Finding $\mu(\Delta_E)$ via root numbers

Holly Green

Goal: For an elliptic curve E over $\mathbb{Q}$, find $(-1)^{\text{rank } E/\mathbb{Q}}$ or $w_{E/\mathbb{Q}}$ without factorising Δ_E.

Will do so by studying the distribution of the root number of a particular family of quadratic twists.

1 Motivation

One of the basic general problems in analytic number theory is to try to understand the Möbius function, defined on natural numbers as

$$\mu(n) = \begin{cases} (-1)^{\#\text{distinct prime factors of } n} & \text{for } n \text{ square-free,} \\ 0 & \text{otherwise.} \end{cases}$$

Its importance can be seen from its connection to the Riemann-Zeta function, i.e. (the Dirichlet series which generates the Möbius function) for $s \in \mathbb{C}$ with Re $s > 1$,

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}.$$

In fact, we can reformulate the notorious Riemann hypothesis as

$$\text{`for each } \varepsilon > 0, \sum_{1 \le n \le x} \mu(n) = O(x^{\frac{1}{2}+\varepsilon}).\text{'}$$

Calculating $\mu(n)$ boils down to finding the number of distinct prime factors of n, a calculation which costs $\sqrt{n}$. This is clearly inefficient for large values of n so we look for a more cost effective method.

Consider an elliptic curve over $\mathbb{Q}$ given by

$$E : y^2 = x^3 + ax + b \,(= f(x)).$$

We have that $\Delta_E = -16(4a^3 + 27b^2)$ and will assume that this quantity is square-free.

The 'global' root number of E is defined via the product of 'local' root numbers, i.e.

$$w_{E/\mathbb{Q}} = -\prod_{p \mid \Delta_E} w_{E/\mathbb{Q}_p},$$

where

$$w_{E/\mathbb{Q}_p} = \begin{cases} -1 & \text{split multiplicative reduction at } p, \\ 1 & \text{non-split multiplicative reduction at } p, \end{cases}$$

(noting that at no primes do we have additive reduction due to Δ_E being square-free).

Using the characterisation of multiplicative reduction type at a prime $p \mid \Delta_E$ via Legendre symbols, i.e.

$$E \text{ has split multiplicative reduction at } p \Leftrightarrow \left(\frac{-c_6}{p}\right) = +1,$$

our expression for $w_{E/\mathbb{Q}}$ becomes

$$w_{E/\mathbb{Q}} = -(-1)^{\#\text{distinct prime factors of } \Delta_E} \prod_{p \mid \Delta_E} \left(\frac{-c_6}{p}\right) = -\mu(\Delta_E)\left(\frac{-c_6}{\Delta_E}\right),$$

where we use the 'Jacobi symbol'. The upshot of this is that the quantity we're interested in can be determined from $w_{E/\mathbb{Q}}$ through

$$\mu(\Delta_E) = -w_{E/\mathbb{Q}}\left(\frac{-c_6}{\Delta_E}\right).$$

Such a Jacobi symbol is quick to compute (incurring a cost of only $\log \Delta_E$), so if we know $w_{E/\mathbb{Q}}$ (or assuming the parity conjecture, the parity of rank $E/\mathbb{Q}$) then we have a quicker way to find $\mu(\Delta_E)$ – hence our goal.

2 Quadratic twists

For $d \in \mathbb{Z}$ square-free, consider the quadratic twist of E by d, i.e.

$$E_d : dy^2 = x^3 + ax + b.$$

If $\gcd(d, \Delta_E) = 1$, it can be shown [1] that

$$w_{E/\mathbb{Q}} = w_{E_d/\mathbb{Q}} \cdot \operatorname{sign}(d) \cdot \left(\frac{d}{\Delta_E}\right).$$

Similarly to what we saw previously, the means that $w_{E/\mathbb{Q}}$ can be determined from $w_{E_d/\mathbb{Q}}$ in a computation of cost $\log \Delta_E$.

The Minimalists conjecture refers to the distribution of the rank within a 'suitably random' family of elliptic curves (where suitably random is a term that has no precise definition), i.e. a family of twists. It should provide an indication of how $w_{E_d/\mathbb{Q}}$ behaves, and if we're lucky, this should tell us what $w_{E/\mathbb{Q}}$ is.

The conjecture can be interpreted in 2 ways, both of which are quite vague. A more precise statement says:

Conjecture 2.1 (Minimalists Conjecture A)**.** *For* 100% *of curves within the family,*

$$\textit{rank } E/\mathbb{Q} = 0 \textit{ or } 1.$$

Whereas a weaker statement is:

Conjecture 2.2 (Minimalists Conjecture B)**.** *For* 100% *of curves within the family, the rank is 'as small as possible' subject to the root number.*

We can assert which formulation is valid upon choosing a particular family.

Consider the family of twists arising from taking $d = f(n)$ for $n \in \mathbb{Z}$, i.e.

$$\mathcal{F} = \{E_{f(n)} \,|\, n \in \mathbb{Z} \text{ or some interval}\}.$$

An observation is that amongst this family the rank is almost always at least 1: obvious rational points are given by $(n, \pm 1)$ and these typically have infinite order.

This implies that statement A is incorrect – it it were true, 100% of curves in this family would have rank 1 which computational evidence contradicts.

3 An Example

An explicit example is given by taking

$$E : y^2 + y = x^3 - x^2,$$

this elliptic curve has $\Delta_E = -11$. A linear transformation to short Weierstrass form gives

$$f(x) = x^3 - \frac{1}{3}x + \frac{19}{108}$$

and preserves Δ_E.

- Varying n from -10000 to 10000 gives an equal distribution of root numbers, i.e. 50% of the $w_{E_{f(n)}/\mathbb{Q}}$ are $+1$ and 50% are -1.
- Varying n from 0 to 10000 gives an unequal distribution of root numbers, i.e. 37% of the $w_{E_{f(n)}/\mathbb{Q}}$ are $+1$ and 63% are -1.
- Varying n from 0 to 10000 within a fixed congruence class gives:
  - 100% of $w_{E_{f(n)}/\mathbb{Q}}$ are $+1$ when n is 1, 6, 7 or 8 mod 11
  - 100% of $w_{E_{f(n)}/\mathbb{Q}}$ are -1 when n is 0, 2, 4, 5, 9, 10 mod 11
  - 4% of the $w_{E_{f(n)}/\mathbb{Q}}$ are $+1$ and 96% are -1 when n is 3 mod 11

Other examples, for curves of small discriminant, show that there are usually a small number of congruence classes that misbehave. Unfortunately I was unable to find a pattern amongst the misbehaving congruence classes that would describe this further.

I was also able to observe that when the conductor of the curve in question becomes large, we obtain an equal distribution of root numbers when varying n from 0 to 10000. Therefore, being able to determine $w_{E/\mathbb{Q}}$ via probabilistic methods is hopeless.

References

[1] Dokchitser, V., "Root numbers of non-abelian twists of elliptic curves". *Proceedings of the London Mathematical Society, 91*(2), pp.300-324, 2005.