E: Elliptic curves

$E: y^2 = x^3+Ax+B$, here: $A,B\in\mathbb{Z}$ $(E/\mathbb{Z})$

or

$\Delta = -16(4A^3+27B^2) \neq 0$

$\left[\tilde{E}: \tilde{y}^2 = 4\tilde{x}^3 - g_2\tilde{x} - g_3,\ \tilde{\Delta} = 16(g_2^3 - 27g_3) \neq 0\right]$

$$n_p := \#\{\underbrace{(x,y)}_{\text{mod } p} \mid y^2 \equiv x^3+Ax+B\ (p)\}$$

$$= p + \underbrace{\sum_{x(p)} \left(\frac{x^3+Ax+B}{p}\right)}_{\text{small}}$$

← Legendre symbol

$$a_p := p - n_p = -\sum_{x(p)} \left(\frac{x^3+Ax+B}{p}\right)$$

<u>Hasse bound</u>: $|a_p| \leq 2\sqrt{p}$

Dirichlet character mod n (1

$$\chi: \mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow S^1$$

↑ completely multiplicative

$$\chi(m) := 0 \quad \text{if } (m,n) \neq 1$$

<u>Example</u>: Legendre symbol, p odd

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } \underset{\neq 0}{a} = \square^2 \bmod p \\ -1 & \text{if } \underset{\neq 0}{a} \neq \square^2 \bmod p \\ 0 & \text{if } a = 0 \bmod p \end{cases}$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),\quad \left(\frac{a+kp}{p}\right) = ($$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1\ (4) \\ -1 & \text{if } p \equiv 3\ (4) \end{cases}$$

<u>Hasse-Weil-L-function</u>:

$$L_E(s) := \prod_{p\mid\Delta} (1 - a_p p^{-s})^{-1} \prod_{p\nmid\Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

$$\Lambda_E(s) := \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s) L_E(s),$$ where $N\in\mathbb{N}$ is the "conductor" of E.

<u>Conjecture (Hasse)</u>: (very deep)

$L_E(s)$ possesses A.C. to an entire function and satisfies:

$$\Lambda_E(s) = \varepsilon \Lambda_E(2-s), \quad \text{for } \varepsilon \in \{\pm 1\}$$

This conjecture follows from the (stronger) Taniyama-Shimura-Weil / Modularity-conjecture

proved by:

Wiles, Breuil, Conrad, Diamond, Taylor, ...

$\big[L_E(s) = L(f,s)$, for $f \in S_2(\Gamma_0(N))$ a HEF and EF of Fricke involution

We now look at the congruent #-curve (easy):

$E_1: y^2 = x^3 - x$, $\Delta = 64$, $g_3 = 0$ ($\rightsquigarrow \tau = i$)
$\rightsquigarrow$ CM-curve

<u>For $p=2$:</u> $E_1/\mathbb{F}_2 = \{(0,0), \overset{1=-1}{(1,0)}\} \rightsquigarrow n_2 = 2 \rightsquigarrow \underline{a_2 = 0}$

<u>For $p \equiv -1$ (4):</u> $a_p = -\sum_{x(p)} \left(\frac{x^3-x}{p}\right) \underset{\substack{(x \to -x) \\ 1\text{-}1}}{=} \underbrace{\left(\frac{-1}{p}\right)}_{=-1} \left(-\sum_{x(p)} \left(\frac{x^3-x}{p}\right)\right) = 0$

<u>Remains: $p \equiv 1$ (4):</u>

<u>Lemma:</u> $E_1 \setminus \{(0,0)\} \xrightarrow[\text{birationally}]{\cong} E': V^2 = U^4 + 4$

$(y,x) \longmapsto (2x - y^2 x^{-2}, y x^{-1})$

$(\tfrac{1}{2}U(V+U^2), \tfrac{1}{2}(V+U^2)) \longleftarrow\!\shortmid (V,U)$

<u>Pf:</u> ommited (straight forward)

In particular: $n_p = 1 + \#\{(u,v) \mid v^2 \underset{(p)}{\equiv} u^4 + 4\}$

$= 1 + 4\#\{v \mid \underset{\neq 0}{v^2 - 4} = \square^4\} + \underset{\substack{\uparrow \\ v = \pm 2}}{2}$

Let η be a Dirichlet character mod p of order 4, i.e.

$\eta: \mathbb{Z}_p^* \longrightarrow \{\pm 1, \pm i\} \subset S^1$

$v = g^l \longmapsto \eta(v) = i^l$ for some generator g of $\mathbb{Z}_p^*$ $\leftarrow$ cyclic, order $p-1$

$\rightsquigarrow \eta: \mathbb{Z} \to \{\pm 1, \pm i\}$, $\eta(n) = 0$ if $(n,p) \neq 1$, $(\eta(0) = 0)$

<u>Lemma:</u> $a_p = -(J(\eta) + \overline{J(\eta)})$, where $J(\eta) := \sum_{v(p)} \eta(v^2 - 4)$

<u>Proof:</u> $$n_p = 1+2+4\#\underbrace{\{v \mid 0 \neq v^2-4 = \square^4\ (p)\}}_{\Leftrightarrow\ \eta(v^2-4)=1}$$

$$\overset{\text{Claim}}{=} \left[\sum_{v(p)} \underbrace{1+\eta(v^2-4)+\eta^2(v^2-4)+\eta^3(v^2-4)}\right] + 1$$

$$\checkmark \quad = \begin{cases} \dfrac{\eta^4(v^2-4)-1}{\eta(v^2-4)-1} = 0, & \text{if } \eta(v^2-4) \neq 0,1 \\ 1, & \text{if } \eta(v^2-4) = 0 \quad (v=\pm 2) \\ 4, & \text{if } \eta(v^2-4) = 1 \end{cases}$$

$$= p+1+\underbrace{\sum_{v(p)} \eta(v^2-4)}_{J(\eta)} + \underbrace{\overline{\eta(v^2-4)}}_{\overline{J(\eta)}} + \sum_{v(p)} \underbrace{\eta^2(v^2-4)}_{=\left(\frac{v^2-4}{p}\right)}$$

$$\overset{(w=v+2)}{=} \sum_{w(p)} \left(\frac{w^2-4w}{p}\right) = \sum_{w(p)}^{*\ \leftarrow \text{ exclude } 0\ \left(\left(\frac{0}{p}\right)=0\right)} \left(\frac{w}{p}\right)\left(\frac{w-4}{p}\right)$$

$$= \sum_{w(p)}^{*} \underbrace{\left(\frac{w^2}{p}\right)}_{=1} \left(\frac{1-4/w}{p}\right) \underset{(x=-4/w)}{=} \sum_{\substack{x(p)\\ x\neq 1}} \left(\frac{x}{p}\right) = \underbrace{\sum_{x(p)} \left(\frac{x}{p}\right)}_{=0} - \underbrace{\left(\frac{1}{p}\right)}_{=1}$$

$= -1$, so

$$n_p = p+1-1+J(\eta)+\overline{J(\eta)} \Longrightarrow a_p = -J(\eta)-\overline{J(\eta)} \quad \blacksquare$$

We have: $J(\eta) = \sum_{v(p)} \eta(v^2-4) \overset{4}{=} \sum_{w(p)} \eta(w(w-1))$

$$= \eta(-1) \sum_{x(p)} \eta(x)\eta(1-x) = \eta(-1)\, J(\eta,\eta) \leftarrow \text{Jacobi sum}$$

$$J(\chi,\psi) := \sum_{x(p)} \chi(x)\psi(1-x)$$

<u>Lemma</u>: $\chi, \psi, \chi\psi \neq$ trivial, then

$$J(\chi,\psi) = \frac{G(\chi)\,G(\psi)}{G(\chi\psi)}, \text{ where}$$

$$G(\chi) = \sum_{x(p)} \chi(x)\, e^{\frac{2\pi i x}{p}}$$ Gauss sum, <u>known</u>: $\chi \neq$ trivial $\Rightarrow$ $|G(\chi)| = \sqrt{p}$

<u>Proof</u>: $J(\chi,\psi)\,G(\chi\psi) = \sum_{a,b(p)} \chi(a)\psi(a)\chi(b)\psi(1-b)\, e^{\frac{2\pi i a}{p}}$

$$= \sum_{a,b(p)} \chi(ab)\psi(a(1-b))\, e^{\frac{2\pi i a}{p}} = \sum_{\substack{a\neq 0,\\ b}(p)} \chi(ab)\psi(a(1-b))\, e^{\frac{2\pi i a}{p}}$$

$$= \sum_{\substack{u,v(p)\\ u+v\neq 0}} \chi(u)\psi(v)\, e^{\frac{2\pi i u}{p}} e^{\frac{2\pi i v}{p}} + \underbrace{\sum_{b(p)} \chi(0)\psi(0)}_{=0 \ (\mathrm{mod}\ p \neq 1)}$$

$$\left\{\begin{matrix}(a,b)\\ a\neq 0\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}(u=ab,\ v=a(1-b))\\ u+v\neq 0\end{matrix}\right\}$$

$$\left(a=u+v,\ b=\frac{u}{u+v}\right)$$

$$= \sum_{u,v(p)} \chi(u)\psi(v)\, e^{\frac{2\pi i u}{p}} e^{\frac{2\pi i v}{p}} = G(\chi)\,G(\psi)$$ $\blacksquare$

$$\left(\sum_{u(p)} \chi(u) \underbrace{\psi(-u)}_{\psi(u)} \underbrace{e^{\frac{2\pi i u}{p}} e^{\frac{-2\pi i u}{p}}}_{1} = 0\right)$$

Corollary: $a_p = -(J(\eta) + \overline{J(\eta)})$, $J(\eta) \in \mathbb{Z}[i]$, $|J(\eta)| = \sqrt{p}$

$|G(\chi)| = \sqrt{p}$

$$|a_p| \leq 2|J(\eta)| = 2\sqrt{p} \quad \text{(Hasse bound)}$$

and $J(\eta)$ is a Gaussian prime factor of p
(prime # of $\mathbb{Z}[i]$)

Recall: $\mathbb{Z}[i]$ is a PID, units $U = \{\pm 1, \pm i\}$, primes

- $u(1+i)$, $-i(1+i)^2 = 2 \Rightarrow$ 4 prime divisors of 2
- $u \cdot (a+bi)$, $(a+bi)\overline{(a+bi)} = p \equiv 1 \ (4)$ ← case above → 8 prime divisors of p
  splits
- $u \cdot p$, $p \equiv -1 \ (4)$ ← 4 ass. primes, $N(a+bi) = (a+bi)\overline{(a+bi)} = a^2 + b^2$

Q: Which prime divisor of p is $J(\eta)$? (up to conjugation)

We use: $1, -1, i, -1$ mod $\alpha = ((1+i)^3) = (2(1+i))$ are all non-congruent
(they are congruent mod $(1+i)$)

$$J(\eta) = \sum_{0 \leq v \leq p-1} \eta(v^2 - 4) \overset{((-v)^2-4 = v^2-4)}{=} \underset{v=2}{1} + 2 \underbrace{\sum_{\substack{0 < v \leq \frac{p-1}{2} \\ v \neq 2}} \overbrace{\eta(v^2-4)}^{\in \{\pm 1, \pm i\} \equiv 1 \bmod (1+i)}}_{\equiv \frac{p-1}{2} - 1 \bmod (1+i)}$$

$$\equiv 2\left(\tfrac{p-1}{2} - 1\right) = p - 3 \bmod \underset{\alpha}{(2(1+i))}$$

but $p \equiv 1 \ (4)$
and $4 = 2(1+i)(1-i) = \alpha(-i) \equiv 0 \bmod \alpha$

so $J(\eta) \equiv 1 + 1 - 3 = -1 \bmod \alpha$

Lemma: For $p \equiv 1 \ (4)$ we have $a_p = \pi_p + \overline{\pi}_p$, where
$\pi_p \in \mathbb{Z}[i]$ is uniquely determined up to conjugation by $\pi \equiv 1 \bmod \alpha$, $\pi_p \overline{\pi}_p = p$

Remark: This has been done more generally/elegantly by Tate using the adelic interpretation. Here: classical the following

$$\left(\mathbb{Z}[i]/\alpha\right)^* = \{1, -1, i, -i \ (\alpha)\} \quad \left(\longleftrightarrow (\mathbb{Z}/n\mathbb{Z})^*\right) \rightsquigarrow \boxed{\text{character: modulo } (\alpha) \text{ on } \mathbb{Z}[i]}$$

$$\varrho: \mathbb{Z}[i] \longrightarrow U(\mathbb{Z}[i]) = \{\pm 1, \pm i\} \subset S^1 \quad (\longleftrightarrow \mathbb{Z} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \{\pm 1\})$$

$$w \longmapsto \varrho(w) = \begin{cases} u \text{ s.t. } u \cdot w \equiv 1 \ (\alpha), & \text{if } (w, \alpha) = 1 \\ 0, & \text{if } (w, \alpha) = 0 \end{cases}$$

<u>Put:</u> $\chi(w) := \varrho(w) w$

We can consider this as a character on ideals of $\mathbb{Z}[i]$

$$\chi: I(\mathbb{Z}[i]) \longrightarrow \mathbb{Z}[i] \quad (\text{actually to } 1 + (\alpha) \text{ or } 0)$$

$$\underset{\substack{\uparrow \\ \text{determined} \\ \text{up to a unit}}}{(w)} \longmapsto \chi((w)) = \chi(w) = \varrho(w) w \quad (= 0 \text{ if } (w, \alpha) \neq 1)$$

$$N(I = (w)) := N(w) \quad \left(N(u) = \checkmark \text{ well def.}\right), \quad N(w) = |w|^2$$

χ Grossencharacter, invented by Hecke $\rightsquigarrow$ L-Function

$$L(s, \chi) := \prod_{\substack{\mathfrak{P} \text{ prime ideal} \\ \text{in } \mathbb{Z}[i]}} \left(1 - \chi(\mathfrak{P}) N(\mathfrak{P})^{-s}\right)^{-1}$$

$$\underset{\text{(as sheet 4 task 3d)}}{=} \sum_{\substack{I \text{ ideals} \\ \text{in } \mathbb{Z}[i]}} \chi(I) N(I)^{-s} = \sum_{n=1}^{\infty} \left(\sum_{\substack{I \\ N(I) = n}} \chi(I) \right) n^{-s}$$

$$= \frac{1}{4} \sum_{n=1}^{\infty} \left(\sum_{\substack{w \in \mathbb{Z}[i] \\ |w|^2 = n}} \varrho(w) w \right) n^{-s}$$

[χ trivial $\rightsquigarrow$ $L(s, \chi_{\text{triv.}}) = \zeta_{\mathbb{Q}(i)}(s)$ Dedekind-Zeta function for $\mathbb{Q}(i)$

$$= \sum_{I} N(I)^{-s}$$]

Prop: $L(s,\chi) = L_E(s)$

Proof:
$$L_E(s) = \underbrace{\prod_{\substack{p\mid\Delta=64\\ p=2}} (1-\underbrace{a_p}_{=a_2=0} p^{-s})^{-1}}_{=1} \prod_{p\equiv -1(4)} (1-\overbrace{a_p p^{-s}}^{=0}+p^{1-2s})^{-1}$$
$$\prod_{p\equiv 1(4)} (1-\underbrace{(\pi_p+\overline{\pi}_p)}_{a_p} p^{-s}+p^{1-2s})$$

On the other hand:
$$L(s,\chi) = \prod_{(1+i)} (\ )^{-1} \prod_{\substack{(p)\\ p\equiv -1(4)}} (\ )^{-1} \prod_{\substack{(\pi),(\overline{\pi})\\ N(\pi)=p\equiv 1\ (4)}} (\ )^{-1}$$
$$= \underbrace{(1-\underbrace{\chi(1+i)}_{=0}\underbrace{N(1+i)}_{=2}{}^{-s})^{-1}}_{=1} \prod_{\substack{(p)\\ p\equiv -1(4)\\ (\rho(p)=-1)}} (1-\overbrace{\underbrace{\rho(p)\cdot p}_{\overset{\text{indep. of rep.}}{=p}}\, N(p)^{-s}}^{p^{-2s}})^{-s}$$
$$\cdot \prod_{\substack{p\equiv 1(4)\\ p=\pi\overline{\pi}}} (1-\rho(\pi)\pi \underbrace{N(\pi)^{-s}}_{p^{-s}})(1-\overline{\rho(\pi)\pi}\, p^{-s})$$
$$= \prod_{p\equiv -1(4)} (1+p^{1-2s}) \prod_{p\equiv 1(4)} (1-\overbrace{(\rho(\pi)\pi+\overline{\rho(\pi)\pi})}^{=a_p\,!}p^{-s} + \underbrace{\rho(\pi)\overline{\rho(\pi)}\,\pi\overline{\pi}}_{1\cdot p})$$
$$= L_E(s) \quad \blacksquare$$

By applying the inverse Mellin-transform to $L(s,\chi)$ we get a Theta-function (studied by Hecke):

$$\Theta_\chi := \frac{1}{4}\sum_{\alpha\in\mathbb{Z}[i]} \rho(\alpha)\,\alpha\, e(z|\alpha|^2)$$
using Poisson summation we find its transf. behaviours

↪ By applying the Mellin-transformation this gives:

$\Lambda_E(s) \overset{?}{=} \pm \Lambda_E(2-s)$ Hasse's conjecture for E_1

actually one can show: (a bit more work) $\Theta_\chi \in S_2(\Gamma_0(32))$ + Θ_χ is HEF + EF of Fricke involution!

(Taniyama-Shimura-Weil-conjecture for E_1)

Slightly more general: congruent number "-elliptic curves

$$E_n: y^2 = x^3 - n^2 x, \qquad n>0 \text{ squarefree}, \quad \Delta = 64\cdot n^2,$$
$$a_p = 0 \text{ for } p \mid \Delta$$

$$a_{p,r} = -\sum_{x(p)} \left(\frac{x^3 - r^2 x}{p}\right) \overset{x \mapsto rx}{=} - \underbrace{\left(\frac{r^3}{p}\right)}_{=\left(\frac{r}{p}\right) = \chi_r(n)} \sum_{x(p)} \left(\frac{x^3 - r^2 x}{p}\right)$$

$$= \left(\frac{r}{p}\right) \underbrace{a_p}_{\text{from } E_1}$$

$$\rightsquigarrow L_{E_r}(s) = \prod_{p \neq 2} \left(1 - \chi_r(p)\, a_p\, p^{-s} + \chi_r^2(p)\, p^{1-2s}\right)^{-1}$$
$$= \sum \chi_r(n)\, a(n)\, n^{-s} = L_E(s, \chi_r)$$
$$= L(s, \chi, \chi_r)$$
$$= L(s, \Theta_\chi, \chi_r)$$

Def: $n \in \mathbb{Z}_{>0}$ (squarefree) is a congruent # iff n is the area of a right angled triangle with rational sides.

Lemma:
$$\underbrace{E_n \setminus \{(*,0)\} /_{\mathbb{Q}}}_{\{(y,x) \in \mathbb{Q}^2 \mid y^2 = x^3 - n^2 x,\ y \neq 0\}} \overset{\cong \text{ birational}}{\underset{1-1}{\longleftrightarrow}} \{(a,b,c) \in \mathbb{Q}^3 \mid a^2 + b^2 = c^2,\ \tfrac{ab}{2} = n\}$$

$\neq \emptyset$ iff n is a congruent number

$$\Big(\underset{= y}{\frac{2n^2}{c-a}}, \underset{= x}{\frac{nb}{c-a}}\Big) \longleftarrow\!\shortmid \ (a,b,c)$$

$$(y, x) \longmapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right)$$

$\{P \in E_n \text{ with } y = 0\} = E_n[2](\mathbb{Q})$ torsion points and these are the only ones

Corollary: n is a congruent number $\Longleftrightarrow$ $E_n(\mathbb{Q})$ has infinitely many points

$$\Longleftrightarrow \operatorname{rk}(E_n(\mathbb{Q})) > 0 \underset{\text{BSD}}{\Longleftrightarrow} L_{E_n}(1) = L(1, \Theta_\chi, \chi_r) \overset{!}{=} 0$$

Prop (Waldspurger)

$L(1, \Theta_\chi, \chi_r) = b(r)^2 \cdot \overset{0}{\overset{\#}{c}}$, where $b(r)$ is the r^{th} coefficient of ~~the~~ some Shimula lift of Θ_χ :

modular forms of half integer weight $\frac{k}{2} \longleftrightarrow$ modular forms of weight k

$$f \rightsquigarrow L(f \times \Theta, s) = L(F, s)$$

F of weight $k-1$

Here $L(1, \Theta_\chi, \chi_r) = 0$ iff $b(r) = 0$

Prop (Tunnel)

$b(r) =$ (some counting formula)

Corollary: n congruent # iff (some counting formula) $= 0$