E_1, E_2, induces an injection of function fields $\phi^* : \bar{K}(E_2) \hookrightarrow \bar{K}(E_1)$. The degree of ϕ is defined as the degree of this extension.*

Theorem 6. *$deg([m]) = m^2$ and the $m-$torsion subgroup of $E(\overline{K})$, denoted $E[m]$ is isomorphic to $\frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$*

Proof. The proof involves the dual isogeny and is omitted. □

Theorem 7. *Isogenies are group homomorphisms.*

Proof. Note that ϕ induces a homomorphism $\phi_* : Pic^0 E_1 \rightarrow Pic^0(E_2)$. The equivalence of the geometric group structure on E and the algebraic group structure of Pic^0 shows that ϕ is a homomorphism. The details are left to the reader. □

3.3 Weil Pairing

We construct the Weil e_m-pairing, which is a map $e_m : E[m] \times E[m] \rightarrow \mu_m$ where μ_m is the group of the m^{th} roots of unity. This pairing is bilinear, alternating, nondegenerate, galois invariant, and compatible. Recall that a divisor $\sum n_i(P_i)$ is the divisor of some function if and only if $\sum n_i = 0$ and $\sum [n_i]P_i = O$.

Now let $T \in E[m]$. Then there exists $f \in \bar{K}(E)$ with

$$div(f) = m(T) - m(O)$$

Now take a $T' \in E$ with $[m]T' = T$. Similarly, there exists $g \in \bar{K}(E)$ with

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

Note that $f \circ [m]$ and g^m have the same divisor since the divisor of g^m is

$$\sum_{R \in E[m]} (m(T' + R) - m(R))$$

which is also the divisor of $f \circ [m]$. Therefore, we have up to a constant in $\bar{K}*$, $f \circ [m] = g^m$. Now let $S \in E[m]$. We have for any $X \in E$,

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

Therefore, if we consider the function $g(X+S)/g(X)$ as a function of X, it must be a m-th root of unity. But since there are only m possible values, this function is a morphism $E \rightarrow \mathbb{P}^1$ which is not surjective, so it is constant. Therefore, we, have a well defined pairing

$$e_m : E[m] \times E[m] \rightarrow \mu_m$$

defined by

$$e_m(S, T) = \frac{g(X + S)}{g(X)}$$

Theorem 8. *The Weil* e_m *pairing satisfies the following*

(a) It is bilinear

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

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

(b) It is alternating

$$e_m(T, T) = 1$$

(c) It is nondegenerate: If $e_m(S, T) = 1$ for all $S \in E[m]$, then $T = O$

(d) It is Galois invariant

$$e_m(S, T)^\sigma = e_m(S^\sigma, T^\sigma)\ \forall \sigma \in G_{\bar{K}/K}$$

(e) It is compatible:

$$e_{mm'}(S, T) = e_m([m']S, T)$$

for all $S \in E[mm']$ and $T \in E[m]$.

The proof is not useful for our purposes and omitted. An important corollary is that part (a) implies that if S, T generate $E[m]$, then $e_m S, T$ is a primitive m-th root of unity.

4 Application to Cryptography

4.1 Three-way Diffie-Hellman

The reader is likely familiar with the Diffie-Hellman key exchange algorithm, which allows Alice and Bob to securely exchange an unspecified key. The Weil pairing provides a 3-way key exchange system (invented by Joux) but the pairing must be slightly modified. This is because the Weil e_m pairing is alternating, i.e. $e_m(T, T) = 1$. We want $e_m(T, T)$ to be a primitive n^{th} root of unity. One way around this is to use a curve that has a distortion map, an isogeny $\phi : E \to E$ such that there exists $T \in E$ such that $\{T, \phi(T)\}$ is a basis for for $E[n]$. Then we can define the modified Weil pairing

$$\langle \cdot, \cdot \rangle : E[n] \times E[n] \to \mu_n$$

$$\langle P, Q \rangle = e_n(P, \phi(Q))$$

Then we have $\langle T, T \rangle$ is a primitive n^{th} root of unity.

Here is how the Tripartite Diffie-Hellman key exchange works. Alice, Bob, and Carl agree on a finite field $\mathbb{F}_q$, a prime p, an elliptic curve $E/\mathbb{F}_q$ that has a distortion map, and a point $T \in E(\mathbb{F}_q)[p]$. Alice, Bob, and Carl choose secret integers a, b, c. Alice computes $A = [a]T$, Bob computes $B = [b]T$, and Carl computes $C = [c]T$, and each publishes these points. The key is $\langle T, T \rangle^{abc}$. Alice computes $\langle B, C \rangle^a$, Bob computes $\langle A, C \rangle^b$, and Carl computes $\langle A, B \rangle^c$. It is easily verified that this works. This is secure because the elliptic curve discrete logarithm problem is believed to be secure.