On the distribution of root numbers in families of elliptic curves

Harald Helfgott, Princeton University

May 09, 2003

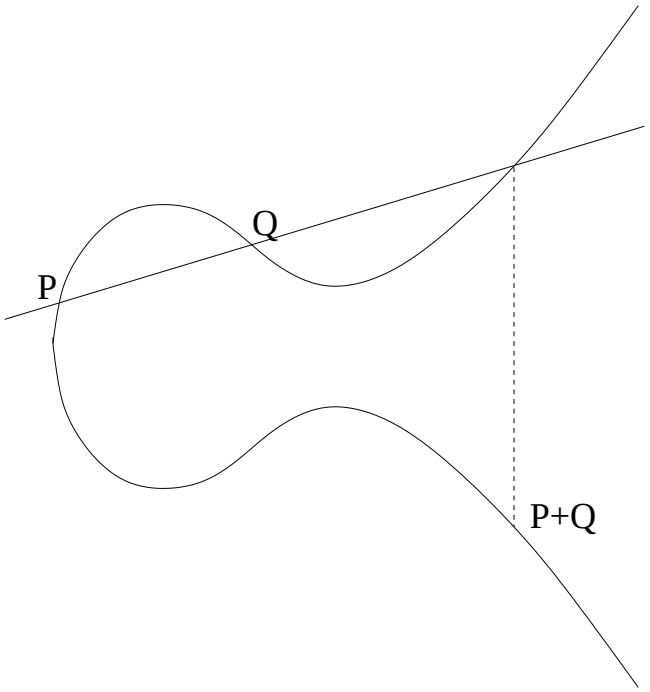
Elliptic curve E over $\mathbb{Q}$:

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q},\ 4a^3 + 27b^2 \neq 0.$$

Set of rational points

$$E(\mathbb{Q}) = \{x, y \in \mathbb{Q} : y^2 = x^3 + ax + b\}$$

has a group structure:



$E(\mathbb{Q})$ is a finitely generated abelian group (Mordell).

L-function associated to E:

$$L(E,s) = \prod_{p \text{ good}} (1 - a_p p^{-s} + p^{1-2s})^{-1} \cdot \prod_{p \text{ bad}} (1 - a_p p^{-s})^{-1}$$

where

$a_p = p - \#$

$\# =$ n. of sols. to $y^2 \equiv x^3 + ax + b \bmod p$.

E is modular (Wiles and BCDT). Hence $L_E(s)$ has analytic continuation and functional equation.

Philosophy: get global properties of object from its L-function

BSD Conjecture: $\operatorname{rank} E(\mathbb{Q}) = \operatorname{ord}_{s=1} L(E,s)$

Functional equation:

$$\mathcal{N}_E^{(2-s)/2}(2\pi)^{s-2}\Gamma(2-s)L(E,2-s) = W(E)\mathcal{N}_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s).$$

The *root number* W_E is 1 or -1.

$$\operatorname{ord}_{s=1} L_E(s) = \begin{cases} \text{even} & \text{if } W(E) = 1 \\ \text{odd} & \text{if } W(E) = -1. \end{cases}$$

In particular, $E(\mathbb{Q})$ infinite if $W_E = -1$.

Family $\mathcal{E}$ of elliptic curves:

$$y^2 = x^3 + ax + b, \;\; a, b \in \mathbb{Q}(t), \; 4a^3 + 27b^2 \neq 0.$$

For almost all t, $\mathcal{E}(t)$ is an elliptic curve.

Distribution of $\operatorname{rank} \mathcal{E}(t)$: hard, even conditionally

But:

$$\operatorname{av} \operatorname{rank} \mathcal{E}(t) \geq \operatorname{rank} \mathcal{E} + \frac{1 - \operatorname{av} W(\mathcal{E}(t))}{2}$$

(Likely to be an equality)

What is known about $\operatorname{av} W(\mathcal{E}(t))$?

Vox populi: $\operatorname{av} W(\mathcal{E}(t)) = 0$

Actually:

1. If $\mathcal{E}$ constant, $\operatorname{av} W(\mathcal{E})(t)$ anything (Rohrlich, Rizzo)

2. If $\mathcal{E}$ non-constant but (technical condition), $\operatorname{av} W(\mathcal{E})(t)$ anything, but infinity of $+$, $-$ (Manduchi)

3. General case: not treated so far, believed to be analytically hard

Subject of talk: (3)

Family $\mathcal{E}$ an elliptic curve over $\mathbb{Q}(t)$

ν a place of $\mathbb{Q}(t)$

Polynomial $P_\nu(x, y)$

$$B_{\mathcal{E}}(x, y) = \prod_{\nu \text{ bad}} P_\nu(x, y)$$

$$M_{\mathcal{E}}(x, y) = \prod_{\nu \text{ multiplicative}} P_\nu(x, y)$$

Conjecture $\mathfrak{A}$ (general square-free sieve):

If $P \in \mathbb{Z}[x]$ square-free,

$\#\{-N \leq x \leq N : \exists p > N^{1/2} \text{ s. t. } p^2 | P(x)\} = o(N)$.

If homogeneous $P \in \mathbb{Z}[x, y]$ square-free,

$\#\{-N \leq x, y \leq N : \exists p > N \text{ s. t. } p^2 | P(x, y)\} = o(N^2)$

Known for $\deg P \leq 3$, resp. $\deg P \leq 6$

Bounds improved

Conjecture $\mathfrak{B}$ (Chowla)

If $P \in \mathbb{Z}[x]$ not constant times square,

$$\sum_{n \equiv a \bmod m} \lambda(P(n)) = o(N),$$

where $\lambda(p_1^{e_1} \cdots p_m^{e_m}) = (-1)^{\sum e_i}$. If $P \in \mathbb{Z}[x, y]$ not constant times square,

$$\sum_{\substack{1 \le x,y \le N \\ (x,y) \in S \cap L}} \lambda(P(x, y)) = o(N^2).$$

Thm.

$\mathfrak{A}(B_{\mathcal{E}}(x,1))$ & $\mathfrak{B}(M_{\mathcal{E}}(x,1))$

$$\Rightarrow \mathsf{av}_{\mathbb{Z}}\, W(\mathcal{E}(t)) = 0$$

$\mathfrak{A}(B_{\mathcal{E}})$ & $\mathfrak{B}(M_{\mathcal{E}})$

$$\Rightarrow \mathsf{av}_{\mathbb{Q}}\, W(\mathcal{E}(t)) = 0$$

$\mathfrak{A}(B_{\mathcal{E}}(x,1))$ & $\mathsf{av}_{\mathbb{Z}}\, W(\mathcal{E}(t)) = 0$

$$\Rightarrow \mathfrak{B}(M_{\mathcal{E}}(x,1))$$

$\mathfrak{A}(B_{\mathcal{E}})$ & $\mathsf{av}_{\mathbb{Q}}\, W(\mathcal{E}(t)) = 0$

$$\Rightarrow \mathfrak{B}(M_{\mathcal{E}})$$

Thm. Chowla holds for two variables, $\deg P = 3$.

More precisely:

Let $f(x,y) \in \mathbb{Z}[x,y]$ be a homogeneous polynomial of degree 3. Let S be a convex subset of $[-N,N]^2$. Let $L \subset \mathbb{Z}^2$ be a lattice coset of index $[\mathbb{Z}^2 : L] \leq (\log N)^A$, where A is an arbitrarily high constant. Then

$$\sum_{(x,y) \in S \cap L} \mu(f(x,y))$$

is at most a constant times

$$\frac{(\log\log N)^5 (\log\log\log N)}{\log N} \frac{\mathrm{Area}(S)}{[\mathbb{Z}^2 : L]} + \frac{N^2}{(\log N)^A},$$

where the implied constant depends only on f and on A.

Old error terms for square-free sieve:

$\deg_{\text{irr}}(P)$	$\delta(P(x))$	$\delta(P(x,y))$
1	$\sqrt{N}$	1
2	$N^{2/3}$	N
3	$N/(\log N)^{1/2}$	$N^2/\log N$
4		$N^2/\log N$
5		$N^2/\log N$
6		$N^2/(\log N)^{1/2}$

Improved error terms:

$\deg_{\text{irr}}(P)$	$\delta(P(x))$	$\delta(P(x,y))$
3	$N/(\log N)^{0.5718\ldots}$	$N^{3/2}/\log N$
4		$N^{4/3}(\log N)^A$
5		$N^{(5+\sqrt{113})/8+\epsilon}$

Wanted: upper bound for the total # of int. points of low height on

$$E_d : dy^2 = f(x)$$

canonical height $\widehat{h}(x, y) \sim log|x|$

$$\widehat{h}(x, y) \geq \frac{1}{8} \log |d| + C$$

$$\text{rank}(E_d) \leq \omega_K(d) - \omega(d) + C'$$

lattice

can eliminate d outside $(N/(\log N)^A, N/(\log N)^\delta)$; can focus on integer points of height $\sim \log N$

Given int. points P, P' on $E_d : dy^2 = f(x)$, d square-free,

$$\hat{h}(P + P') \leq 3\max(\hat{h}(P), \hat{h}(P')) + C.$$

Hence: integer points of height close to each other are separated by almost 60° (at least)

Sphere packing (kissing number in n dim)

$\# \leq 2^{0.401\ldots \cdot n}$