On the Distribution of the Number of Points on Elliptic Curves in a Tower of Extentions of Finite Fields

Omran Ahmadi and Igor Shparlinski

Claude Shannon Institute
and
Macquarie University

Introduction

Sizes of many algebraic geometry objects are distributed in accordance with the *Sato-Tate* density:

$$\mu_{ST}(\beta, \gamma) = \frac{2}{\pi} \int_{\beta}^{\gamma} \sqrt{1 - \alpha^2} d\, \alpha,$$

Two most famous examples:

Elliptic Curves and Kloosterman Sums

Elliptic Curves

By the *Hasse theorem*, for an elliptic curve $E/\mathbb{F}_q$:

$$\frac{\#E(\mathbb{F}_q) - q - 1}{2q^{1/2}} \in [-1, 1]. \qquad (1)$$

Sato–Tate conjecture:
If E is defined over Q and q runs through primes $p \le x$ then the number of the ratios (1) (for reductions of E modulo p) which belong to $[\beta, \gamma]$ is $\sim \mu_{ST}(\beta, \gamma)\pi(x)$.

R. Taylor (2007):
The Sato–Tate conjecture holds for all non-CM elliptic curves with a non-integral j-invariant.

B. J. Birch (1968):
An analogue of the Sato–Tate conjecture in the dual case when the finite field $\mathbb{F}_q$ is fixed and the ratios (1) are taken over all elliptic curves $\mathbb{E}$ over $\mathbb{F}_q$.

S. Baier and L. Zhao (2007); *W. D. Banks and I.S.* (2008); *I.S.* (2009):
A series of works showing that similar type of behavior also holds in mixed situations (when both the field and the curve vary) over various families of curves.

Kloosterman Sums

For $a \in \mathbb{F}_q^*$ and a fixed nonprincipal additive character ψ of $\mathbb{F}_q$ we define the Kloosterman sum

$$K_q(a) = \sum_{x \in \mathbb{F}_q^*} \psi\left(\left(x + ax^{-1}\right)\right).$$

By the *Weil theorem*:

$$\frac{K_q(a)}{2q^{1/2}} \in [-1, 1].$$

An analogue of the Sato–Tate conjecture can and has been formulated.

Unfortunately the result and method of *R. Taylor* does not apply to Kloosterman sums.

However an analogue of the result of Birch was obtained by *N. M. Katz* (1988) and put in a quantitative form by *H. Niederreiter* (1991).

There are also function field analogues by *C.-L. Chai and W.-C. W. Li* (2004).

Our Results

Set-up

We fix an ordinary elliptic curve E over $\mathbb{F}_q$ and consider analogue of the ratios (1) taken in the consecutive extensions of $\mathbb{F}_q$:

$$\frac{\#E(\mathbb{F}_{q^n}) - q^n - 1}{2q^{n/2}} \in [-1, 1], \quad n = 1, 2, \ldots . \quad (2)$$

We show, that, surprisingly enough, distribution of the ratios (2) is not governed by $\mu_{ST}(\beta, \gamma)$ but rather by a different distribution function

$$\lambda(\beta, \gamma) = \frac{1}{\pi} \int_{\beta}^{\gamma} \left(\sqrt{1 - \alpha^2}\right)^{-1} d\,\alpha.$$

<u>Supersingular elliptic curves:</u>

$\#E(\mathbb{F}_{q^n}) = q^n + 1$ and $\#E(\mathbb{F}_{q^n}) = (q^{n/2} - 1)^2$

for odd and even n, respectively.

Precise Formulation

Put

$$\alpha_n = \frac{\#E(\mathbb{F}_{q^n}) - q^n - 1}{2q^{n/2}}$$

and define

$$T_{\beta,\gamma}(N) = \#\left\{n = 1, \ldots, N \;\;:\;\; \frac{\#E(\mathbb{F}_{q^n}) - q^n - 1}{2q^{n/2}} \in [\beta, \gamma]\right\}$$

Theorem 1 *There is a constant* $\eta > 0$ *depending only on* q *such that uniformly over* $-1 \le \beta \le \gamma \le 1$ *we have*

$$T_{\beta,\gamma}(N) = \lambda(\beta, \gamma)N + O(N^{1-\eta}).$$

Frobenius Angles

Our method is based on the explicit formula

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \tau^n - \overline{\tau}^n \qquad (3)$$

where $\overline{\tau}$ means the complex conjugate of τ.

The *Frobenius eigenvalues* $\tau, \overline{\tau}$ satisfy

$$|\tau| = |\overline{\tau}| = q^{1/2} \qquad (4)$$

We write (4) as

$$\tau = q^{1/2} e^{\pi i \vartheta} \qquad \text{and} \qquad \overline{\tau} = q^{1/2} e^{-\pi i \vartheta}, \qquad (5)$$

with some $\vartheta \in [0, 1]$ which we call the *Frobenius angle*.

Note: Sometimes $\pi\vartheta$ is called the Frobenius angle.

Lemma 2 *If E is ordinary, then Frobenius angle ϑ is irrational.*

Proof. if $\vartheta = r/s$ then $\tau^{2s} = \overline{\tau}^{2s} = q^s$. $\Longrightarrow$ None of them can be a p-adic unit. This contradicts the definition of ordinary curve. □

7

Reformulation

We see from (3) and (5) that

$$\alpha_n = \cos(\pi\vartheta n).$$

Consider the interval

$$\mathcal{I}(\beta,\gamma) = [\pi^{-1}\arccos\gamma,\ \pi^{-1}\arccos\beta]$$

Then $T_{\beta,\gamma}(N)$ counts the number of fractional parts $\{\vartheta n\} \in \mathcal{I}(\beta,\gamma)$

$$T_{\beta,\gamma}(N) = \#\{n = 1,\ldots,N \ :\ \{\vartheta n\} \in \mathcal{I}(\beta,\gamma)\}.$$

$$\Downarrow$$

We use tools from the theory of uniformly distributed sequences to estimate $T_{\beta,\gamma}(N)$.

For an N-element finite set $\mathcal{A} \subseteq [0,1]$, we define its *discrepancy* as

$$\Delta(\mathcal{A}) = \sup_{\gamma \in [0,1]} \left| \frac{\#\{\alpha \in \mathcal{A} : \alpha < \gamma\}}{N} - \gamma \right|,$$

Let $\|z\|$ be the distance between a real z and the closest integer.

Lemma 3 *Suppose that ϑ is irrational and for some function $\varphi(t)$ such that $\varphi(t)/t$ is monotonically increasing for real $t \geq 1$ we have*

$$\|k\vartheta\| \geq \frac{1}{\varphi(|k|)}, \qquad k \in \mathbf{Z},\ k \neq 0.$$

Then the discrepancy $D(N)$ of the sequence

$$\{\vartheta n\}, \qquad n = 1, \ldots, N,$$

satisfies

$$D(N) \ll \frac{\log N \log \varphi^{-1}(N)}{\varphi^{-1}(N)},$$

where $\varphi^{-1}(t)$ is the inverse function of $\varphi(t)$.

Linear Forms in Logarithms

We present a classical result of *A. Baker* (1966) in a more convenient multiplicative form

Lemma 4 *For arbitrary algebraic numbers* $\xi_1, \ldots, \xi_s$ *there are constants* $C_1 > 0$ *and* $C_2 > 1$ *such that the inequality*

$$O < |\xi_1^{k_1} \ldots \xi_s^{k_s} - 1| \\ \le C_1 \left(\max\{|k_1|, \ldots, |k_s|\} + 1\right)^{-C_2}$$

has no solution in $(k_1, \ldots, k_s) \in \mathbf{Z}^s \setminus (0, \ldots, 0)$.

Diophantine Properties of Frobenius Angles

We are now ready to establish a necessary result which is needed for an application of Lemma 3.

Lemma 5 *There are constants* $c_1 > 0$ *and* $c_2 > 1$ *depending only on* q *such that*

$$\|k\vartheta\| \geq c_1 |k|^{-c_2}$$

for any non-zero integer k*.*

Proof. Assume that for some integer m we have

$$k\vartheta - m = \delta$$

where δ is sufficiently small.

Lemma 2 $\implies \delta > 0$

Recalling (5), we derive

$$\tau^{2k} = q^k e^{2\pi i \delta}$$

Applying Lemma 4, we obtain the desired result with c_1 and c_2 depending on ϑ.

For each q, there are only finitely many choices for $\vartheta \implies c_1, c_2$ can be taken to depend only on q. $\square$

Concluding the Proof

We see from Lemma 5 that Lemma 3 applies to the discrepancy $\Delta(N)$ of the points $\{\vartheta n\}, n = 1, 2, \ldots, N$ with $\varphi(t) = c_1(t+1)^{c_2}$, thus

$$\Delta(N) = O\left(N^{-\kappa}\right)$$

where κ depends only on q.

Recalling that

$$T_{\beta,\gamma}(N) = N|\mathcal{I}(\beta,\gamma)| + O\left(\Delta(N)\right),$$

and that

$$|\mathcal{I}(\beta,\gamma)| = \lambda(\beta,\gamma)$$

we conclude the proof.

Comments

Kloosterman Sums

Similar results.
No new ideas required.

Curves of Higher Genus

For an ordinary curve $\mathcal{C}/\mathbb{F}_q$, the problem splits:

- Studing the cardinalities of $\mathcal{C}(\mathbb{F}_{q_n})$;
- Studing the cardinalities of the Jacobians $J(\mathcal{C}(\mathbb{F}_{q_n}))$;

Same techniques apply but become more involved.

The bottle neck is proving the **multiplicative independence** of Frobenius roots.
E. Kowalski (2008): statistical results for certain families of curves.

Genus two curves which are ordinary and have absolutely simple Jacobians have been settled.