Size and cancellations in Sato Tate sequences

Florian Luca

November 13, 2013

Example of interest for us: Elliptic curves

Let E be an elliptic curve over the field of rational numbers given by the minimal *global* Weierstraß *equation*:

$$E \;:\; y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6 \qquad (1)$$

and let Δ be its discriminant. For each prime p we put

$$a_p = p + 1 - \#E(\mathbb{F}_p),$$

where $E(\mathbb{F}_p)$ is the reduction of E modulo p. If $p \mid \Delta$, then $E(\mathbb{F}_p)$ has a singularity and we put

$$a_p = \begin{cases} 0 & \text{for the case of a cusp,} \\ 1 & \text{for the case of a split node,} \\ -1 & \text{for the case of a non–split node.} \end{cases}$$

We have $|a_p| \le 2\sqrt{p}$. The L-function associated to E is given by

$$L(s, E) = \prod_{p\mid\Delta} \frac{1}{1 - a_p p^{-s}} \prod_{p\nmid\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

The infinite product above is convergent for $\mathrm{Re}(s) > 3/2$ and therefore we can expand it into a series

$$L(s, E) = \sum_{n\ge1} a_n n^{-s}.$$

Other example of interest for us: The Ramanujan τ-function

Let $\tau(n)$ be the Ramanujan function given by

$$\sum_{n\ge 1}\tau(n)q^n = q\prod_{i\ge 1}(1-q^i)^{24} \qquad (|q|<1).$$

Ramanujan observed but could not prove the following three properties of $\tau(n)$:

(i) $\tau(mn)=\tau(m)\tau(n)$ whenever $\gcd(m,n)=1$.

(ii) $\tau(p^{r+1})=\tau(p)\tau(p^r)-p^{11}\tau(p^{r-1})$ for p prime and $r\ge 1$.

(iii) $|\tau(p)|\le 2p^{11/2}$ for all primes p.

These conjectures were proved by Mordell and Deligne.

Fibonacci numbers

Let $\{F_m\}_{m\geq 0}$ be the Fibonacci sequence given by $F_0 = 0,\ F_1 = 1$ and

$$F_{m+2} = F_{m+1} + F_m \qquad \text{for all} \quad m \geq 0.$$

Let $\{a_n\}_{n\geq 1}$ be the sequence of coefficients of the L-function of an elliptic curve E.
We put

$$\mathcal{A}_E = \{n : |a_n| = F_m\},$$

and for a positive x we put $\#\mathcal{A}_E(x) = \#\left(\mathcal{A}_E \cap [1, x]\right)$.

Before we start, we remark that there could be many n such that a_n is a Fibonacci number simply because it may happen that $a_p = 0$ for some prime p, in which case $n = p\ell$ with any positive integer ℓ coprime to p has the property that $a_n = 0 = F_0$. To discard this instance, let

$$\mathcal{M}_E = \{n : a_n \neq 0\}.$$

Putting $\mathcal{M}_E(x) = \mathcal{M}_E \cap [1, x]$, we have $\#\mathcal{M}_E(x) \gg x$ in case of non CM curves (Serre, **1981**).

Theorem (L., Yalçiner)

Let E be a non-CM curve with non-trivial 2-torsion. The estimate

$$\#\mathcal{N}_E(x) = O\left(\frac{x}{(\log x)^{0.0007}}\right) = O\left(\frac{\#\mathcal{M}_E(x)}{(\log \#\mathcal{M}_E(x))^{0.0007}}\right)$$

holds for all $x \geq 2$. The implied constant depends on E.

Later, we proved a more general result.

Theorem (L., Oyono, Yalçiner)

Let E be an elliptic curve defined over and $\mathbf{u} = \{u_m\}_{m \ge 0}$ be a nondegenerate binary recurrent sequence. There is a positive number $c = c(E, \mathbf{u})$ depending on E and $\mathbf{u}$ such that the estimate

$$\#\mathcal{N}_E(x) = O\left(\frac{\#\mathcal{M}_E(x)}{(\log x)^c}\right)$$

holds for all $x \ge 2$. The implied constant depends on E.

Squares in a certain sequence

Again, $\{a_n\}_{n\geq 1}$ is the sequence of coefficients of the L-function of an elliptic curve E.
We studied the set

$$\mathcal{N}_E = \{n : n^2 - a_{n^2} + 1 = \square\}.$$

The reason we studied this is because if we replace n^2 by p and consider the "extreme case" $a_p = \pm 2\sqrt{p}$, then

$$p - a_p + 1 = p \pm 2\sqrt{p} + 1 = (\sqrt{p} \pm 1)^2$$

looks like a "perfect square".

Theorem (L., Yalçiner)

Let E be a non CM curve for which the Sato–Tate conjecture holds. The estimate

$$\#\mathcal{N}_E(x) = O\left(\frac{x}{(\log x)^{0.00001}}\right)$$

holds for all $x \geq 2$. The implied constant depends on E.

Note that if $p \mid \Delta$ and $a_p = \pm 1$, and $\ell \geq 1$, then $a_{p^\ell} = (a_p)^\ell = (\pm 1)^\ell$, which implies that $n = p^\ell \in \mathcal{N}_E$. Moreover if all prime factors p of n divide Δ and have $a_p = \pm 1$, then $n \in \mathcal{N}_E$.

However, the set of such positive integers n is very thin since the number of such integers $n \leq x$ is $O((\log x)^c)$ for some constant $c \leq \omega(\Delta)$.

Elliptic Carmichael numbers

Again, $\{a_n\}_{n\geq 1}$ is the sequence of coefficients of the L-function of an elliptic curve E.

Slightly relaxing a definition of Silverman, we say that a positive integer n is an E-Carmichael number if

- it is not a prime power;
- for any prime divisor $p \mid n$ we have $p \nmid \Delta$;
- for any point $P \in E(\mathbb{F}_p)$ we have

$$(n+1-a_n)P = O_p, \tag{2}$$

where both the equation and the group law are considered over $\mathbb{F}_p$.

For a real $x \geq 1$, let $N_E(x)$ be the number of E-Carmichael numbers $n \leq x$.

Theorem (L., Shparlinski)

Let E be a non CM curve. For a sufficiently large x

$$N_E(x) \ll x \frac{(\log \log \log x)^{1/2} (\log \log \log \log x)^{1/4}}{(\log \log x)^{1/4}}.$$

Sato–Tate sequences

Let $\mathcal{A}_{\mathrm{ST}}$ be the class of infinite sequences $\{a_n\}_{n\geq 1}$ of real numbers, which satisfy the following properties:

- *Multiplicativity:*

$$a_{mn} = a_m a_n, \quad \text{whenever} \quad \gcd(m,n) = 1.$$

- *Sato-Tate distribution:* for any prime p, $a_p \in [-2,2]$, and for the angles $\vartheta_p \in [0,\pi)$ defined by

$$a_p = 2\cos\vartheta_p,$$

  and $\alpha \in [0,\pi)$, we have

$$\lim_{x\to\infty} \frac{\#\{p \leq x \ : \ p \text{ prime}, \ \vartheta_p \in [0,\alpha]\}}{\pi(x)} = \frac{2}{\pi}\int_0^{\alpha} \sin^2\vartheta \, d\vartheta.$$

- *Growth on prime powers:* There exist a constant $\varrho > 0$ such that for any integer $a \geq 2$ and prime p we have

$$|a_{p^a}| \leq p^{(a-1)/2-\varrho}.$$

The above properties are known to hold both for the Ramanujan function $\tau(n)/n^{11/2}$ as well as for $a_n/n^{1/2}$, where $\{a_n\}_{n\geq 1}$ is the sequence of coefficients arising of an L-function of an elliptic curves with certain conditions, like a non-integral j-invariant.

Theorem (L., Shparlinski)

For any sequence $\{a_n\}_{n\geq 1} \in \mathcal{A}_{\rm ST}$, the inequality

$$|a_n| \leq (\log n)^{-1/2+o(1)}$$

holds for almost all positive integers n.

Theorem (L., Shparlinski)

For any sequence $\{a_n\}_{n\geq 1} \in \mathcal{A}_{\rm ST}$, we have

$$\sum_{n\leq x} a_n = o\left(\sum_{n\leq x} |a_n|\right) \quad (x \to \infty).$$

The proof of the result involving Fibonacci numbers

The proof goes in various steps.

Removing n with a large square full part

Recall that s is a square full number if $p^2 \mid s$ whenever $p \mid s$.

Put $y = \log x$. For each n we write

$$t(n) = \prod_{\substack{p \| n \\ p \nmid 6\Delta}} p \qquad \text{and} \qquad s(n) = n/t(n).$$

Then $s(n) = ab$, where a is square free and $a \mid 6\Delta$ and b is squarefull up to factors of 2 and 3. We put

$$\mathcal{N}_1(x) = \{n \le x : s(n) > y\}. \tag{3}$$

Then

$$\#\mathcal{N}_1(x) \ll \frac{x}{y^{1/2}} = \frac{x}{(\log x)^{1/2}}, \tag{4}$$

where we used that the counting function of the number of square full numbers $s \le t$ is $O(t^{1/2})$.

Removing smooth n

Let $P(n)$ be the largest prime factor of n. Put

$$z = \exp\left(\frac{\log x \log\log\log x}{\log\log x}\right).$$

We let

$$\mathcal{N}_2(x) = \{n \le x : P(n) \le z\}. \tag{5}$$

From known results from the distribution of smooth numbers, in this range for z and x, it is known that

$$\#\mathcal{N}_2(x) = x\exp(-(1+o(1))u\log u) \qquad \text{as} \qquad x \to \infty,$$

where $u = \log x/\log z = \log\log x/\log\log\log x$. Hence,

$$u\log u = (1+o(1))\log\log x,$$

as $x \to \infty$, showing that

$$\#\mathcal{N}_2(x) = x\exp(-(1+o(1))\log\log x) = O\left(\frac{x}{(\log x)^{1/2}}\right). \tag{6}$$

Removing n with too few prime factors

Let $\alpha \in (0, 1)$ to be found later and consider the set

$$\mathcal{N}_3(x) = \{n \le x : \omega(n) < (1-\alpha)\log\log x\}. \tag{7}$$

The results from the book *Divisors* of Hall, Tenebaum, show that

$$\#\mathcal{N}_3(x) \ll \frac{x}{(\log x)^{\beta}}, \tag{8}$$

where

$$\beta = 1 - (1-\alpha)\log\left(\frac{e}{1-\alpha}\right).$$

The final argument

Assume that

$$n \in \mathcal{N}_4(x) = \mathcal{N}_E(x) \setminus (\mathcal{N}_1(x) \cup \mathcal{N}_2(x) \cup \mathcal{N}_3(x)).$$

Since $n \notin \mathcal{N}_1(x)$, we may write

$$n = up_1 \cdots p_\ell, \quad u \le y, \quad p_1 < \cdots < p_\ell, \quad \gcd(u, p_1 \cdots p_\ell) = 1.$$

Furthermore, $p_i \nmid 6\Delta$ for any $i = 1, \ldots, \ell$. Assume that x is large enough so that $z > y$. Then $P(n) = p_\ell$.

Write

$$F_m = a_n = a_u a_{p_1} \cdots a_{p_\ell}.$$

Let $\varepsilon > 0$ be arbitrary. Note that since

$$\omega(u) \ll \frac{\log u}{\log\log u} \ll \frac{\log y}{\log\log y} = o(\log\log x) \qquad \text{as} \qquad x \to \infty,$$

it follows that $\omega(u) < \varepsilon \log\log x$ holds whenever x is sufficiently large.

Put

$$L = \lfloor (1-\alpha-\varepsilon)\log\log x \rfloor.$$

Note that $\ell = \omega(n/u) \geq L$ since $n \notin \mathcal{N}_3(x)$. Note also that since E has 2-torsion, it follows that $\#E(\mathbb{F}_p)$ is always even. Since

$$\#E(\mathbb{F}_p) = p - a_p + 1,$$

it follows that a_p is even whenever p is odd. In particular, $2 \mid a_{p_i}$ for all $i = 1, \ldots, \ell$. Thus, $2^L \mid a_n \mid F_m$. Since the inequality

$$|a_n| \leq d(n)\sqrt{n} < x$$

holds for all sufficiently large x, where $d(n)$ is the number of divisors of n, it follows that $F_m < x$. Since

$$F_m = \frac{\gamma^m - \delta^m}{\gamma - \delta}, \qquad \text{where} \qquad (\gamma, \delta) = \left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right),$$

it follows that $m < c \log x$ holds with some positive absolute constant c which can be taken to be any constant larger than $1/\log\gamma$ provided that x is sufficiently large.

We now exploit the condition $2^L \mid F_m$. It is known that this implies that $3 \times 2^{L-2} \mid m$. Thus, $m = 3 \times 2^{L-2}k$ for some positive integer k satisfying the bound

$$k \leq \frac{c_1 \log x}{3 \times 2^{L-2}} \leq c_2(\log x)^{1-(1-\alpha-\varepsilon)\log 2},$$

where $c_2 = 8c_1/3$. Let M be the above upper bound. Fix $k \leq M$.

Also fix $v = n/p_\ell$. Put $P = p_\ell$. We then have

$$\pm F_m = a_n = a_v a_P.$$

Since v and m are fixed with $a_v \neq 0,\ F_m \neq 0$, it follows that $a_P = \pm F_m/a_v$ takes one of two fixed values. Since also $P \leq x/v$, it follows, by a result of Serre, that the number of possibilities for P is of order at most

$$\pi(x/v)\frac{(\log\log(x/v))^{2/3}(\log\log\log(x/v))^{1/3}}{(\log(x/v))^{1/3}} \ll \frac{x(\log\log x)^{3/4}}{v(\log(x/v))^{4/3}}.$$

Using the fact that $x/v > P > z$, so

$$\log(x/v) > \log z = \frac{(\log x)(\log\log\log x)}{\log\log x},$$

we get that the number shown above is bounded above by

$$\frac{x(\log\log x)^2}{v(\log x)^{4/3}}$$

whenever x is large enough.

Summing over all possibilities for $v < x/z$ and k, we get that

$$\#\mathcal{N}_4(x) \ll \frac{x(\log\log x)^2 M}{(\log x)^{4/3}} \sum_{v<x/z} \frac{1}{v} \ll \frac{x(\log\log x)^2}{(\log x)^{(1-\alpha-\varepsilon)\log 2 - 2/3}}. \tag{9}$$

Comparing (4), (6), (8) and (9), it follows that we must choose α such that

$$1 - (1-\alpha)\log\left(\frac{e}{1-\alpha}\right) = (1-\alpha)\log 2 - 2/3,$$

giving $\alpha = 0.0371929$ with corresponding common values of the above expression equal to 0.00070394.

Taking ε sufficiently small, we get the desired estimate.

What about Sato-Tate sequences?

One might wonder where do we get the exponent $-1/2$ on the $\log n$.

Well, we get it from the improper integral

$$\int_0^{\pi} \sin^2 \vartheta \log |2 \cos \vartheta| d\vartheta = \pi \int_0^1 \sin^2(\pi\omega) \log |2\cos \pi\omega| d\omega = -\frac{\pi}{4}.$$

Namely take some θ. Take all primes p dividing n with

$$\theta_p \in [\theta, \theta + d\theta].$$

By Sato-Tate, the relative density of such primes in the set of all primes is

$$\frac{2}{\pi} \sin^2 \theta d\theta.$$

Since most n have $\log\log n$ primes, then most n have

$$\frac{2}{\pi} \sin^2 \theta d\theta (\log\log n)$$

such prime factors.

So, say assuming that n is square-free, in the product

$$a_n = \prod_{p|n} a_p,$$

the primes in $[\theta, \theta + d\theta]$ will participate with the multiplicative amount

$$|2\cos\theta|^{\frac{2}{\pi}\sin^2\theta d\theta \log\log n} = (\log n)^{\frac{2}{\pi}\sin^2\theta \log|2\cos\theta| d\theta}.$$

Varying θ, we get that the exponent above is exactly

$$\frac{2}{\pi}\int_0^\pi \sin^2\theta \log|2\cos\theta| d\theta = -\frac{1}{2}.$$

The rest is just technicalities, making $d\theta$ of the form $1/K$ for some large K, using sieves and results from the theory of discrepancy of sequences to control the error of approximating the integral with the corresponding Riemann sum.

THANK YOU!