DRP Fall 2020 Outline

Sunay Joshi

July 20, 2026

To-dos.

- Background: groups, fields, projective space.
- SAGE demonstrations: What kinds?
- Add diagrams.
- Fill in "ADD..."

Washington.

Chapter 2 (basics)

Weierstrass equation

In general, over field K, ADD...

For $\operatorname{char} K \neq 2, 3$, a cubic reduces to Weierstrass form $E : y^2 = x^3 + Ax + B$ with discriminant $D = -(4A^3 + 27B^2) \neq 0$.

Group law

Let ∞ be identity. If $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, then the sum $P_3 = (x_3, y_3) = P_1 + P_2$ has coordinates $x_3 = m^2 - x_1^2 - x_2^2$, $y_3 = \ldots$, where m is slope of P_1P_2. $(E(K), +)$ is an abelian group.

Group has different structure over different fields K. $K = \mathbb{F}_q$: finite abelian, $K = \mathbb{Q}$: finitely generated abelian, $K = \mathbb{C}$: a torus.

(Nowadays, no-one uses abelian groups for cryptography, due to quantum computing. Post-quantum cryptography will work with nonabelian groups.)

Endomorphisms

Definition. $\alpha : E(\overline{K}) \to E(\overline{K})$ is an endomorphism if it's a homomorphism whose coordinates are rational functions. (Thus, $\alpha = (R_1(x,y), R_2(x,y))$.)

You can show any endomorphism can be written as $\alpha(x,y) = (r_1(x), r_2(x)y)$.

Endomorphisms will be used to study subgroups of $E(K)$ (specifically, their kernels). Two important ones are the Frobenius map and the $\cdot n$ map.

Definition. Frobenius map $\phi_q : E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})$ is given by $\phi_q(x,y) = (x^q, y^q)$.

By finite field theory, ϕ_q only fixes $\mathbb{F}_q$. Hence $\ker(\phi_q - 1) = E(\mathbb{F}_q)$. To be generalized and used later, for Hasse.

Definition. $\cdot n$ map $\cdot n : E(\overline{K}) \to E(\overline{K})$ is given by $P \mapsto nP$.

Note $\ker(\cdot n) = E[n]$, points of order dividing n.

By studying when endomorphisms are separable, we get more information on the size of their kernel in relation to the degree... ADD (intuitive understanding? roots of denominator of $r_1(x)$?)

Singular ECs

ADD...

Chapter 3 (torsion points)

Structure of $E[n]$

Definition. $E[n]$ is the set of n torsion points, i.e. all P with $nP = 0$, i.e. all points of order dividing n.

Theorem (structure of $E[n]$). if $\operatorname{char} K \nmid n$, then $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$.

The proof is complicated. The key insights are: $E[n] = \ker(\cdot n)$, $\cdot n$ is a separable endomorphism of degree n^2, thus $\#E[n] = n^2$.

Homomorphism as matrix

Note α maps $E[n]$ into $E[n]$ (as $nP = 0 \implies n\alpha(P) = 0$). Further α is linear on $E[n]$. Thus, once we choose a basis (say, $(1,0),(0,1)$) for $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$, we can represent α as a matrix.

(In general, the Fundamental Theorem of Finitely Generated Abelian Groups says any group can be written as $G \simeq \mathbb{Z}^r \oplus G_{torsion}$, where $G_{torsion} \simeq$ ADD...)

Chapter 4 (ECs over finite fields)

Structure of $E(\mathbb{F}_q)$

What's the structure of the finite abelian group $E(\mathbb{F}_q)$?

Theorem. $E(\mathbb{F}_q) \simeq \mathbb{Z}_n$ or $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$.

Proof. ADD...

Size of $E(\mathbb{F}_q)$

Bounding group order

What is it's size? We can provide a bound.

Hasse bound. $|a| \leqslant 2\sqrt{q}$, where $a = q + 1 - \#E(\mathbb{F}_q)$.

Thus $\#E(\mathbb{F}_q)$ lies in the Hasse interval, $[(\sqrt{q}-1)^2, (\sqrt{q}+1)^2]$.

The proof is complicated, but similar to showing $\#E[n] = n^2$. The key insights are: $E(\mathbb{F}_q) = \ker(\phi_q - 1)$, $\phi_q - 1$ is a separable endomorphism of degree $q + 1 - a$, thus $\#E(\mathbb{F}_q) = q + 1 - a$.

As a side result, we get $\phi_q^2 - a\phi_q + q = 0$ as endomorphisms. $x^2 - ax + q$ is the characteristic polynomial of Frobenius.

Determining group order

There are many methods for finding the exact size $\#E(\mathbb{F}_q)$.

The method of subfield curves: find $\#E(\mathbb{F}_{q^n})$ from $\#E(\mathbb{F}_q)$ recursively.

Theorem. If $x^2 - ax + q = (x - \alpha)(x - \beta)$, then $\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$.

Proof. Characteristic polynomial of Frobenius... ADD

Lang Trotter method: a simple explicit count with Legendre symbols.

Theorem. $\#E(\mathbb{F}_q) = q + 1 + \sum \left(\frac{x^3+Ax^2+B}{q}\right)$.

Using points of large order: if there's a point P of large order, since Lagrange's Theorem implies $\operatorname{ord} P \mid \#E(\mathbb{F}_q)$, there are few possibilities for $\#E(\mathbb{F}_q)$ in the Hasse interval. Best case: only 1 multiple of $\operatorname{ord} P$!

For $q = p^1$, this best case happens on either E or its twist E' (ADD...):

Mestre's theorem. For $p > 229$, either $E/\mathbb{F}_p$ or $E'/\mathbb{F}_p$ has a point $\operatorname{ord} P$ with 1 multiple in the Hasse interval

Proof. Involves structure of $E(\mathbb{F}_p)$ and lots of bounding... ADD

Maybe we can't do that good for $\mathbb{F}_q$ in general. But we can still find points of large order.

Suppose $E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$. Then lcm of two random points is likely n_2, the maximum order. ADD...

Cremona–Harley theorem. n_2 determines n_1... ADD

(We've ignored the case when $E(\mathbb{F}_q) \simeq \mathbb{Z}_n$, as it's rare.)

Baby-step giant-step algorithm (BSGS). To find $\operatorname{ord} P$.

The steps of the algorithm are as follows:

Find M:

- Let $Q = (q + 1)P$.
- Choose $m > q^{1/4}$ and compute $\pm jP$ for $0 \leqslant j \leqslant m$.
- Compute $Q + k(2mP)$ for $-m \leqslant k \leqslant m$, until there is a match with the list $\{\pm jP\}$.
- Note that $MP = 0$, where $M = q + 1 + 2mk \mp j$.

Find $\operatorname{ord} P$:

- Let $M = p_1^{e_1} \cdots p_t^{e_t}$.
- Find $\frac{M}{p_i} P$ for all i; if $\frac{M}{p_i} P = 0$ for some i, repeat these steps with $M \to \frac{M}{p_i}$. Else, $M = \operatorname{ord} P$.

Supersingular curves (computational advantage). ADD...

Interlude, Chapter 3.3: Weil pairing

ADD...

Chapter 6 (ECC)

Cryptography

Setup. Use public key to setup symmetric key. Most protocols use the difficulty of the discrete log problem (DLP).

Diffie–Hellman encryption. A, B want to communicate. They have secret keys a, b, and a public key $P \in E/\mathbb{F}_q$. A sends aP to B, and B sends bP to A. Then both compute $Q = abP$ and extract a common key.

It's hard to find abP because that requires finding a or b, which is hard.

Massey–Omura encryption. Similar to the famous king communication puzzle (?). A wants to send B a message $P \in E(\mathbb{F}_q)$. A, B have secret keys $m_A, m_B \in \mathbb{Z}_N$, where $N = \#E(\mathbb{F}_q)$. He "locks" with m_A by sending $m_A P$ to B. Then B "locks" with m_B and sends $m_B m_A P$ back to A. Then A "unlocks" by sending $m_B P = m_A^{-1}(m_B m_A P)$. Finally, B retrieves the original message by "unlocking" $P = m_B^{-1}(m_B P)$.

Boneh–Franklin encryption (identity-based). ... ADD

Digital signatures

Setup. How to sign a document.

ElGamal digital signature. A wants to sign a document, and B wants to verify.

Initialize:

- Choose $E/\mathbb{F}_q$, $A \in E(\mathbb{F}_q)$ with $\operatorname{ord} A = N$, $B = aA$, $f : E(\mathbb{F}_q) \to \mathbb{Z}$ with few collisions
- Release all of these except the secret key a

A signs:

- Represents message as integer m with hash H
- Chooses a random k with $(k, N) = 1$ and computes $R = kA$
- Computes integer $s \equiv k^{-1}(m - af(R)) \pmod{N}$
- Releases signed message (m, R, s)

B verifies:

- Computes $V_1 = f(R)B + sR$
- Computes $V_2 = mA$
- Checks if $V_1 = V_2$

Important: different k's must be chosen each time (?)

Digital Signature Algorithm (ECDSA). Variant of ElGamal that is quicker to verify.

Initialize:

- Choose $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = fr$ for f small and r prime, $G \in E(\mathbb{F}_q)$ with $\operatorname{ord} G = r$, $Q = aG$
- Release all of these except the secret key a

A signs:

- Represents message as integer m with hash H
- Chooses a random $k \in [r]$ and computes $R = kG = (x, y)$
- Computes integer $s \equiv k^{-1}(m + ax) \pmod{r}$
- Releases signed message (m, R, s)

B verifies:

- Computes $u_1 \equiv s^{-1}m \pmod{r}$
- Computes $u_2 \equiv s^{-1}x \pmod{r}$
- Checks if $R = u_1G + u_2Q$

Exposition from Katz Lindell

Definition 0.1 (3-round identification scheme)**.**

- *The prover generates an initial message $I = P_1(sk)$ and sends it to the verifier.*
- *The verifier generates a challenge r based on pk and sends it to the prover.*
- *The prover generates a response $s = P_2(sk, r)$ and sends it to the verifier.*
- *The verifier checks that $V(pk, r, s) = I$; if this is true, the prover is authenticated.*

Definition 0.2 (Fiat–Shamir transform)**.**

- *Generate an initial message I.*
- *Generate a challenge $r = H(I, m)$, where H is a hash function.*
- *Generate a response s to the challenge.*
- *Sign your message with (r, s).*

To verify the signature, a person computes $I = V(pk, r, s)$ and verifies that $H(I, m) = r$.

Definition 0.3 (Schnorr identification scheme)**.**

- *The prover generates an initial message $I = g^k$ for a random $k \in \mathbb{Z}_p^\times$ and sends it to the verifier.*
- *The verifier generates a challenge $r \in \mathbb{Z}_p^\times$ at random and sends it to the prover.*
- *The prover generates a response $s \equiv rx + k \pmod{p}$ and sends it to the verifier.*
- *The verifier checks that $g^s \cdot y^{-r} = I$; if this is true, the prover is authenticated.*

Definition 0.4 (DSA/ECDSA identification scheme)**.**

- *The prover generates an initial message $I = g^k$ for a random $k \in \mathbb{Z}_p^\times$ and sends it to the verifier.*
- *The verifier generates a challenge $r, \alpha \in \mathbb{Z}_p$ at random and sends it to the prover.*
- *The prover generates a response $s \equiv k^{-1}(\alpha + rx) \pmod{p}$ and sends it to the verifier.*
- *The verifier checks that $s \neq 0$ and $g^{\alpha s^{-1}} \cdot y^{rs^{-1}} = I$; if this is true, the prover is authenticated.*

Fiat–Shamir variant.

- Generate an initial message I.
- Generate a challenge $r = F(I)$ and $\alpha = H(m)$, where $F : G \to \mathbb{Z}_p$ and H are hash functions.
- Generate a response s to the challenge.
- Sign your message with (r, s).

Chapter 5 (attacks on DLP)

General attacks

Index calculus. For $\mathbb{F}_p^\times$, given a generator g, how to compute $L(h) = \log_g h$?

Idea: factor $h = p_1^{e_1} \cdots p_k^{e_k}$ and find $L(p_i)$ instead!

- Choose factor base $B = \{\text{small primes } p_i\}$
- Compute $g^0, g^1, \ldots$ to find a system of equations in $L(p_i)$
- Solve for $L(p_i)$ with linear algebra
- Compute $hg^0, hg^1, \ldots$ until it factors into primes in B and solve for $L(h)$

This can be extended to $\mathbb{F}_q^\times$ with algebraic NT.

For the next few sections, we consider the general DLP: given group G with $\#G = N$, P, and Q, find k.

BSGS. Last time, used BSGS to find $\operatorname{ord} P$, i.e. M such that $MP = \infty$. Now, we modify it to find k such that $kP = Q$.

- Fix $m \geqslant \sqrt{N}$, find mP
- Store iP for $0 \leqslant i < m$ (baby step)
- Compute $Q - jmP$ for $0 \leqslant j < m$ until it matches something in $\{iP\}$ (giant step)
- Return $k \equiv i + jm \pmod N$

This works because $k = m(\text{quotient}) + \text{remainder}$, where $\text{quotient}, \text{remainder} < m$.

$O(\sqrt{N})$ time/space.

Pollard ρ. This offers a space improvement over BSGS.

Take a random walk around G. Choose random function $f : G \to G$. Starting from P_0, generate sequence $P_{i+1} = f(P_i)$. The sequence is periodic, hence $P_i = P_j$ for some i, j. (That's why it's the ρ method.)

How do we choose f to solve DLP?

- Partition $G = S_1 \sqcup S_2 \cdots \sqcup S_s$
- Choose $2s$ random $a_i, b_i \pmod N$
- Let $M_i = a_i P + b_i Q$ (possible steps)
- Define f piecewise by $f(g) = g + M_i$ if $g \in S_i$

When we find $P_i = P_j$, we know $c_i P + d_i Q = c_j P + d_j Q \implies mQ = nP$ for some m, n. Only finitely many possible k.

Pollard ρ can be optimized by storing fewer points.

Pohlig–Hellman. A base q approach (?).

Idea: suppose $\operatorname{ord} P = N = q_1^{e_1} \cdots q_k^{e_k}$. Let's find $k \pmod{q_i^{e_i}}$ for all i, then use CRT to determine $k \pmod N$, i.e. k.

For a given $q^e = q_i^{e_i}$, imagine $k = k_0 + k_1 q + k_2 q^2 + \ldots$ is its base-q representation:

- Compute $T = \{k(\frac{N}{q}P) | 0 \leqslant k < q\}$.

Let $Q_0 = Q$; for $1 \leqslant r < e$:

- Compute $Q_r = Q_{r-1} - k_{r-1} q^{r-1} P$.
- Find $k_r(\frac{N}{q}P) \in T$ such that $\frac{N}{q^{r+1}} Q_r = k_r(\frac{N}{q}P)$.

Once done, return $k_0 + k_1 q + \ldots \pmod{q^e}$.

Fix order of iteration... ADD

EC specific attacks

Decision Diffie–Hellman attack. Although DH is hard, a modified version of DH can be solved: decision DH.

Decision DH: given P, Q, decide if $Q = abP$.

This can be solved by defining the modified Weil pairing $\tilde{e}_n$... ADD

MOV attack. Reduces DLP in $E(\mathbb{F}_q)$ to DLP in $\mathbb{F}_{q^m}^\times$.

Setup: given $P, Q \in E(\mathbb{F}_q)$, $\operatorname{ord} P = N$, $(q, N) = 1$, find k such that $Q = kP$.

Know that e_n tells us when k exists.

- Choose m such that $E[N] \subset E(\mathbb{F}_{q^m})$. Then $\mu_N \subset E(\mathbb{F}_{q^m})$

  We first find a random point $T_1 \in E[N]$.
- Choose random $T \in E(\mathbb{F}_{q^m})$
- Find $M = \operatorname{ord} T$
- Let $d = (M, N)$ and compute $T_1 = \frac{M}{d}T$. Then $\operatorname{ord} T_1 = d \mid N \implies T_1 \in E[N]$

  Now we find $k \pmod d$.
- Find $\zeta_1 = e_N(P, T_1)$ and $\zeta_2 = e_N(Q, T_1)$; these are both in $\mu_d \subset E(\mathbb{F}_{q^m})$
- Solve the DLP $\zeta_2 = \zeta_1^k$ in $\mathbb{F}_{q^m}^\times$ to find $k \pmod d$
- Combine $k \pmod d$ for many d to get $k \pmod N$, i.e. k

To avoid having to work in $\mathbb{F}_{q^m}$ with m large, use supersingular curves, which guarantee $m = 2$.

Supersingular curves are good for encryption, but also good for attacks... ADD

Anomalous-curve attack. ADD...

Chapter 7 (other applications)

Interlude, Chapter 2.11: ECs mod n

ADD... (overlap with Silverman?)

Factoring

$p - 1$ method, Lenstra's algorithm... ADD

Primality testing

Pohlig Lehrman test, EC version?... ADD

Chapter 11 (divisors)

Goal of chapter: how to construct/compute the Weil pairing.

Divisors

First, we introduce divisors.

Definition. A divisor D is a formal linear combination $a_1[P_1] + \ldots + a_m[P_m]$ for $P_i \in E(\overline{K})$.

Definition. The degree of a divisor is $\deg D = \sum a_j$.

Definition. The sum of a divisor is $\mathrm{sum}(D) = \sum a_j P_j$.

Definition. The group $\mathrm{Div}^0 E$ is the set of degree 0 divisors.

Functions

A seemingly unrelated concept is that of a function on an EC.

Definition. A function $f : E(\overline{K}) \to \overline{K}$ is a rational function $f(x, y) = \frac{a(x,y)}{b(x,y)}$.

We often homogenize f.

Definition. $P = (x : y : z)$ is a zero of f if $a(x : y : z) = 0$.

Definition. $P = (x : y : z)$ is a pole of f if $b(x : y : z) = 0$.

Definition. The order $\mathrm{ord}_P(f)$ of f at P is the multiplicity of P in the numerator/denominator, or 0 otherwise.

Principal divisors

Now comes the connection between divisors and rational functions.

Definition. The divisor of f is $\operatorname{div}(f) = \sum_{P \in E(\overline{K})} \operatorname{ord}_P(f) \cdot [P]$. Such a divisor is called a principal divisor.

Properties of principal divisors:

- $\operatorname{div}(f)g = \operatorname{div}(f) + \operatorname{div}(g)$
- $\operatorname{div}(f) = 0 \iff f \equiv c$ (complex analysis, but intuitive)
- $\operatorname{div}(f) = \operatorname{div}(g) \iff f = cg$
- $\operatorname{div}(f) \in \operatorname{Div}^0 E$ for all f (complex analysis, but kinda intuitive)

It turns out that there is an easy classification for principal divisors.

Principal Divisor Theorem. suppose $D \in \operatorname{Div}^0 E$. Then D principal iff $\operatorname{sum}(D) = \infty$.

Proof. Key idea: express $[P_1] + [P_2]$ in terms of $[P_1 + P_2]$ ("addition formula"). There are two functions (both lines) involved.

Consider line containing $P_1, P_2, P_3 = -(P_1 + P_2)$ with equation $ax + by + c = 0$. Then

$$\operatorname{div}(ax + by + c) = [P_1] + [P_2] + [P_3] - 3[\infty].$$

Also, using the vertical through $P_3 = (x_3, y_3)$,

$$\operatorname{div}(x - x_3) = [P_3] + [-P_3] - 2[\infty].$$

Subtracting, we get

$$[P_1] + [P_2] = [P_1 + P_2] + [\infty] + \operatorname{div}\left(\frac{ax + by + c}{x - x_3}\right).$$

(A trick we used: figure out order of ∞ by requiring sum $= 0$.)

From here, the proof follows from repeatedly applying the addition formula, bunching up the $a_j[P_j]$'s in D with $a_j > 0$ and similarly for $a_j < 0$.

Note that the proof provides a way to find f such that $D = \operatorname{div}(f)$. Unfortunately, it's slow. (But it generalizes to curves besides ECs.)

Weil pairing

Back to the main point – defining the Weil pairing.

Suppose $T \in E[n]$. By the Principal Divisor Theorem, there exists f such that $\operatorname{div}(f) = n[T] - n[\infty]$.

Let $T' \in E[n^2]$ such that $T = nT'$. Then by the Principal Divisor Theorem, there exists g such that

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

This is independent of T' (?).

Define the composition $f \circ n$, where n is $\cdot n$. Then $\operatorname{div}(f \circ n) = \operatorname{div}(g^n) \implies f \circ n = g^n$, up to scaling.

Finally, note that if $P \in E(\overline{K})$, $S \in E[n]$, we may define $\frac{g(P+S)}{g(P)} \in \mu_n$. This is independent of P by analysis (?).

Definition. The Weil pairing is $e_n(S,T) = \frac{g(P+S)}{g(P)}$.

Properties: ADD...

Note that computing the Weil pairing requires us to find g such that $\operatorname{div}(g) =$ sum of n^2 things. Our approach from the proof of the Principal Divisor Theorem is $O(N^2)$, too slow!

There's a slightly more efficient definition of the Weil pairing.

Definition. Let $S, T \in E[n]$. Let $D_S, D_T \in \operatorname{Div}^0 E$. Suppose f_S, f_T are such that $\operatorname{div}(f)_S = nD_S$ and $\operatorname{div}(f)_T = nD_T$. Then $e_n(S,T) = \frac{f_T(D_S)}{f_S(D_T)}$. (?)

A natural choice of D_S, D_T is $D_S = [S] - [\infty]$ and $D_T = [T + R] - [R]$.

Miller's algorithm

Now we only need an algorithm that can solve $\operatorname{div}(f) = n[P + R] - n[R]$ fast, and evaluate $f(Q_1)/f(Q_2)$ as well.

Miller's algorithm. Initial idea: compute f_j such that $\operatorname{div}(f)_j = j[P + R] - j[R]$, and use successive doubling to get to $f_n = f$. (In fact, don't even compute f_j explicitly; just the fraction needed!)

But sum $j[P + R] - j[R] \neq 0$! Add terms: $\operatorname{div}(f)_j = j[P + R] - j[R] - [jP] - [\infty] = D_j$.

Key formula: given $f_j(Q_1)/f_j(Q_2)$ and $f_k(Q_1)/f_k(Q_2)$, can quickly find $f_{j+k}(Q_1)/f_{j+k}(Q_2)$.

Why? From the addition formula,

$$D_{j+k} = D_j + D_k + \operatorname{div}(h) \implies \operatorname{div}(f)_{j+k} = \operatorname{div}(f)_j f_k h \implies f_{j+k} = f_j f_k h \gamma$$

$$\implies \frac{f_{j+k}(Q_1)}{f_{j+k}(Q_2)} = \frac{f_j(Q_1)}{f_j(Q_2)} \frac{f_k(Q_1)}{f_k(Q_2)} \frac{\text{stuff}}{\text{stuff}}.$$

Chapters 9 & 10 (CM: complex multiplication)

ECs over $\mathbb{C}$

Goal. Show that an elliptic curve is the same as a complex torus.

First, we show any torus yields an elliptic curve.

It turns out we can parametrize complex points on an EC with the ρ function.

Definition. Given a lattice $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, the Weierstrass ρ function is

$$\rho(z) = \frac{1}{z^2} + \sum_{\omega \in L, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

ρ is doubly periodic with periods ω_1, ω_2; hence it induces a map from $\mathbb{C}/L \to \mathbb{C}$.

We can expand the reciprocals in ρ to get a Laurent series. The coefficients are in terms of the Eisenstein series $G_k = \sum_{\omega \in L, \omega \neq 0} \frac{1}{\omega^k}$.

Lemma. $\rho(z) = \frac{1}{z^2} + \sum (2j+1) G_{2j+2} z^{2j}$.

With the above lemma, the following differential equation follows.

Lemma. $\rho'^2 = 4\rho^3 - g_2\rho - g_3$, where $g_2 = 60G_4$ and $g_3 = 140G_6$.

It can be shown that $\Delta \neq 0$ for the cubic. But this is the equation of an EC!

Theorem. The map $\Phi : \mathbb{C}/L \to E(\mathbb{C})$ given by $\Phi : z \mapsto (\rho(z), \rho'(z))$ is an isomorphism.

Proof. Mainly need to check Φ is a homomorphism... ADD

Next, we show that any elliptic curve comes from a torus.

Theorem. Given the EC $y^2 = 4x^3 - Ax - B$, there exists a lattice L such that $g_2(L) = A$ and $g_3(L) = B$. Further, there is an isomorphism $\mathbb{C}/L \simeq E(\mathbb{C})$.

Idea: given an EC $y^2 = 4x^3 - Ax - B$, find L such that $g_2(L) = A$ and $g_3(L) = B$.

It turns out we can do this if we just match the j invariant of E with the j invariant of (a scaled version of) L.

But what is $j(L)$? It's what you'd expect. Definition: $j(L) = 1728\frac{g_2^3}{\Delta}$.

To find an expression for $j(L)$, we can find expansions for $g_2(L)$ and $g_3(L)$. To do this, it's convenient to rewrite as follows. Let $L_\tau = \mathbb{Z}\tau + \mathbb{Z}$, where WLOG $\tau = \omega_1/\omega_2 \in \mathcal{H}$. Then $g_i(\tau) = g_i(L_\tau)$.

Lemma. $g_2(\tau) = \frac{4\pi^4}{3}(1 + 240q + \ldots)$ and $g_3(\tau) = \frac{8\pi^6}{27}(1 + 504q + \ldots)$, where $q = e^{2\pi i\tau}$.

Proof. Differentiate the Euler product formula for sin to find an expression for G_{2k}.

Lemma. $j(\tau) = j(L) = \frac{1}{q} + 744 + 196884q + \ldots$.

Proof. Divide the two expansions. To see why j is unchanged under homothety, note that g_2 and g_3's scalings cancel out in its expression.

j satisfies some other properties related to the modular group $\mathrm{SL}_2(\mathbb{Z})$. [Other interesting properties?... ADD]

Lemma. $j(M\tau) = j(\tau)$ for all $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, where $M\tau = \frac{a\tau+b}{c\tau+d}$ is a Mobius transformation.

Proof. See how G_{2k} changes.

It turns out j is meromorphic with fundamental domain $\mathcal{F}$... ADD? By restricting to $\mathcal{F}$, we also get the following.

Theorem. $\operatorname{ord}_{i\infty} f + \frac{1}{3}\operatorname{ord}_\rho f + \frac{1}{2}\operatorname{ord}_i f + \sum \operatorname{ord}_z f = 0$, where $\rho = e^{2\pi i/3}$.

Proof. Follows more generally from functions defined on Riemann surfaces? Directly, use complex integration... ADD?

As a result, we get find that $j : \mathcal{F} \to \mathbb{C}$ is bijective.

Theorem. For all $z \in \mathcal{H}$, there exists a unique $\tau \in \mathcal{F}$ such that $j(\tau) = z$.

Theorem. Let $\tau_1, \tau_2 \in \mathcal{H}$. Then $j(\tau_1) = j(\tau_2)$ iff there exists $M \in \mathrm{SL}_2(\mathbb{Z})$ such that $M\tau_1 = \tau_2$.

We can even translate this back in terms of lattices.

Theorem. Let L_1, L_2 be lattices. Then $j(L_1) = j(L_2)$ iff L_1 is homothetic to L_2.

Finally, we're ready to prove that every EC comes from a lattice!

Proof. Let $j = 1728\frac{A^3}{D}$ be the j invariant of E. By our result, we may choose τ such that $j(\tau) = j(L_\tau) = j$. Next, if $g_2(L) \neq 0$, choose λ such that $g_2(\lambda L) = A$. Then, either λL works or $i\lambda L$ works. The case $g_2(L) = 0$ is similar.

We can now think geometrically about n torsion points of E. These are $\{\frac{j}{n}\omega_1 + \frac{k}{n}\omega_2\}$.

CM for ECs over $\mathbb{C}$

CM occurs when the endomorphism ring $\mathrm{End}(E)$ is larger than $\mathbb{Z}$. We know that $\cdot n \in \mathrm{End}(E)$ for all n, hence $\mathbb{Z} \subset \mathrm{End}(E)$. But how much bigger is it?

For E over $\mathbb{C}$, if $\alpha \in \mathrm{End}(E)$, we get a corresponding homomorphism $\tilde{\alpha} : \mathbb{C}/L \to \mathbb{C}/L$. This is analytic on $U \ni 0$ (?) and satisfies Cauchy's functional equation, hence $\tilde{\alpha}(z) = \beta z$ for some $\beta \in \mathbb{C}$. The following tells us that these are all the endomorphisms.

Theorem. If E is an EC over $\mathbb{C}$ with lattice L, then $\mathrm{End}(E) \simeq \{\beta \in \mathbb{C} \mid \beta L \subset L\}$.

We can even say more about $\mathrm{End}(E)$. It turns out $\mathrm{End}(E)$ is either $\mathbb{Z}$ or an order in an imaginary quadratic field. What's the latter? An imaginary quadratic field is simply $K = \mathbb{Q}(\sqrt{-D})$. The ring of integers O_K is $\mathbb{Z}[\delta]$ for $\delta = \ldots$ ADD. It's all the algebraic integers in K. Finally, an order is simply a subring $\mathbb{Z} \subset R \subset O_K$.

Theorem. $\mathrm{End}(E)$ is either $\mathbb{Z}$ or an order in an imaginary quadratic field.

Proof. ADD...

CM for ECs over finite fields

ADD...

$j(L)$ is an algebraic integer

ADD...

Silverman:

ECs over $\mathbb{Q}$

Nagell Lutz, Mordell Weil, Mazur... ADD

Mordell Weil Theorem

Mordell–Weil Theorem. $E(\mathbb{Q})$ is finitely generated.

Key idea: given $P \in C(\mathbb{Q})$, use descent to write as sum of elements of a generating set.

Need measure of points. Use the height:

- Height of rational: $H(m/n) = \max(|m|, |n|)$
- Height of point: $H(x, y) = H(x)$
- "Small H" height: $h = \log H$

Need 4 lemmas.

Lemma 0.5 (Lemma 1, finiteness property)**.** $\forall M$, $\{x \in C(\mathbb{Q}) \mid h(x) \leqslant M\}$ *finite*

Proof. Clear, from finiteness property of $h(m/n)$. □

Lemma 0.6 (Lemma 2)**.** $\forall P_0, \exists k_0$ *depending on* P_0 *s.t.* $\forall P$, $h(P + P_0) \leqslant 2h(P) + k_0$

Lemma 0.7 (Lemma 3)**.** $\exists k$ *s.t.* $\forall P$, $h(2P) \geqslant 4h(P) - k$

Lemma 0.8 (Lemma 4)**.** $[C(\mathbb{Q}) : 2C(\mathbb{Q})]$ *finite.*

We may rephrase Mordell Weil more generally.

Theorem 0.9. Γ *abelian group.* $h : \Gamma \to [0, \infty)$ *function. Suppose Lemmas 1-4 hold. Then* Γ *is finitely generated.*

Proof. Suppose $P \in \Gamma$. We apply descent to reduce P to sum of elements of generating set.

Choose representatives $Q_1, \ldots, Q_n$ of cosets of 2Γ. Suppose $P \in Q_{i_1} + 2\Gamma$, i.e. $P = Q_{i_1} + 2P_1$ for some i_1, P_1. Repeat on P_1, then on P_2, etc. to find:

$$P_1 = Q_{i_2} + 2P_2$$

$$P_2 = Q_{i_3} + 2P_3$$

$$\ldots$$

$$P_{m-1} = Q_{i_m} + 2P_m$$

Substituting, find $P = \sum 2^{j-1} Q_{i_j} + 2^m P_m$.

Claim: $\forall P$, there exists m s.t. $h(P_m) < \epsilon$ for a fixed ϵ. (Hence, we can reduce to P_m in finite set.)

To see this, use Lemmas 1-3:

Know $\exists k'$ s.t. $h(P - Q_i) \leqslant 2h(P) + k' \ \forall P, i$

Hence know $4h(P_j) \leqslant h(2P_j) + k = h(P_{j-1} - Q_{i_j}) + k \leqslant 2h(P_{j-1}) + k' + k$ (i.e. $h(P_j) \approx \frac{1}{2} h(P_{j-1})$)

There exists m s.t. $h(P_m) \leqslant k + k'$, as desired.

Follows that can reduce P to an element of finite gen set $\{Q_i\} \cup \{P_m\}$, as desired. □

Height of $P + P_0$

ADD...

Background

Group theory

Definition of a group

Abelian and non abelian groups

Cyclic groups

Subgroups

Homomorphisms and isomorphisms

Left and right cosets (affine subgroups):

Given $H \leqslant G$, the left cosets of H partition G.

Motivation: want to form group out of cosets. Ex: $H = 3\mathbb{Z}_{12} \leqslant G = \mathbb{Z}_{12}$.

Normal subgroup: $aH = Ha$ for all $a \in G$. (a's left and right cosets are the same.)

- All subgroups of an abelian group are normal.

Quotient group: G/H, consisting of cosets aH with operation $(aH)(bH) = abH$.

Define $\pmod H$ equivalence relation. (Equal if differ by $h \in H$.) Equivalence classes are left cosets.

- Well defined? Yes...
- Work with representatives.
- Note: $\mathbb{Z}_{mn}/\mathbb{Z}_m \simeq \mathbb{Z}_n$.

Simple group: no normal subgroups other than $\{e\}$ and G. "Indivisible."

Quotient mapping theorem: Let $H \leqslant G$. Then H is normal **iff** there exists a homomorphism $\phi : G \to G/H$ with $\ker \phi = H$.

- $\{\text{normal subgroups}\} \iff \{\text{homomorphisms out of } G\}$
- $(\to)$ Naturally, $\phi(g) = gH$. $(\leftarrow)$ ...

First isomorphism theorem: Let $\phi : G \to H$ be a homomorphism. Then:

- $K = \ker \phi$ is a normal subgroup of G (see above).
- $I = \operatorname{im} \phi$ is a subgroup of H (check).
- $I \simeq G/K$.

- Third point: quick way to characterize quotient groups. Ex...

Direct product/sum group: $G \otimes H = \{(g, h) \mid g \in G, h \in H\}$. Use $\oplus$ if abelian.

Finite groups: Lagrange's theorem

Sylow's theorem (partial converse) (?)

Structure theorem for finite abelian groups (see below)

Structure theorem for finitely generated abelian groups:

$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \cdots \oplus \mathbb{Z}_{p_k^{e_k}} \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \cdots \oplus \mathbb{Z}_{n_k}$$

with $n_i \mid n_{i+1}$ for all i.

Examples of groups...

PROOFS?

Ring theory

Definition of a ring (commutative with 1)

Subring

Units: $U(R)$ is the multiplicative subgroup of elements with a multiplicative inverse.

Zero divisors: x is zero divisor if there exists $y \neq 0$ with $xy = 0$.

Group ring: given ring R and finite group G, define $RG\ldots$

Integral domain (ID): a ring with no zero divisors. ("Field without inverses.")

- Can do cancellation.
- Finite ID = field.

Ideals:

Motivation: corresponding concept to normal subgroups. Invariant under conjugation $\implies$ invariant under multiplication.

Definition. Subring I is ideal if $rI \subset I$ for all $r \in R$.

- Ex: $n\mathbb{Z}$ in $\mathbb{Z}$.
- Note: if I contains a unit, $I = R$.

Quotient ring: can quotient by any subring R' to get additive quotient group R/R'. But when quotienting by ideal, get a quotient *ring* R/I.

Define $\pmod I$ equivalence relation. (Equal if differ by $x \in I$.) Equivalence classes are translates rI.

Exs:

- $\mathbb{Z}/n\mathbb{Z}$, the ring $\mathbb{Z}_n$.
- $\mathbb{Z}_2[x]/(x^2 + x + 1) \simeq \{0 + I, 1 + I, x + I, (x + 1) + I\} = \{0, 1, x, x + 1\}$, a finite field with 4 elements.

Ring homomorphisms and isomorphisms: much carries over from groups.

Homomorphism: preserves $+$ and $\cdot$.

Exs:

- Reduction $\pmod n$ map.
- Evaluation map by a polynomial $p(x) \in \mathbb{R}[x]$.

First isomorphism theorem: Let $\phi : R \to S$ be a homomorphism. Then:

- $K = \ker \phi$ is an ideal of R.
- $I = \operatorname{im} \phi$ is a subring of S.
- $I \simeq R/K$.

Maximal ideal: I is maximal if the only bigger ideal containing it is R.

I is maximal iff R/I is a field.

Ex: $R = \mathbb{Z}_2[x], I = (x^2 + x + 1)$; any irreducible?

[Prime ideal: P is prime if $ab \in P \iff a \in P$ or $b \in P$.

P is prime iff R/P is an ID. (Hence, maximal $\implies$ prime.) (?)]

Focusing on IDs:

We are used to $\mathbb{Z}, \mathbb{R}, \mathbb{C}$, so to study extensions, we focus on IDs. Many familiar properties fail in general, like unique factorization, Euclidean algorithm, etc.

Divisibility

a is an associate of b if $a \mid b$ and $b \mid a$.

Irreducible: only divisors are units and associates.

Primes: $p \mid ab \implies p \mid a$ or $p \mid b$.

In general, prime $\implies$ irreducible, but irreducible $\not\implies$ prime. (Ex: $\mathbb{Z}[\sqrt{-5}]$.)

For "nice" rings, principal ideal domains (PID), it does hold.

Definition. A principal ideal is of the form (a).

Definition. A PID is an ID R whose ideals are all principal.

PIDs have gcds, lcms, and irreducible $\implies$ prime.

Exs: $\mathbb{Z}, F, F[x]$ (?). Not $\mathbb{Z}[x]$, since $(2, x)$ is not principal.

Lemma. If $a, b \in R^*$, then $\gcd(a, b)$ exists. Further, there exist x, y such that $ax+by = \gcd(a, b)$.

Corollary. Irreducible $\implies$ prime.

Another notion:

Definition. A UFD is an ID with unique factorization into irreducibles, i.e.:

(1) any element can be factored into a product of irreducibles.

(2) irreducible $\implies$ prime.

Exs: $\mathbb{Z}$ (FTA), $F[x, y], \mathbb{Z}[x]$.

Theorem. PID $\implies$ UFD. (?)

Another notion:

Definition. A Euclidean domain is an ID where there is an analogue of the Euclidean algorithm. (Need a Euclidean function to measure size in the division algorithm.) (purpose?)

Exs: $\mathbb{Z}, F[x], \mathbb{Z}[i]$.

Theorem. Euclidean $\implies$ PID.

Algebraic integers:

Definition. An algebraic integer is a root of a monic polynomial in $\mathbb{Z}[x]$.

Definition. The ring of integers O_K in the field $K = \mathbb{Q}(\sqrt{d})$ is the set of algebraic integers in K.

Properties of O_K...

Norm in $\mathbb{Q}(\sqrt{d})$... when is O_K norm Euclidean?... when is O_K Euclidean?...

PROOFS?

Examples of rings...

Polynomial rings (see Gunning / Conrad)...

ADD Katy's notes from meetings...

Field theory

. . .

Examples of fields. . .

https://www.math.utah.edu/ schwede/math435/index.html