Math 571

Taught by Tom Weston
Scribed by Ben Burns

UMass Amherst

Spring 2022

Contents

1 Elliptic Curves

In the 1980s, Lenstra found a way to apply the very developed theory of elliptic curves to cryptography and factorization.

Definition 1. An elliptic curve is a plane cubic curves given by an equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Q}$ s.t $\Delta = 4a^3 + 27b^2 \neq 0$

Remark 2. Most general equation, the Weierstrass equation: $y^2 = a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$

1.1 Point addition Define $E := y^2 = x^3 + ax + b$. The key thing is the addition law. Given P, Q points on E, construct a third point $P \oplus Q$

Theorem 3 (Bezout's Theorem)**.** *A curve of degree* d *and a curve of degree* d' *have* dd' *points of intersection*

Two cocentric circles won't have any intersections → requires complex numbers.

Take elliptic curve of degree 3, and a line of degree one. By Bezout's Theorem, there will be two points of intersection. Two of which are P and Q, and call the third R. Set $P \oplus Q$ to be the reflection of R across the x-axis. With a few other conditions, we get a group law.

Example. $y^2 = x^3 - 15x + 18$. P = (7, 16) Q = (1, 2)

$y - 2 = \frac{7}{3}(x-1) \implies y = \frac{7}{3}x - \frac{1}{3}$. Insert into elliptic curve $(\frac{7}{3}x - \frac{1}{3}) = x^3 - 15x + 18 \implies \frac{49}{9}x^2 - \frac{14}{9}x + \frac{1}{9} = x^3 - 15x + 18 \implies x^3 - \frac{49}{9}x^2 + \ldots = 0$. Move all terms to one side, and solve the cubic.

Don't need the cubic equation, because we know that P and Q are on the intersection, or $x = 7$ and $x = 1$ are two zeros. $(x-1)(x-7)(x-x_0) \implies x^3 - (8 + x_0)x^2 + \ldots$, equate the quadratic coefficients $\frac{-49}{9} = -(8 + x_0) \implies x_0 = \frac{-23}{9}$. Therefore R has an x value of $\frac{-23}{9}$.

Caveats: if we take the same point twice, take the tangent line rather than a secant line. If you take two points on a vertical line, your third is the projective point at infinity.

$E(\mathbb{R}) = \{(x, y) \in \mathbb{R}^2 | y^2 = x^3 + ax + b\} \cup \{\mathbb{O}\}$, where $\mathbb{O}$ is the point at infinity.

Assuming we have the two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, where $x_1 \neq x_2$.

1) (Secant) Line PQ
$Y = y_1 + \lambda(X - x_1), \lambda = \frac{y_2 - y}{x_2 - x}$

2) Insert into cubic
$(y_1 + \lambda(X - x_1))^2 = X^3 + aX + b$
$0 = X^3 + (-\lambda)X^2 + \dots$

We know this must factor into $(X - x_1)(X - x_2)(X - x_3)$ since P and Q are on the line and on E.

3) Equate coefficient of X^2
$-\lambda^2 = -(x_1 + x_2 + x_3)$
$x^3 = \lambda^2 - x_1 - x_2$

4) Plug $X = x_3$ into line
$y_3 = t_1 + \lambda(x_3 - x_1)$

5) $P \oplus Q = (x_3, -y_3)$

Remark 4. This exercise is not to suggest memorizing this algorithm, just to demonstrate that there is a general solution method for two points with distinct x values on E.

1.2 Special Cases

Now we address more special cases of point addition

1) $\mathbb{O} \oplus Q = Q$, $P \oplus \mathbb{O} = P$.

2) $P = (x, y)$
$-P = (x, -y)$ (reflection across x-axis)
$P \oplus -P = \mathbb{O}$

3) $P \oplus P$: The only difference from the general case is that, here, λ is the slope of the tangent line of E at P, which can be determined by implicit differentiation $\implies 2YY' = 3X^2 + a \implies Y' = \dfrac{3X + a}{2Y} \implies \lambda = \dfrac{3x_1^2 + a}{2y_1}$.

Remark 5. In this 3rd case, if y_1 is zero, this obviously doesn't work. However, that is just where P is on the x-axis, and is therefore its own reflection, so $P \oplus P = P \oplus -P = \mathbb{O}$

Proposition 6. $E(\mathbb{R}) = \{(x, y) \in \mathbb{R}^2 | y^2 = x^3 + ax + b\} \cup \{\mathbb{O}\}$, *where* $\mathbb{O}$ *is the point at infinity, is an abelian group under the operation* $\oplus$ *with identity* $\mathbb{O}$.

Proof
Binary operation $\oplus$ which preserves $E(\mathbb{R})$. Check axioms.

1) Identity: $P \oplus \mathbb{O} = \mathbb{O} \oplus P = P$ for all P.

2) Inverses: $P \oplus -P = \mathbb{O}$

3) Abelian: Computing secant lines with different order of endpoints gives the same line, so $\oplus$ commutes

4) Associativity: In principle, this can be done by algebra with exhaustive case study. Alternatively,
$\rightarrow$ 4.1) do this in projective geometry, use Pascal's theorem
$\rightarrow$ 4.2) Develop theory of algebraic curves enough, it becomes obvious (tensor product with Picard group, that is a group and is associative, so this is associative)

1.3 Introducing other fields

Remark 7. We don't actually care about $E(\mathbb{R})$, but variations are useful in cryptography

Definition 8. $E(\mathbb{Q}) = \{(x, y) \in \mathbb{R}^2 | y^2 = x^3 + ax + b\} \cup \{\mathbb{O}\} \subset E(\mathbb{R})$

Remark 9. It is possible for there to be no rational points and $E(\mathbb{Q})$ is just $\mathbb{O}$

Claim: $E(\mathbb{Q})$ is a subgroup of $E(\mathbb{R})$ under $\oplus$

1) $\mathbb{O} \in E(\mathbb{Q})$ (either by definition of $E(\mathbb{Q})$ or since $\mathbb{O}$ is (0, 0, 1) in projective geometry

2) $P \in E(\mathbb{Q}) \implies -P \in E(\mathbb{Q})$, obvious since $-P = (x_1, -y_1)$

3) $P, Q \in E(\mathbb{Q}) \implies P \oplus Q \in E(\mathbb{Q})$. All special cases are obvious. For the general case, all of the suboperations are closed under rational numbers, so the entire operation is a rational operation.

Remark 10. A field is a set K with operations $+, \cdot$ satisfying a collection of axioms that satisfy all the expected axioms as under real numbers $(+, -, \cdot, /)$

Example. $R, \mathbb{Q}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p$ where p prime.

Remark 11. Modulus has to be prime since $\mathbb{Z}/n$ can have elements without an inverse (not even integral domain)

Definition 12. For field K, an elliptic curve over K is $Y^2 = X^3 + aX + b$ where $a, b \in K$ s.t $\Delta_E = 4a^3 + 27b^2 \neq 0$.

$E(K) = \{(x, y) \in K \times K | Y^2 = X^3 + aX^2 + b \in K\} \cup \{\mathcal{O}\}$ is an abelian group under $\oplus$.

Example. $E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 | Y^2 = X^3 + aX^2 + b \pmod p\} \cup \{\mathcal{O}\}$
$E = y^2 = x^3 + x + 1, K = \mathbb{F}_p$

x	$x^3 + x + 1$	y s.t $y^2 = x^3 + x + 1$
0	1	± 1
1	3	X
2	4	± 2
3	3	X
4	6	X
5	5	X
6	6	X

$E(\mathbb{F}_7) = \{\mathcal{O}, (0, 1), (0, -1), (2, 2), (2, -2)\}$

$(0, 1) \oplus (2, 2)$

$$\lambda = \frac{2-1}{2-0} = \frac{1}{2} = 4$$
$$\implies x_3 = \lambda^2 - x_1 - x_2 = 16 - 0 - 2 = 14 = 0$$
$$\implies y_3 = 1 + 4(0 - 0) = 1$$
$$\implies (0, 1) \oplus (2, 2) = -(0, 1) = (0, -1)$$

1.4 Classifying E

What kind of groups are we getting?

Example. $E(\mathbb{F}_p)$ is a finite abelian group. $|E(F_p)| \leqslant p^2 + 1$, but we can do far better, since for each x coordinate can give us at most 2 y coordinates, so $|E(F_p)| \leqslant 2p + 1$.

This bound still isn't best, but it's better

Example. $E(\mathbb{R})$ is either S^1 or $S^1 \times \mathbb{Z}/2$, where S^1 is the circle group under addition of angles.

Which one it is is detectable based on how many roots E has. Only 1 compact lie group of dimension 1, which is S^1.

Example. $E(\mathbb{C})$ is the torus, $S^1 \times S^1$

Theorem 13 (Mordell-Weil Theorem). *$E(\mathbb{Q})$ is a finitely generated abelian group $\implies E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$, where $r \geqslant 0$, and T is the torsion group. (which is finite)*

Example. $E(\mathbb{Q}) \cong \mathbb{Z}$, there is a point $P_0 \in E(\mathbb{Q})$ s.t every point in $E(\mathbb{Q})$ is nP_o for some $n \in \mathbb{Z}$

$nP_o := P_o \oplus P_o \oplus \cdots \oplus P_o$ for $n > 0$, or $-P_o \oplus -P_o \oplus \ldots \oplus -P_o$ for $n < 0$.

Theorem 14 (Mazar, 1977). *$T \cong \mathbb{Z}/n$ for $n = 1, 2, \ldots, 10, 12$ or $\mathbb{Z}/2 \times \mathbb{Z}/n$ for $n = 2, 4, 6, 8$*

"Mazar is the best number theorist of the 20th century, but I'm a bit biased" - man advised by Mazar.

What about r? Called the rank. r is 0, 50% of the time, and $r = 1$ 50%. $r \geqslant 2$ occurs but rarely. Record r is probably around 30, hypothesis is that r is unbounded.

There are certain algorithms to compute r and $E(\mathbb{Q})$

Remark 15. There is a conjectural analytic formula for r. Bircht and Swinaton-Dyer

2 Elliptic Curves over Finite Fields

$E : y^2 = x^3 + ax^2 + b$, where $a, b \in \mathbb{F}_p$

How big can $E(\mathbb{F}_p)$?

How to compute?

First approach: for each $x = x_0$, look at $x_0^3 + ax_0 + b. = \left(\frac{x_0^3 + ax_0^2 + b}{p}\right) + 1$ (Legandre symbol)

$\implies$ if this is a nonzero square, 2 points. For nonsquare, 0 points. zero, 1 point.

$|E(\mathbb{F}_p)| = \sum_{x_0=0}^{p-1} \left(\frac{x_0^3 + ax_0^2 + b}{p}\right) + 1 + 1 = p + 1 + \sum_{x_0=0}^{p-1} \left(\frac{x_0^3 + ax_0^2 + b}{p}\right) + 1$

Since $\left(\frac{a}{p}\right)$ is 1 or -1 equally often, expect sum to be fairly small.

Theorem 16 (Riemann Hypothesis for elliptic curves over finite fields)**.** $|\sum_{x_0=0}^{p-1} \left(\frac{x_0^3 + ax_0^2 + b}{p}\right)| \leqslant 2\sqrt{p}$,

Really called the Hasse Theorem, but Hasse applied to the Nazi party, and Weston doesn't cite Nazis

$N_p = \#E(\mathbb{F}_p)$
$a_p = p + 1 - \#E(\mathbb{F}_p)$
$|a_p| \leqslant 2\sqrt{p}$
$|\#E(\mathbb{F}_p)| - p - 1 \leqslant 2\sqrt{p}$