NUMBER FIELDS VS ELLIPTIC CURVES

$K = \mathbb{Q}(\alpha)$ where $f(\alpha)=0$, $f(x)\in\mathbb{Z}[x]$.

$\mathcal{O}_K$ ring of integers of K
(those $\beta\in K$ roots of monic $g(x)\in\mathbb{Z}[x]$)

THM: $\mathcal{O}_K$ is a finitely generated abelian group.

$\mathcal{O}_K^\times$ units in $\mathcal{O}_K$.

THM: $\mathcal{O}_K^\times$ is a fin. gen. ab. gp. of rank r_1+r_2-1
(DIRICHLET'S UNIT THEOREM) where

$$[K:\mathbb{Q}] = n = r_1 + 2r_2$$

$$\Rightarrow \mathcal{O}_K^\times \cong \underbrace{(\mathcal{O}_K^\times)_{tors}}_{\mu(K) \text{ roots of unity in } K} \oplus \mathbb{Z}^{r_1+r_2-1}$$

$$Cl(K) = \text{fract. ideals of } K \,/\, \text{princ. ideals}$$

ideal class gp

"arithmetic complexity" of $\mathcal{O}_K$

$\}$ failure of local-to-global principality of ideals.

$E: y^2 = x^3 + Ax + B$, $A,B\in\mathbb{Q}$, smooth, (projective)

$E(\mathbb{Q}) = \{(x,y)\in E : x,y\in\mathbb{Q}\} \cup \{\underset{\mathcal{O}}{[0:1:0]}\}$

THM (Mordell-Weil) $E(\mathbb{Q})$ is a f.g. ab. gp

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

Q: DESCRIPTION OF $R_{E/\mathbb{Q}}$??

Ш$(E/\mathbb{Q})$ - Shafarevich-Tate group
"arithmetic complexity of $E(\mathbb{Q})$"
determines the failure of the local-to-global principle for $E/\mathbb{Q}$.

NUMBER FIELDS VS ELLIPTIC CURVES

$\zeta_K(s)$ = Dedekind zeta function

$$= \sum_{I \subseteq \mathcal{O}_K} \left(N^K_{\mathbb{Q}}(I)\right)^{-s}$$

$$= \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{1 - \left(N^K_{\mathbb{Q}}(\mathfrak{p})\right)^{-s}}$$

~1839

THM. (ANALYTIC CLASS NUMBER FORMULA)

$$\lim_{s \to 0} \frac{\zeta_K(s)}{s^{r_1+r_2-1}} \overset{!}{=} -\frac{R_K \cdot h_K}{\#\mu(K)}$$

R_K = regulator of $\mathcal{O}_K^\times$

h_K = class # of K = # $Cl(K)$

$\mu(K)$ = roots of unity in $\mathcal{O}_K^\times$.

$L(E_{/\mathbb{Q}}, s)$ = Hasse-Weil L-function

$$= \sum_{n \geq 1} a_n n^{-s}$$

Fourier coefficients.

$$\text{"="} \prod_{\text{good } p} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \cdot \prod_{\text{bad } p} \ldots$$

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

CONJECTURE! BIRCH-SWINNERTON-DYER (1965)

$$\underbrace{\lim_{s \to 1} \frac{L(E,s)}{(s-1)^{R_E}}}_{} \overset{?}{=} \frac{\#Ш \cdot \Omega_E \cdot Reg_{E/\mathbb{Q}} \cdot \prod_p c_p}{\left(\# E(\mathbb{Q})_{tors}\right)^2}$$

order vanishing of $L(E,s)$ at $s=1$

"analytic rank"

NUMBER FIELDS

$[K:\mathbb{Q}]=2$
$= 2+2\cdot 0$
$r_1=2$
$r_2=0$

$$K=\mathbb{Q}(\sqrt{5})$$

$$\mathcal{O}_K=\mathbb{Z}\Big[\underbrace{\tfrac{1+\sqrt{5}}{2}}_{\text{root of } x^2-x-1=0}\Big]$$

$$\mathcal{O}_K=\mathbb{Z}+\left(\tfrac{1+\sqrt{5}}{2}\right)\mathbb{Z}$$

$\mathcal{O}_K^\times$ rank $2+0-1=1.$

$$=\left\{\pm\left(\tfrac{1+\sqrt{5}}{2}\right)^n : n\in\mathbb{Z}\right\}$$

$$\cong \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}.$$

$Cl(K)=\{e\}$, $h_K=1$

(note: $Cl(\mathbb{Q}(\sqrt{-5}))=\mathbb{Z}/2\mathbb{Z}$)

ELLIPTIC CURVES

$$E:\quad y^2=x^3-2x$$

$$E(\mathbb{Q})=\langle(0,0),(2,2)\rangle$$

$$\cong\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}$$

$R_{E/\mathbb{Q}}=1.$

$Ш(E/\mathbb{Q})=\{e\}$ trivial

(note: $y^2=x^3-113x$ $Ш\cong(\mathbb{Z}/2\mathbb{Z})^2$)

NF's

$K = \mathbb{Q}(\sqrt{5})$

$\zeta_K(s) = 1 + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{9^s} + \frac{2}{11^s} + \dots$

No $\frac{1}{2^s}, \frac{1}{3^s}$ b/c no ideals in $\mathcal{O}_K$ of norm 2 or 3

$R_K = \log\left(\frac{1+\sqrt{5}}{2}\right) \approx 0.48121182\dots$

$h_K = 1$

$\mu(K) = \{\pm 1\} \quad \#\mu(K) = 2$

$$\lim_{s\to 0} \frac{\zeta_K(s)}{s} = -\frac{\log\left(\frac{1+\sqrt{5}}{2}\right)}{2}$$

numerical + theoretical

$r_1 + r_2 - 1 = 2 + 0 - 1 = 1$

EC's

$y^2 = x^3 - 2x$

$L(E,s) = 1 - \frac{4}{5^s} - \frac{3}{9^s} - \frac{4}{13^s} - \frac{2}{17^s} + \frac{11}{25^s} - \frac{4}{29^s} + \dots$

$\#\underline{Ш} = 1$

$R_{E/\mathbb{Q}}$ = Canonical height of $(2,2)$ $\doteq \underline{0.608709051 9}\dots$

$(\sim \log 2)$

$|E(\mathbb{Q})_{tors}| = \#\langle(0,0)\rangle = 2$

$\Omega_E = 2.204878\dots$

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)} = \frac{1\cdot\Omega\cdot R_E\cdot 2}{4}$$

$R_{E/\mathbb{Q}} = 1$

numerically.