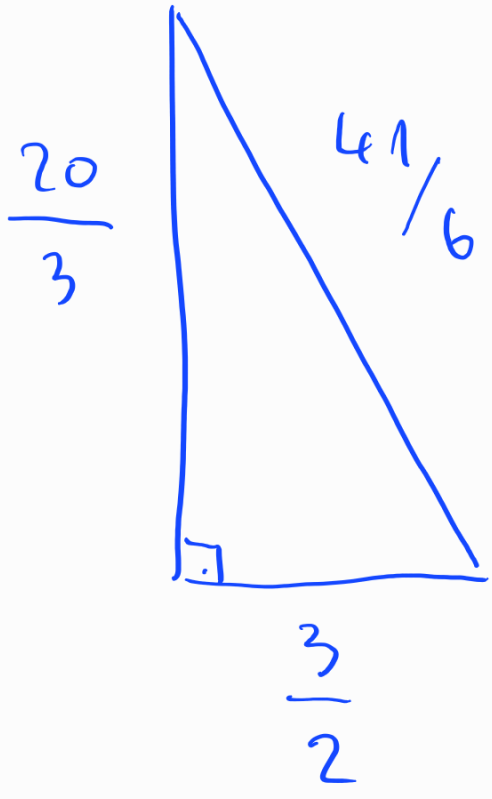
Congruent number problem

N. Koblitz: Introduction to Elliptic Curves and Modular Forms

kongruentan broj (congruent number)

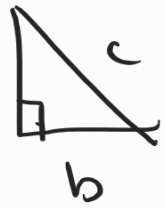
Problem: Odredite sve prirodne brojeve n koji su jednaki površini nekog pravokutnog trokuta s racionalnim stranicama.

↑ proučavan u 10. st. arapski matematičari



$P = 5$ (najmanj.) je kongruentan broj

D.z. Dokažite da 1 nije kongr. broj.

Neka je 

i $\frac{1}{2}ab = n$, onda

za $x = \frac{n(a+c)}{b}$ i $y = \frac{2n^2(a+c)}{b^2}$ vrijedi

$$E_n : y^2 = x^3 - n^2 x$$

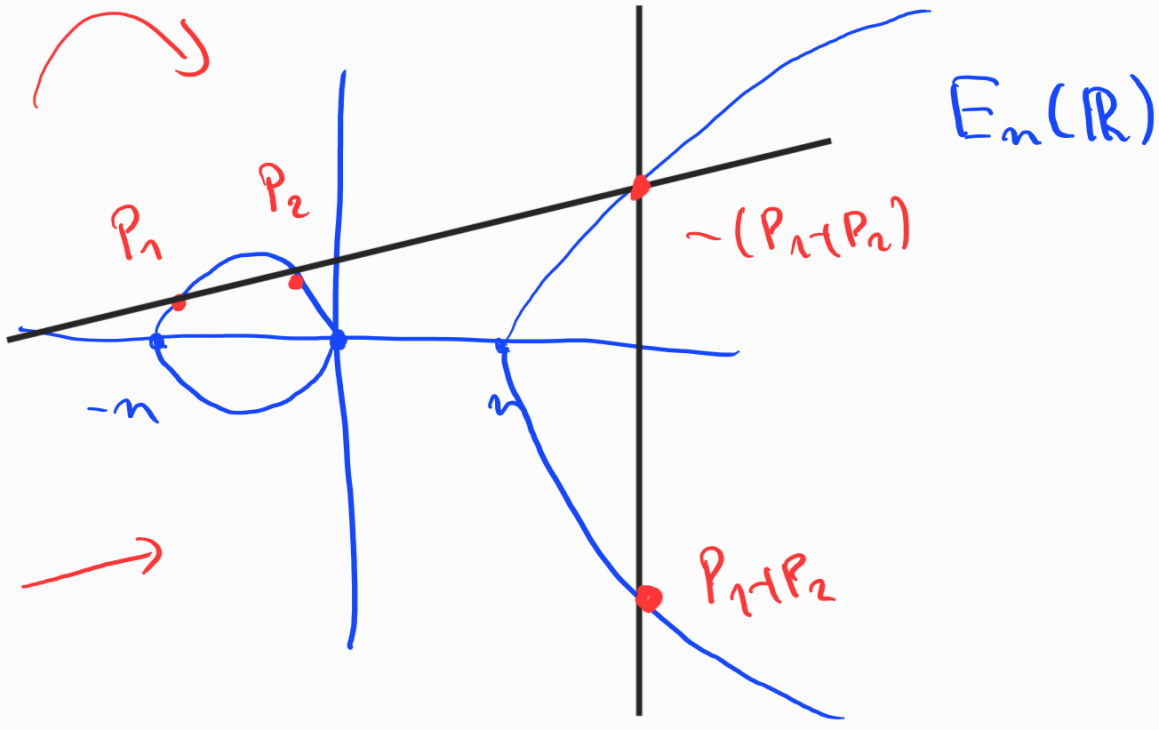
eliptička krivulja nad $K = \mathbb{Q}$

(krivulja genusa 1 s K-racionalnom točkom)

- $E_n(\mathbb{Q})$ – skup $\mathbb{Q}$-racionalnih točaka

(zajedno s točkom u beskonačnosti)

grupa!



asocijativnost → mi je očita

Mordell-Weilov teorem $\Rightarrow E_n(\mathbb{Q})$ je konačno-generirana grupa

$$E_n(\mathbb{Q}) \simeq \mathbb{Z}^{r} + E_{tor}$$

(E_{tor}: konačna grupa; r: rang eliptičke krivulje)

Teorem (d.z.): n je kongruentni broj ako i samo ako $\text{rang}(E_n(\mathbb{Q})) > 0$.

Zeta funkcija eliptičke krivulje (E_n)

Fiksirajmo p prost, $p \nmid 2n$. (kondaktor) Označimo

$$N_r = N_{r,p} = \#E_n(\mathbb{F}_q) \quad \text{gdje je } q = p^r.$$

broj rješenja u $\mathbb{F}_q$ + točka u ∞

Def:

$$Z(E_n/\mathbb{F}_p; T) := \exp\left(\sum_{r=1}^{\infty} \frac{N_r \cdot T^r}{r}\right).$$

racionalna funkcija

Teorem:

$$Z(E_n/\mathbb{F}_p; T) = \frac{1 - a_p \cdot T + p T^2}{(1-T)(1-pT)}$$

gdje je $a_p = p + 1 - \#E_n(\mathbb{F}_p)$.

Sličan rezultat vrijedi za sve nesingularne projektivne alg. mnogostrukosti nad konačnim poljima $\rightsquigarrow$ **Weilove slutnje** [1949]

$\rightarrow$ dokazano Deligne 1973 (etale cohomology)

u slučaju krivulja:

i) zeta fja. se racionalna fja.

ii) stupanj brojnika je $2 \cdot \text{genus}$

iii) ako je $\frac{1}{\alpha}$ nultočka brojnika, onda je to i $\frac{\alpha}{p}$

iv) $\left|\frac{1}{\alpha}\right| = \sqrt{p}$

Krivulja E_m je posebna (kažemo da ima kompleksno množenje), pa se a_p može eksplicitno izračunati!

$$a_p = \begin{cases} \pm 2 \cdot a, & p \equiv 1 \ (4) \quad \text{gdje je } a^2 + b^2 = p \text{ i } a \text{ neparan} \\ 0, & p \equiv 3 \ (4) \end{cases}$$

Hasse-Weilova L-funkcija $L(E_m, s)$

$$L(E_m, s) := \frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E_m/\mathbb{F}_p, p^{-s})}$$

$$= \prod_{p \nmid 2m} \frac{1}{1 - a_p \cdot p^{-s} + p^{1-2s}}$$

Eulerovi faktori se mogu definirati i za $p \mid 2m$

$$= \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

a_n - ovi se mogu lako izračunati pomoću a_p - ovih ... npr.

$a_{mn} = a_m \cdot a_n$ za $(m,n) = 1$.

Dirichletov red, konvergira za $\operatorname{Re} s > \frac{3}{2}$!

Riemannova zeta funkcija se može neprekidno proširiti do $\mathbb{C}$. Što je s $L(E,s)$?

Teorem o modularnosti:

Isto vrijedi za $L(E,s)$ (nema polova).

Kako konstruirati analitičko proširenje?

↝ Modularne forme

Već se javljaju kod analitičkog proširenja $\zeta(s)$!

Mellinova transf. tlete funkc.

Ideja $\zeta(s)$ "$= \int_0^{+\infty} \Theta(t)\, t^s \frac{dt}{t}$"

gdje je $\Theta(t) := \sum_{n=-\infty}^{+\infty} e^{-\pi t \cdot n^2}$ za $t > 0$.

Tada analitičko proširenje od $\zeta(s)$ kao i funkcijsku jednadžbu slijedi iz funkcijske jednadžbe

$$\Theta(t) = \frac{1}{\sqrt{t}}\, \Theta(1/t).$$

$\check{\Theta}(\tau) = 1 + \sum_{n=1}^{\infty} q^{n^2}$ i gdje je $q = e^{\pi i \tau}$,

je modularna forma težine $1/2$.

esencijalno

Def. (modularna forma) Neka je $\Gamma < SL_2(\mathbb{Z})$ podgrupa i $k \in 2\mathbb{N}$. Kažemo da je holomorfna fja. $f: \mathbb{H} \to \mathbb{C}$ modularna forma težine k za podgrupu Γ ako za svaku matricu $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ vrijedi

$\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau), \quad \forall \tau \in \mathbb{H}$$

i ako je f holomorfna u kaspovima.

Ako f poništava sve kaspove, onda kažemo da je f kasp forma. Oznake:

$M_k(\Gamma) \supset S_k(\Gamma)$

↑ kasp forme

Teorem o modularnosti: $E/\mathbb{Q}$ el. krivulja konduktora N. Tada je

$$f_E(\tau) = \sum_{n=1}^{\infty} a_n q^n \in S_2(\Gamma_0(N))$$

gdje je $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : N \mid c \right\}$

U tom slučaju

$$L(E,s) \text{"}=\text{"} \int_0^{i\infty} f_E(i\tau)\, t^s \frac{dt}{t},$$

kao i funkcijska jednadžba

pa holomorfno proširenje Dirichletovog reda

$L(E,s)$ slijedi iz funkcijske jednadžbe

od f_E.

Sad samo spremni za BSD - slutnju!

Birch i Swinnerton-Dyerova slutnja

Funkcijska jednadžba povezuje $L(E,s)$ i $L(E,2-s)$. Točka $s=1$ je u "centru" pa zato broj $L(E,1)$ zovemo kritičnu vrijednost L-funkcije.

Slutnja (BSD) $L(E,1)=0$ ako i samo ako je $\operatorname{rang}(E/\mathbb{Q})>0$, tj. ako i samo ako je skup $E(\mathbb{Q})$ beskonačan.

Općenitije, ako je r red poništavanja fje. $L(E,s)$ u $s=1$ (još taj broj zovemo **analitički rang**), onda je $\operatorname{rang}(E/\mathbb{Q})=r$.

↗ algebarski rang.

Slutnja originalno nije bila formulirana

preko L-funkcija nego preko produkta:

Vanjski:

$$\prod_{\substack{p \le x \\ (p \nmid N_E)}} \frac{\#E(\mathbb{F}_p)}{p} \sim A (\log x)^{\text{rang}(E)}$$

(sumnjiva) heuristika: e.k. visokog ranga će imati "puno" točaka mod p

gdje je $A > 0$ neka konstanta.

Veza s L-funkcijom je preko Eulerovog produkta

u točki $s=1$:

$$\left. \frac{1}{1 - a_p p^{-s} + p \cdot p^{1-2s}} \right|_{s=1}$$

$$= \frac{p}{p+1-a_p} = \frac{p}{\#E(\mathbb{F}_p)}$$

Što se zna o BSD?

(Kolyvagin) $L(E,1) \neq 0 \Rightarrow \text{rang}(E) = 0$

(Gross-Zagier) Ako je $r=1$ onda $\text{rang}(E) > 0$.

↑ konstruirali su točku beskonačnog reda

(Možda kasnije: kako računati $L(E,1)$?)

Natrag na congr. number problem...

Modularne forme pola-cijele težine

↑ nećemo definirati...

samo primjer ↓

Propozicija: Neka su $\Theta(\tau) = 1 + 2\sum_{n=1}^{\infty} q^{n^2}$

i $F(\tau) = \sum_{\substack{n>0 \\ \text{neparan}}} \sigma_1(n) q^n$. Pritom je (težina?) stupanj

$\frac{1}{2}$ (težina) fji. Θ i stupanj 2 fji. F. Tada je

$M_{k/2}(\tilde{\Gamma}_0(4))$ (metaplektička kovrt od $\Gamma_0(4)$) prostor svih polinoma

u $\mathbb{C}[\Theta, F]$ stupnja $k/2$

Zašto nam trebaju? Postoje modularne forme čiji Fourierovi koef. sadrže informaciju o $L(E_m, 1)$!

Shimura, Waldspurger, Tunnell ...

Teorem (Tunnel) Postoji forma

$$f = \sum a_n q^n \in S_{3/2}(\tilde{\Gamma}_0(128)) \quad i$$

forma $f' = \sum a'_n q^n \in S_{3/2}(\tilde{\Gamma}_0(128))$

realni parni

takva da je $\beta := \int_1^\infty \frac{dx}{\sqrt{x^3 - x}} = 2.622\ldots$

$$L(E_n, 1) = \begin{cases} \frac{\beta}{4\sqrt{n}} a_n^2 & za\ n\ neparan \\ \frac{\beta}{2\sqrt{n}} a'^2_{n/2} & za\ n\ paran \end{cases}$$

Poseban, $L(E_n, 1) = 0$ ako i samo ako

$a_n = 0$ (za n neparan) ili $a'_{n/2} = 0$ (za n paran).

Konkretno

$$f(\tau) = \left(\Theta(\tau) - \Theta(4\tau)\right)\left(\Theta(32\tau) - \frac{1}{2}\Theta(8\tau)\right)\Theta(2\tau)$$

i $f'(\tau) =$ —||— $\Theta(4\tau)$

↑ ↗

možemo izračunati koeficijente, sve ji eksplicitno.

Teorem (Tunnell) Neka je n kvadratnoslobodan i neparan (slična tvrdnja vrijedi i za parne n) prirodan broj. Ako je n površina pravokutnog trokuta s racionalnim stranicama tada vrijedi

$$\#\{(x,y,z) \in \mathbb{Z}^3 \mid n = 2x^2 + y^2 + 32z^2\} =$$

$$\frac{1}{2}\#\{(x,y,z) \in \mathbb{Z}^3 \mid n = 2x^2 + y^2 + 8z^2\}$$

Ako vrijedi BSD slutnja za krivulje E_n

onda vrijedi i obrat.