Hanoi, School & Workshop. (2024. 10. 28 –)

Lecture 1. Elliptic curves

< Affine & projective algebraic sets >

Def. Let K be a field ($K=\mathbb{C}$, $\mathbb{R}$ or $\mathbb{Q}$, $\mathbb{F}_q$, $\overline{\mathbb{F}}_q$, $\mathbb{Q}_p$).

The n-dim'l affine space is $\mathbb{A}^n(K) = \{(a_1, \dots, a_n) \mid a_i \in K\}$.

Define a relation on $\mathbb{A}^{n+1}(K) - \{(0,\dots,0)\}$ by

$(a_0, \dots, a_n) \sim (b_0, \dots, b_n)$ in $\mathbb{A}^{n+1}(K) - \{(0,\dots,0)\}$

$\Leftrightarrow \exists\, c \in K^\times$ (i.e. $K - \{0\}$) s.t. $(a_0, \dots, a_n) = (cb_0, \dots, cb_n)$.

Then, $\sim$ is an equivalence relation on $\mathbb{A}^{n+1}(K) - \{(0,\dots,0)\}$.

The n-dim'l projective space is

$$\mathbb{P}^n(K) := \mathbb{A}^{n+1}(K) - \{(0,\dots,0)\} \Big/ \sim$$

$\ni (a_0 : a_1 : \cdots : a_n)$, an equivalence class.

Fact. (1) Let $U_i := \mathbb{P}^n(K) \cap \{(x_0 : \cdots : x_n) \mid x_i \neq 0\}$.

$$= \{(x_0/x_i : x_1/x_i : \cdots : \underbrace{1}_{i\text{-th}} : \cdots : x_n/x_i) \mid \underset{x_i \in K-\{0\}}{x_j \in K}\}.$$

So $\exists$ a bijection $U_i \longrightarrow \mathbb{A}^n(K)$ by

$$(x_0/x_i : \cdots : 1 : \cdots x_n/x_i) \longmapsto (x_0/x_i, \dots, \widehat{x_i/x_i}, x_{i+1}/x_i, \dots, x_n/x_i)$$

i.e. ith place is omitted.

So $\mathbb{P}^n(K)$ can be covered by $n+1$ "open" sets U_i each of which is bijective to $\mathbb{A}^n(K)$.

(2) $\mathbb{P}^n(K) = \mathbb{A}^n(K) \sqcup \mathbb{A}^{n-1}(K) \sqcup \cdots \sqcup \mathbb{A}^1(K) \sqcup \{\text{a point}\}$.

(disjoint union)

By Induction,

$n=1$: $(a_0 : a_1) = \begin{cases} (a_0/a_1 : 1) & \text{if } a_1 \neq 0 \longrightarrow \mathbb{A}^1(K) \\ (a_0 : 0) & \text{if } a_1 = 0 \longrightarrow \{\text{a pt} = (1:0)\}. \end{cases}$ disjoint

$(a_0 : 0) \overset{\times a_0}{\sim} (1:0)$

So $\mathbb{A}^1(K) \sqcup \{\text{a pt}\}$

$n=2$: $(a_0 : a_1 : a_2) = \begin{cases} (a_0/a_2 : a_1/a_2 : 1) & \text{if } a_2 \neq 0. \longrightarrow \mathbb{A}^2(K) \\ (a_0 : a_1 : 0) & \text{if } a_2 = 0 \end{cases}$ disjoint.

$\rightsquigarrow \mathbb{P}^1(K)$.

So $\mathbb{A}^2(K) \sqcup \mathbb{P}^1(K) = \mathbb{A}^2(K) \sqcup \mathbb{A}^1(K) \sqcup \{\text{a pt}\}$.

Def. (1) Let $f \in K[x_1, \cdots, x_n]$ be a nonzero poly. over K.

$$V_K(f) := \{(a_1, \cdots, a_n) \in \mathbb{A}^n(K) \mid f(a_1, \cdots, a_n) = 0\}.$$

called an affine alg. set, (hyperplane by f.)

For $f_1, \cdots, f_r \in K[x_1, \cdots, x_n]$, nonzero,

$I = (f_1, \cdots, f_r)$ ideal.

$$V_K(I) := \bigcap_{i=1}^{r} V_K(f_i)$$

(2) Let $F \in K[x_0, \cdots, x_n]$ be a nonzero homogeneous poly. over K.

(i.e. each term of F has the same total degree.)

Then, for $c \in K^\times$, $F(cx_0, \cdots, cx_n) = c^{\deg(F)} F(x_0, \cdots, x_n)$.

So $F((a_0 : a_1 : \cdots : a_n)) = 0 \iff F(a_0, a_1, \cdots, a_n) = 0$.

well-defined.

& $V_K(F) := \{(a_0 : \cdots : a_n) \in \mathbb{P}^n(K) \mid F(a_0 : \cdots : a_n) = 0\}$

called a projective alg. set by F.

(It is called a proj. variety if it is irred., i.e. $V_K(F) \neq V_1 \cup V_2$)

Def. Homogenization: If $f \in K[x_1, \cdots, x_n]$ of degree n (highest deg.),

$F(x_0, x_1, \cdots, x_n) := x_0^n f\left(\frac{x_1}{x_0}, \cdots, \frac{x_n}{x_0}\right)$ is homogeneous of degree n.

Dehomogenization: If $F \in K[x_0, \cdots, x_n]$ is homogeneous of deg. n,

$f(x_1, \cdots, x_n) := F(1, x_1, \cdots, x_n)$ is dehomogenization at x_0.

So $V_K(F) \approx V_K(f) \subseteq \mathbb{A}^n \cup V_K(F(0, x_1, \cdots, x_n)) \subseteq \mathbb{P}^{n-1}$.

Ex. $F(x, y, z) = x^n + y^n - z^n$ $(\Rightarrow f(x, y, 1) = x^n + y^n - 1.)$

$z = 0 \Rightarrow x^n + y^n = 0 \Rightarrow (x : y : 0) \in V_K(x^n + y^n)$

$z \neq 0 \Rightarrow \left(\frac{x}{z}\right)^n + \left(\frac{y}{z}\right)^n = 1 \Rightarrow (x' : y' : 1) \in V_K(f)$.

< Elliptic curves >

Def. Let K be a field (with char $\neq 2, 3$.) (Let's check $=0$.)

An elliptic curve over K is a smooth projective curve of genus 1 in $\mathbb{P}^2_K$ with a point defined over K.
(called a K-rational point)

It can be defined by a smooth cubic equation over K :

$$E/K : y^2z + a_1xyz + a_2yz^2 = x^3 + a_3x^2z + a_4xz^2 + a_5z^3, \quad a_i \in K.$$ in $\mathbb{P}^2$

$z=0$: $x^3=0 \Rightarrow (0:Y:0) = (0:1:0) \in E(K)$.

$z\neq 0$: $x' = \frac{x}{z}$, $y' = \frac{y}{z}$, $\Rightarrow y'^2 + a_1x'y' + a_2y' = x'^3 + a_3x'^2 + a_4x' + a_5$.

& moreover, by change of variables, we can eliminate x'^2-term, & $x'y'$ & y'-term if char $\neq 2,3$,
So in general, it can be defined by the affine equation

$$E/K : y^2 = x^3 + ax + b, \quad a, b \in K$$

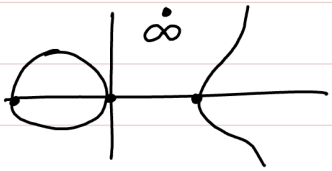
s.t. $\Delta := -2^4(4a^3 + 27b^2) \neq 0$ ← it has 3 distinct zeros.
(Δ : discriminant of x^3+ax+b)

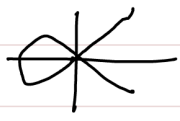
called a Weierstrass eq'n.

together with a K-rational point $(0:1:0) =: \infty$.

Ex. $y^2 = x(x-a^n)(x+b^n)$ for $a^n + b^n = c^n$. Frey Curve.

Ex : $y^2 = x^3 - x$ over $\mathbb{R}$



Non-Ex :
- $y^2 = x^3$: not smooth at $(0,0)$,  cusp
- $y^2 = x^3 + x^2$: not smooth at $(0,0)$,  node

~~Let K be a # field. (i.e. an ext'n over $\mathbb{Q}$ s.t. $[K:\mathbb{Q}] < \infty$)~~

Def. For an elliptic curve over K, E/K : $y^2 + a_1xy + a_2y = x^3 + a_3x + a_4$

$$E(K) := \{(x,y) \in K \times K \mid y^2 + a_1xy + a_2y = x^3 + a_3x + a_4\} \cup \{\infty\}.$$

the set of K-rational points of E.

Ex. $E/\mathbb{Q} : y^2 = x^3 + 17$. Easy to see that $(2,5), (-1,4) \in E(\mathbb{Q})$.

Q. Can we find more $\mathbb{Q}$ or K-rational points of E? How many?

< Groups >

Def. G is called a group, if it satisfies $(G1)\sim(G3)$ under a binary operation $*: G\times G \to G$:

$(G1)$ $*$ is associative

$(G2)$ $\exists\ e\in G$ s.t. $e*a = a = a*e$ for $\forall a\in G$ (identity)

$(G3)$ For each $a\in G$, $\exists\ a^{-1}\in G$ s.t. $a*a^{-1} = e = a^{-1}*a$. (inverse)

If $a*b = b*a$ for $\forall a, b\in G$, G is called abelian.

Ex. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +_{\bmod n})$: abelian grps.

$(M_n(\mathbb{R}), +)$, $(GL_n(\mathbb{R}), \cdot)$, $(SL_2(\mathbb{Z}), \cdot)$.

Def. G is called a cyclic grp, if $\exists\ a\in G$ s.t. $G = \{a^n \mid n\in\mathbb{Z}\} = \langle a\rangle$.

G is called f.g. if $\exists\ \{a_1, \dots, a_n\}\subseteq G$ s.t. $G = \{a_{i_1}^{m_1}\cdots a_{i_k}^{m_k} \mid m_i\in\mathbb{Z},\ a_{i_j}\in S\} = \langle a_1, \dots, a_n\rangle$. (generating set $= S$)

Ex. ① $(\mathbb{Z}, +) = \langle 1\rangle$. cyclic. $(S_3, \circ) = \langle (123), (12)\rangle$ not cyclic, not abelian.

② $(SL_2(\mathbb{Z}), \cdot) = \langle S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\rangle$.

Note that even if G is infinite, but G is f.g., then we can just list a generating set of G to represent G explicitly.

Thm. (Fundamental thm of finitely generated abelian grps)

If G is a f.g. abelian grp,

then $G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$.

($\mathbb{Z}^r$: free subgrp of G; $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$: torsion subgrp. of G.)

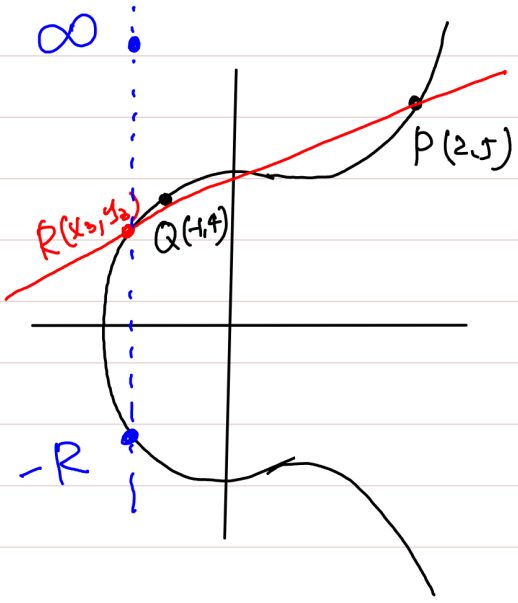
r = rank of G.

Ex. $\begin{cases} \mathbb{Z} \text{ is a f.g. abelian grp. of rank 1 \& trivial torsion.} \\ \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}/2 \text{ is a f.g. abelian grp. of rank 2 \& torsion } \mathbb{Z}/2. \end{cases}$

< Group law on $E(K)$ >

Let's go back to Ex. : $E/\mathbb{Q}: y^2 = x^3 + 17$,

recall that $P = (2,5)$, $Q = (-1,4) \in E(\mathbb{Q})$.



(How to define a binary operation)

(1) Find the secant line connecting P & Q.

$$L: \ y - 5 = \frac{5-4}{2-(-1)}(x-2)$$

$$\Leftrightarrow \ y = \frac{1}{3}x + \frac{13}{3}$$

(2) Find the 3rd intersection point $R = (x_3, y_3)$ of the line L & the curve E. (by Bézout's theorem)

Set $\begin{cases} y = \frac{1}{3}x + \frac{13}{3} \\ y^2 = x^3 + 17 \end{cases}$ ⊛

$$\Rightarrow \ x^3 + 17 = y^2 = \left(\frac{1}{3}x + \frac{13}{3}\right)^2$$

$$\Rightarrow \ x^3 - \frac{1}{9}x^2 + \square x + \square = 0 \ \text{⊛ has zeros that are } x\text{-coordinates of P, Q \& R.}$$

$2, -1$ & x_3

So $\quad 2 + (-1) + x_3 = \frac{1}{9} \ \Rightarrow \ \boxed{x_3 = -\frac{8}{9}}$

& $y_3 = \frac{1}{3}x_3 + \frac{13}{3} = \boxed{\frac{109}{27}}$.

So $\quad R = \left(-\frac{8}{9}, \frac{109}{27}\right) \in E(\mathbb{Q})$

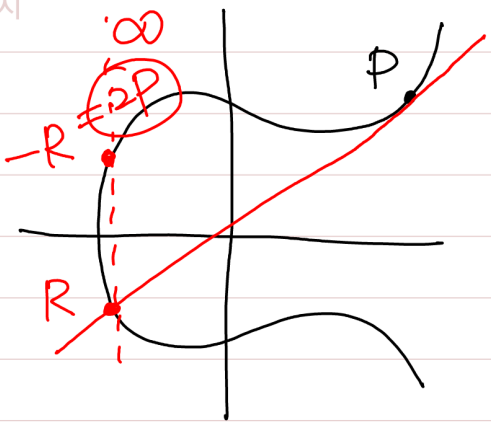
(3) Define $P + Q$ = the reflection of R about x-axis.

$$= \left(-\frac{8}{9}, -\frac{109}{27}\right) \in E(\mathbb{Q}).$$

(4) For $P+P$, we let L be the tangent line at P of E.

$2yy' = 3x^2 \ \Rightarrow \ y' = \frac{3x^2}{2y} \ \Rightarrow$ slope of L at P is $\frac{-3 \cdot 5^2}{2 \cdot 4} = \left(\frac{-75}{8}\right)$

$$\Rightarrow \ L: \ y - 5 = -\frac{75}{8}(x-4) \ \Rightarrow \ \boxed{y = -\frac{75}{8}x + \frac{85}{2}}$$



Then L intersects E at P, P & the 3rd intersection $R=(x_3, y_3)$.

Set $\begin{cases} y = -\frac{75}{8}x + \frac{85}{2} \\ y^2 = x^3 + 17. \end{cases}$

$\Rightarrow x^3 + 17 = \left(-\frac{75}{8}x + \frac{85}{2}\right)^2$

$\Leftarrow$ has zeros which are the x-coords of P, P & R, so,

$2 + 2 + x_3 = \left(\frac{75}{8}\right)^2 \Rightarrow \boxed{x_3 = \frac{75^2}{64} - 4 = \frac{5369}{64}}$

& $\boxed{y_3 = -\frac{75}{8}x_3 + \frac{85}{2}.} = -\frac{380915}{512}.$

$\Rightarrow R = \left(\frac{5369}{64}, -\frac{380915}{512}\right) \in E(\mathbb{Q})$

(5) Define $2P = P+P =$ reflection of R about x-axis

$= \left(\frac{5369}{64}, \frac{380915}{512}\right) \in E(\mathbb{Q}).$

K: # field

Recitation: Try to find the formulae of $P+Q$ & $2P$ for $E/K: y^2 = x^3 + ax + b$, $a, b \in K$ & $P=(x_1, y_1)$ & $Q=(x_2, y_2) \in E(K)$,

& make sure that $P+Q$ & $2P$ are K-rational.

Thm. For $P_1, P_2, P_3 \in E(K)$,

(1) $P_1 + P_2 \in E(K)$ (by formula) So $E(K)$ is closed under the operation

(2) $P_1 + P_2 = P_2 + P_1$ (clearly by construction), so abelian

(3) $P_1 + (P_2 + P_3) = (P_1 + P_2) + P_3$. so associative. (very messy to check)

Notations/Definitions:

(1) For $P=(x,y) \in E(K)$, set $-P = (x, -y) \in E(\mathbb{Q})$ inverse

(2) Define $P + (-P) = \infty$ (since they are collinear)

(3) For $P = \infty \in E(K)$, set $\infty + \infty = \infty$ & $-\infty = \infty$.

(4) For $P \neq \infty \in E(K)$, Set $n \cdot P = \begin{cases} \underbrace{P + \cdots + P}_{n \text{ times}} & \text{if } n > 0 \\ \infty & \text{if } n = 0 \\ \underbrace{(-P) + \cdots + (-P)}_{-n \text{ times}} & \text{if } n < 0. \end{cases}$

Lecture 2. Mordell-Weil Thm.

Q. What is the group structure of $E(K)$?

Thm. (Mordell-Weil Thm) For a number field K & an elliptic curve E/K, $E(K)$ is a f.g. abelian gp.

so $E(K) \cong \mathbb{Z}^r \times E(K)_{tor}$.

r = rank of E over K.

So this implies that $r < \infty$ & $E(K)_{tor}$ is a finite set.

& $E(K) = \langle \underbrace{P_1, \dots, P_r}_{\text{of infinite order}}, \underbrace{Q_1, \dots, Q_t}_{\text{torsion points}} \rangle$

Remark. There is no efficient algorithm to compute r or classify $E(K)_{tor}$.

(Some known results on $E(K)_{tor}$)

- Mazur (1978): $E(\mathbb{Q})_{tor} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z}, & 1 \le n \le 10 \text{ & } n = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 3, 4. \end{cases}$

Project 1: $E/\mathbb{Q}: y^2 + y = x^3 + x + 1 \Rightarrow Y^2 = X^3 + AX + B$.

Find $E[2](\overline{\mathbb{Q}}) = ?$

$E/\mathbb{Z}_2\mathbb{Z}: y^2 + y = x^3 + x + 1$.

Find $E[2](\overline{\mathbb{Z}_2\mathbb{Z}}) = ?$

Recitation project 2: How many 3-torsion points exist in $E(\overline{K})$, $\mathrm{char} K = 0$? 4-torsion

Find division polynomials.

Ex. (1) $E/\mathbb{Q}: y^2 = x^3 + 7x$, $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \Rightarrow rk = 0$. generated by $(0,0)$

(2) $E/\mathbb{Q}: y^2 = x^3 + 4x^2 + 20x$, $E(\mathbb{Q}) \cong \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \Rightarrow rk = 1$.

generated by $(0,0), (2,0)$ & $(1,-3)$

& $E(\mathbb{Q}(\sqrt{3})) \cong \mathbb{Z}^2 \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \Rightarrow rk = 2$.

generated by $(0,0), (2,0)$ & $(1,-3)$ & $(4, 4\sqrt{3})$.

Known large rank: $\mathrm{rank}(E(\mathbb{Q})) \ge 28$, (Elkies, 2006)

Project 3: Find $E/\mathbb{Q}$ s.t. $rk(E(\mathbb{Q})) \ge 1$.

< Sketch of the proof of the Mordell-Weil Thm >

Thm. (Weak Mordell-Weil Thm) For $m \geq 2$, The gp. $E(K)/mE(K)$ is finite.

Thm. (Descent Thm). Let A be an abelian gp. ($A = E(K)$)

If $\exists\, m \geq 2$ & a function $h: A \to \mathbb{R}$ s.t.:

(1) For any $Q \in A$, $\exists\, C_Q$ s.t. for $\forall P \in A$,
$$h(P+Q) \leq 2h(P) + C_Q \quad (C_Q \text{ constant});$$

(2) $\exists$ a finite C s.t. for $\forall P \in A$, $h(mP) \geq m^2 h(P) - C$;

(3) For any $k \in \mathbb{R}$, $h(P) \leq k$ only holds for finitely many $P \in A$;

(4) A/mA is finite,

then A is f. g.

(Proof of Weak M-W. Thm.)

Lemma 1. For a field K & E/K, if L/K is a finite Galois ext'n with G, & if $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is also finite.

(Pf) $E(K)/mE(K) \to E(L)/mE(L)$: well-defined
$$P + mE(K) \mapsto P + mE(L)$$

$\Rightarrow$ an exact seq.: $0 \to \dfrac{E(K) \cap mE(L)}{mE(K)} \to E(K)/mE(K) \to E(L)/mE(L)$.

Φ :=

Define $\varphi: \Phi \to \{\lambda : G \to E[m]\}$ (finite since G & $E[m]$ are finite.) by

$$P \mapsto \lambda_P(\sigma) = Q^\sigma - Q \quad \text{for } Q \in E(L) \text{ s.t. } mQ = P.$$

Then φ is injective, so Φ is finite. ∎

So we may assume that $E[m] \subseteq E(K)$.

(Proof of Thm. of Descent).

Suppose $\exists$ a ftn. h. satisfying (1) ~ (4).

By (4) suppose A/mA is finite. Pick coset representatives $Q_1, \dots, Q_n \in A$ & for each $P \in A$, denote the coset $Q_P \ni P$.

So let $P \in A$. Then $P \in Q_P \Rightarrow P = Q_P + mP_1$ for some $P_1 \in A$.

Similarly, $P_1 = Q_{P_1} + mP_2$, $\dots$, $P_k = Q_{P_k} + mP_{k+1}$, for $k \geq 1$.

By (1), $m^2 h(P_k) \leq h(mP_k) + C$, $\quad mP_k = P_{k-1} - Q_{P_{k-1}}$.

$$\Rightarrow h(P_k) \leq \frac{1}{m^2}\left(h\left(P_{k-1} - Q_{P_{k-1}}\right) + C\right). \quad \text{---} (*)$$

Let $C_{max} = \max_{1 \leq i \leq n} C_{(-Q_i)}$ given in (1) (C_Q)

Then, by (1) $h(P_{k-1} + (-Q_{P_{k-1}})) \leq 2h(P_{k-1}) + C_{(-Q_{P_{k-1}})} \leq 2h(P_{k-1}) + C_{max}$.

by (*) & before, $h(P_k) \leq \frac{1}{m^2}\, 2h(P_{k-1}) + \frac{1}{m^2}(C_{max} + C)$

$(m \geq 2)$

$$\Rightarrow \leq \frac{1}{2} h(P_{k-1}) + \frac{1}{4}(C_{max} + C)$$

$$\Rightarrow h(P_k) - \frac{1}{2}(C_{max} + C) \leq \frac{1}{2}\left(h(P_{k-1}) - \frac{1}{2}(C_{max} + C)\right)$$

So for any P $\exists k$ s.t. $h(P_k) - \frac{1}{2}(C_{max} + C) \leq 1$.

i.e $h(P_k) \leq M = 1 + \frac{1}{2}(C_{max} + C)$

constant.

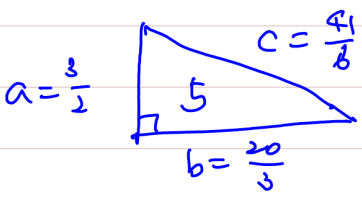
this M is indep. of P

So any $P \in A$ can be written as a sum using only elts of ht. $\leq M$. By (3), $\exists$ only finitely many such elts A. & $Q_1, \dots, Q_n$.

< Congruent #s & Elliptic curves >

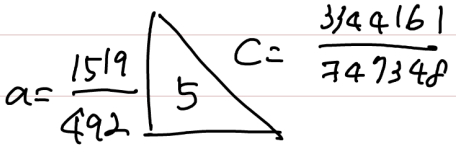
Q. Is there a right $\triangle$ whose sides are rational #s and whose area is 5 ?

Ans.



Fibonacci

,



....

Def. A square-free positive integer n is called **a congruent #**, if n is the area of a right $\triangle$ with rational sides a, b & c.

i.e. V_n : $\begin{cases} a^2+b^2=c^2 \\ ab=2n \end{cases}$ has a (positive) rational point (a, b, c).

Ex. 5 is a congruent #.

Thm. (Fermat, 1640) 1 is not a congruent #.

(Pf) Suppose $\exists\ \frac{a}{d}, \frac{b}{d}, \frac{c}{d}$ where a, b, c & $d \in \mathbb{Z}^{>0}$ & $\left(\frac{a}{d}\right)^2+\left(\frac{b}{d}\right)^2=\left(\frac{c}{d}\right)^2$ & $\frac{1}{2}\cdot\frac{a}{d}\cdot\frac{b}{d}=1$.

$\Leftrightarrow$ $\begin{cases} a^2+b^2=c^2 \\ ab=2d^2 \end{cases}$ for $a, b, c, d \in \mathbb{Z}^{>0}$. —— (*)

Step 1 : We may assume that $(a, b)=1$. by dividing by (a, b).

Step 2 : a or b is even, but not both.

So c is odd. We may assume a is even & b is odd. by symmetry.

Since $ab=2\cdot d^2$, $a=2k^2$ & $b=l^2$ for some k, l odd $l \in \mathbb{Z}^{>0}$. (k, l odd)

$\Rightarrow \quad 4k^4 + b^2 = c^2 \quad \Rightarrow \quad \frac{c+b}{2} \cdot \frac{c-b}{2} = k^4.$

& $\left(\frac{c+b}{2}, \frac{c-b}{2}\right) = 1$, since b & c : odd. & relatively prime.

$\Rightarrow \quad \frac{c+b}{2} = r^4, \quad \frac{c-b}{2} = s^4$ for some $r, s \in \mathbb{Z}^{>0}$ s.t. $(r,s)=1$.

$\Rightarrow \begin{cases} b = r^4 - s^4, \\ c = r^4 + s^4. \end{cases} \Rightarrow \quad l^2 = r^4 - s^4 = (r^2+s^2)(r^2-s^2).$

l: odd. $\quad$ (r^2+s^2) & (r^2-s^2): relatively prime

$\Rightarrow \begin{cases} r^2+s^2 = t^2, \\ r^2-s^2 = u^2 \end{cases}$ for odd $t, u \in \mathbb{Z}^{>0}$. & $(t,u)=1$.

$\Rightarrow \quad r^2 = \frac{t^2+u^2}{2} = \left(\frac{t+u}{2}\right)^2 + \left(\frac{t-u}{2}\right)^2$ & $\frac{t \pm u}{2} \in \mathbb{Z}$.

Letting $a' = \frac{t+u}{2}$, $b' = \frac{t-u}{2}$, $c' = r$, we get

$(a')^2 + (b')^2 = (c')^2$ & $(a', b') = 1$, since $(t,u)=1$.

& $a'b' = \frac{t^2-u^2}{4} = \frac{2s^2}{4} = 2\left(\frac{s}{2}\right)^2 = 2(d')^2$ for $d' := \frac{s}{2} \in \mathbb{Z}$.

So we get a new solution (a', b', c', d') to (*) with $(a', b') = 1$.

Since $0 < c' = r \le r^4 < r^4 + s^4 = c$, by repeating the process, we get infinitely many integers between 0 & c, $\not\in$.

This method is called Fermat's descent method. ▨

Remark. Fermat proved 1 & 2 are not congruent #s.

(Elliptic curves & congruent #s.)

Congruent number elliptic curve E_n : $y^2 = x^3 - n^2 x$, for $n \ge 0$ ← square-free.

- $\exists$ one-to-one correspondence between the following sets.

$$V_n = \{(a,b,c) \mid a^2+b^2=c^2,\ ab = 2n\} \longleftrightarrow \{(x,y) \in E_n \mid y \neq 0\}$$

$$(a,b,c) \longmapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right) \neq 0.$$

$$\left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right) \longleftarrow (x,y),\ y \neq 0$$

Easy to check!

Note that

(1) $c \neq a$ so $c-a \neq 0$, since if $c=a$, then $b=0 \Rightarrow n=0$ ↯.

(2) preserving positivity: If $a, b, c > 0$, then $(c-a)(c+a) = b^2 > 0$,

so $c-a > 0$. $\Rightarrow$ $x = \frac{nb}{c-a} > 0$, $y = \frac{2n^2}{c-a} > 0$.

If $x, y > 0$, then since $y^2 = x^3 - n^2 x = x(x^2 - n^2)$,

$x^2 - n^2 > 0 \Rightarrow$ a, b, c are positive.

(3) for rational $n > 0$, (a, b, c) is rational $\Leftrightarrow (x, y)$ is rational.

(4) Since $ab = 2n > 0$, a & b have the same sign, so we can assume that a & $b > 0$, & assume $c > 0$ as well.

(Conclusion of the above correspondence)

- $n > 0$ is a congruent # $\Leftrightarrow$ E_n has a rational point (x, y) with $y \neq 0$.
- $n > 0$ is not a congruent # $\Leftrightarrow$ E_n has only rational points $(x, y) = (0, 0), (n, 0)$ & $(-n, 0)$. with ∞.

Ex. By Fibonacci, we know that $(a, b, c) = \left(\frac{3}{1}, \frac{20}{3}, \frac{41}{6}\right)$ forms a right triangle with area $5 = n$.

$\Rightarrow (x, y) = \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right) = \left(\frac{25}{4}, \frac{75}{8}\right) \in E_5(\mathbb{Q})$

Ex. Check that $(25, 120) \in E_7(\mathbb{Q})$.

$\Rightarrow (a, b, c) = \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right) = \left(\frac{24}{5}, \frac{35}{12}, \frac{337}{60}\right)$

forms a right $\triangle$ with area 7.

The important thinking about congruent #s in terms of E_n goes far beyond this interesting correspondence.

Thm. 4.11. (Tunnell, 1983). Let n be a square-free positive integer.

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

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

$h(n) = \#\{(x,y,z) \in \mathbb{Z}^3 \mid x^2+4y^2+8z^2 = \frac{n}{2}\}$

$k(n) = \#\{(x,y,z) \in \mathbb{Z}^3 \mid x^2+4y^2+32z^2 = \frac{n}{2}\}$.

(1) For odd n, if n is a congruent #, then $f(n) = 2g(n)$.

(2) For even n, if n is a congruent #, then $h(n) = 2k(n)$.

(3) If BSD conjecture is true for E_n, then the converse of (1) & (2) is true.:

If n is odd & $f(n) = 2g(n)$, then n is a cong. #.

If n is even & $h(n) = 2k(n)$, then n is a cong. #.

In fact, these $f(n)$, $g(n)$, $h(n)$ & $k(n)$ can appear as coefficients of certain automorphic forms.

Ex. (1) $f(1) = 2$ & $g(1) = 2$, $f(3) = g(3) = 4$,

$\Rightarrow f(1) \neq 2g(1)$ & $f(3) \neq 2g(3)$ $\Rightarrow$ 1 & 3 are not cong. #s by Tunnell's criterion.

(2) $h(2) = 2$ & $k(2) = 2$. $\Rightarrow h(2) \neq 2k(2)$, so 2 is not a cong #.

(3) $f(5) = g(5) = 0$ & $f(7) = g(7) = 0$.

$\Rightarrow f(5) = 2g(5)$ & $f(7) = 2g(7)$

$\Rightarrow$ Under BSD conjecture, Tunnell's result implies that 5 & 7 are cong. #s. (Unconditionally, we saw that 5 & 7 are Cong. #'s.")

(4) Note that $h(10)=4$ & $k(10)=4$, $\Rightarrow h(10) \nmid 2k(10)$

So Tunnell's thm says that "10 is not a cong. #".

Thm. (Birch, Heegner, Monsky) p: a prime.

- If $p \equiv 5, 7 \pmod 8$, p is a cong. #
- If $p \equiv 3 \pmod 8$, p is not a cong. #
- If $p \equiv 3, 7 \pmod 8$, $2p$ is a cong. #.

- If $p \equiv 3$, $q \equiv 7$ or $p \equiv 5$, $q \equiv 5 \pmod 8$, pq is a cong. #.
- If $p \equiv 3$, $q \equiv 5$ or $p \equiv 5$, $q \equiv 7 \pmod 8$, $2pq$ is a cong. #.

Thm. (Tian) For each $k \geq 1$, $\exists$ ∞ly many cong #s with k prime factors. More precisely, for $e \in \{3, 5, 7\}$, if $p_0 \equiv e \pmod 8$ & $p_i \equiv 1 \pmod 8$ for $i = 1, \cdots, k-1$, & $\mathbb{Q}(\sqrt{-n})$ has order 4 elt. in its ideal class gp.) then $n = p_0 p_1 \cdots p_{k-1}$ is a cong. #.

< θ-cong. #s >

Def. For a real # θ s.t. $0 < \theta < \pi$ & $\cos\theta = \frac{s}{r}$ (rational), $r, s \in \mathbb{Z}$, $r > 0$,

a square-free positive integer n is a θ-cong. #,

if $n\sqrt{r^2 - s^2}$ is the area of $\triangle$ with rational side & angle θ.

($\frac{\pi}{2}$-cong. # is the original cong. #.)

($r=1$, $s=0$)

$$V_{n,\theta}: \begin{cases} a^2 + b^2 - 2ab\frac{s}{r} = c^2, \\ ab = 2rn. \end{cases}$$

$$E_{n,\theta}: y^2 = x(x + (r+s)n)(x - (r-s)n).$$

is the θ-cong. # elliptic curves.

Thm. (I- & Harold Kim)

(1) We found a parametrization V of S_t of a θ-cong. #s, & showed & for sufficiently large N,

$$\#\{t \in [1,N] \mid S_t \text{ is a } \theta\text{-cong. \#}\} = cN + O(N^{\frac{2}{3}+\varepsilon})$$

for $c>0$ & ε is arbitrary small.

(2) $\exists$ ∞ly many θ-cong. #s with at least n distinct prime factors $p_1, \dots, p_n$ s.t. $\exists$ $i_1, i_2, i_3, i_4 \in \{1,2,\dots,n\}$ s.t. $p_{i_1} \equiv 1 \pmod 5$, $p_{i_2} \equiv 3 \pmod 4$.

In fact, we proved that V a given prime p is a factor of S_n in at least $\frac{2n+1}{p+1}$ for $p > 2n$.))

Idea:

$$\begin{cases} X = fg \\ X + (r+s)n = gh \\ X - (r-s)n = fg \end{cases}$$

& Falting's result

& Hilbert's Irreducibility.

< Modular forms & Elliptic curves >

Def. $\mathcal{H} := \{ z \in \mathbb{C} \mid z = x+yi \mid x, y \in \mathbb{R},\ y > 0 \}$.

upper half plane.

$SL_2(\mathbb{Z})$ acts on $\mathcal{H}$ by:

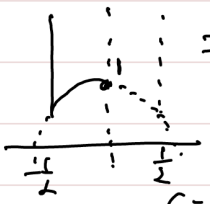
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

($z \in \mathcal{H}$, $\frac{az+b}{cz+d} \in \mathcal{H}$)

(Check: If $\mathrm{Im}(z) > 0$, then $\mathrm{Im}\left(\frac{az+b}{cz+d}\right) > 0$.)

- **Project 1:** • Prove that $SL_2(\mathbb{Z}) = \langle S, T \rangle$, where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ & $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

S: inversion. T: for $n \in \mathbb{Z}$.



• Find the fundamental domain for $SL_2(\mathbb{Z})$.

(i.e. $\mathcal{H}/SL_2(\mathbb{Z}) = \{$ representatives of $SL_2(\mathbb{Z})$-orbits $\}$)

Def. A modular form f of wt k is a holomorphic fn. on $\mathcal{H}$

s.t. (1) $f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z\right) = (cz+d)^k f(z)$ for $\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

(2) f has a Fourier expansion at ∞,

$$f(z) = \sum_{n \ge 0} a(n)\, e^{2\pi i n z}.$$

($\Rightarrow f$ is holomorphic at ∞)

(periodic fn. with period 1)

(so $f(-\frac{1}{z}) = z^k f(z)$ & $f(z+1) = f(z)$.)

(Also, for $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in SL_2(\mathbb{Z})$, $f\left(\frac{-z}{-1}\right) = (-1)^k f(z) \Rightarrow f(-z) = (-1)^k f(z)$.

So k = odd $\Rightarrow f = 0$. So we assume k: even)

Ex. Eisenstein series of wt $2k$ $(k \ge 2)$ is a modular form

defined by $G_k(z) = \sum_{(c,d) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(cz+d)^k}$.

Project 2: Show that $G_k(z)$ has the Fourier coefficient,

$$G_k(z) = 2\zeta(k) + 2 \cdot \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n, \quad k > 2,\ k \text{: even}.$$

where $\sigma_{k-1}(n) = \sum_{1 \le m \mid n} m^{k-1}$ & $\zeta(k) = \sum_{d=1}^{\infty} \frac{1}{d^k}$.

Recall that

Def. < Congruence subgps >

a subgp. of $SL_2(\mathbb{Z})$ with finite index.

Ex. $\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{n} \right\}$

$\cup$ with $[SL_2(\mathbb{Z}) : \Gamma_0(n)] = n \cdot \prod_{p \mid n} \left(1 + \frac{1}{p}\right)$.

$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{n} \right\}$.

$\cup$ with $[SL_2(\mathbb{Z}) : \Gamma_1(n)] = n^2 \prod_{p \mid n} \left(1 - \frac{1}{p^2}\right)$

$\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{n} \right\}$.

with $[SL_2(\mathbb{Z}) : \Gamma(n)] = n^3 \prod_{p \mid n} \left(1 - \frac{1}{p^2}\right)$.

Def. $E_k(z) = G_k(z)/2\zeta(k) = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$, B_k: k-th Bernoulli #.

the generating poly. of B_k is $\frac{t}{e^t-1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}$.

Ex. Delta fn. $\Delta(z) = q\cdot\prod_{n\geq 1}(1-q^n)^{24} = \left(\sum_{n\geq 1}\tau(n)\cdot q^n\right) = q - 24q^2 + 252q^3 - 1472q^4 + \cdots$ (Ramanujan-Taufta) — mod. form of wt. 12 for $SL_2(\mathbb{Z})$.

Fact. • $E_4^2 = E_8$, $E_4E_6 = E_{10}$, $E_6E_8 = E_{14}$, ...

• The $\mathbb{C}$-vector space spanned by modular forms for $SL_2(\mathbb{Z})$ is $\mathbb{C}[E_4, E_6]$.

< An application of some quasi-modular forms to sums of 4 squares >

Def. The theta function

$$\theta(z) = \sum_{x\in\mathbb{Z}} q^{x^2}, \quad q = e^{2\pi i z}, \quad z\in h$$

& $\theta(z,k) = \theta(z)^k$ for $k\geq 1$, $z\in h$.

Then, • $\theta(z,k)$ is absolutely conv. for $k\geq 4$, $z\in h$.

• $\theta(z,k_1)\,\theta(z,k_2) = \theta(z, k_1+k_2)$, $z\in h$

• $\theta(z+1,k) = \theta(z,k)$.

(• $\theta(z) = \theta(z,1) = \sum_{n\in\mathbb{Z}} e^{2\pi i n^2 z}$)

Let $\theta(z,k) := \sum_{n=1}^{\infty} a(n,k)q^n = (\theta(z))^k$.

Then, — $a(n,k) = \#\{(n_1,\ldots,n_k)\in\mathbb{Z}^k \mid n = \sum_{i=1}^{k} n_i^2\}$

sums of k squares.

($\because$ $\theta(k)^k = \left(\sum_{x\in\mathbb{Z}} q^{x^2}\right)^k = \sum_{n\in\mathbb{Z}}\left(\sum_{(x_1,\ldots,x_k)\ \text{s.t.}\ \sum x_i^2 = n} 1\right) q^n$)

— $\theta(\gamma\cdot z, 4) = (cz+d)^2\theta(z,4)$ for $\gamma\in\left\langle \pm\begin{pmatrix}1&1\\0&1\end{pmatrix}, \pm\begin{pmatrix}1&0\\4&1\end{pmatrix}\right\rangle$

$\left(\subset \pm\Gamma_0(4).\right)$

— In fact, $\theta(\gamma\cdot z, 2) = \chi_{-4}(a)(cz+d)\,\theta(z,2)$ for $\gamma\in\Gamma_0(4)$.

& $\theta(z,4) = 8\left(G_2(z) - 4G_2(4z)\right)$, quasi-modular form G_2.

" $\Rightarrow$ $a(n,4) = 8\cdot\sum_{d\mid n,\ d\not\equiv 4\mathbb{Z}} d$. "

$\left(G_2(\gamma\cdot z) = (cz+d)^2\left(E_2(z) + \frac{6}{\pi i}\cdot\frac{c}{cz+d}\right)\right)$

Thm. (Tunnell, modular form version)

Let $g(z) = q \cdot \prod_{n=1}^{\infty}(1-q^{8n})(1-q^{16n})$ & $\theta_t(z) = \sum_{t=-\infty}^{\infty} q^{tn^2}$

& $g(z)\theta_2(z) := \sum_{n=1}^{\infty} a(n) q^n$ & $g(z)\theta_4(z) := \sum_{n=1}^{\infty} b(n) q^n$.

For the square-free part m of n,

if m is odd & $a(m) \neq 0$, then m (so n) is not a cong. #,

& if m is even & $b(\frac{m}{2}) \neq 0$, then m (so n) is not a cong. #.

Under the BSD conjecture, converses of both hold.

In fact, $g(z)\theta_2(z) = q^{1} + 2q^{3} + q^{9} - 2q^{11} - 4q^{17} - 2q^{19} - 3q^{25} + 4q^{33} - 4q^{35} + \cdots$

$\Rightarrow$ 1, 3, 11, 17, 19, 33, 35, ---- are not cong. #s.

$g(z)\theta_4(z) = q^{1} + 2q^{5} - q^{9} - 2q^{13} + \cdots$

$\Rightarrow$ $2 \cdot 1 = 2$, $2 \cdot 5 = 10$, $2 \cdot 13 = 26$, ---- are not cong. #s.

Idea: **Thm.** (Coates & Wiles) If $L(E,1) \neq 0$, then $rk(E(\mathbb{Q})) = 0$.

$L(E_n, 1) = a(n)^2 \cdot \beta \cdot \frac{1}{4\sqrt{n}}$

$L(E_{2n}, 1) = b(n)^2 \cdot \beta \cdot \frac{1}{2\sqrt{2n}}$, where β is the real period of E_1.

So it follows from Thm.

[$a(m) = f(m) - 2g(m)$ & $b(m) = h(m) - 2k(m)$.].

Q. For an elliptic curve E/K over a # field K,

(1) over which finite ext'n L/K does the rank of E grow?

i.e. $rank(E(L)) \gneq rank(E(K))$?

(2) are there only many linearly disjoint finite ext'ns L_i over K s.t. $rk(E(L_i)) \gneq rank(E(K))$?

Remark. If $\{L_i\}_{i=1}^{\infty}$ are linearly disjoint over K & $\exists P_i \in E(L_i)$, then only many of P_i are linearly independent (in $E(K)$).

(Over quadratic extensions)

Def. For $E/K : y^2 = x^3 + ax + b$ & $d \in K^\times - (K^\times)^2$,

the quadratic twist of E by d is $E^d/K : dy^2 = x^3 + ax + b$.

$(\cong y^2 = x^3 + ad^2x + bd^3)$

Thm. $\operatorname{rank}(E(K(\sqrt{d}))) = \operatorname{rank}(E(K)) + \operatorname{rank}(E^d(K))$.

Remark. Thm implies that rank growth over quad. ext'ns $K(\sqrt{d})$
$\iff$ rank of the twist E^d is positive.

(Goldfeld's Conjecture) For $x \in \mathbb{R}^{>0}$, let $S(x) = \{\text{square-free } d \in \mathbb{Z} \mid |d| \le x\}$.

$$\lim_{x \to \infty} \frac{\sum_{d \in S(x)} \operatorname{rank}(E^d(\mathbb{Q}))}{|S(x)|} = \frac{1}{2}.$$

Goldfeld's conjecture predicts that

the set of $E^d/\mathbb{Q}$ s.t. $\operatorname{rank}(E_d(\mathbb{Q})) = 0$ has density $\frac{1}{2}$,

" s.t. $\operatorname{rank}(E_d(\mathbb{Q})) = 1$ " " $\frac{1}{2}$,

& " s.t. $\operatorname{rank}(E_d(\mathbb{Q})) \ge 2$ " " 0.

Thm. (Bhargava & Skinner, 2015)

At least 20.6 % of $E/\mathbb{Q}$ have rank 0,

& at least 93.75 % of $E/\mathbb{Q}$ have rank <u>at most 1</u>.

And the average rank is at most 0.885.

Remark. Since we can choose only many $d \in K^\times - (K^\times)^2$ s.t. $K(\sqrt{d})$'s are disj. over K, $\operatorname{rank}(E(K^{ab})) = \infty$, where K^{ab} is the max'l ab. ext'n. of K in $\overline{K}$.

Def. An abelian variety A/K is a smooth projective variety that is an alg. gp.

<known results on the existence of only linearly disjoint ext'ns with rank growth>

(1) $\mathbb{Z}/2\mathbb{Z}$-ext'ns for E/K by Remark.

(2) (Fearley, Kisilevsky & Kuwata, 2012) $\mathbb{Z}/3\mathbb{Z}$-ext'ns for $E/\mathbb{Q}$, if $|E(\mathbb{Q})| \ge 6$.

(3) (Wong & Rosen, 2002) $\mathbb{Z}/n\mathbb{Z}$-ext'ns, for the Jacobian variety of a curve X/K s.t. $\exists$ a cyclic cover $X \to \mathbb{P}^1$ of degree n.

(4) (I- & Larsen, 2008) For an abelian variety A/k,
"non-abelian"
$\exists$ an odd prime q_0 & only finitely disjoint A_{2q_0}-ext'ns $\{L_i/k\}$ s.t. $\mathrm{rk}(A(L_i)) \gneq \mathrm{rk}(A(k))$.

Coro. For each $\sigma \in \mathrm{Gal}(\bar{k}/k)$, $\mathrm{rk}(A(\bar{k}^{\sigma})) = \infty$.

(Idea of the proof: geometric approach)

We find a gp. G acting on A & find a variety V on which "G acts & is associated with A" s.t. $\exists$ projective line $\mathbb{P}^1 \subseteq V/G$ satisfying

$$\begin{array}{ccccc} p \in X & \longrightarrow & V & \longrightarrow & A \\ \downarrow & & \downarrow & & \\ t \in \mathbb{P}^1 & \longrightarrow & V/G & & \end{array} \qquad \tilde{p} \in A$$

For example, $A = V = E^{n-1}$ & $G = A_n$ for even n.

Apply Hilbert's irreducibility thm to find only many G-ext'n L_i/k & $p_i \in X(L_i) - X(k)$ s.t. $\tilde{p}_i \notin A(L_i) \setminus A(k)$.

ex. X : the klein quartic,

Thm. (I- & Wallace, 2018)

(1) If $\exists$ a morphism $X \to \mathbb{P}^1$ over k of degree d, $\exists$ only many (finitely disj. degree d-ext'ns L_i/k s.t. $\mathrm{rk}(\mathrm{Jac}(X)(L)) \gneq \mathrm{rk}(\mathrm{Jac}(X)(k))$.
may not be Galois.

(2) $\exists$ an infinite family $\{E_i/\mathbb{Q}\}$ s.t. for each E_i, $\exists$ only $\mathbb{Z}/3\mathbb{Z}$-ext'ns $L_i/\mathbb{Q}$ over which E_i has rank gain. (unconditional result, cf. FKK.)

Their j-invariants are parametrized by

$$j(E_i) = 256 \cdot \frac{(a^4+54)^3 a^4}{(4a^4-27)^3} = \frac{f(f+216)^3}{(f-27)^3} \quad \text{by letting } a^4 = f,$$

where $f \in M(\Gamma_0(3))$, defined by

$$f(z) = \left(\frac{\eta(z)}{\eta(3z)}\right)^{12} = q^{-1} + 15 + 54q - 76q^2 - 243q^3 + 1188q^4 - \cdots$$

Thm. (I- & S. Choi, 2024, preprint)

For A/k, suppp. $\exists$ a morphism $f: V \to A$ from a smooth proj. variety V/k & $\exists\, G \leq \mathrm{Aut}(V)$ s.t. X/G is a rational variety over k, and $\sum_{g \in G} f(g \cdot p) = 0$, for $\forall\, p \in V$.

Suppose $\exists\, \sigma \in G$ of order p, a prime.

(1) If ① $f - f\sigma$ is non-constant, then $\exists$ only f. d. $\{L_i/k\}$ s.t.

$$\mathrm{rk}(A(L_i)) \geq \mathrm{rk}(A(k)) + (p-1) \quad -\otimes$$

(2) If ① holds & $f + f\sigma + \cdots + f\sigma^{p-1}$ is non-constant, then

$\otimes$ is improved to $\mathrm{rk}(A(L_i)) \geq \mathrm{rk}(A(k)) + p$.

As examples which satisfy the conditions,

Corr. For $\{E_a/k : y^2 = x(x-1)(x-a)\}_{a \in k - \{0,1\}}$ s.t. $a^2 - a + 1 \neq 0$, & $k \ni \zeta_4$ & $\sqrt{a(1-a)(a^2-a+1)}$,

$$\mathrm{rk}(E_a(L_i)) \geq \mathrm{rk}(E_a(k)) + \underline{\underline{2}}. \quad \text{for only } A_4\text{-exts } L_i/k.$$

For $\{E_b/k : y^2 = (x^2+b)(x+2)\}_{b \in k - \{0,-4\}}$ with some mild assumption,

$$\mathrm{rk}(E_b(L_i)) \geq \mathrm{rk}(E_b(k)) + \underline{\underline{2}}, \quad \text{for only } C_4\text{-exts } L_i/k.$$