Elliptic Curves over Finite Fields

An Example

Theorem (Hasse's bound) Let E be an elliptic curve over a fin. field K with $q = p^n$ elements. Then

$$|\#E(K) - q - 1| \leq \lfloor 2\sqrt{q} \rfloor$$

$$q+1-2\sqrt{q} \leq \#E(K) \leq q+1+2\sqrt{q}$$

Example Let $E/\mathbb{F}_p : \underbrace{y^2 = x^3 + x}_{\Delta_E \equiv -64 \neq 0 \text{ if } p \neq 2 \bmod p}$, where p is an odd prime.

$(\Rightarrow \Delta_E \equiv 0 \bmod 2, p \neq 2)$

$p=3$ $\{\mathcal{O}, (0,0), (2,1), (2,2)\}$, $|\#E(\mathbb{F}_3) - 4| = 0 \leq 2\sqrt{3} = 3.46\ldots$

$p=5$ $\{\mathcal{O}, (0,0), (2,0), (3,0)\}$, $|\#E(\mathbb{F}_5) - 6| = 2 \leq 2\sqrt{5} = 4.47\ldots$

$E : y^2 = x^3 + x$

$-a_p$ = trace of Frobenius

p	$\#E(\mathbb{F}_p)$	$2\sqrt{p}$	$\#E(\mathbb{F}_p) - p - 1$
2	BAD	BAD	BAD
3	4	3.46...	0
5	4	4.47...	-2
7	8	5.29...	0
11	12	6.63...	0
13	20	7.21...	6
17	16	8.24...	-2
19	20	8.71...	0
23	24	9.59...	0
29	20	10.77...	-10
⋮	⋮	⋮	⋮

$y^2 = x^3 + x \,/\, \mathbb{Q}$

Birch, Swinnerton-Dyer

$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}$

$R_{E/\mathbb{Q}} >> 0 \overset{??}{\Longrightarrow} \#E(\mathbb{F}_p) >> p+1$ for "many" primes

$\rightsquigarrow$ B-SD conjecture.

$p + 1 - \#E(\mathbb{F}_p) = 2\sqrt{p}\cos\theta_p$

$\theta_p \rightsquigarrow$ prob. distribution

$\rightsquigarrow$ Sato-Tate conjecture (in 2011) over tot. real fields.

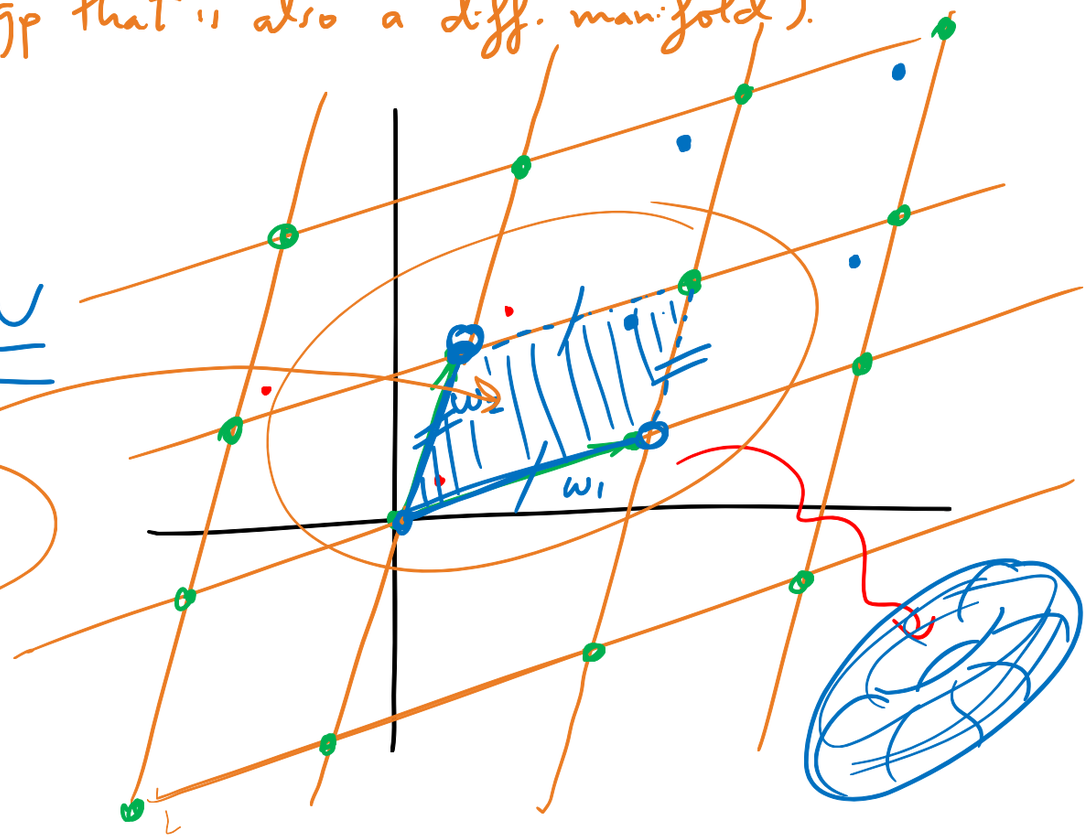
Elliptic Curves over $\mathbb{C}$

GOAL: Let $E/\mathbb{C}$ be an elliptic curve. Then, there exists a lattice $\Lambda \subseteq \mathbb{C}$, unique up to homothety (scaling), and a complex-analytic isomorphism $\phi : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$ of complex Lie groups (a gp that is also a diff. manifold).

$$y^2 = x^3 + Ax + B$$
$$A, B \in \mathbb{C}$$
$$4A^3 + 27B^2 \neq 0.$$

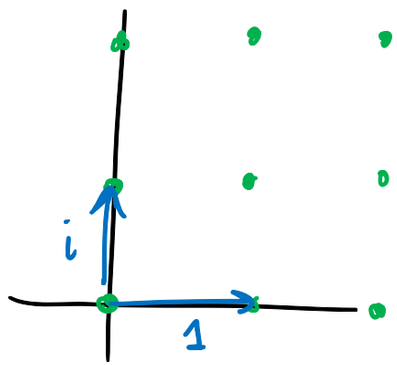
$$E(\mathbb{C}) = \{(x,y) \in E : x, y \in \mathbb{C}\} \cup \{\mathcal{O}\}$$

$\simeq$



Def A lattice $\Lambda \subseteq \mathbb{C}$ is a discrete (add.) subgp. of $\mathbb{C}$ which contains an $\mathbb{R}$-basis of $\mathbb{C}$.

ex $\mathbb{Z}[i]$



$\left(\mathbb{C}/\mathbb{Z}[i] \cong E(\mathbb{C}) \right.$
$\left. y^2 = x^3 - x \right)$

$\mathbb{C}/\mathbb{Z}[i] \to \mathbb{C}/\mathbb{Z}[i]$

$z \longmapsto$

extra endomorphism!

$[i] : (x, y) \longmapsto (-x, iy)$