Math 571

Taught by Tom Weston
Scribed by Ben Burns

UMass Amherst

Spring 2022

Contents

1 First Exam

Remark 1. I did not take notes for the first third of the course. This section serves as an index of what the reader is missing.

- Discrete Logs
- Diffie-Hellman Key Exchange

- Shanks Algorithm
- RSA
- Factorization (p-1 method, trial division, difference of squares)

Example 2. Fiven a few explicity congruences $c_i \equiv a_i^2 \pmod{n}$ explain how you can find a factor of n

2 Factorization by difference of squares

(1) Find lots of congruences $a_1^2 \equiv c_i \pmod{n}$ with c_i product of small primes. Fix small number B, and require all prime factors $p \leq B$
(2) Elimination: Find a subset of these congruences which multiply to give $x^2 \equiv y^2 \pmod{n}$ ($\mathbb{F}_2$ linear algebra)
(3) Compute $\gcd(x \pm y, n)$, hope its a proper factors of n

Review finding kernel, Gaussian Elimination $\mathbb{F}_2$, book of (2)

Algorithm: Find numbers a such that $a^2 \pmod{n}$ is a product of small primes

$m = \lfloor\sqrt{n}\rfloor + 1$. Try $a = m, m+1, m+2, \cdots$, $a^2 \pmod{n} = a^2 - n$.

This is relatively small since $a \approx \sqrt{n}$, so has a better chance of factoring into small primes

$Q(x) = x^2 - n$

Looking at $x = m, m+1, m+2$, we find $x^2 \equiv Q(x) \pmod{n}$, where $x^2 = a_i$ and $Q(x) = c_i$.

Problem: Given n, a, how do you determine if $Q(a) = a^2 - n$ is a product of small primes without factoring?

Remark 3. Roughly half of primes will never be factors of $Q(a)$

Why? Suppose $p|Q(a)$ for some a. Then $p|a^2 - n \implies a^2 \equiv n \pmod{p} \implies n$ is a square mod p.

Fix odd prime p

Definition 4. Given $t \in \mathbb{F}_p$ such that $t \neq 0$, we say t is a quadratic residue mod p if $\exists s \in \mathbb{F}_p$ such that $s \equiv s^2 \pmod{p}$

For example, $p = 11$

"Squares are always squares" - :D

There are always exactly $\dfrac{p-1}{2}$ squares and $\dfrac{p-1}{2}$ non-squares

2.1 Legendre Symbols

Definition 5 (Legendre Symbol). $\left(\dfrac{t}{p}\right) = +1$ if t square mod p, -1 if t non-square, 0 if $t = 0 \pmod{p}$.

Remark 6. The quadratic resides of $\mathbb{F}_p$ are the even powers of any generator g.

Fix a generator $g \in \mathbb{F}_p$. Fix $t \in \mathbb{F}_p$. Write $t = g^e$ for some e s.t $0 \leq e \leq p-1$. If e is even then $t = (g^{e/2})^2 \implies \left(\dfrac{t}{p}\right) = 1$. Since this already gives $(p-1)/2$ squares for $e = 0, 2, 4, \ldots p-3$, so it follows that e odd $\implies \left(\dfrac{t}{p}\right) = -1$.

Definition 7 (Properties of Legendre Symbol)**.** (1) $\left(\dfrac{t}{p}\right) \equiv t^{\frac{p-1}{2}} \pmod{p}$

(2) $\left(\dfrac{st}{p}\right) = \left(\dfrac{s}{p}\right)\left(\dfrac{t}{p}\right)$

(3) $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$ if $p \equiv 1 \pmod{4}$, -1 is $p \equiv 3 \pmod{4}$

Proof:
(1) FLT for squares, polynomial counting argument for non-squares
(2) right side of (1) is multplicative, so left side has to be as well

Definition 8 (Quadratic Reciprocity Law)**.** Let p, q be distinct odd positive primes. Then $\left(\dfrac{p}{q}\right)$ $= \dfrac{q}{p}(-1)^{\dfrac{p-1}{2}\dfrac{q-1}{2}}$.

Equivalently, if either p or q is congruent to 1 mod 4, then the reciprocity holds. Else, they are negations.

Definition 9 (Quadratic Sieve)**.**

Manufacture many congruences of the form $c_i \equiv a_i^2 \pmod{n}$ where a_i where a is a product of primes less than some fixed bound B

Set $Q(x) = x^2 - n$, then try $Q(m), Q(m+1)\cdots$, where $m = \rfloor\sqrt{n}\lfloor +1$. To check if $Q(a_i)$ is only divisible by primes $\leq B$ we use a sieve to simultaneously find all small prime factors of $Q(x)$ via linear congruences.

Definition 10. Fix B. An integer m is B-smooth if all primes factors of m are $\leq B$

Definition 11. $\psi(x, B) = \#$ B-smooth numbers $\leq x$

Theorem 12. *Let* $L(x) = e^{\sqrt{\ln x \cdot \ln \ln x}}$. *Fix* $0 < c < 1$. *Then* $\psi(x, L(x)^c) = xL(x)^{-\dfrac{1}{2c}(1+o(1))}$

This holds if you replace $o(1)$ by some constant, and that constant goes to 0 as $x \to \infty$

3 Elliptic Curves

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

Definition 13. 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 14. Most general equation, the Weierstrass equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$

3.1 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 15 (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. $y^2 = x^3 - 15x + 18$. $P = (7,\ 16)$ $Q = (1,\ 2)$

$y - 2 = \dfrac{7}{3}(x-1) \implies y = \dfrac{7}{3}x - \dfrac{1}{3}$. Insert into elliptic curve $(\dfrac{7}{3}x - \dfrac{1}{3}) = x^3 - 15x + 18 \implies \dfrac{49}{9}x^2 - \dfrac{14}{9}x + \dfrac{1}{9} = x^3 - 15x + 18 \implies x^3 - \dfrac{49}{9}x^2 + \ldots = 0$. 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 $\dfrac{-49}{9} = -(8 + x_0) \implies x_0 = \dfrac{-23}{9}$. Therefore R has an x value of $\dfrac{-23}{9}$.

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 16. 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.

3.2 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 17. 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 18. *$E(\mathbb{R}) = \{(x, y) \in \mathbb{R}^2 | y^2 = x^3 + ax + b\} \cup \{\mathbb{O}\}$, 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,
→ 4.1) do this in projective geometry, use Pascal's theorem
→ 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)

3.3 Introducing other fields

Remark 19. We don't actually care about $E(\mathbb{R})$, but variations are useful in cryptography

Definition 20. $E(\mathbb{Q}) = \{(x, y) \in \mathbb{R}^2 | y^2 = x^3 + ax + b\} \cup \{\mathbb{O}\} \subset E(\mathbb{R})$

Remark 21. 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 22. 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 23. Modulus has to be prime since $\mathbb{Z}/n$ can have elements without an inverse (not even integral domain)

Definition 24. 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	$\pm$ 1
1	3	X
2	4	± 2
3	3	X
4	6	X
5	5	X
6	6	X

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

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

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

3.4 Classifying E

What kind of groups are we getting?

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

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 25 (Mordell-Weil Theorem). *$E(\mathbb{Q})$ is a finitely generated abelian group $\implies$ $E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$, where $r \geq 0$, 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 26 (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%. $r \geq 2$ 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 27. There is a conjectural analytic formula for r. Birch and Swinnerton-Dyer

4 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 $x_0^3 + ax_0 + b .= \left(\frac{x_0^3 + ax_0^2 + b}{p}\right) + 1$ (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 28 (Riemann Hypothesis for elliptic curves over finite fields)**.** $|\sum_{x_0=0}^{p-1} \left(\frac{x_0^3 + ax_0^2 + b}{p}\right)| \leq 2\sqrt{p}$,

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

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

Remark 29. $\#\ E(\mathbb{F}_p) = p + 1$, where everything cancels out, is the supersingular case. $\#\ E(\mathbb{F}_p) = p \rightarrow$ "anomolous primes", discrete log problem is really easy to solve

4.1 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 $|\#E(\mathbb{F}_p) - 102| \leq 20 \implies 82\# \leq \#E(\mathbb{F}_p) \leq 122$. 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 30. 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 $l|s \approx \frac{1}{l^4}$

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	$\#E(\mathbb{F}_p)$	$p + 1 - \#E(\mathbb{F}_p) \leq 2\sqrt{p}$
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 31. Wiles (in proving Fermat's Last Theorem) the a_p are the Fourier coefficients of a modular form

Remark 32. $E(\mathbb{Q})$ infinite $\iff \prod_p \frac{p}{\#E(\mathbb{F}_p)} = 0$

4.2 Elliptic Curve Discrete Log Problem (ECDLP)

Definition 33. 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 34. Similar to fast powering, this algorithm can also be adapted to minimize storage requirements.

Remark 35. 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 36. For regular discrete log problem, there exist subexponential algorithms for general prime p. Additionally, there exist this idea of "bad primes" p, which we are able to break even faster. Here, the best algorithm is obviously exponential.

Remark 37. In essence, Shor's algorithm is really good at computing orders of elements mod p very quickly

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

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

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

After repeatitively nesting f, you must eventually see some element repeat (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 38. In Chapter 5, How large to you expect T to be? $M + T \approx O(\sqrt{N})$

4.4 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.

There are really three pictures here, your ρ mod n, mod p, and mod q.

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 39 (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 $O(\sqrt{p}) \overset{?}{=} O(n^{1/4})$. If p is much smaller, then it runs much better

Remark 40. This assumes n exists. This is very bad at deciding if n exists, so we're only going to apply it if we know there is one.

In practice with our elliptic curve, we calculate

$$\begin{array}{cc} A_0 = P & B_0 = P \\ A_1 = f(A_0) & B_1 = F(F(B_0)) \\ A_2 = f(A_1) & B_2 = F(F(B_1)) \\ \vdots & \vdots \end{array}$$

where at each step we check if $A_i = B_i$

Remark 41. $A_i = a_i P + a'_i Q$, $B_i = b_i P + b'_i Q$

Once we have our collision, we can regroup terms: $A_i = B_i \implies a_i P + a'_i Q = b_i P + b'_i Q \implies (a_i - b_i)P = (a'_i - b'_i)Q$.

Remark 42. You need to know the order of $P \in E(\mathbb{F}_p)$, denoted R. Note that there is a separate algorithm for that, which we do not have yet. What we have done is, using order of P and RH, determine $\#E(\mathbb{F}_p)$

Reduce $a_i, b_i \pmod R$

If $\gcd(b'_i - a'_i, R) = 1$ then set $c \equiv (b'_i - a'_i)^{-1} \pmod R$, so $c(a_i - b_i)P = Q$

Expected running time: $O(\sqrt{\#E(\mathbb{F}_p)}) = O(\sqrt{p})$

Remark 43. This is the best known general algorithm. Again, there are some cases which can be done quite fast (anomolous and supersingular), which we want to avoid.

4.5 Elliptic Curve Diffie-Hellman (ECDHP)

Recall that the goal of Diffie-Hellman is for two parties to agree on a secret key over a public channel

Public: prime p, elliptic curve $E/\mathbb{F}_p$, and point $P \in E(\mathbb{F}_p)$

Alice and Bob want to agree on some sort of secret key. They each choose some large integer n_A and n_B. Then compute $Q_A = n_A \cdot P$ and $Q_A = n_B \cdot P$. Alice sents Q_A to Bob, and Bob sends Q_A to Alice. Alice computes the left hand side, $n_A Q_B = n_A n_B P = n_B Q_A$, and Bob computes the right hand side, which are of course equal.

Remark 44. In some cases you will want your key to be a point. In some contexts you want it to be a certain value, in which case you can just pick a coordinate or the sum.

If Eve can solve $ECDLP$, she recovers n_A and n_B from Q_A, Q_B (and knowing p, E, P) can compute $n_AQ_B = n_BQ_A$. Therefore ECDLP solves ECDHP. There is no known way to approach ECDHP without ECDLP.

Example. $p = 2411$. $E : y^2 = x^3 + 83x + 1137$. $P = (10, 571)$

Alice chose $n_A = 1211$, Bob chose $n_B = 693$. Using fast powering, they compute $n_AP = (401, 1439)$ and $n_BP = (1312, 802)$, and then they each compute $n_AQ_B = n_BQ_A = n_An_BP = (116, 988)$

4.6 Elliptic Curve El Gamal

Again, we're just going to adapt ECDHP to be a cryptosystem.

Choose prime p, elliptic curve $E/\mathbb{F}_p$, and point $P \in E(\mathbb{F}_p)$

Alice chooses n_A and computes $Q = n_AP$

Public: prime p, elliptic curve $E/\mathbb{F}_p$, and point $P \in E(\mathbb{F}_p)$, Q

Bob wants to send message $M \in E(\mathbb{F}_p)$. (It is a lot harder to coerce the message into the curve than a message into an integer). Bob picks k, and sends $C_1 = kP$ and $C_2 = M + kQ$.

Alice receives them, and computes $C_2 - n_AC_1 = M + kQ - nA(kP) = M + kn_AP - n_AkP = M$

Once again, if you can solve ECDLP, then you can braek EC El Gamal (which is equivalent to ECDHP)

5 Lensta's Elliptic Curve Factorization

Analogue to Pollard's $p - 1$ algorithm

Factor $n = pq$. Find L such that (for $\gcd(a, N) = 1$)$a^L \equiv 1 \pmod p$, $a^Q \not\equiv 1 \pmod q$, so $p = gcd(n, a^L - 1)$. Try $L = k!$, $k = 1, 2, 3, \ldots$. Works well if $p - 1$ has only smallish prime factors.

Goal: Factor $n = pq$

Example. $n = 187$, $E : y^2 = x^3 + 3x + 7$, $P = (38, 112)$

Our curve is over $\mathbb{Z}/n$, which is a problem because it's not a field, and division doesn't work. Things break, but that's what we want.

Start computing $2P, 3P, 4P, \ldots$, using the normal formulas. $\lambda = \dfrac{3x^2 + A}{2y} \equiv \dfrac{338^2 + 3}{2 \cdot 112} \pmod n$. $\gcd(224, n) = 1$, so we're safe.

$x_{2P} = \lambda^2 - 2x_P$, $y_{2P} = \lambda(x_{2P} - x_P) + y_P$, $2P = (43, 126)$.

Then use secant method for $3P = 2P + P = (54, 105)$, $4P = 3P + P = (93, 64)$

Why is this useful? Well, when we compute $5P$, things break.

$5P = 3P + 2P$. $\lambda = \dfrac{y(3P) - y(2P)}{x(3P) - x(2P)} = \dfrac{105 - 126}{54 - 43} = \dfrac{-21}{11} \pmod n$. We cannot compute the inverse of 11 mod n, meaning that $\gcd(11, 187) \neq 1$. The computation fails, but more importantly we have a factor of n, which is $\gcd(11, 187) = 11$

Explanation $P \in E(\mathbb{Z}/187)$ can be reduced into both $P \in E(\mathbb{Z}/11)$ and $P \in E(\mathbb{Z}/17)$. $P \mod 11 = (5, 2)$ on $E(\mathbb{F}_{11})$. Turns out $5P = \mathbb{O}$. Our computation failed because a different formula is required to get $\mathbb{O}$. We don't need to know 11 is a factor to get their, much less know the order in $E(\mathbb{F}_11)$

Remark 45. We don't want to compute additively, because if the orders are huge, then this will take a while. However, we can use factorial like Pollard's $p - 1$

Fix $P = (a, b)$, $a, b \in \mathbb{Z}/n$. Fix $A \in \mathbb{Z}/n$. Set $B = b^2 - a^3 - Aa$. Then P is a point on $E : y^2 = x^3 + Ax + B$.

For $j = 2, 3, 4, \ldots$, let $Q_1 = P$, and $Q_j = j \cdot Q_{j-1} = j!P$. We still don't have to compute $j!$, since we only multiply once at each step, rather than recomputing $j!$ everytime, just like $p - 1$ method.

If at step j the computation fails (because the denominator in λ is not relatively prime to n), then recover a factor as gcd(n, denominator of λ).

Remark 46. If the gcd is n, pick a new P, A, and start over.

Example. $n = 15811$

Pick $P = (11, 13)$, and $A = 1 \implies B = 14638, E : y^2 = x^3 + x + 14638$

$P = (11, 13), Q_2 = 2P = (174, 13516)$

$3Q_2 = 2Q_2 + Q_2 : \lambda = \dfrac{3516 - 13}{174 - 11}$. 174 -11 = 163, $\gcd(n, 163) = 163$. Therefore 163 is a factor.s

Why did this work? 15811 = 163·97. $P \in E(\mathbb{Z}/n) \implies E(\mathbb{F}_{163})$, order of 3.

Running time: Recall the quadratic sieve was $O(e^{\sqrt{\log n \log \log n}})$. Elliptic curve was $O(e^{\sqrt{2 \log p \log \log p}})$. If $p \approx q$, then the 2 goes away and they are roughly the same. However, if p is much smaller, then we will find it much quicker.

6 Finite Fields

Recall: A field F is a set with binary operations $+, \cdot$ satisfying all usual algebraic axioms, including that all non-zero elements are units (meaning they have multiplicative inverses)

A finite field is a field with a finite number of elements.

Example. $\mathbb{Z}/n$

The units in here are the numbers relatively prime to the modulus n. If we want all nonzero elements to be units, then we obviously want n to be prime, which we typically denote $\mathbb{F}_p = \mathbb{Z}/p$.

6.1 Preliminaries

Are there other finite fields? Yes there are, there are infinitely many, but there aren't that many.

Theorem 47. *There exists a field of size n if and only if $n = p^k$ for a prime p and $k \geq 1$*

Theorem 48. *If F and F' are two finite fields with the same order, then they are isomorphic*

Write $\mathbb{F}_p^n$ for "the" field of p^n elements

Why are we doing this? It is very easy for a computer to play with $\mathbb{Z}/2$, but it's not very big. However, if you can pass it F_2^{100}, that's a lot bigger and a lot more complicated. Also when we get to torsion points, it's a lot easier to fixed p and vary n.

Example. Build using polynomial rings

$\mathbb{F}_p[X]$ = ring of polynomials in X with coefficients in $\mathbb{F}_p$. Elements look like $a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \in \mathbb{F}_p[X], a_i \in \mathbb{F}_p$

We have a theory of divisibility: $f | g \iff fg = g$ for some $h \in \mathbb{F}_p[X]$.

If we have $f, g \in \mathbb{F}_p[X], g \neq 0$. Then there exist a pair of polynomials q and r with $\deg r < \deg g$ such that $f = gq + r$. This directly implies unique factorization into irreducible polynomials in $\mathbb{F}_p[X]$.

Definition 49. $f \in \mathbb{F}_p[X]$ is irreducible if f has no non-constant divisors of smaller degree

My note: this definition is for $\mathbb{F}_p$ since it is a field, this is weaker than general irreducibility.

Example. $p = 2$, irreducible polynomials

Degree 0, none. Degree 1, X, $X + 1$.

Degree 2 has four polynomials: $x^2 = x \cdot x$, $x^2 + x = x(x + 1)$, $x^2 + 1 = (x + 1)^2$, and $x^2 + x + 1$, which is irreducible.

We want to look for polynomials with a non-zero constant term, and an odd amount of terms. Degree 3 has two such: $x^3 + x^2 + 1$ and $x^3 + x + 1$.

Now with degree 4, we don't need to have a root to reduce. The four without roots are x^4+x^3+1, x^4+x^2+1, x^4+x+1, and $x^4+x^3+x^2+x+1$. However, the only way to get a degree 4 as a product of irreducible quadratics is to square our only irreducible quadratic, getting $(x^2+x+1)^1 = x^4+x^2+1$

You can use induction and unique factorization to get a precise formular for the number of irreducible polynomials of any degree.

6.2 Constructing a finite field of prime power size Find irreducible polynomial $f \in \mathbb{F}_p[X]$ with $\deg f = n$.

Quotient rings $\mathbb{F}_p[X]/f(x)$ are polynomials modulo f. For $g, h \in \mathbb{F}_p[X]$: $g+h$ is still degree $< n$, so it's already in here. $g \cdot h$, apply division to gh and f to get r's degree down below f's. Set $g \cdot h = r$. Then this is "the" finite field $\mathbb{F}_{p^n}$

Example. $\mathbb{F}_4 = \mathbb{F}_2[X]/(x^2+x+1)$

elements are $\{0, 1, X, X+1\}$. Most are obvious except $x \cdot x = x^2 = 1(x^2+x+1)+x+1$, so $x^2 = x+1$. $(x+1)^2 + (x^2+x+1)+x$, and $x(x+1) = (x^2+x+1)+1 = 1$

Example. $\mathbb{F}_{27} = \mathbb{F}_3[x]/(x^3+2x+1)$

The elements will be quadratic polynomials with coefficients in $\mathbb{F}_3$

Remark 50. Finite fields are cyclic, so $\mathbb{F}_{27}$ will have an element with order 26.

Remark 51. Fix $n \geq 1$, and take $x^{p^n} - x$, this factors exactly as a product of every irreducible polynomial of degree dividing n

Remark 52. $\mathbb{F}_{p^2}$. If $p \equiv 3 \pmod 4$ then $\left(\frac{-1}{p}\right) = -1$ (-1 is not a square $\mod p$) It follows that x^2+1 is irreducible in $\mathbb{F}_p[X]$.

$p \equiv 3 \pmod 4$, $\mathbb{F}_{p^2} = \mathbb{F}_p[X]/x^2+1 = \mathbb{F}_p[i] = \{a+bi | a, b \in \mathbb{F}_p\}, i^2 = -1$.

7 Elliptic Curves over Finite Fields (again)

$E: y^2 = x^3+ax+b$, with $a, b \in \mathbb{F}_{p^n}$. We always assume $a, b \in \mathbb{F}_p$. $\Delta = -4a^3 - 27b^2$, $\Delta \neq 0$

This is where the book concedes that this formulata for Δ is incomplete. $\Delta = 16(-4a^3-27b^2)$ so if $p = 2, \Delta = 0$ automatically.

Generalized Weierstrass equations $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in \mathbb{F}_p$. Equation for Δ is really complicated in terms of a's, but we need it to not be zero.

The group law still works, formaulas are just more complicated.

Look at $E(\mathbb{F}_{p^n})$ as n varies

Example. $p = 3$, $E: y^2 = x^3+x+1$

n	$\#E(\mathbb{F}_{3^n})$
1	4
2	16
3	28
4	64
5	244
6	784

We still have the Riemann hypothesis, but for $|\#E(\mathbb{F}_{p^n}) - p^n - 1| \leq 2p^{n/2}$

More precise statement: $t = p+1-\#E(\mathbb{F}_p)$ so $|t| \leq 2\sqrt{p}$. Consider $x^2 - tz + p$.

Let $\alpha, \beta \in \mathbb{C}$ be the complex roots $x^2 - tz + p = (z-\alpha)(z-\beta)$. Note this means $\alpha + \beta = t$, and $\alpha\beta = p$.

Then $\#E(\mathbb{F}_{p^n}) = p^n + 1 - \alpha^n - \beta^n$

Example. $p = 3$

$z^2+3=(z+\sqrt{3}i)(z-\sqrt{3}i)$, $\alpha=\sqrt{3}i$, $\beta=-\sqrt{3}i$

$\#E(\mathbb{F}_{3^n})=3^n+1-(\sqrt{3})^n-(-\sqrt{3})^n=\begin{cases}3n+1 & n\equiv 1 \pmod 2\\ 3^n-2\cdot 3^{n/2}+1 & n\equiv 0 \pmod 4\\ 3^n+2\cdot 3^{n/2}+1 & n\equiv 2 \pmod 4\end{cases}$ First case is easy because the negative remains, and α and β powers cancel. For the second and third, it is a matter of what value i takes on.

Example. $p=3$, $y^2=x^3+x+1$

$E(\mathbb{F}_{3^{1000}})$. $1000\equiv 0 \pmod 4$, $\#=3^{1000}-2\cdot 3^{500}+1$. This says nothing about the group structure, but we know size.

Remark 53. Consider α and β. The Riemann hypothesis that $|t|\le 2\sqrt{p} \iff a,b\notin\mathbb{R}$.

The key fact to this is that $\alpha\beta=p$, so if they are not real, they must be complex conjugates with modulus $\sqrt{p}$, and must add up to t

7.1 Frobenius Map

No one ever seems to know his first name, he's just Frobenius, since his last name is cool.

Definition 54 (Frobenius Map)**.** $\tau:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$, where $\tau(\alpha)=(\alpha^n)$.

Lemma 55. *This is a ring homomorphism*

$\tau(\alpha\beta)=(\alpha\beta)^p=\alpha^p\beta^p=\tau(\alpha)\tau(\beta)$

$\tau(\alpha+\beta)=(\alpha+\beta)^p=\alpha^p+\ldots+\beta^p=\alpha^p+\beta^p$ since all of the middle terms are divisible by p.

This is an automorphism, is an element of the Galois group of this extension and so on :D.

Remark 56. $\tau(\alpha)=\alpha^p=\alpha$. α is a root of $x^p-x=x(x-1)(x-2)\ldots(x-(p-1))$, so $\alpha\in\{0,1,\ldots,p-1\}\implies\alpha\in\mathbb{F}_p$

8 Weil Pairing

$E/\mathbb{F}_p$, Fix $m\ge 2$. Find k such that $E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\times\mathbb{Z}/m$. Then pairing $e_m:E(\mathbb{F}_p)[m]\times E(\mathbb{F}_p)[m]\to\mathbb{F}_{p^k}^k$

8.1 Key Properties

$P,Q\in E(\mathbb{F}_{p^k})[m]$

- $e_m(P,Q)^m=1$
- $e_m(P,P)=1$
- $e_m(P_1+P_2,Q)=e_m(P_1,Q)\cdot e_m(P_2,Q)$, same for Q
- Non-degeneracy $e_m(P,Q)=1$ for all $Q\in E[m]\implies P=\mathbb{O}$

$e_m(P,Q)=\dfrac{f_p(Q+S)}{f_p(S)}\dfrac{f_Q(-S)}{f_Q(P-S)}$ Where S is a random point on $E(\mathbb{F}_{p^k})$, f_P and f_Q are rational functions on E such that $div(f_P)=n[P]-n[\mathbb{O}]$ and $div(f_Q)=n[Q]-n[\mathbb{O}]$

8.2 MOV Algorithm

ECDLOP: Given P,Q find (if it exists) $n\le 1$ such that $Q=nP$.

DLP in $\mathbb{F}_{p^k}$ Given $\alpha,\beta\in\mathbb{F}_{p^k}^k$ find (if it exists) $n\le 1$ such that $\beta=\alpha^n$ "Index calculus" method subexponential.

To compute e_m, need a fast algorithm to find f_P,f_Q

1) $P,Q\in E(\mathbb{F}_{p^k})$, $\lambda=$ slope of line $\overline{PQ}$

$$\lambda=\begin{cases}\dfrac{y_Q-y_P}{x_Q-x_P} & x_Q\ne x_P\\ \dfrac{3x_P^2+1}{2y_P} & P=Q\\ \infty & P=-Q\end{cases}$$

Define a rational function f_n on E.

$$g_{P,Q} = \begin{cases} \dfrac{y - y_P - \lambda(x - x_P)}{x + x_P = x_Q - \lambda^2} & \lambda \neq \infty \\ x - x_p & \lambda = \infty \end{cases}$$

Claim $div(g_{P,Q}) = [P] + [Q] - [P+Q] - [\mathbb{O}]$

Schedule for the rest

1. Lattices (1 class)
2. GGG cryptosystem (.5 class)
3. NTRU cryptosystem (1.5) class
4. LLL algorithm (2 classes)
5. Quantum Computing (2 classes)

Yesterday OpenSSH incorporating NTRU Prime into security, invented by the authors of book.

9 Lattices

$\vec{v_1}, \dots, \vec{v_n} \in \mathbb{R}^m$ (have n vectors with m real entries)

Assume that they are linearly independent over $\mathbb{R}$: $a_1\vec{v_1} + \dots a_n\vec{v_n} = 0$, for $a_i \in \mathbb{R}$, then $a_i = 0$ for all i ($\implies n \leq m$)

Definition 57. Define a lattice $L =< \vec{v_1}, \dots, \vec{v_n} >= \{a_1\vec{v_1} + \dots + a_n\vec{v_n} | a_i \in \mathbb{Z}\}$

Example 58. $m = n = 2$, $\vec{v_1} = (1,0)$, $\vec{v_2} = (0,1)$

Gaussian lattice, is annoying. If you rotate it 90 degrees, you get the same thing back

Example 59. $\vec{v_1} = (1,0)$ and $\vec{v_2} = (1,1)$

$a_1\vec{v_1} + a_2\vec{v_2} = (a_1 + a_2, a_2)$ is the same lattice. We choose a_2 arbitrarily, then chose a_1 off of it to make x arbitrary. Same lattice, different basis.

9.1 Changing bases

Start with lattice $L =< \vec{v_1}, \dots, \vec{v_n} >$

Pick $a_{ij} \in \mathbb{Z}$ set
$\vec{w_1} = a_{11}\vec{v_1} + a_{12}\vec{v_2} + \dots + a_{1n}\vec{v_n}$ $\vec{w_2} = a_{21}\vec{v_1} + a_{22}\vec{v_2} + \dots + a_{2n}\vec{v_n}$
...
$\vec{w_n} = a_{n1}\vec{v_1} + a_{n2}\vec{v_2} + \dots + a_{nn}\vec{v_n}$

Clearly, $\vec{w_1} \dots \vec{w_n} \in L$. Are they a basis? Rewrite with matricies

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{11} & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ a_{n1} & \dots & & a_{nn} \end{pmatrix}$$

V = vector of $\vec{v_i}$, W = vector of $\vec{w_1}$. $W = A \cdot V$

Lemma 60. *$\vec{w_1}, \dots, \vec{w_n}$ form a basis $\iff$ $detA = \pm 1$*

Proof If $\vec{w_1}, \dots, \vec{w_n}$ is a basis of L, then we can express $\vec{v_1}$ in terms of the $\vec{w_i}$: $V = BW$ for some B. Have $W = AV$, so $V = B(AV) = (BA)V$

Since $\vec{v_1}, \dots, \vec{v_n}$ are linealy independent. V has rank n. It folloes that $A \cdot B = I_n$
$\implies detA \cdot detB = 1$.
$detA \cdot detB \in \mathbb{Z} \implies detA = \pm 1$

Example 61. $V = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $A = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$

$\implies W = AV = A = \begin{pmatrix}3 & 4\\ 2 & 3\end{pmatrix}$, $(3,4)$ and $(2,3)$ also a basis.

$\vec{v_1}, \vec{v_2}$ are orthogonal, $\vec{v_1} \cdot \vec{v_2} = 0$.

$\vec{w_1}, \vec{w_2}$ are not orthogonal. $\vec{w_1} \cdot \vec{w_2} = 18$

9.2 Fundamental domain

Definition 62. $L =< \vec{v_1}, \ldots, \vec{v_n} >$, $? = \{t_1\vec{v_1} + \ldots + t_n\vec{v_n} | 0 \leq t < 1, t_i \in \mathbb{R}\}$.

Geometrically, the fundamental domain is a parallelogram in 2D lattices

Remark 63. Volume of ? is independent of the basis

Proof $W = A \cdot V$, vol(?) $= |detA| \cdot vol(?)$, det $= 1$.

Lemma 64. *$\vec{v_1}, \ldots, \vec{v_n} \in \mathbb{R}^n$ linearly independent, let $L =< \vec{v_1}, \ldots, \vec{v_n} >$ lattice. Any vector $\vec{w} \in \mathbb{R}^n$ can be uniquely written $\vec{w} = \vec{t} + \vec{v}$ with $\vec{v} \in L$, $\vec{t} \in ?_v$*

Because $\vec{v}$ are a basis of the integer lattice, we just take the coordinate that closely overshoots it and round the coefficients down to $\vec{w}$ by the real parts of $\vec{t}$

9.3 Shortest Vector Problem (SVP)

Given a lattice L, find the shortest nonzero $\vec{v} \in L$

$\vec{v} \in L$, $\vec{v} = (c_1, \ldots, c_m) \in \mathbb{R}^m$. $||\vec{v}|| = \sqrt{c_1^2 + \ldots + c_m^2} = \vec{v} \cdot \vec{v}$

Remark 65. The shortest vector problem is often the way to break these cryptosystems

Example 66. $L =< (1,0), (0,1) >= (3,4), (2,3) >$

It's obvious that in terms of the first basis, that the shortest vectors are ± the basis vectors. Because the second basis is the same lattice, it's going to be the same vectors, just with a more complicated vector expression in terms of the new basis.

The key difference is that the first basis is orthogonal, whereas the second is definitely not.

As it turns out, in an orthogonal basis, the shortest vector has to be a basis vector.

9.4 Closest Vector Problem (CVP)

$L \subseteq \mathbb{R}^m$ given $\vec{w} \in \mathbb{R}^m$, find $\vec{v} \in L$ such that $||\vec{v} - \vec{m}||$ is minimized.

We also have approx SVP and approx CVP. LLL can't guarantee to find the shortest vector, but it very quickly finds a very small vector for small dimensional Lattices

To study SVP, first question: given a lattirce L, what short of length should you expect for the smallest nonzero vector L

Expect to depend on $volL = detL$

Theorem 67 (Heimite's Thm)**.** *There is a nonzero $\vec{v} \in L$ such that $||\vec{v}|| \leq \sqrt{n} \cdot (detL)^{1/n}$*

Remark 68. Define constant γ_n as the smallest constant such that every n dimensional lattice has a vector $\vec{v}$ with $||\vec{v}|| \leq \gamma_n \cdot (detL)^{2/n}$

Hermite's says $\gamma_n \leq n$. Can you find optimal γ_n? Known for $n = 1, \ldots, 8, 24$. Dimension 24 has the Leech lattice.

For large n, $\dfrac{n}{2\pi e} \leq \gamma_n \leq \dfrac{n}{\pi e}$

To prove Hermite, we use

Theorem 69 (Minkowski's Thm)**.** *$L \subseteq \mathbb{R}^n$ lattice of dimension n. $S \subseteq \mathbb{R}^n$ subset. Assume S is*
bounded:there is $R > 0$ s.t $||\vec{s}|| \leq R$ for all $s \in S$
symmetric: $\vec{s} \in S \implies -\vec{s} \in S$,
and convex $\vec{s_1}, \vec{s_2} \in S$, then the line segment s_1s_2 is in S

here bounded is that there is $R > 0$ s.t $||\vec{s}|| \leq R$ for all $s \in S$

If $VolS > 2^n detL$ then S contains a nonzero point of L

Remark 70. S always contains origin by symmetry and convexity

Proof (of Minkowski) Basis $L =< \vec{v_1}, \dots, \vec{v_r} >$, $\mathbb{F}$ = fundamental domain. For any $\vec{s} \in S$, write $\vec{s} = \vec{w_s} + \vec{v_s}$ with $\vec{w_s} \in \mathbb{F}, \vec{v_s} \in L$

Consider $\frac{1}{2}S \subseteq S$ by symmetry and convexity. Define $f : \frac{1}{2}S \to \mathbb{F}$

The function f preserves volume since s is bounded, there are a finite set of vectors $\vec{x_N} \in L$ such that every $\vec{s} \in S$ has $\vec{v_s} = \vec{x_i}$ for some i.

For such an s, f is just translation by $-\vec{x_i}$

Note $vol(\frac{1}{2}S) = 2^{-n}volS$, assumed $volS > 2^n detL = vol\mathbb{F}$. So $vol(\frac{1}{2}S) > vol\mathbb{F}$. It follows that there are $\vec{s_1}, \vec{s_2} \in \frac{1}{2}S$ such that $\vec{w_{s_1}} = \vec{w_{s_2}}$

So $\vec{s_1} = \vec{v_{s_1}} + \vec{w_{s_1}}$, same for s_2, the second sntries are equal, $\vec{s_1} - \vec{s_2} = \vec{v_1} - \vec{v_2} \in L$. Check $\vec{s_1} - \vec{s_2} \in S$. Both are in $\frac{1}{2}S$, then symmetry and convexity.

Proof (of Hermite) $L \subseteq \mathbb{R}^n$ lattice, S hypercube centered at origin, side length $2B$, vol$S = (2B)^n$. Need $volS > 2^n detL$, so take $B = (detL)^{1/n}$

Minkowski implies that S contains a nonzero point $\vec{v} \in L$. $|c_i| < (detL)^{1/n} \implies ||\vec{v}||^2 \leq n(detL)^{2/n}$.

This gives a worst case for SVP of $\sqrt{n}(detL)^{1/n}$ Do we expect a smallest answer?

No. Redo Hermite with hypersphere (what is the volume in higher dimensions? n-dim with radius R is $\frac{\pi^{n/2}R^n}{\Gamma\left(1+\frac{n}{2}\right)}$.

Use the usual $\Gamma(s) = (s-1)!$ for $s \in \mathbb{Z}, s \geq 1$, odd n, use that $\Gamma(s+1) = s\Gamma(s), \Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$, use Stirling's formula $\approx (\sqrt{\frac{2\pi e}{n}}R)^n$