MATH REVIEW 2464773 (SWINNERTON-DYER)

One of the most actively studied areas in elliptic curve arithmetic is that of the behavior of the ($\mathbb{F}_2$)-rank of the 2-Selmer group of an elliptic curve $E_{/\mathbb{Q}}$ under quadratic twists. The present paper offers a striking new result in this area. Suppose that $E_{/\mathbb{Q}}$ is an elliptic curve with $E[4](\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Let $\mathcal{S}$ be the set consisting of 2 and the primes of bad reduction for E. Say an integer b is **admissible** (terminology introduced by the reviewer) if it is squarefree and is a unit in $\mathbb{Z}_p$ for all $p \in \mathcal{S}$. For an admissible integer b, we denote by E^b the quadratic twist of E by b.

Let b_0 be an admissible integer, let d_0 be the 2-Selmer rank of E^{b_0}, and let $d \geq 2$ be an integer such that $d \equiv d_0 \pmod 2$. Then a qualitative consequence of the paper's main result (Theorem 1) is the following: there exist infinitely many admissible integers b such that the 2-Selmer rank of E^b is d.

Theorem 1 itself is stronger, and stranger. The author fixes a positive integer N, considers the set of admissible integers b with exactly N prime factors and observes that although this is an infinite set, the rank d_b of the 2-Selmer group of E^b depends only on the sign of d_b, its images in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ for $p \in \mathcal{S}$ and the quadratic characters of the prime divisors of b with respect to each other, so it is in some sense governed by a finite set of values. He then defines a suitable probability distribution on this finite set of values and considers the quantity π_d^N, the probability that one of these values is equal to d for some $d \geq 2$ and of the same parity as d_0. Theorem 1 states that

$$\lim_{N\to\infty} \pi_d^N = \alpha_{d-2},$$

where for an integer $k \geq 0$,

$$\alpha_k = \frac{2^k \prod_{n=0}^{\infty}\left(1 - 2^{-2n-1}\right)}{\prod_{j=1}^{k}(2^j - 1)}.$$

The α_k's appear also in (Heath-Brown, MR1292115), wherein it is shown that $\sum_{k=0}^{\infty} \alpha_{2k} = \sum_{k=0}^{\infty} \alpha_{2k+1} = 1$.

The argument is quite intricate. However, it is almost completely self-contained and "middlebrow", the only exception (on both counts) being the proofs of some key facts on 2-descent, recalled from (Colliot-Thelene, Skorobogatov and Swinnerton-Dyer, MR1660925) and (Skorobogatov and Swinnerton-Dyer, MR2183385). Swinnerton-Dyer has written Section 3 – "An algorithm for 2-descent" – so as to be comprehensible to (sufficiently intrepid) readers who are not experts on 2-descent. The lucid exposition of Section 3 should be of independent interest, and use, to many. The endgame is an unusual one for a paper in this area: the final step is an invocation of the main theorem on Markov chains!

Some further remarks:

(1) According to the author, the entire proof goes through over a number field for which the conic $X^2+Y^2+Z^2=0$ has no rational points, in particular any field with at least one real place.

(2) The interested reader will surely also want to consult the recent preprint of B. Mazur and K. Rubin, "Ranks of twists of elliptic curves and Hilbert's 10th problem", which nicely complements the present paper in that the results it presents are strongest inthe case of elliptic curves over number fields without rational points of order 2.

(3) The parity condition in the statement of Theorem 1 is a natural one. In this regard, one should consult the recent paper of T. Dokschitser and V. Dokchitser (MR2491537) which characterizes elliptic curves over number fields K with constant 2-Selmer parity (such K are necessarily totally imaginary). It would be interesting to explicitly verify that the methods of the present paper carry over to a case of constant 2-Selmer parity. By contrast, Mazur and Rubin conjecture that for any elliptic curve E over a real number field K, a positive proportion of the quadratic twists of E have 2-Selmer rank equal to any preassigned integer $r \geq \dim_{\mathbb{F}_2} E(K)[2]$.