Math 571

Taught by Tom Weston
Scribed by Ben Burns

UMass Amherst

Spring 2022

Contents

1 Elliptic Curves **1**
- 1.1 Point addition . . . 1
- 1.2 Special Cases . . . 2
- 1.3 Introducing other fields . . . 2
- 1.4 Classifying E . . . 3

2 Elliptic Curves over Finite Fields **4**
- 2.1 Algorithms to compute #E(F) . . . 4
- 2.2 Elliptic Curve Discrete Log Problem (ECDLP) . . . 5
- 2.3 Collision Algorithms . . . 5
- 2.4 Pollard's factorization algorithm . . . 6

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 $\to$ 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
$Y = y_1 + \lambda(X - x_1), \lambda = \dfrac{y_2 - y}{x_2 - x}$

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,
$\to$ 4.1) do this in projective geometry, use Pascal's theorem
$\to$ 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 $\Delta_E = 4a^3 + 27b^2 \neq 0$.

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

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

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

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

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

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

1.4 Classifying E What kind of groups are we getting?

Example. $E(\mathbb{F}_p)$ is a finite abelian group. $|E(\mathbb{F}_p)| \leqslant p^2 + 1$, 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). $\begin{cases} T \cong \mathbb{Z}/n & n = 1, 2, \ldots, 10, 12 \\ T \cong \mathbb{Z}/2 \times \mathbb{Z}/n & n = 2, 4, 6, 8 \end{cases}$

"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. Birch and Swinnerton-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 $E(\mathbb{F}_p)$ be?

How to compute?

First approach: for each $x = x_0$, look at $x_0^3 + ax_0 + b.= \left(\dfrac{x_0^3 + ax_0^2 + b}{p}\right) + 1$ (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 $\left(\dfrac{a}{p}\right)$ is 1 or -1 equally often, expect sum to be fairly small.

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

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

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

Remark 17. # $E(\mathbb{F}_p) = p + 1$, where everything cancels out, is the supersingular case. # $E(\mathbb{F}_p) = p \to$ "anomolous primes", discrete log problem is really easy to solve

2.1 Algorithms to compute #E(F)

Given $E/\mathbb{F}_{101}$, suppose we have $P \in E/\mathbb{F}_{101}$ of order 47. This directly implies that $\#E(\mathbb{F}_p) = 94$.

Why? Riemann hypothesis tells us that the number of points must be within $|\#E(\mathbb{F}_p) - 102| \leqslant 20 \implies 82\# \leqslant \#E(\mathbb{F}_p) \leqslant 122$. Lagrange's theorem tells us that, since $E/\mathbb{F}_{101}$ is finite, then order of P must divide $\#E(\mathbb{F}_p)$. The only number that satisfies both of these properties is 94.

To compute $\#E(\mathbb{F}_p)$: find orders of elements until Lagrange forces a unique possible field order via Riemann Hypothesis.

How to find orders?
1) Shanks Baby Step – Giant Step (Collision): take big powers and find collision. Going to take $O(\sqrt{p})$, might need to make multiple tries before you get a useful collision

2) Schoof (Elkies + Atkin). Using division polynomials, runs in $O(\log^6 p)$. The constants were originally huge, so you need lots of digits for it to be useful/practical.

Remark 18. Any finite abelian group can be expressed as the product of finite cyclic groups. $E(\mathbb{F}_p)$ can be a product of at most two cyclic groups: $E(\mathbb{F}_p) \cong \mathbb{Z}/st \times \mathbb{Z}/s$, where t is large and s is small. For example, prime $l|s \approx \dfrac{1}{l^4}$

Example. Another way to look at RH. Take $y^2 = x^3 - 7x - 6$. Vary p, count $\#E(F_p)$ for each p, and compare to Riemann hypothesis

p	$\#E(\mathbb{F}_p)$	$p+1-\#E(\mathbb{F}_p) \leqslant 2\sqrt{p}$
2	-	-
3	4	0
5	-	-
7	12	-4
11	8	4
13	16	-2
17	16	2
19	16	4

Middle columns are all multiples of four, the third column will therefore all be even.

Remark 19. Wiles (in proving Fermat's Last Theorem) the a_p are the Fourier coefficients of a modular form

Remark 20. $E(\mathbb{Q})$ infinite $\iff \prod_p \frac{p}{\#E(\mathbb{F}_p)} = 0$

2.2 Elliptic Curve Discrete Log Problem (ECDLP)

Definition 21. Take $P, Q \in E(\mathbb{F}_p)$. Find n such that $Q = n \cdot P$, where n is an additive power using the addition law of E/F_p

Example. $E/\mathbb{F}_{101}$, $y^2 = x^3 + x + 3$. $P = (46, 83)$, $Q = (31, 63)$

How do we find n such that $Q = nP$? $n = 37$ works. In other words, $\log_p Q = 37$

We need a basic algorithm to compute $n \cdot P$ quickly for $P \in E(\mathbb{F}_p), n > 0$. "double and add"

Example. $E : y^2 = x^3 + 31x + 1000$ over $\mathbb{F}_{32003}$

Find P on $E(\mathbb{F}_p)$. Try $x = 1 \implies y^2 = 1032$. Compute $\left(\frac{1032}{32003}\right) = +1 \implies y$ exists. $y = \pm 21953$. Take $P = (1, 21953)$.

Compute $1297 \cdot P$. Decompose it as a power of 2: 1297 = 1024 + 256 + 16 + 1.

$P = (1, 21953)$. $P + P = (10821, 20322), 4P = 2P + 2P = (\dots)$

$16P = 8P + 8P = (8878, 16557)$
$256P = (19325, 10689)$
$1024P = (13434, 22968)$
$1297P = 1024P + 256P + 16P + P = (544, 26812)$

Remark 22. Similar to fast powering, this algorithm can also be adapted to minimize storage requirements.

Remark 23. There is no Fermat's Little Theorem here, because we don't know the order of the group

ECDLP: Recover 1297 from (544, 26812) and (1, 21953).

Best known algorithms are collision algorithms taking $O(\sqrt{p})$ steps. These are slow, which are good for cryptographic reasons.

Remark 24. For regular discrete log problem, there exist subexponential algorithms for general prime p. Additionally, there exist this idea of bad primes p. Here, the best algorithm is obviously exponential.

Remark 25. In essence, Shor's algorithm is really good at computing orders of elements mod p very quickly

2.3 Collision Algorithms

These are essentially an adaptation of Baby Step – Giant Step

S finite set, $\#S = N$. Define $f : S \to S$ that is "sufficiently random".

Example. $S = \mathbb{Z}/n, f(x) = x^2 + 1$.

We are more interested in $S = E(\mathbb{F}_p)$

Given $P, Q \in E(\mathbb{F}_p)$

$$F(A) = \begin{cases} A + P & x \equiv 1 \pmod 3 \\ 2A & x \equiv 2 \pmod 3 \\ A + Q & x \equiv 0 \pmod 3 \end{cases} \quad \text{for } A \in E(\mathbb{F}_p) = (x, y), 0 \leqslant x \leqslant p - 1$$

Idea: Fix $x_0 \in S$. $x_1 = f(x_0)$, $x_2 = f(x_1)$, $\cdots$

Mapping points to points, and eventually you will have a cycle because we are dealing with a finite set. Call the first point in the cycle you see x_T, the last point in the cycle x_{T+M-1}, and then x_T repeats as x_{T+M}, where T and M are minimum

Remark 26. In Chapter 5, How large to you expect T to be? $O(\sqrt{N})$

2.4 Pollard's factorization algorithm

Assume we have $n = pq$, $S = \mathbb{Z}/n$, $f(x) = x^2 + 1$. $x_0 = 1$

Suppose $x_{T_n} = x_{T_n+M_n}$ is the first repeat mod n, $T_n = O(\sqrt{n})$. Probably, we get a repeat mod p (or q) much much sooner: $x_{T_p} = x_{T_p+M_p}, T_p = O(\sqrt{p}) = O(n^{1/4})$. Take $\gcd(x_{T_p} - x_{T_p+M_p}, n) = p$, and we can probably recover something.

Implementation Problems: You need to compute $\gcd(x_i - x_j, n)$ for every pair i, j, because we have no idea where this repeat is going to be. This becomes a huge number as i increases. Additionally, you have to store every point, which is infeasible.

Definition 27 (Pollard ρ–method)**.** Traverse twice. Start with $x_0 = y_0$, and compute $x_i = f(x_i - 1)$, $y_i = f(f(y_{i+1}))$. At each step, compute $\gcd(x_i - y_i, n)$. If it fails, throw it away. If it works, we have $x_T = x_{M+T}$.

Example. $n = 31861$, $f = x^2 + 1, x_0 = 1$

i	x_i	y_i	$\gcd(x_i - y_i, n)$
0	1	1	n
1	2	5	1
2	5	677	1
3	26	29508	1
4	677	27909	151

Unless we get unlucky, and q hits at the exact same moment, we have that 151 is a factor of n.

Running time depends on the smallest prime factor $O(\sqrt{p}) \stackrel{?}{=} O(n^{1/4})$. If p is much smaller, then it runs much better