Ranks of Elliptic Curves

Vladimir Dokchitser

October 11, 2022

20th century Elliptic Curves

$$E : y^2 = x^3 + Ax + B$$

Poincaré

$E(\mathbb{Q})$ is an abelian group.

Mordell

$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times (\text{finite})$.

Cassels; Selmer...

$E(\mathbb{Q})/nE(\mathbb{Q}) = \frac{Sel_n E}{Ш_E[n]}$.

Shafarevich–Tate Conj: Ш finite.

Birch; Swinnerton–Dyer; Tate

BSD Conj: $\mathrm{ord}_{s=1} L(E,s) = r$.

True for $E/\mathbb{F}_p(t)$ if Ш finite.

Modular forms | Galois Representations | Motives | Iwasawa Theory

Heegner: intelligent point in $E(\mathbb{Q})$

Frey: $y^2 = x(x - A^p)(x + B^p)$ for $A^p + B^p = C^p$

Kolyvagin ...

$\mathrm{ord}_{s=1} L(E,s) \leq 1 \implies$ BSD true.

(Euler Systems)

Wiles ...

$L(E,s)$ is analytic.

(Langlands programme)

21st century Elliptic Curves (so far)

Freitas–Le Hung–Siksek

$L(E,s)$ is analytic for elliptic curves over $\mathbb{Q}(\sqrt{d})$ with $d>0$.

Elkies

Found a curve with $r \geq 28$.
Found a family of curves with $r \geq 19$.

Mazur–Rubin

By varying E we can reduce $Sel_2 E$.
For all number fields K there is E with $E(K)=0$.

Bhargava–Shankar

Average size of $Sel_2 E, Sel_3 E$ and $Sel_5 E$ is small.
Positive proportions of E have $E(\mathbb{Q})=0$ and $\simeq \mathbb{Z}$.

Skinner

If $\# Sel_p E = p$ then $E(\mathbb{Q}) \cong \mathbb{Z}$ (under some mild hypotheses).

Granville; Park–Poonen–Voight–Wood

Ranks of elliptic curves over $\mathbb{Q}$ are probably bounded.

Dokchitser^2

BSD and $Sel_p E$ give compatible predictions for r modulo 2.

Smith(?)

100% of curves $y^2 = x^3 - n^2 x$ with $n \equiv 1,2,3(8)$ have rank 0.

Open problems

$E(\mathbb{Q}) = \Delta \times \mathbb{Z}^r$.

Can the rank r be arbitrarily large?

Do 50% of elliptic curves have rank 0, and 50% rank 1?

Is $Ш_E$ is finite for a single E with $r \geq 2$?

Is the BSD conjecture for a single E with $r \geq 4$?

Is $E(\mathbb{Q})$ infinite for all $E : y^2 = x^3 - n^2 x$ with $n \equiv 5, 6$ or $7 \bmod 8$?

Does $E : y^2 + y = x^3 + x^2 + x$ have infinitely many solutions over $\mathbb{Q}(\sqrt[3]{m})$ for all m?

Do all $E/\mathbb{Q}$ have even rank over $\mathbb{Q}(i, \sqrt{17})$?

...

Explicit arithmetic of Jacobians

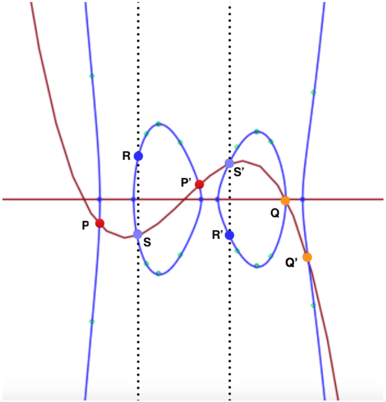
Curve of genus 2:
$C/K : y^2 = f(x), \quad deg(f) = 6.$

Abelian surface:
$A = Jac(C).$

Points in $A(\bar{K})$:
Pairs $[P, P'], \quad P, P' \in C(\bar{K}).$

Points in $A(K)$:
$P, P' \in C(\bar{K}), \quad Gal(\bar{K}/K)$-stable.

Addition law:
Draw $y = cubic$ through P, P', Q, Q'.
$[P, P'] + [Q, Q'] + [S, S'] = 0, \quad [S, S'] = [R, R'].$



Mordell–Weil Theorem

$A(K) \simeq \Delta \times \mathbb{Z}^r$

Extending the field and extending the curve

$E/\mathbb{Q}$ an elliptic curve.

$K/\mathbb{Q}$ number field.
Then $E(K) \supseteq E(\mathbb{Q})$.
If $K/\mathbb{Q}$ Galois with Galois group G, then $E(K)^G = E(\mathbb{Q})$.
- $E(\mathbb{Q}) \subset E(\mathbb{Q}(\zeta_p)) \subset E(\mathbb{Q}(\zeta_p^2)) \subset E(\mathbb{Q}(\zeta_p^3))$... — Iwasawa theory.
- $E/\mathbb{Q}(\sqrt{d}) \sim E \times E_d$ — Mazur–Rubin'ology.
- E over intermediate fields of a D_{2p}-extension — D&D parity conjecture.

$C \to E$ a cover of curves, e.g. $C : y^2 = x^6 + Ax^2 + B$;
Then $\mathrm{Jac}(C)(\mathbb{Q}) \supseteq E(\mathbb{Q})$.
If the cover is Galois with Galois group G, then $\mathrm{Jac}(C)(\mathbb{Q})^G = E(\mathbb{Q})$.
- Rational points, heights, L-functions, Selmer groups behave as for number fields.
- Galois representations, local theory, L-values... ?
- New applications.

Thank you!