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.

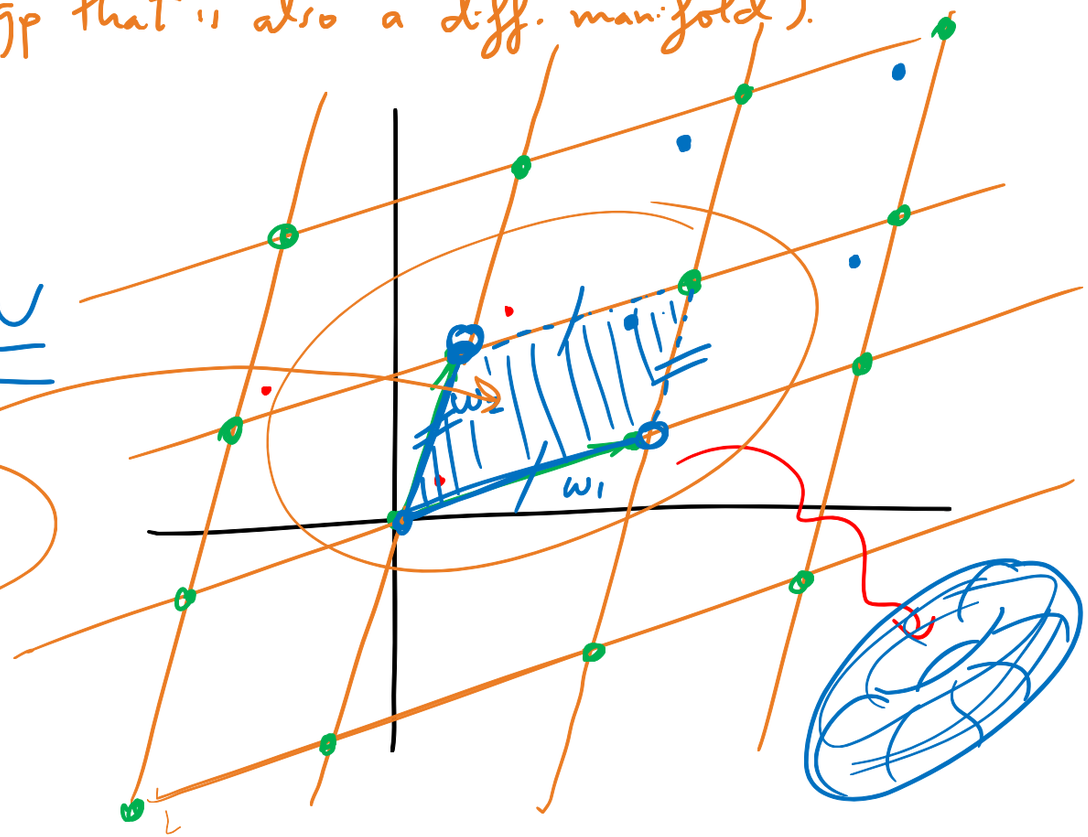
Elliptic Curves over $\mathbb{C}$

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).

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

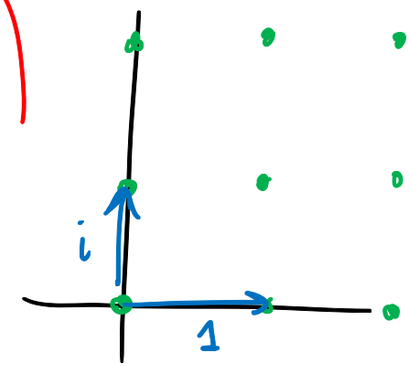
$$E(\mathbb{C}) = \{(x,y) \in E : x, y \in \mathbb{C}\} \cup \{\mathcal{O}\}$$

$\simeq$



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 $\mathbb{Z}[i]$



(if $\tau\mathbb{Z}[\tau]=\mathbb{Z}[\tau]$ $\Rightarrow \tau^2 = a+b\tau$)

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

E has CM if $\mathrm{End}(E) \supsetneq \mathbb{Z}$

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

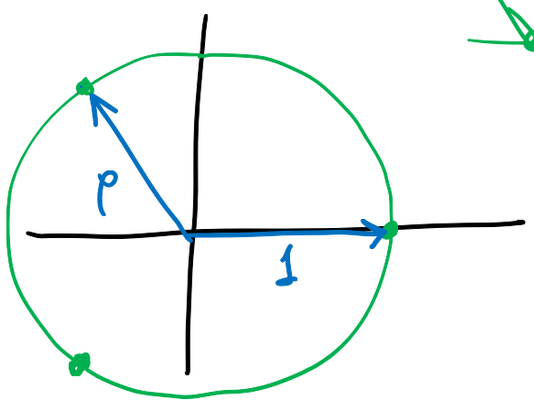
$z \longmapsto iz$ $\quad (i\mathbb{Z}[i] = \mathbb{Z}[i])$

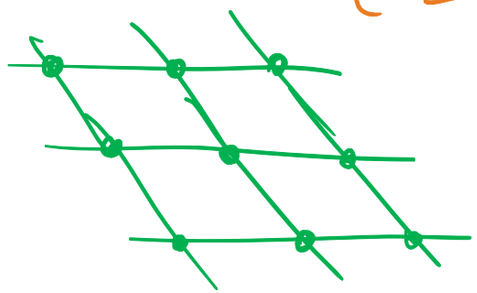
extra endomorphism!

$[i] : (x,y) \longmapsto (-x, iy) \neq [n]$, $n \in \mathbb{Z}$

$z \bmod \mathbb{Z}[i] \longmapsto iz \bmod \mathbb{Z}[i]$

ex $\mathbb{Z}[\rho]$





$\mathbb{C}/\mathbb{Z}[\rho] \cong E(\mathbb{C}) : y^2 = x^3 + 1$

$(x,y) \longmapsto (\rho x, y)$

$\neq [n]$, $n \in \mathbb{Z}$.

$\rho \cdot \mathbb{Z}[\rho] = \mathbb{Z}[\rho]$

$\mathbb{C}/\mathbb{Z}[\rho] \longmapsto \mathbb{C}/\mathbb{Z}[\rho]$

$z \bmod \Lambda \longmapsto \rho \cdot z \bmod \Lambda$

Def. An elliptic function (relative to Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ s.t. $f(z+w) = f(z)$ for all $z \in \mathbb{C}$ and all $w \in \Lambda$.

(In particular, f induces a fn. on $\mathbb{C}/\Lambda$.)

The set of all such functions is $\mathbb{C}(\Lambda)$.

Rk An elliptic fn. with no zeros or poles in $\mathbb{C}$ is constant!

(no zeros or poles $\Longrightarrow$ bounded on a fund. parallelogram

$\Longrightarrow |f(z)|$ is bounded on $\mathbb{C}$

Liouville's thm

$\Longrightarrow f$ is constant on $\mathbb{C}$.)

ex The Weierstrass $\wp$-function.

$$\wp(z) = \wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{(z-w)^2} - \frac{1}{w^2}$$

lwp

(converges uniformly on compact subsets of $\mathbb{C} - \Lambda$. Meromorphic on $\mathbb{C}$ w/ double poles at each $w \in \Lambda$.)

ex Eisenstein series of weight $2k$

$$G_{2k}(\Lambda) = \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{w^{2k}}$$ (absolutely convergent for $k>1$)

NOTE: $$G_{2k}(\alpha\Lambda) = \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{(\alpha w)^{2k}} = \frac{1}{\alpha^{2k}} \cdot \sum \frac{1}{w^{2k}} = \frac{1}{\alpha^{2k}} G_{2k}(\Lambda)$$

$$\left(G_{2k}(\Lambda) = \alpha^{2k} G_{2k}(\alpha\Lambda) \right)$$

Thm If $\Lambda \subseteq \mathbb{C}$ is a lattice, then

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z)).$$

Thm (a) The Laurent series for $\wp(z)$ about $z=0$ is

$$\wp(z) = z^{-2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}(\Lambda)\, z^{2k}$$

(b) For all $z \in \mathbb{C}$, $z \notin \Lambda$,

$$\left(\wp'(z)\right)^2 = 4\,\wp(z)^3 - 60 G_4(\Lambda)\,\wp(z) - 140 G_6(\Lambda).$$

$y^2 = 4x^3 + Ax + B$

Set: $g_2 = g_2(\Lambda) = 60\, G_4(\Lambda)$, $g_3 = g_3(\Lambda) = 140\, G_6(\Lambda)$.

Prop. Let Λ be a lattice w/ g_2, g_3 as above. Let $E/\mathbb{C}$ be $y^2 = 4x^3 - g_2 x - g_3$.

$\cong y^2 = x^3 - \frac{g_2}{4}x - \frac{g_3}{4}$.

Then $E/\mathbb{C}$ is an elliptic curve and

$$\phi : \mathbb{C}/\Lambda \longrightarrow E$$
$$z \longmapsto [\wp(z), \wp'(z), 1]$$

is an iso. of $\mathbb{C}$-Lie gps.

(i.e., it is an iso. of Riemann surfaces which is also a gp hom.)

Fact $\mathbb{C}/\Lambda_1 \cong \mathbb{C}/\Lambda_2 \iff \Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbb{C}^*$

Cor Let $E_1, E_2/\mathbb{C}$ be ell. curves, corresponding to Λ_1, Λ_2 resp.

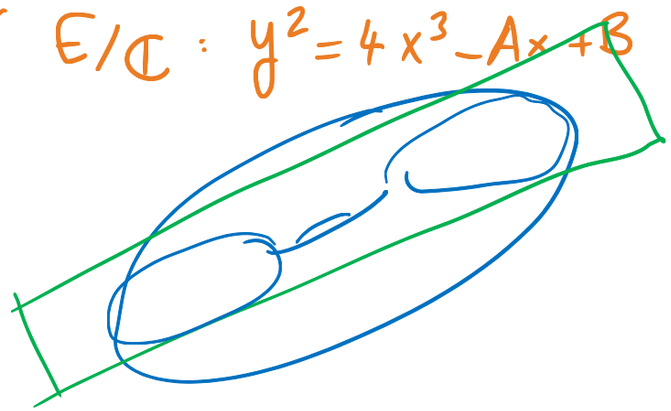
Then $E_1 \underset{\mathbb{C}}{\cong} E_2$ iff $\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbb{C}^*$.

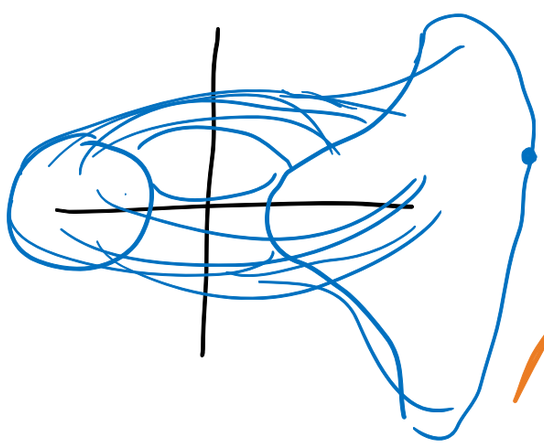
Thm (Uniformization Theorem)

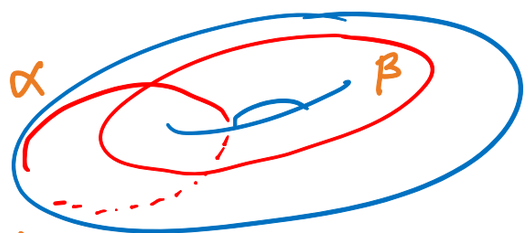
Let $A, B \in \mathbb{C}$, w/ $A^3 - 27B^2 \neq 0$, then there is a unique lattice $\Lambda \subseteq \mathbb{C}$ s.t. $g_2(\Lambda) = A$, $g_3(\Lambda) = B$.

$(\Rightarrow \mathbb{C}/\Lambda \cong E(\mathbb{C})$ w/ $E: y^2 = 4x^3 - g_2 x - g_3)$

$E/\mathbb{C}: y^2 = 4x^3 - Ax + B$







Homology $H_1(E, \mathbb{Z}) = \langle \alpha, \beta \rangle$

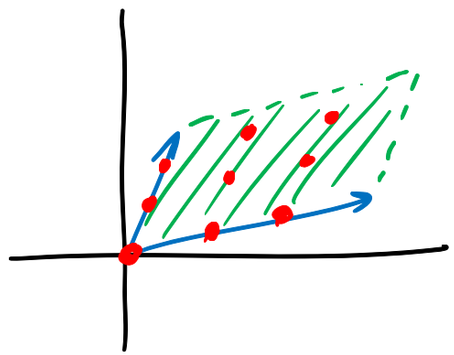
$\Lambda = \left\langle \omega_1 = \int_\alpha \frac{dx}{y},\ \omega_2 = \int_\beta \frac{dx}{y} \right\rangle$

Consequences: E/k, k char 0.

- Recall: $E[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$

- Alternatively: K char 0, $k \subseteq \mathbb{C}$

$$E[m] = E(\mathbb{C})[m] \cong \underbrace{(\mathbb{C}/\Lambda)[m]}$$



$$(\mathbb{C}/\Lambda)[m] \cong \frac{\mathbb{C}/\Lambda}{m(\mathbb{C}/\Lambda)} \cong \frac{\Lambda}{m\Lambda} \cong \frac{\mathbb{Z}\oplus\mathbb{Z}}{m(\mathbb{Z}\oplus\mathbb{Z})}$$

$$\cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

ex $\Lambda = \mathbb{Z}[i]$ satisfies $i \cdot \Lambda = \Lambda$

$\Rightarrow g_3(\Lambda) = g_3(i\cdot\Lambda) = i^{-6} g_3(\Lambda) = -g_3(\Lambda) \Rightarrow g_3(\Lambda) = 0.$

$G_{2k}(\alpha\Lambda) = \alpha^{-2k} G_{2k}(\Lambda)$

$\Rightarrow E : y^2 = 4x^3 - g_2(\Lambda)x \cong y^2 = x^3 - \frac{g_2(\Lambda)}{4}x \underset{\mathbb{C}}{\cong} y^2 = x^3 - x$

$j = 1728$

(Hurwitz: $g_2(\mathbb{Z}[i]) = 64\left(\int_0^1 \frac{dt}{\sqrt{1-t^4}}\right)^4$)

ex $\Lambda = \mathbb{Z}[\rho]$, $\rho \cdot \Lambda = \Lambda \Rightarrow g_2(\Lambda) = g_2(\rho\Lambda) = \rho^{-4} g_2(\Lambda) = \rho^2 g_2(\Lambda)$

$\Rightarrow g_2(\Lambda) = 0$

$\Rightarrow E : y^2 = 4x^3 - g_3(\Lambda)$

$\underset{\mathbb{C}}{\cong} y^2 = x^3 + 1$ $\}$ $j = 0.$