AVERAGE ROOT NUMBERS
IN FAMILIES OF ELLIPTIC CURVES

OTTAVIO G. RIZZO

(Communicated by David E. Rohrlich)

Abstract. We introduce a height measure on $\mathbb{Q}$ to count rational numbers. Through it, we prove a density result on the average value of the root numbers of families of twists of elliptic curves.

Zagier and Kramarz computed in [11] the rank of the curves $x^3 + y^3 = m$, with $m$ an integer $< 70,000$. These data suggest that the rank is even for exactly half of the twists of $x^3 + y^3 = 1$. This conjecture has been proved (conditionally on the Birch and Swinnerton-Dyer conjecture) by Mai in [4]. Define, as usual, the root number $W(E)$ of an elliptic curve $E$ as the sign of the functional equation of the $L$ series associated to $E$ (see C.16 of [9]). According to the parity conjecture, $W(E) = (-1)^{\text{rank}(E)}$.

Given a proper definition of average, we can express Mai’s result as saying that the average value of the root numbers of the quadratic twists of $x^3 + y^3 = 1$ is 0.

Let $H(m/n) = \max\{|m|, |n|\}$ be the height of $m/n$, where $m$ and $n$ are relatively prime integers.

Definition. The average value of a function $\psi : \mathbb{Q} \to \mathbb{R}$ is

$$\text{Av}_\psi(t) = \lim_{T \to \infty} \frac{\sum_{H(t) < T} \psi(t)}{\sum_{H(t) < T} 1},$$

where $t$ varies in $\mathbb{Q}$, provided that the limit exists.

Fix throughout this paper an elliptic curve $E$: $y^2 = x^3 + Ax + B$ defined over $\mathbb{Q}$, and a polynomial $f(t) \in \mathbb{Q}[t]$. Denote by $E_f(t)$ the family of twists $f(t)y^2 = x^3 + Ax + B$. One would expect $\text{Av}_W(E_f(t))$ to be 0, as in the Zagier–Kramarz case—actually, we have exactly the opposite result:

Theorem 1. Let $E$ be a fixed elliptic curve defined over $\mathbb{Q}$. Given any open subset $I$ of $[-1,1]$, there exists a polynomial $f(t) \in \mathbb{Q}[t]$ of degree at most four, such that $\text{Av}_W(E_f(t)) \in I$.

To prove this result, we introduce a height measure on $\mathbb{Q}$, and we express the average value of a function as an integral. Using results of Rohrlich [6], we find enough polynomials to realize the conditions of the theorem.
1. The height measure

Definition. For any subset $U$ of $Q$, we define its height measure to be the following limit, provided it exists:

$$\mu(U) = \lim_{t \to \infty} \frac{\# \{ r \in U : H(r) \leq t \}}{\# \{ r \in Q : H(r) \leq t \}}.$$ 

If the limit exists, we say that $U$ is $\mu$-measurable.

Remark 2. There exist subsets of $Q$ which are not $\mu$-measurable.

Recall that a set field is a non-empty family $\Sigma$ of subsets of a set $S$ that contains the empty set, the complement of each element of $\Sigma$, and every finite union of elements of $\Sigma$. Unfortunately, the height measure is not a measure in the classic sense, since it is not $\sigma$-additive: $Q = \bigcup_{r \in Q} \{ r \}$, but $\mu(Q) = 1$, while $\sum_r \mu(\{ r \}) = 0$.

On the other hand, it is a positive valued additive set function on the set field generated by intervals (see III.1 of [3]).

Proposition 3. Let $U$ and $U'$ be $\mu$-measurable subsets of $Q$. Then the following properties hold:

1. $\mu(\emptyset) = 0$;
2. $U \cup U'$ is $\mu$-measurable, and $\mu(U \cup U') \leq \mu(U) + \mu(U')$, with equality holding if $U$ and $U'$ are disjoint;
3. $\mu(Q) = 1$.

Proof. Points 1 and 3 follow immediately from the definition of $\mu$, as does point 2 when $U$ and $U'$ are disjoint. To prove point 2 in general, one uses the identity $U \cup U' = (U \setminus U') \cup (U \cap U') \cup (U' \setminus U)$.

Theorem 4. $\mu$ is an additive set function on the set field generated by the intervals in $Q$. Furthermore, its value is given by

$$\mu((-\infty, x]) = \begin{cases} -\frac{1}{4} & \text{if } x \leq -1, \\ \frac{1}{2} + \frac{x}{4} & \text{if } |x| \leq 1, \\ 1 - \frac{1}{16} & \text{if } x \geq 1. \end{cases}$$

Definition. For every integer $t > 0$, we define

$$\Phi(t) = \{ r \in Q : H(r) = t \},$$

$$\Phi(t, x) = \{ r \in Q : H(r) = t, r \leq x \}.$$

Lemma 5. If $t > 1$, then $\#\Phi(t) = 4\phi(t)$.

Proof. If we write $r = m/n$, with $m$ and $n$ relatively prime integers and with $n > 0$, then $\Phi(t) = \{ m/n : (m, n) \in \mathbb{Z} \times \mathbb{Z}^\times, \max\{|m| , n\} = t, \gcd(m, n) = 1 \}$.

If $t > 1$, then clearly $\pm t/t \notin \Phi(t)$ and

$$\Phi(t) = \{ \pm t/n : n \in \mathbb{Z}, 1 \leq n \leq t, \gcd(n, t) = 1 \} \\
\cup \{ m/t : m \in \mathbb{Z}, -t \leq m \leq t, \gcd(m, t) = 1 \},$$

whose order is $4\phi(t)$.

Definition. In analogy to Euler’s $\phi$ function, we define for any positive integer $t$ and any positive number $x$, a function

$$\phi(t, x) = \#\{ \text{positive integers } \leq x \text{ which are relatively prime to } t \}.$$
and a function
\[ \hat{\phi}(t, x) = \#\{ \text{positive integers } < x \text{ which are relatively prime to } t \}. \]

**Proposition 6.** Suppose \( t > 1 \). Then
\[
\#\Phi(t, x) = \begin{cases} 
\phi(t, -t/x) & \text{if } x \leq -1, \\
2\phi(t) - \hat{\phi}(t, -xt) & \text{if } -1 \leq x \leq 0, \\
2\phi(t) + \phi(t, xt) & \text{if } 0 \leq x \leq 1, \\
4\phi(t) - \hat{\phi}(t, -t/x) & \text{if } x \geq 1.
\end{cases}
\]

**Proof.** Analogously to the proof of Lemma 5, we can rewrite \( \Phi(t, x) \) as
\[
\{ m/n : (m, n) \in \mathbb{Z} \times \mathbb{Z}^+, \max\{|m|, n\} = t, \gcd(m, n) = 1, m \leq xn \}.
\]
Suppose now that \( x \leq -1 \); then \( m \leq -n \) and \( t = H(m/n) = -m \). Thus
\[
\Phi(t, x) = \{ -t/n : n \in \mathbb{Z}, \gcd(n, t) = 1, 1 \leq n \leq -t/x \}.
\]
Hence, \( \#\Phi(t, x) = \phi(t, -t/x) \). The other cases are similar. \( \square \)

**Proposition 7.** For any \( x \) and \( t > 0 \) we have that \( \left| \phi(t, x) - \frac{x}{t} \phi(t) \right| \leq d(t) \), where \( d(n) \) is the number of divisors of \( n \). As \( T \) increases to infinity,
\[
\sum_{t \leq T} \phi(t, x) = \frac{x}{2\zeta(2)} T^2 + O(T \log T),
\]
where the \( O \)-constant is independent of \( x \). The same estimates hold when \( \phi \) is replaced by \( \hat{\phi} \).

**Proof.** By definition, \( \phi(t, x) \) is equal to
\[
\phi(t, x) = \sum_{\substack{n \leq x \\
\gcd(n, t) = 1}} 1.
\]
Let \( \mu(n) \) be as usual the Môbius function of \( n \). We have that, for every positive integer \( n \),
\[
\sum_{d|n} \mu(d) = \begin{cases} 
1 & \text{if } n = 1, \\
0 & \text{if } n > 1.
\end{cases}
\]
(See, for example, Theorem 2.1 of [1].) Then
\[
\phi(t, x) = \sum_{n \leq x} \sum_{d|n} \mu(d) = \sum_{d|t} \sum_{n \leq x \atop \gcd(n, d) = 1} \mu(d) = \sum_{d|t} \left\lfloor \frac{x}{d} \right\rfloor \mu(d)
\]
\[
= \sum_{d|t} \frac{\mu(d)}{d} x - \sum_{d|t} \mu(d) \left( \frac{x}{d} - \left\lfloor \frac{x}{d} \right\rfloor \right).
\]
It is well known (see Theorem 2.3 of [1]) that \( \sum_{d|t} \mu(d)/d = \phi(t)/t \). Therefore, since
\[
\left| \mu(d) \left( \frac{x}{d} - \left\lfloor \frac{x}{d} \right\rfloor \right) \right| \leq 1,
\]
we have that
\[
\left| \phi(t, x) - \frac{\phi(t)}{t} x \right| \leq d(t).
\]
Analogously, we have that
\[ \tilde{\phi}(t, x) = \sum_{d \mid t} \sum_{n \leq x, n \equiv 0 (d)} \mu(d) = \sum_{d \mid t} \frac{\mu(d)}{d} x + \sum_{d \mid t} \mu(d) \left( \left\lfloor \frac{x}{d} \right\rfloor - \frac{x}{d} - 1 \right). \]

Once again we get
\[ |\mu(d) \left( \left\lfloor \frac{x}{d} \right\rfloor - \frac{x}{d} - 1 \right)| \leq 1, \]
thus
\[ |\tilde{\phi}(t, x) - \frac{\phi(t)}{t} x| \leq d(t). \]

The second part follows at once from the following formulae, as \( T \) tends to infinity (see Theorems 3.3, 11.7, and 3.7 of [1]):
\[ \sum_{n \leq T} d(n) = T \log T + O(T), \]
\[ \sum_{n \leq T} \phi(n) = \frac{1}{2\zeta(2)} T^2 + O(T \log T). \]

\( \square \)

**Proof of Theorem 4.** Suppose that eq. (1) holds: it follows immediately that intervals are \( \mu \)-measurable. By Proposition 3, all finite combinations of intervals are \( \mu \)-measurable. Thus, \( \mu \) is additive on the set field generated by intervals.

We are left to prove eq. (1): we have that
\[ \lim_{T \to \infty} \frac{\# \{ r \in \mathbb{Q} : H(r) \leq T, r \leq x \}}{\# \{ r \in \mathbb{Q} : H(r) \leq T \}} = \lim_{T \to \infty} \frac{\sum_{t=1}^{T} \# \Phi(t, x)}{\sum_{t=1}^{T} \# \Phi(t)}. \]

Suppose that \( x \leq 1 \). Then, by Lemma 5 and Proposition 6,
\[ \lim_{T \to \infty} \frac{\sum_{t=1}^{T} \# \Phi(t, x)}{\sum_{t=1}^{T} \# \Phi(t)} = \lim_{T \to \infty} \frac{\sum_{t=1}^{T} \phi(t, -t/x)}{\sum_{t=1}^{T} 4\phi(t)}. \]

By Proposition 7 and eq. (2), this is
\[ \lim_{T \to \infty} \frac{\sum_{t=1}^{T} \left( -\phi(t) \frac{1}{x} + O(d(t)) \right)}{\sum_{t=1}^{T} 4\phi(t)} = \frac{1}{4x} + O \left( \frac{T \log T}{\sum_{t=1}^{T} \phi(t)} \right). \]

By eq. (3), the error term is actually \( O(\log T/T) \), so that the limit converges and \( \mu(x) = -1/4x \). The remaining cases are proved in a similar way. \( \square \)

**Definition.** The height measure \( \mu \) of \( \mathbb{R} \) is the measure induced on the Borel sets of \( \mathbb{R} \) by the function \( \mu(x) \).

**Remark 8.** Since \( \mu(x) \) is a bounded monotone increasing continuous function, differentiable at every \( x \neq \pm 1 \), by standard measure theory \( \mu \) is well defined (see, for example, Chapter 7 of [8], in particular Exercise 13), and it is absolutely continuous with respect to the standard Lebesgue measure.

**Proposition 9.** Let \( f \) be a step function over \( \mathbb{Q} \), i.e., \( f = \sum_{i=0}^{n} a_i \chi_i \), where \( a_i \in \mathbb{Q} \) and \( \chi_i \) is the characteristic function of an interval. Then \( \text{Av} f(t) = \int_{\mathbb{R}} f(t) d\mu(t) \).
Proof. If $\chi$ is the characteristic function of some interval $I$, then it is clear that

$$\text{Av}_{\chi}(t) = \lim_{T \to \infty} \frac{\# \{ r \in \mathbb{Q} : H(r) \leq T, r \in I \}}{\# \{ r \in \mathbb{Q} : H(r) \leq T \}} = \mu(I) = \int_{\mathbb{R}} \chi(t) \, d\mu(t).$$

By linearity, we get the same result for $f$. \hfill $\square$

2. Root numbers

Recall that the root number of an elliptic curve has an intrinsic definition (see [2], [10] and especially [7]) independent of any conjectures, as a product of local factors.

**Definition.** Given an elliptic curve $E$ and a polynomial $f(t)$, we say that $f(t)$ is a Rohrlich polynomial for $E$ if, for every $t$ such that $f(t) \neq 0$, $W(E^{f(t)}) = \epsilon \text{sgn} f(t)$, where $\epsilon = 1$ is independent of $t$.

**Proposition 10.** Let $m$, $n$ be even integers with $0 \leq m \leq n$. If $E$ does not satisfy the technical condition (§) of [6], we further suppose that $n$ is divisible by 4. Then there exists an irreducible polynomial $f(t) \in \mathbb{Q}[t]$, Rohrlich for $E$, of degree $n$, and exactly $m$ real zeros, all of them simple.

*Proof.* See Proposition 8 of [6]. \hfill $\square$

**Notation.** Given a real function $f(t)$, write $s_f(t)$ for the function $\text{sgn} f(t)$.

**Proposition 11.** Let $f$ be a Rohrlich polynomial for $E$ of even degree $n$. For any rational number $r \neq 0$, define $f_r(t) = r^n f(t/r)$. Then $f_r(t)$ is a Rohrlich polynomial for $E$.

*Proof.* Since $n$ is even, $f_r(t) \equiv f(r/t) \mod \mathbb{Q}^*$. Hence,

$$W(E^{f_r(t)}) = W(E^{f(t/r)}) = \text{sgn} f(t/r) = \text{sgn} f_r(t/r).$$

\hfill $\square$

**Lemma 12.** Suppose $f(t)$ is a Rohrlich polynomial for $E$. Then, for every $r \in \mathbb{Q}$, $g(t) = f(t - r)$ is Rohrlich.

*Proof.* Obvious. \hfill $\square$

**Proposition 13.** Let $f$ be a polynomial with real coefficients, even degree, and an even number of real roots. Let $\epsilon = \lim_{|t| \to \infty} s_f(t)$. Define a map

$$\lambda: \mathbb{R} \to \mathbb{R}, \quad r \mapsto \int_{\mathbb{R}} s_{f_r}(t) \, d\mu(t).$$

Assume that $\epsilon f(0) < 0$. Then $\lambda(\mathbb{Q})$ is dense in $[-1, 1]$.

*Proof.* The idea is to prove that:

1. $\lim_{r \to \infty} \lambda(r) = \epsilon$.
2. $\lim_{r \to 0} \lambda(r) = s_f(0)$.
3. $\lambda$ is a continuous function from $\mathbb{R}$ to $\mathbb{R}$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Thus, if the two limits are +1 and −1, then \( \lambda(r) \) spans \([-1,1]\) as \( r \) runs from 0 to \( \infty \). Restricting \( r \) to \( Q \) leaves the image of \( \lambda \) dense.

Let \( x_1, \ldots, x_m \) be the real roots of \( f \), and let \( x_0 = -\infty, x_{m+1} = +\infty \). By assumption \( f(0) \neq 0 \), say \( x_{i_0} < 0 < x_{i_0+1} \). Let \( \chi_i \) be the characteristic function of \((x_i, x_{i+1})\). Since we assumed that \( f \) has even degree and an even number of real roots, we can decompose \( s_f(t) = \sum_{i=0}^{m} (-1)^i \chi_i(t) \). Since \( s_f(t) = s_f(t/r) \),
\[
\lim_{r \to \infty} \int_{\mathbb{R}} s_f(t) \, d\mu(t) = \epsilon \sum_{i=0}^{m} (-1)^i \lim_{r \to \infty} \int_{\mathbb{R}} \chi_i(t/r) \, d\mu(t),
\]
where we can exchange the limit with the sum, since the latter is finite. By Theorem 4,
\[
(4) \quad \lim_{r \to \infty} \int_{\mathbb{R}} \chi_0(t/r) \, d\mu(t) = \lim_{r \to \infty} \mu(x_0/r) - \mu(-\infty) = \mu(0) - \mu(-\infty) = \frac{1}{2}.
\]
Analogously,
\[
(5) \quad \lim_{r \to \infty} \int_{\mathbb{R}} \chi_m(t/r) \, d\mu(t) = \frac{1}{2}.
\]
On the other hand, for any \( i = 1, \ldots, m-1 \),
\[
(6) \quad \lim_{r \to \infty} \int_{\mathbb{R}} \chi_i(t/r) \, d\mu(t) = \lim_{r \to \infty} \mu(x_{i+1}/r) - \mu(x_i/r) = 0.
\]
Putting (4), (5) and (6) together, we have proved that
\[
\lim_{r \to \infty} \int_{\mathbb{R}} s_f(t) \, d\mu(t) = \epsilon.
\]
Consider now the same problem as \( r \) decreases to 0. If \( i \neq i_0 \), then \( \chi_i(t/r) \to 0 \); on the other hand, \( \chi_{i_0}(t/r) \to 1 \). Hence,
\[
\lim_{r \to 0} \int_{\mathbb{R}} \chi_i(t/r) \, d\mu(t) = \begin{cases} 1 & \text{if } i = i_0, \\
0 & \text{otherwise.} \end{cases}
\]
Therefore,
\[
\lim_{r \to 0} \int_{\mathbb{R}} s_f(t) \, d\mu(t) = s_f(0).
\]
We are left to prove the continuity of \( \lambda \). Since \( s_f \) is a finite linear combination of characteristic functions of intervals, it is enough to prove that the map
\[
r \to \int_{\mathbb{R}} \chi(a,b)(t/r) \, d\mu(t) = \int_{ar}^{br} \mu(t) = \mu(br) - \mu(ar)
\]
is continuous for any \(-\infty \leq a \leq b \leq \infty \), where \( \chi(a,b) \) is the characteristic function of \((a,b)\). Since \( \mu \) is bounded and \( \mu(t) \) is continuous by Theorem 4, we are done.

**Proof of Theorem 1.** By Proposition 10, we can choose a polynomial \( f \) of degree two or four, with exactly two real roots \( x_1 < x_2 \), both simple. By Lemma 12, we can suppose that \( x_1 < 0 < x_2 \). By Propositions 9 and 11,
\[
(7) \quad \text{Av} W\left(E_{f(t)}\right) = \int_{\mathbb{R}} s_f(t) \, d\mu(t).
\]
But \( f \) satisfies the conditions of Proposition 13, and this proves the statement of the theorem.
3. Example

Let \( E \) be the modular curve \( X_0(11) \): \( y^2 + y = x^3 - x^2 - 10x - 20 \), and let \( f(t) = 11 - t^2 \). It is shown in 4.2.1 of [5], using the machinery of [6], that \( W(E^{f(t)}) = -\text{sgn}(f(t)) \).

**Proposition 14.** If \( E \) and \( f \) are as above, we have that:

1. For any \( r \in \mathbb{Q}, r > 0 \),
   \[
   \text{Av}_t W(E^{f_r(t)}) = \begin{cases} 
   1 / (r\sqrt{11}) - 1 & \text{if } r\sqrt{11} > 1, \\
   1 - r\sqrt{11} & \text{if } r\sqrt{11} < 1.
   \end{cases}
   \]

2. The set \( \{ \text{Av}_t W(E^{f_r(t)}) : r \in \mathbb{Q}, r > 0 \} \) is dense in \([-1, 1]\).

**Proof.** As in eq. (7), we have that
   \[
   \text{Av}_t W(E^{f_r(t)}) = \int_{\mathbb{R}} -\text{sgn}(11r^2 - t^2) \, d\mu(t),
   \]
   since the roots of \( 11r^2 - t^2 \) are \( t = \sqrt{11}r \), this is
   \[
   = 1 + 2\mu(-r\sqrt{11}) - 2\mu(r\sqrt{11}).
   \]
   Item 1 now follows from Theorem 4. Item 2 follows either from 1 or from Theorem 1.

**References**


Department of Mathematics, Brown University, Box 1917, Providence, Rhode Island 02912

Current address: Department of Mathematics and Statistics, Queen’s University, Kingston, Ontario, Canada K7L 3N6

E-mail address: otto@math.brown.edu

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use