18.783 Elliptic Curves
Lecture 23

Andrew Sutherland

May 2, 2022

Function fields

Recall that the function field $k(C)$ of a smooth plane curve $C\colon f(x,y,z)=0$ over k is the field of rational functions g/h, where $g,h\in k[x,y,z]$ are homogeneous polynomials of the same degree with $h\notin(f)$, modulo the equivalence relation

$$\frac{g_1}{h_1}\sim\frac{g_2}{h_2}\qquad\Longleftrightarrow\qquad g_1h_2-g_2h_1\in(f).$$

Alternatively, we can view the function g/h as a rational map $(g:h)$ from C to $\mathbb{P}^1$. Our assumption that C is smooth implies that this rational map is a morphism.

Example

Consider the function x/z on the elliptic curve $E\colon y^2z=x^3+Axz^2+Bz^3$. We can evaluate the map $(x:z)$ at any affine point, but not at $(0:1:0)$. However,

$$(x:z)\sim(x^3:x^2z)\sim(y^2z-Axz^2-Bz^3:x^2z)\sim(y^2-Axz-Bz^2:x^2).$$

Local rings

Definition

For $P \in C(\bar{k})$ the local ring (or ring of regular functions) at P is

$$\mathcal{O}_P := \{f \in k(C) : f(P) \neq \infty\} \subseteq k(C),$$

where $\infty := (1 : 0) \in \mathbb{P}^1$. It is a principal ideal domain (PID) with maximal ideal

$$\mathfrak{m}_P := \{f \in \mathcal{O}_P : f(P) = 0\},$$

where $0 := (0 : 1) \in \mathbb{P}^1$. Any generator u_P for $\mathfrak{m}_P = (u_P)$ is a uniformizer at P.

Remark

When k is not algebraically closed it makes more sense to work with closed points: for any $P \in C(\bar{k})$ the rings $\mathcal{O}_Q$ are necessarily the same for all Q in the Galois orbit of P.

Discrete valuations

Definition

A discrete valuation on a field F is a surjective homomorphism $v\colon F^\times \to \mathbb{Z}$ that satisfies the inequality

$$v(x+y) \geq \min(v(x), v(y)).$$

for all $x, y \in F^\times$, which we formally extend to F by defining $v(0) := \infty$.

If v is a discrete valuation on F, then the valuation ring

$$R := \{x \in F : v(x) \geq 0\}$$

is a PID with the unique maximal ideal

$$\mathfrak{m} := \{x \in R : v(x) \geq 1\},$$

and every nonzero ideal (x) of R is then of the form $\mathfrak{m}^n$, where $n = v(x)$.
Any generator u of the maximal ideal $\mathfrak{m} = (u)$ is called a uniformizer for R.

Discrete valuation rings

Given a PID R with unique nonzero maximal ideal $\mathfrak{m} = (u)$, if we define $v(0) := \infty$ and

$$v(x) := \min\{n \in \mathbb{Z} : u^{-n}x \in R\},$$

then v is a discrete valuation on the fraction field F of R, and R is its valuation ring.

Definition

A PID with unique nonzero maximal ideal, equivalently, an integral domain that is the valuation ring of a discrete valuation on its fraction field, is a discrete valuation ring.

If C/k is a smooth projective curve with $P \in C(\bar{k})$ then $\mathcal{O}_P$ is a discrete valuation ring (DVR) whose valuation v_P measures the "order of vanishing" of $f \in k(C)$ at P.

This is clear when $k = \mathbb{C}$ and in general one can formally define the Laurent series expansion $g \in k((t))$ of f at P so that $v_P(f)$ is the exponent of its leading term.

Rational maps of smooth projective curves are morphisms

A projective curve C/k is smooth at P if and only if the local ring $\mathcal{O}_P$ is a DVR (one can take this as an alternative definition of smoothness). It is this property that forces rational maps from smooth projective curves to be morphisms (as noted in Lecture 4).

Theorem

Let C_1/k be a smooth projective curve. Rational maps $\phi\colon C_1 \to C_2$ are morphisms.

Proof: Let $\phi = (\phi_0 : \cdots : \phi_m)$, let $P \in C_1(\bar{k})$, let u_P be a uniformizer at P, and let $n = \min_i v_P(\phi_i)$. Then

$$\phi = (u_P^{-n}\phi_0 : \cdots : u_P^{-n}\phi_m)$$

is defined at P because $v_P(u_P^{-n}\phi_i) \geq 0$ for all i and $v_P(u_P^{-n}\phi_i) = 0$ for at least one i.

Some examples

Example

For the function $x := x/z$ on the elliptic curve $E\colon y^2 = x^3 + Ax + B$ we have

$$v_P(x) = \begin{cases} 0 & \text{if } P = (1 : * : *) \\ 1 & \text{if } P = (0 : \pm\sqrt{B} : 1) \quad (B \neq 0) \\ 2 & \text{if } P = (0 : 0 : 1) \quad (B = 0) \\ -2 & \text{if } P = (0 : 1 : 0) \end{cases}$$

and for the function $y := y/z$ we have

$$v_P(y) = \begin{cases} 0 & \text{if } P = (* : 1 : z_0) \quad (z_0 \neq 0) \\ 1 & \text{if } P = (x_0 : 0 : 1) \quad (x_0^3 + Ax_0 + B = 0) \\ -3 & \text{if } P = (0 : 1 : 0) \end{cases}$$

The degree of a morphism

Recall that the the degree of $f \in k(C)$ is $\deg f := [k(C) : f^*(k(\mathbb{P}^1))]$.

Theorem

Let C be a smooth projective curve over $k = \bar{k}$ and $f \in k(C)^\times$. If $Q \in \mathbb{P}^1(k)$ then

$$\deg f = \sum_{f(P)=Q} v_P(u_Q \circ f).$$

where $u_Q \in k(\mathbb{P}^1)$ denotes any uniformizer for m_Q.

Corollary

Let C be a smooth projective curve over $k = \bar{k}$. For every $f \in k(C)^\times$ we have

$$\sum v_P(f) = 0,$$

with $v_P(f) = 0$ for almost all P. We have $v_P(f) = 0$ for all P if and only if $f \in k^\times$.

The degree of a closed point

Definition

The degree of a closed point on C/k is its cardinality (as a Galois orbit in $C(\bar{k})$).

When $k \neq \bar{k}$ the degree formula becomes

$$\deg f \deg Q = \sum_{f(P)=Q} v_P(u_Q \circ f) \deg P,$$

which holds for any closed point Q of $\mathbb{P}^1/k$, and we have

$$\sum v_P(f) \deg P = 0,$$

where the sum is over closed points P.

The divisor group of a curve

Definition

Let C/k be a smooth projective curve. For all $P \in C(\bar{k})$ we define a formal symbol $[P]$. The divisor group of C is the free abelian group on the set $\{[P] : P \in C(\bar{k})\}$, denoted $\operatorname{Div} C$. Its elements are called divisors. Each is a finite sum of the form

$$D = \sum n_P [P]$$

in which the n_P are integers (so $n_P = 0$ for all but finitely many P). The integer n_P is the valuation of D at P, and we may write $v_P(D) := n_P$. We also define the support $\operatorname{supp}(D) := \{[P] : v_P(D) \neq 0\}$ and the degree $\deg D := \sum v_P(D)$.

The map $\operatorname{Div} C \to \mathbb{Z}$ defined by $D \mapsto \deg D$ is a surjective homomorphism of abelian groups whose kernel is the subgroup $\operatorname{Div}^0 C$ of divisors of degree zero.

Remark

When working with closed points P one defines $\deg D := \sum v_P(D) \deg P$.

The divisor class group of a curve

Associated to each function $f \in k(C)^\times$ is a divisor

$$\operatorname{div} f := \sum v_P(f)[P],$$

that is called a principal divisor. We have $\operatorname{div} fg = \operatorname{div} f + \operatorname{div} g$, and the map

$$\operatorname{div}\colon k(C)^\times \to \operatorname{Div} C$$

is a group homomorphism whose image $\operatorname{Princ} C$ is a subgroup of $\operatorname{Div} C$.

Definition

The Picard group of a smooth projective curve C/k is the quotient

$$\operatorname{Pic} C := \operatorname{Div} C / \operatorname{Princ} C.$$

Now $\operatorname{Princ} C \subseteq \operatorname{Div}^0 C$, and we have a degree map $\deg\colon \operatorname{Pic} C \to \mathbb{Z}$ whose kernel

$$\operatorname{Pic}^0 C := \operatorname{Div}^0 C / \operatorname{Princ} C$$

is the (degree zero) divisor class group (isomorphic to the Jacobian if $C(k) \neq \emptyset$).

The Abel-Jacobi map

We have an exact sequence

$$1 \longrightarrow k^\times \longrightarrow k(C)^\times \longrightarrow \mathrm{Div}^0 C \longrightarrow \mathrm{Pic}^0 C \longrightarrow 0.$$

Definition

Let C/k be a smooth projective curve and let $O \in C(k)$ be a rational point. The map

$$\begin{aligned} C(k) &\to \mathrm{Pic}^0 C \\ P &\mapsto [P] - [O] \end{aligned}$$

is the Abel-Jacobi map.

When $k = \bar{k}$ the Abel-Jacobi map of a genus g curve is surjective if and only if $g \leq 1$ and injective if and only if $g \geq 1$. Smooth projective curves of genus 1 with a rational point (elliptic curves!) are precisely the curves for which it is an isomorphism.

The Jacobian of an elliptic curve

Let E/k be an elliptic curve with distinguished point O (the point at infinity).

For $P, Q \in E(k)$ we use $L_{P,Q} \in k(E)$ to denote the function given by the line through P and Q (tangent when $P = Q$). It $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are distinct then

$$L_{P,Q} = (y - y_1)(x_2 - x_1) - (x - x_1)(y_2 - y_1) \in k(E)$$

has zeros at $P, Q, -(P + Q)$ and defines a morphism $L_{P,Q} \colon E \to \mathbb{P}^1$. We have

$$\operatorname{div} L_{P,Q} = [P] + [Q] + [-(P + Q)] - 3[O].$$

The Jacobian of an elliptic curve

If we now define $G_{P,Q} := L_{P,Q}/L_{P+Q,-(P+Q)}$ then

$$\begin{aligned}\operatorname{div} G_{P,Q} &= [P] + [Q] + [-(P+Q)] - 3[O] - ([P+Q] + [-(P+Q)] + [O] - 3[O]) \\ &= [P] + [Q] - [P+Q] - [O]\end{aligned}$$

Since $\operatorname{div} G_{p,q}$ is a principal divisor, $[P] + [Q]$ and $[P+Q] + [O]$ represent the same equivalence class in $\operatorname{Pic} E$; such divisors are linearly equivalent, and we write

$$[P] + [Q] \sim [P+Q] + [O].$$

Theorem

Let E/k be an elliptic curve the distinguished point O. The Abel-Jacobi map $E \mapsto \operatorname{Pic}^0 E$ defined by $P \mapsto [P] - [O]$ is a group isomorphism.

Proof: To the board!

The Weil pairing

Definition

Let C/k be a smooth projective curve, and let $f \in k(C)^\times$. For each $D \in \operatorname{Div} C$ with support disjoint from $\operatorname{div} f$ we define

$$f(D) := \prod_{P \in \operatorname{supp}(D)} f(P)^{v_P(D)} \in k^\times,$$

with $f(D_1 + D_2) = f(D_1)f(D_2)$ for any D_1, D_2 with support disjoint from $\operatorname{div} f$.

Let us fix a rational point $O \in C(k)$ and a uniformizer u_O for $\mathcal{O}_O$. For each nonzero principal divisor $D \in \operatorname{Princ} C$ there is a unique $f \in k(C)^\times$ for which $\operatorname{div} f = D$ and

$$(u_O^{-v_O(f)} f)(O) = 1.$$

We call this the normalized function for the divisor $\operatorname{div} f$.

The Weil pairing

Definition

Let $n \in \mathbb{Z}_{>0}$ be prime to the characteristic of $k = \bar{k}$. Let C/k be a smooth projective curve and let D_1, D_2 be divisors with disjoint support representing n-torsion elements of $\mathrm{Pic}^0 C$ (so $D_1, D_2 \in \mathrm{Div}^0 C$ and $nD_1, nD_2 \in \mathrm{Princ}\, C$). Let $f_1, f_2 \in k(C)^\times$ be the normalized functions for which $nD_1 = \mathrm{div}\, f_1$ and $nD_2 = \mathrm{div}\ f_2$. The Weil pairing

$$e_n(D_1, D_2) := \frac{f_1(D_2)}{f_2(D_1)} \in k^\times$$

is a map from $(\mathrm{Pic}^0 C)[n] \times (\mathrm{Pic}^0 C)[n]$ to $k^\times$.

The Weil pairing actually defines a map

$$e_n \colon (\mathrm{Pic}^0 C)[n] \times (\mathrm{Pic}^0 C)[n] \to \mu_n \subseteq \bar{k}^\times = k^\times,$$

where μ_n is the group of nth roots of unity in $\bar{k}$.

The Weil reciprocity law

Theorem (Weil reciprocity law)

Let C be a smooth projective curve over $k = \bar{k}$ and let $f, g \in k(C)^\times$ be functions whose divisors have disjoint support. Then

$$f(\operatorname{div} g) = g(\operatorname{div} f).$$

Proof: See exercise 2.11 in Silverman.

Corollary

The value of the Weil pairing $e_n(D_1, D_2) \in k^\times$ depends only on the divisor classes of D_1 and D_2 and is an element of $\mu_n \subseteq k^\times$.

Proof: See notes.

Properties of the Weil pairing

Theorem

Let $n \in \mathbb{Z}_{>0}$ be prime to the characteristic of $k = \bar{k}$ and let C/k be a smooth projective curve. Let D_1, D_2, D_3 be divisors with disjoint support representing elements of $(\mathrm{Pic}^0 C)[n]$. The Weil pairing $e_n \colon (\mathrm{Pic}^0 C)[n] \times (\mathrm{Pic}^0 C)[n] \to \mu_n$ satisfies:

- *bilinear: $e_n(D_1 + D_2, D_3) = e_n(D_1, D_3) e_n(D_2, D_3)$;*
- *alternating: $e_n(D_1, D_2) = e_n(D_2, D_1)^{-1}$.*

Proof: Easy check.

The Weil pairing has many other properties that hold in general, but to simplify matters we now restrict to the case where C is an elliptic curve.

The Weil pairing on an elliptic curve

For an elliptic curve E/k, the isomorphism $E \xrightarrow{\sim} \operatorname{Pic}^0 E$ given by the Abel-Jacobi map $P \mapsto [P] - [O]$ allows us to view the Weil pairing as a map

$$e_n \colon E[n] \times E[n] \to \mu_n$$

defined on pairs of n-torsion points of E/k (for n prime to the characteristic of k). At first glance it might appear that we have a problem, since for $P, Q \in E[n]$ the divisors $[P] - [O]$ and $[Q] - [O]$ obviously do not have disjoint support.

But we can always translate these divisors to linearly equivalent divisors with disjoint support by picking some point $T \neq 0, Q, -P, Q - P$ and replacing $[P] - [O]$ with the linearly equivalent divisor $[P + T] - [T]$; this does not change the element of $\operatorname{Pic}^0 E$ represented by $[P] - [O]$ nor does it change the value of the Weil pairing.

Miller functions

To explicitly (and efficiently) compute $e_n(P,Q)$ in practice, one uses Miller functions.

Definition

Let E/k be an elliptic curve and let $P \in E(k)$. For $n \in \mathbb{Z}$ we recursively define $f_{n,P}$ via

$$f_{0,P} = f_{1,P} := 1, \qquad f_{n+1,P} := f_{n,P}G_{P,nP}, \qquad f_{-n,P} := (f_{n,P}G_{nP,-nP})^{-1},$$

where $G_{P,Q} = L_{P,Q}/L_{P+Q,-(P+Q)}$ as above with $L_{P,Q}$ and $L_{P+Q,-(P+Q)}$ normalized.

Lemma

The functions $f_{n,P}$ satisfy the following properties:

(i) $\operatorname{div} f_{n,P} = n[P] - (n-1)[O] - [nP]$;
(ii) $f_{m+n,P} = f_{m,P}f_{n,P}G_{mP,nP}$;
(iii) $f_{mn,P} = f_{m,P}^n f_{n,mP} = f_{n,P}^m f_{m,nP}$.

This lemma allows us to evaluate $f_{n,P}(Q)$ using $O(\log n)$ field operations in k.

Miller functions

Lemma

Let E/k be an elliptic curve, let $n \geq 1$ be prime to the characteristic of k, and let $P, Q \in E(k)[n]$. For any point $T \notin \{0, Q, -P, Q - P\}$ on E we have

$$e_n(P, Q) = \frac{f_{n,Q}(T) f_{n,P}(Q - T))}{f_{n,P}(-T) f_{n,Q}(P + T)}.$$

Proof: See notes.

Corollary

Let E/k be an elliptic curve with distinct points $P, Q \in E(k)[n]$, where $n \geq 1$ is prime to the characteristic of k. Then

$$e_n(P, Q) = (-1)^n \frac{f_{n,P}(Q)}{f_{n,Q}(P)}.$$

The Weil pairing on an elliptic curve

Theorem

Let E/k be an elliptic curve and let m and n be positive integers prime to the characteristic of k. The Weil pairing $e_n\colon E[n] \times E[n] \to \mu_n$ satisfies the following:

- *bilinear:* $e_n(P+Q,R) = e_n(P,R)e_n(Q,R)$, $e_n(P,Q+R) = e_n(P,Q)e_n(P,R)$;
- *alternating:* $e_n(P,P) = 1$ *and* $e_n(P,Q) = e_n(Q,P)^{-1}$;
- *nondegenerate: If* $P \neq 0$ *then* $e_n(P,Q) \neq 1$ *for some* $Q \in E[n]$;
- *compatibility:* $e_{mn}(P,Q) = e_n(mP,Q)$ *for all* $P \in E[mn]$ *and* $Q \in E[n]$;
- *Galois-equivariant:* $e_n(P^\sigma, Q^\sigma) = e_n(P,Q)^\sigma$ *for all* $\sigma \in \mathrm{Gal}(\bar{k}/k)$;
- *endomorphisms:* $e_n(\alpha(P),\alpha(Q)) = e_n(P,Q)^{\deg \alpha}$ *for all* $\alpha \in \mathrm{End}(E)$;
- *surjective: for each* $P \in E[n]$ *we have* $\{e_n(P,Q) : Q \in E[n]\} = \mu_{\mathrm{ord}(P)}$.

Proof: See notes.

A few theoretical applications of the Weil pairing

Corollary

Let $\phi\colon E_1 \to E_2$ and $\psi\colon E_1 to E_2$ be isogenies of elliptic curves. Then $\widehat{\phi+\psi} = \hat{\phi}+\hat{\psi}$.
Proof: Show $e_{2^n}(P_1, (\widehat{\phi+\psi})(P_2)) = e_{2^n}(P_1, (\hat{\phi}+\hat{\psi})(P_2))$ for $P_1, P_2 \in E[2^n]$, $n \geq 1$.

Corollary

Let E/k be an elliptic curve and let n be a positive integer prime to the characteristic of k. If $E[n] \subseteq E(k)$ then $\mu_n \subseteq k^\times$. In particular, if $k = \mathbb{Q}$ then $E[n] \subseteq E(k)$ can occur only for $n \leq 2$, and if $k = \mathbb{F}_q$ then $E[n] \subseteq E(k)$ can occur only if $q \equiv 1 \bmod n$.

Corollary

Let E/k be an elliptic curve and let $P \in E(\bar{k})$ be a point of order n prime to the characteristic of k. For every $Q \in E[n]$ the order of $e_n(P,Q)$ in μ_n is the largest integer m for which $E[m] \subseteq \langle P, Q\rangle$, equivalently, the least integer m for which $mQ \in \langle P\rangle$. In particular, $e_n(P,Q) = 1$ if and only if $\langle P, Q\rangle$ is cyclic.

Practical application: tripartite Diffie–Hellman

To begin the protocol, Alice, Bob, and Carol pick random integers a, b, c, respectively. Alice sends $P_A := aP$ and $Q_A := aQ$ to Bob and Carol, Bob sends $P_B := bP$ and $Q_B := bQ$ to Alice and Carol, Carol sends $P_C := cP$ and $Q_C := cQ$ to Alice and Bob.

Alice computes

$$e_n(P_B, Q_C)^a = e_n(bP, cQ)^a = e_n(P, Q)^{bca},$$

Bob computes

$$e_n(P_A, Q_C)^b = e_n(aP, cQ)^b = e_n(P, Q)^{acb},$$

Carol computes

$$e_n(P_A, Q_B)^c = e_n(aP, bQ)^c = e_n(P, Q)^{abc}.$$

The common value $e_n(P, Q)^{abc} \in \mu_n$ is now known to Alice, Bob, and Carol.

If one assumes DLP is hard, an eavesdropper cannot easily determine any of a, b, c, and if one further assumes that the computational Diffie-Hellman problem is hard, an eavesdropper cannot easily determine μ_n either.

The embedding degree of an elliptic curve

Definition

Let E/k be an elliptic curve and $n \in \mathbb{Z}_{>0}$. The embedding degree of E with respect to n is the degree of the minimal extension L/k for which $E[n] \subseteq E(L)$.

An easy lower bound on the embedding degree s arises from the fact that the Weil pairing $E[n] \times E[n] \to \mu_n$ is surjective. If $E[n] \subseteq \mathbb{F}_{q^s}$ then we must have $\mu_n \subseteq \mathbb{F}_{q^s}^\times$. The group $\mathbb{F}_{q^s}^\times$ is cyclic, so this is the same as requiring $q^s \equiv 1 \bmod n$. When $E(\mathbb{F}_q)$ contains a cyclic group of order n, this necessary condition is also sufficient.

Lemma

Let $E/\mathbb{F}_q$ be an elliptic curve, let $n \perp q$ be a prime divisor of $\#E(\mathbb{F}_q)$, and let π_n be the restriction of the Frobenius endomorphism π_E to $\mathrm{End}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Then either $E[n] \subseteq E(\mathbb{F}_q)$ or $E[n] \simeq \ker(\pi_n - 1) \oplus \ker(\pi_n - q)$, and the embedding degree of E with respect to n is the least integer $s > 0$ such that $q^s \equiv 1 \bmod n$.

Pairing-friendly curves

Practical applications of the Weil pairing are feasible only when the embedding degree s is small for a large divisor n of $\#E(\mathbb{F}_q)$ (often $n = \#E(\mathbb{F}_q)$ is prime or near prime). It is possible to have $s \leq 2$ when E is supersingular (see Problem Set 12), but this is too small for cryptographic applications: as you will show on Problem Set 12, one can transfer the discrete logarithm problem in $E(\mathbb{F}_q)$ to the discrete logarithm problem in $\mathbb{F}_{q^s}^\times$ where it can be solved in subexponential time.

Ideally one wants s to be around 10 or 20 to balance the difficulty of the discrete logarithm problems in $E(\mathbb{F}_q)$ and $\mathbb{F}_{q^s}^\times$; for $q \approx 2^{256}$ using $s = 12$ yields $\#\mathbb{F}_{q^s}^\times \approx 2^{3072}$, in which case the discrete logarithm problems have similar difficulty.

Elliptic curves with embedding degrees in this range are said to be pairing friendly. They are quite rare, far too rare to find by brute force search, but they can be constructed using the CM method.

The Tate pairing

In most practical applications of pairings, rather than the Weil pairing one uses the Tate pairing, or variations thereof, which can be computed much more efficiently.

Definition

Let $n > 2$ be an integer and let $E/\mathbb{F}_q$ be an elliptic curve over a finite field with embedding degree d with respect to n. The (modified) Tate pairing is the map $t_n \colon E[n] \times E[n] \to \mu_n$ defined by

$$t_n(P, Q) := \left(\frac{f_{n,P}(Q + T)}{f_{n,P}(T)} \right)^{(q^d - 1)/n}$$

where $T \in E[n] - \{0, P, -Q, P - Q\}$.

Like the Weil pairing, the Tate pairing is a non-degenerate bilinear pairing that is surjective and Galois-equivariant. Unlike the Weil pairing, the Tate pairing is not alternating, and may have $t_n(P, P) \neq 1$; this is an advantage in many practical applications, because it means that the pairing may be non-trivial even when we restrict to points in a cyclic subgroup of $E[n]$, which is never true of the Weil pairing.