Distribution of ranks of elliptic curves

Izzy Rendell

LSGNT

18th April 2023

Rank of an elliptic curve

Let E be an elliptic curve, then by Mordell-Weil:

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

$r = 0$ means no rational solutions exist, $r > 0$ means infinitely many rational solutions exist.

Birch and Swinnerton-Dyer Conjecture

The Taylor expansion of $L(E, s)$ at $s = 1$ has the form

$$L(E, s) = c(s-1)^r + \text{higher order terms}$$

with $c \neq 0$ and $r = rank(E(\mathbb{Q}))$.

Consequence: $L(E, 1) = 0$ if and only if $E(\mathbb{Q})$ is infinite.
A Smith: uses matrix determinants to find the rank of $E^{(n)}$ where

$$E^{(n)} : y^2 = x^3 - n^2 x$$

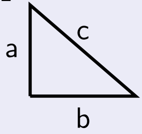
and $n \equiv 5, 6, 7 \ mod \ 8$ is a positive squarefree integer.

Congruent Number Problem

Congruent number definition

A positive integer n is called a congruent number if there exists a right-angle triangle with rational sides such that n is the area of the triangle.

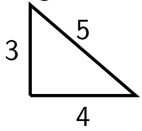
$$a, b, c \in \mathbb{Q}, \qquad \frac{1}{2}ab = n, \qquad a^2 + b^2 = c^2.$$



Congruent Number Problem: which positive integers n are congruent?

Some results for CNP

- 6 is a congruent number, 30 (5, 12, 13) and 60 (8, 15, 17) are also congruent



- 1 is not a congruent number - infinite descent
- $r^2 s$ is congruent if and only if s is congruent, $r, s \in \mathbb{N}$
- $p \equiv 3$ (8), p is not congruent but $2p$ is
- $p \equiv 5$ (8), p is congruent
- $p \equiv 7$ (8), $p, 2p$ are congruent
- Tunnell's Theorem and BSD give algorithm with finite steps

Relation to Elliptic Curves

There is a bijection between the following sets:

$$\{(a,b,c) \in \mathbb{Q}^3 \mid \frac{1}{2}ab = n, a^2 + b^2 = c^2, a, b, c \neq 0\},$$

$$\{(x,y) \in \mathbb{Q}^2 \mid y^2 = x^3 - n^2 x, y \neq 0\}.$$

It turns out that $E^{(n)}(\mathbb{Q})_{tors} = \{\mathcal{O}, (0,0), (n,0), (-n,0)\}$, and we know that

$$E^{(n)}(\mathbb{Q}) \cong E^{(n)}(\mathbb{Q})_{tors} \times \mathbb{Z}^r.$$

Congruent Number Problem (alternative version): n is a congruent number if and only if the rank of $E^{(n)}$ over $\mathbb{Q}$ is positive.

Matrix construction - Legendre symbols

Let the odd part of n be written $p_1 \ldots p_r$. Define the additive Legendre symbol

$$\left(\frac{d}{p}\right)_+ := \frac{1}{2}\left(1 - \left(\frac{d}{p}\right)\right)$$

$$y_i := \left(\frac{-1}{p_i}\right)_+ \quad \mathbf{y} := \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix}, \quad z_i := \left(\frac{2}{p_i}\right)_+ \quad \mathbf{z} := \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix}.$$

$$A_{ij} := \begin{cases} \left(\frac{p_j}{p_i}\right)_+ & \text{for } i \neq j \\ \sum\limits_{\substack{k=1 \\ k \neq i}}^{r} A_{ik} & \text{for } i = j. \end{cases}$$

Example

$n = 30 = 2 \cdot 3 \cdot 5$, $n \equiv 6 \ mod \ 8$. $p_1 = 3$ and $p_2 = 5$.

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \qquad \mathbf{y} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad \mathbf{z} = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

$$M_6 = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Therefore $det(M_6) = 1$, and so $rank(E^{(30)}) = 1 > 0$ (as expected).

Significance of $\mathscr{L}_x$

Sums $\mathscr{L}_x(n)$ defined using a recursive function, definition varies depending on $n \ mod \ 8$.

Theorem (Tian, Yuan, Zhang.)

Let n be a positive squarefree integer. If $n \equiv x \ (8)$ for $x \in \{5, 6, 7\}$, then the analytic rank of $E^{(n)}$ is exactly one if $\mathscr{L}_x(n)$ is nonzero.

A Smith: calculated matrices M_x such that $\mathscr{L}_x = det(M_x)$.

Theorem

- *Of the positive squarefree integers equal to* 5 *mod* 8*, at least 62.9 % are congruent numbers. Same holds for* $n \equiv 7$ *mod* 8*.*
- *Of the positive squarefree integers equal to* 6 *mod* 8*, at least 41.9 % are congruent numbers.*

Motivation - matrices using Legendre symbols

Monsky: the rank of the 2-Selmer group of $E^{(n)}$ can be determined as the corank of a matrix over $\mathbb{F}_2$ determined by $n \textit{ mod } 2$ and Legendre symbols

Tian, Yuan, Zhang: parity of $\mathscr{L}(E^{(n)})$ can be determined by same Legendre symbols, where

$$\mathscr{L}(E) = \frac{L(E,1) \cdot |E_{tors}|^2}{\Omega(E) \prod_{p|2N} c_p(E)},$$

where c_p are Tamagawa factors and $\Omega(E)$ is the least positive real period of E.

BSD implies $\mathscr{L}(E) = |Sha(E)|$.

Matrix properties - coranks

To use T-Y-Z Theorem in terms of density, need to calculate how often $\mathscr{L}_x(n) \neq 0$, for $n \equiv 5, 6, 7\ (8)$.

Corank definition

If M is an $m \times n$ matrix, and M has rank r, then its corank is $m - r$.

We have

$$corank(M) = 0 \text{ and } rank(M) = m \text{ if and only if } det(M_x) \neq 0.$$

Aim: adapt this type of method for other families of elliptic curves.