

AVERAGE ROOT NUMBERS IN FAMILIES OF ELLIPTIC CURVES

OTTAVIO G. RIZZO

(Communicated by David E. Rohrlich)

ABSTRACT. We introduce a height measure on \mathbf{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 $\psi : \mathbf{Q} \rightarrow \mathbf{R}$ is

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

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

Fix throughout this paper an elliptic curve $E: y^2 = x^3 + Ax + B$ defined over \mathbf{Q} , and a polynomial $f(t) \in \mathbf{Q}[t]$. 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 \mathbf{Q} . Given any open subset I of $[-1, 1]$, there exists a polynomial $f(t) \in \mathbf{Q}[t]$ 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 \mathbf{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.

Received by the editors September 15, 1997.

1991 *Mathematics Subject Classification.* Primary 11G05; Secondary 11D25, 11C08, 28C10.

This research was partially written while the author was supported by a grant of the Istituto Nazionale di Alta Matematica of Rome.

1. THE HEIGHT MEASURE

Definition. For any subset U of \mathbf{Q} , we define its *height measure* to be the following limit, provided it exists:

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

If the limit exists, we say that U is μ -measurable.

Remark 2. There exist subsets of \mathbf{Q} which are not μ -measurable.

Recall that a set field is a non-empty family Σ of subsets of a set S that contains the empty set, the complement of each element of Σ , and every finite union of elements of Σ . Unfortunately, the height measure is not a measure in the classic sense, since it is not σ -additive: $\mathbf{Q} = \bigcup_{r \in \mathbf{Q}} \{r\}$, but $\mu(\mathbf{Q}) = 1$, 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 μ -measurable subsets of \mathbf{Q} . Then the following properties hold:*

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

Proof. Points 1 and 3 follow immediately from the definition of μ , 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. μ is an additive set function on the set field generated by the intervals in \mathbf{Q} . Furthermore, its value is given by

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

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

$$\begin{aligned} \Phi(t) &= \{r \in \mathbf{Q} : H(r) = t\}, \\ \Phi(t, x) &= \{r \in \mathbf{Q} : H(r) = t, r \leq x\}. \end{aligned}$$

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 $\Phi(t) = \{m/n : (m, n) \in \mathbf{Z} \times \mathbf{Z}^{>0}, \max\{|m|, n\} = t, \gcd(m, n) = 1\}$.

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

$$\begin{aligned} \Phi(t) &= \{\pm t/n : n \in \mathbf{Z}, 1 \leq n \leq t, \gcd(n, t) = 1\} \\ &\cup \{m/t : m \in \mathbf{Z}, -t \leq m \leq t, \gcd(m, t) = 1\}, \end{aligned}$$

whose order is $4\phi(t)$. □

Definition. In analogy to Euler's ϕ 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

$$\tilde{\phi}(t, x) = \#\{\text{positive integers } < x \text{ which are relatively prime to } t\}.$$

Proposition 6. *Suppose $t > 1$. Then*

$$\#\Phi(t, x) = \begin{cases} \phi(t, -t/x) & \text{if } x \leq -1, \\ 2\phi(t) - \tilde{\phi}(t, -xt) & \text{if } -1 \leq x \leq 0, \\ 2\phi(t) + \phi(t, xt) & \text{if } 0 \leq x \leq 1, \\ 4\phi(t) - \tilde{\phi}(t, -t/x) & \text{if } x \geq 1. \end{cases}$$

Proof. Analogously to the proof of Lemma 5, we can rewrite $\Phi(t, x)$ as

$$\{m/n : (m, n) \in \mathbf{Z} \times \mathbf{Z}^{>0}, \max\{|m|, n\} = t, \gcd(m, n) = 1, m \leq xn\}.$$

Suppose now that $x \leq -1$; then $m \leq -n$ and $t = H(m/n) = -m$. Thus

$$\Phi(t, x) = \{-t/n : n \in \mathbf{Z}, \gcd(n, t) = 1, 1 \leq n \leq -t/x\}.$$

Hence, $\#\Phi(t, x) = \phi(t, -t/x)$. The other cases are similar. □

Proposition 7. *For any x and $t > 0$ we have that $|\phi(t, x) - \frac{x}{t}\phi(t)| \leq d(t)$, 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 ϕ is replaced by $\tilde{\phi}$.

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 Möbius 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

$$\begin{aligned} \phi(t, x) &= \sum_{n \leq x} \sum_{d|(n, t)} \mu(d) = \sum_{d|t} \sum_{\substack{n \leq x \\ n \equiv 0 \pmod{d}}} \mu(d) = \sum_{d|t} \left\lfloor \frac{x}{d} \right\rfloor \mu(d) \\ &= \sum_{d|t} \frac{\mu(d)}{d} x - \sum_{d|t} \mu(d) \left(\frac{x}{d} - \left\lfloor \frac{x}{d} \right\rfloor \right). \end{aligned}$$

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

$$\tilde{\phi}(t, x) = \sum_{d|t} \sum_{\substack{n < x \\ n \equiv 0 \pmod{d}}} \mu(d) = \sum_{d|t} \frac{\mu(d)}{d} x + \sum_{d|t} \mu(d) \left(\left\lceil \frac{x}{d} \right\rceil - \frac{x}{d} - 1 \right).$$

Once again we get

$$\left| \mu(d) \left(\left\lceil \frac{x}{d} \right\rceil - \frac{x}{d} - 1 \right) \right| \leq 1,$$

thus

$$\left| \tilde{\phi}(t, x) - \frac{\phi(t)}{t} x \right| \leq d(t).$$

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]):

$$(2) \quad \sum_{n \leq T} d(n) = T \log T + O(T),$$

$$(3) \quad \sum_{n \leq T} \phi(n) = \frac{1}{2\zeta(2)} T^2 + O(T \log T).$$

□

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

We are left to prove eq. (1): we have that

$$\lim_{T \rightarrow \infty} \frac{\#\{r \in \mathbf{Q} : H(r) \leq T, r \leq x\}}{\#\{r \in \mathbf{Q} : H(r) \leq T\}} = \lim_{T \rightarrow \infty} \frac{\sum_{t=1}^T \#\Phi(t, x)}{\sum_{t=1}^T \#\Phi(t)}.$$

Suppose that $x \leq 1$. Then, by Lemma 5 and Proposition 6,

$$\lim_{T \rightarrow \infty} \frac{\sum_{t=1}^T \#\Phi(t, x)}{\sum_{t=1}^T \#\Phi(t)} = \lim_{T \rightarrow \infty} \frac{\sum_{t=1}^T \phi(t, -t/x)}{\sum_{t=1}^T 4\phi(t)}.$$

By Proposition 7 and eq. (2), this is

$$= \lim_{T \rightarrow \infty} \frac{\sum_{t=1}^T (-\phi(t) \frac{1}{x} + O(d(t)))}{\sum_{t=1}^T 4\phi(t)} = -\frac{1}{4x} + O\left(\frac{T \log T}{\sum_{t=1}^T \phi(t)}\right).$$

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. □

Definition. The *height measure* μ of \mathbf{R} is the measure induced on the Borel sets of \mathbf{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 μ 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 \mathbf{Q} , i.e., $f = \sum_{i=0}^n a_i \chi_i$, where $a_i \in \mathbf{Q}$ and χ_i is the characteristic function of an interval. Then $\text{Av } f(t) = \int_{\mathbf{R}} f(t) d\mu(t)$.

Proof. If χ is the characteristic function of some interval I , then it is clear that

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

By linearity, we get the same result for f . □

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 $f(t) \neq 0$, $W(E^{f(t)}) = \epsilon \operatorname{sgn} f(t)$, 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 $f(t) \in \mathbf{Q}[t]$, Rohrlich for E , of degree n , and exactly m real zeros, all of them simple.*

Proof. See Proposition 8 of [6]. □

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

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, $f_r(t) \equiv f(r/t) \pmod{\mathbf{Q}^{*2}}$. Hence,

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

□

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

Proof. Obvious. □

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

$$\begin{aligned} \lambda: \mathbf{R} &\longrightarrow \mathbf{R} \\ r &\longmapsto \int_{\mathbf{R}} s_{f_r}(t) \, d\mu(t). \end{aligned}$$

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

Proof. The idea is to prove that:

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

Thus, if the two limits are +1 and -1, then $\lambda(r)$ spans $[-1, 1]$ as r runs from 0 to ∞ . Restricting r to \mathbf{Q} leaves the image of λ dense.

Let x_1, \dots, 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 χ_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 $s_f(t) = \sum_{i=0}^m (-1)^i \epsilon \chi_i(t)$. Since $s_{f_r}(t) = s_f(t/r)$,

$$\lim_{r \rightarrow \infty} \int_{\mathbf{R}} s_{f_r}(t) \, d\mu(t) = \epsilon \sum_{i=0}^m (-1)^i \lim_{r \rightarrow \infty} \int_{\mathbf{R}} \chi_i(t/r) \, d\mu(t),$$

where we can exchange the limit with the sum, since the latter is finite. By Theorem 4,

$$(4) \quad \lim_{r \rightarrow \infty} \int_{\mathbf{R}} \chi_0(t/r) \, d\mu(t) = \lim_{r \rightarrow \infty} \mu(x_0/r) - \mu(-\infty) = \mu(0) - \mu(-\infty) = \frac{1}{2}.$$

Analogously,

$$(5) \quad \lim_{r \rightarrow \infty} \int_{\mathbf{R}} \chi_m(t/r) \, d\mu(t) = \frac{1}{2}.$$

On the other hand, for any $i = 1, \dots, m - 1$,

$$(6) \quad \lim_{r \rightarrow \infty} \int_{\mathbf{R}} \chi_i(t/r) \, d\mu(t) = \lim_{r \rightarrow \infty} \mu(x_{i+1}/r) - \mu(x_i/r) = 0.$$

Putting (4), (5) and (6) together, we have proved that

$$\lim_{r \rightarrow \infty} \int_{\mathbf{R}} s_{f_r}(t) \, d\mu(t) = \epsilon.$$

Consider now the same problem as r decreases to 0. If $i \neq i_0$, then $\chi_i(t/r) \rightarrow 0$; on the other hand, $\chi_{i_0}(t/r) \rightarrow 1$. Hence,

$$\lim_{r \rightarrow 0} \int_{\mathbf{R}} \chi_i(t/r) \, d\mu(t) = \begin{cases} 1 & \text{if } i = i_0, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore,

$$\lim_{r \rightarrow 0} \int_{\mathbf{R}} s_{f_r}(t) \, d\mu(t) = s_f(0).$$

We are left to prove the continuity of λ . Since s_f is a finite linear combination of characteristic functions of intervals, it is enough to prove that the map

$$r \longrightarrow \int_{\mathbf{R}} \chi_{(a,b)}(t/r) \, d\mu(t) = \int_{ar}^{br} d\mu(t) = \mu(br) - \mu(ar)$$

is continuous for any $-\infty \leq a \leq b \leq \infty$, where $\chi_{(a,b)}$ is the characteristic function of (a, b) . Since μ is bounded and $\mu(t)$ is continuous by Theorem 4, we are done. \square

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,

$$(7) \quad \text{Av } W\left(E^{f_r(t)}\right) = \int_{\mathbf{R}} s_{f_r}(t) \, d\mu(t).$$

But f satisfies the conditions of Proposition 13, and this proves the statement of the theorem. \square

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 $W(E^{f(t)}) = -\operatorname{sgn} f(t)$.

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

1. For any $r \in \mathbf{Q}$, $r > 0$,

$$\operatorname{Av}_t W(E^{f_r(t)}) = \begin{cases} 1/(r\sqrt{11}) - 1 & \text{if } r\sqrt{11} > 1, \\ 1 - r\sqrt{11} & \text{if } r\sqrt{11} < 1. \end{cases}$$

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

Proof. As in eq. (7), we have that

$$\operatorname{Av}_t W(E^{f_r(t)}) = \int_{\mathbf{R}} -\operatorname{sgn}(11r^2 - t^2) d\mu(t),$$

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. \square

REFERENCES

- [1] Tom M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1976. MR **55**:7892
- [2] Pierre Deligne, *Les constantes des quations fonctionnelles des fonctions L* , Modular functions of one variable, II, Lecture Notes in Math. 349, Springer-Verlag, Berlin, 1973, pp. 501–597. MR **58**:22020
- [3] Nelson Dunford and Jacob T. Schwarz, *Linear operators, part I*, Wiley, New York, 1988. MR **90g**:47001a
- [4] Liem Mai, *The average analytic rank of a family of elliptic curves*, J. Number Theory **45** (1993), 45–60. MR **95d**:11080
- [5] Ottavio G. Rizzo, *On the variations of root numbers in families of elliptic curves*, Ph.D. thesis, Brown University, Providence, RI, 1997.
- [6] David E. Rohrlich, *Variation of the root number in families of elliptic curves*, Compos. Math. **87** (1993), no. 2, 119–151. MR **94d**:11045
- [7] ———, *Elliptic curves and the Weil-Deligne group*, Elliptic Curves and Related Topics (Hershy Kisilevsky and M. Ram Murty, eds.), CRM Proceedings & Lecture Notes, vol. 4, Centre de Recherches Mathématiques, Amer. Math. Soc., 1994, pp. 125–157. MR **95a**:11054
- [8] Walter Rudin, *Real and complex analysis*, second ed., McGraw-Hill, 1974. MR **49**:8783
- [9] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, GTM 151, Springer-Verlag, New York, 1994. MR **96b**:11074
- [10] John Tate, *Number theoretic background*, Automorphic Forms, Representations and L -Functions, part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1977, pp. 3–26. MR **80m**:12009
- [11] Don Zagier and Gerhard Kramarz, *Numerical investigations related to the L -series of certain elliptic curves*, J. Indian Math. Soc. **52** (1987), 51–69. MR **90d**:11072

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