European Research Council
Established by
the European Commission

Angles of Gaussian primes, Cetraro, July 2017

Zeev Rudnick, TAU, joint with Ezra Waxman

Plan

I have recently examined several problems of analytic number theory in the context of function fields over a finite field, where they can be approached by methods different than those of traditional analytic number theory, among them novel equidistribution results.

The resulting theorems can be used to check existing conjectures over the integers, to generate new ones, and occasionally to be used as part of their proof.

Today I will discuss angles of Gaussian primes.

Primes of the form $a^2 + b^2$

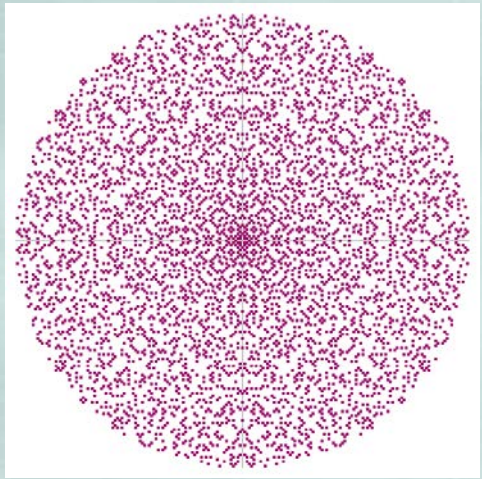
Pierre de Fermat: An odd prime is expressible as $p = a^2 + b^2$ if and only if $p = 1 \bmod 4$ (letter to Mersenne, December 25, 1640). Proof given by Euler (1752-55).

In that case, $a+ib$ is a prime in the Gaussian integers $\mathbf{Z}[i]$, $i = \sqrt{-1}$.

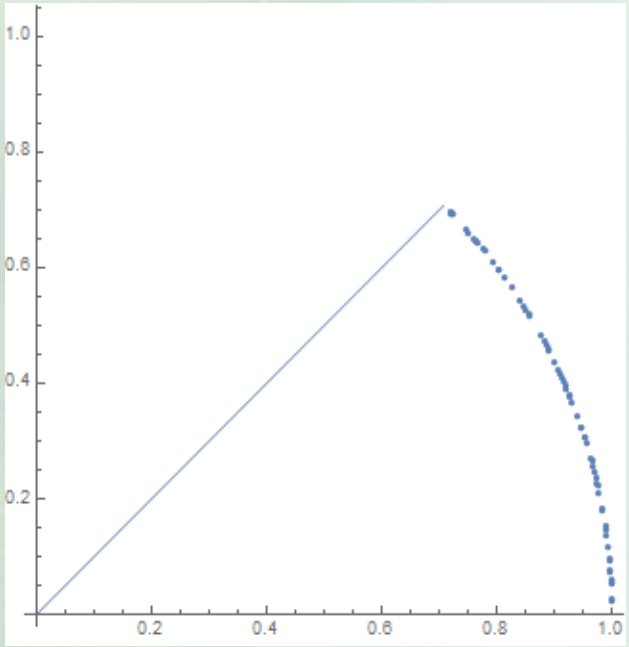
The representation is unique if we assume $a>b>0$.

We can then find a unique angle $\theta_p \in \left[0, \frac{\pi}{4}\right)$ such that $a + ib = \sqrt{p}e^{i\theta_p}$

Goal: understand the distribution of these Gaussian primes in the plane.



Pierre de Fermat
(1601-1665)



Angular distribution $(a + ib)/\sqrt{p}$ of the 67 primes 1000<p<2000, p=1 mod 4, a>b>0

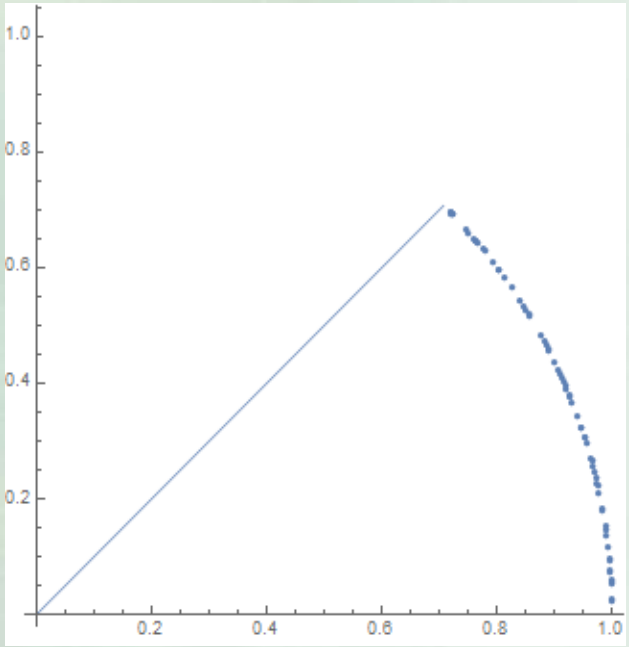
The angular distribution of Gaussian primes

Hecke (1918): The angles of Gaussian primes are uniformly distributed: For fixed $0 \le \alpha < \beta < \pi/4$

$$\lim_{x\to\infty} \frac{\#\{p = 1 \bmod 4, \quad p \le x: \quad \theta_p \in [\alpha, \beta]\}}{\#\{p = 1 \bmod 4, \quad p \le x\}} = \frac{\beta - \alpha}{\pi / 4}$$

Question: Are the Gaussian angles "random"? i.e. do the first N Gaussian angles have the same statistics as N random points in $\left[0, \frac{\pi}{4}\right)$?

"Random Points" – picked independently and uniformly in $\left[0, \frac{\pi}{4}\right)$



Angular distribution $(a + ib)/\sqrt{p}$ of the 67 primes 1000<p<2000, p=1 mod 4, a>b>0

Deviation from randomness: Maximal gap

Question: Are the Gaussian angles "random"? i.e. do the first N Gaussian angles have the same statistics as N random points in $\left[0,\frac{\pi}{4}\right)$?

"Random Points" – picked independently and uniformly in $\left[0,\frac{\pi}{4}\right)$

Claim: The **maximal gap** between the first N angles is $> \frac{1}{\sqrt{N \log N}}$

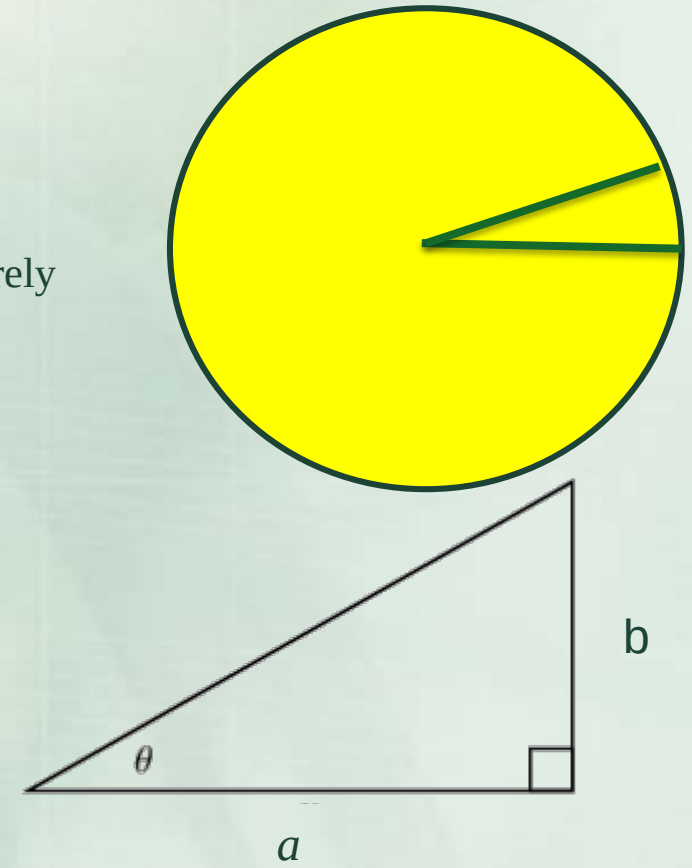
Compare: The maximal gap between N **random** angles is $(\log N)/N$ almost surely - which is much smaller.

Claim: The arc $(0,1/\sqrt{X})$ does not contain any angle of a prime p<X (a forbidden region).

.

Proof: if $p = a^2 + b^2 \le X, \quad 0 < b < a$ has angle θ_p close to zero then

$$\theta_p \sim \tan\theta_p = \frac{b}{a} \ge \frac{1}{a} \ge \frac{1}{\sqrt{a^2+b^2}} \ge \frac{1}{\sqrt{X}}$$



Deviation from randomness: The minimal gap

The **minimal** gap between angles: For N random, independent uniform $\theta_1, \dots, \theta_N \in [0, \frac{\pi}{4})$

$$\min\{|\theta_i - \theta_j|: \quad i \neq j \leq N\} \approx \frac{1}{N^2} \qquad \text{almost} \quad \text{surely}$$

Note that the average gap is 1/N

For the Gaussian angles, we have "repulsion": The minimal distance between the first N angles is $\approx \frac{1}{N \log N}$

$$\min\{|\theta_p - \theta_q|: p \neq q \leq X\} \geq \frac{1}{X} \approx \frac{1}{N \log N}, \qquad N = \#\{p \leq X : p = 1 \bmod 4\}$$

which is much larger than for random points

Small scale distribution of Gaussian angles

Hecke (1918): The angles of Gaussian primes are uniformly distributed: For **fixed** $0 \le \alpha < \beta < \pi/4$

$$\#\left\{p \le x, \quad p = 1 \bmod 4 : \quad \theta_p \in [\alpha, \beta]\right\} \sim \frac{\beta - \alpha}{\pi / 4} \cdot \#\{p \le x, \quad p = 1 \bmod 4\}, \qquad x \to \infty$$

We look for prime angles in "short" (**shrinking**) arcs $\beta - \alpha \to 0$.

To have a good chance to find them, we need the length of the arc to be a bit bigger than

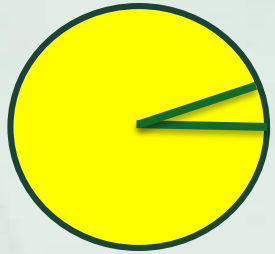
$$\beta - \alpha \gg \frac{1}{\#\{p \le x, p = 1 \bmod 4\}} \approx \frac{\log x}{x}$$

Moreover, we can ask if uniform distribution persists on shrinking arcs.

Assuming GRH, uniform distribution holds for **every** arc of length $\beta - \alpha \gg x^{-\frac{1}{2}+o(1)}$

Unconditionally, this holds with 1/2 replaced by 12/37=0.324… (Kubilius 1952, …, Maknys 1977), Harman & Lewis (2001) 0.381 (existence of angles, without equidistribution).

Note: GRH gives sharp result, since we saw that the arc $(0,1/\sqrt{X})$ does not contain any angle of a prime p<X. (forbidden region)



Comparison: primes in short intervals

The question of Gaussian primes in small sectors behaves differently to the question of primes in short intervals:

The density of primes near x is 1/log x.

RH gives that every interval [x,x+H] contains ~H/log x primes if $H \gg \sqrt{x}$.

However, we do expect every interval [x,x+H] to contain ~H/log x primes if $H \gg X^{\epsilon}$

- but not shorter intervals (Maier)

So we do not expect big forbidden regions in the distribution of primes,
unlike what we see for Gaussian primes.

Almost all short arcs contain an angle

Theorem (ZR & Waxman / Parzanchevski and Sarnak, 2017):

Assuming GRH, **almost all** arcs of length $X^{-1+o(1)}$ contain an angle θ_p, $p \leq X$.

Unconditionally, can get arcs of length $X^{-(\frac{1}{2}+\delta)}$ for a suitable $\delta > 0$ by using a zero-density theorem.

This is achieved by giving a bound on the **variance** of the number of angles in short arcs.

The number variance

Counting angles in a small arc: Divide $[0,\frac{\pi}{4}]$ into K small arcs and ask how many of the N prime angles fall into each:

$$N := \#\{p \le X,\ p = 1 \bmod 4\} \sim \frac{1}{2}\frac{X}{\log X}$$

$$\mathcal{N}_{K,N}(\theta) := \#\left\{ p \le x: \quad \theta_p \in [\theta, \theta + \frac{\pi/4}{K}] \right\}$$

Expected value $$\mathbb{E}(\mathcal{N}_{K,N}) := \frac{1}{\pi/4}\int_0^{\pi/4} \mathcal{N}_{K,N}(\theta)d\theta = \frac{N}{K}$$

Variance:

"Thm": Assume GRH. Then $$\mathrm{Var}(\mathcal{N}_{K,N}) := \frac{1}{\pi/4}\int_0^{\pi/4} \left|\mathcal{N}_{K,N}(\theta) - \frac{N}{K}\right|^2 d\theta << \frac{N}{K}(\log K)^2$$

⇒ Assuming GRH, **almost all** arcs of length $\frac{1}{K}$ contain an angle θ_p, $p \le K(\log K)^3$.

Compare: For N random points, $\mathrm{Var}(\mathcal{N}_{K,N}^{\text{random}}) \sim \frac{N}{K}$

Asymptotic for the variance ?

Conjecture: $$\mathrm{Var}(\mathcal{N}_{K,N}) \sim \frac{N}{K}\min(1, 2\frac{\log K}{\log N})$$

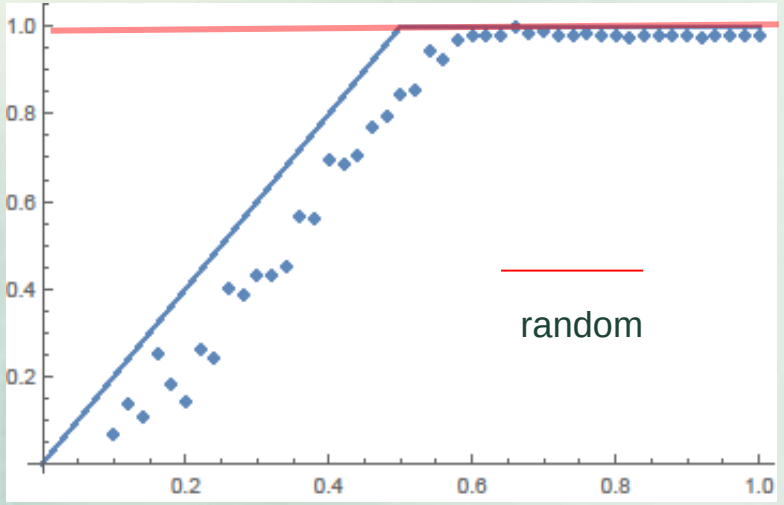
Compare: For N random points,

$$\mathrm{Var}(\mathcal{N}_{K,N}^{\text{random}}) \sim \frac{N}{K}$$

Motivation for conjecture:

a) A **random matrix model**: Express variance via zeros of a certain family of Hecke L-functions, then replace these zeros by eigenphases of a suitable ensemble of random matrices.

b) A **function field analogue**



$$\frac{\mathrm{Var}(\mathcal{N}_{K,N})}{N/K} \quad \text{vs} \quad \log K / \log N$$

Data: 35241 angles of the Gaussian primes $10^8 < p < 2 * 10^8$

A function field analogue

$\mathbf{F}_q[T]$= polynomials $f(T) = a_0+a_1T+a_2T^2+....+a_dT^d$, with coefficients $a_i \in \mathbf{F}_q$

analogues:

integers $\mathbf{Z}$ ↔ polynomials $\mathbf{F}_q[T]$

primes p ↔ irreducible polynomial P(T) ("prime")

positive integer n>0 ↔ monic polynomial $P(T)=T^d+\ldots.$

In both cases we have the Fundamental Theorem of Arithmetic – unique factorization into primes (prime polynomials).

Prime Number Theorem ↔ Prime Polynomial Theorem

Sums of two squares $p = a^2 + b^2$ ↔ polynomials $P(T) = A^2 + TB^2$

Gaussian integers ↔ $\mathbf{F}_q[\sqrt{-T}]$

Advantage of $\mathbf{F}_q[T]$: Can take $q\to\infty$

Analogue of Gaussian integers

$\mathbf{F}_q[\sqrt{-T}]$ Euclidean domain, equipped with Galois conjugation $\sigma(f)(S) \coloneqq f(-S)$
and norm: $\mathrm{Norm}(f) \coloneqq f \cdot \sigma(f) \in \mathbf{F}_q\,[T]$

analogue of the unit circle $S^1 = \{z \in \mathbf{C} : \bar{z}\, z = 1\}$

$$\mathbb{S}^1 \coloneqq \{\ f \in \mathbb{F}_q[[\sqrt{-T}\,]] :\ f(0) = 1,\ \mathrm{Norm}(\ f) = 1\}$$

Direction of Gaussian polynomial

$$U(f) \coloneqq \sqrt{f\,/\,\sigma(f)} \in \mathbb{S}^1 \quad \Leftrightarrow \quad \alpha\,/\,\bar{\alpha} = e^{2\sqrt{-1}\,\theta} \in S^1, \quad \alpha = |\,\alpha\,|\, e^{\sqrt{-1}\,\theta} \in \mathbb{C}$$

Sectors/arcs on the unit circle $\mathrm{Sect}(u;k) \coloneqq \{\, v \in \mathbb{S}^1 :\ \|\,u - v\,\| \le \dfrac{1}{q^k}\,\}$

$$\|\,u - v\,\| \le \frac{1}{q^k} \quad \Leftrightarrow \quad u = v \mod (\sqrt{-T})^k$$

K:=Number of distinct sectors Sect(u;k) $\qquad K = q^{\kappa}, \qquad \kappa = \lfloor k/2 \rfloor$

Sums of two squares in $\mathbf{F}_q[T]$

A monic irreducible $P(T) \in \mathbf{F}_q[T]$, coprime to T, is of the form $P(T) = A(T)^2 + TB(T)^2$ if and only if $P(0)$ is a square in $\mathbf{F}_q$

Equivalently,

$$P(T) = (A(-T) + \sqrt{-T}\,B(-T)) \cdot (A(-T) - \sqrt{-T}\,B(-T))$$

Counting Gaussian prime polynomials in sectors

$$\mathcal{N}_{k,\nu}(u) := \#\{\, P \text{ prime},\ \deg P = \nu,\ U(P) \in \mathrm{Sect}(u,k)\,\} \qquad U(f) := \sqrt{f\,/\,\sigma(f)} \in \mathbb{S}^1$$

mean value

$$\frac{1}{K}\sum_u \mathcal{N}_{k,\nu}(u) = \frac{1}{K}\#\{P \text{ prime} : \deg P = \nu, P(0) = \square\} = \frac{N}{K}$$

$$N := \#\{P \text{ prime} : \deg P = \nu, P(0) = \square\} \sim \frac{q^\nu}{2\nu}$$

Variance in polynomial sectors

Theorem : As $q \to \infty$, the number variance is

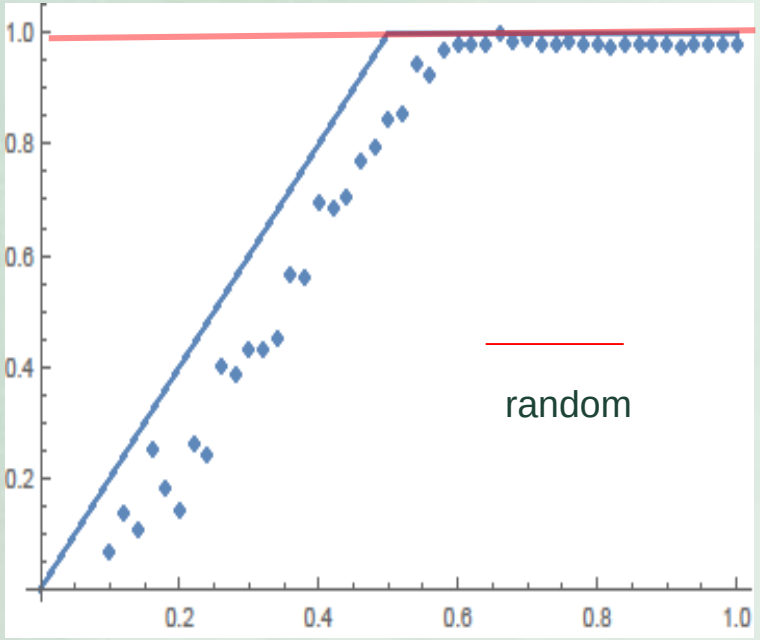
$$\frac{\mathrm{Var}(\mathcal{N}_{\kappa,\nu})}{N/K} \sim \begin{cases} 2\dfrac{\log_q K}{\log_q N} - \dfrac{2}{\log_q N}, & \log_q K \le \dfrac{1}{2}\log_q N \\ 1 + \dfrac{\eta(\log_q N) - 1}{\log_q N}, & \log_q K > \dfrac{1}{2}\log_q N \,. \end{cases}$$

$$\eta(m) = \begin{cases} 1, & m \quad \text{even} \\ 0, & m \quad \text{odd} \end{cases}$$

This matches our conjecture over the integers:

$$\frac{\mathrm{Var}(\mathcal{N}_{K,N})}{N/K} \sim \min\left(2\frac{\log K}{\log N}, 1\right)$$

suggests explanation for bad fit of numerics with theory
– possible secondary terms of size 1/log



Picking out directions in sectors

Main tool – "super-even" Dirichlet characters modulo $S^{2\kappa}, S = \sqrt{-T}$
(analogues of Hecke Grossencharacters)
Definition: A Dirichlet character modulo $S^{2\kappa}$ is a homomorphism

$$\chi : \left(\mathbb{F}_q[S]/(S^{2\kappa})\right)^{\times} \to \mathbb{C}^{\times}$$

It is "even" if it is trivial on the scalars $\mathbf{F}_q^*$
It is "super even" if in addition it is trivial on the subgroup of even polynomials {f(S)=f(-S) modulo $S^{2\kappa}$}

There are exactly $K = q^{\kappa}$ super-even characters modulo $S^{2\kappa}$
Key fact: For a polynomial $f = A^2 + TB^2$, the direction $U(f) := \frac{A+\sqrt{-T}B}{A-\sqrt{-T}B} \in \mathbb{S}^1$
lies in the sector Sect(u, k) if and only if

$$\chi(f) = \chi(u), \qquad \forall \quad \text{super-even} \quad \chi \bmod S^{2\kappa}$$

The L-function for a super-even character

The L-function associated to χ : for Re(s)>1 $$L(s,\chi) := \sum_{f \text{ monic}} \frac{\chi(f)}{\| f \|^s} = \prod_{P \text{ prime}} \left(1 - \frac{\chi(P)}{\| P \|^s}\right)^{-1}$$

Norm of a polynomial: $\|f\| := \#\mathbf{F}_q[S]/(f) = q^{\deg(f)}$ (analogy: for $0 \neq n \in \mathbf{Z}$, $|n| = \#\mathbf{Z}/n\mathbf{Z}$)

If χ is nontrivial ("primitive") character modulo $T^{2\kappa}$ then

- L(s, χ) is a polynomial in q^{-s} of degree $2\kappa - 1$
- If χ is "even" then there is a trivial zero at s=0
- RH (Weil, 1940's): All non-trivial zeros lie on Re(s)=1/2

$$L(s,\chi) = (1 - q^{-s}) \cdot \det(I - q^{1/2-s}\, \Theta_\chi)$$

$$\Theta_\chi \approx \begin{pmatrix} e^{i\theta_1} & & & \\ & e^{i\theta_2} & & \\ & & \ddots & \\ & & & e^{i\theta_N} \end{pmatrix}$$

$\Theta(\chi)$ = unitary m x m matrix, m= 2κ-2, called the **"unitarized Frobenius matrix"**

The variance via super-even characters

Theorem: as $q \to \infty$

$$\mathrm{Var}(\mathcal{N}_{k,\nu}) \sim \frac{N}{K} \times \frac{1}{\nu} \times \underset{\chi \text{ super-even mod } S^{2\kappa}}{\text{Average}} \left\{ \left| \mathrm{trace}(\Theta_\chi^\nu) \right|^2 \right\}$$

N.M. Katz (2016): As $q \to \infty$, the unitarized Frobenius classes $\{\Theta_\chi : \chi \text{ super even mod } S^{2\kappa}\}$ become uniformly distributed in the unitary symplectic group USp(2κ-2)

$$\lim_{q\to\infty} \underset{\chi \text{ super even mod } S^{2\kappa}}{\text{Average}} \left\{ \left| \mathrm{trace}(\Theta_\chi^\nu) \right|^2 \right\} = \int_{\mathrm{USp}(2\kappa-2)} \left| \mathrm{trace}(U^\nu) \right|^2 dU = \begin{cases} 2\kappa - 2, & 2\kappa - 2 < \nu \\ \nu - 1 + \eta(\nu), & 1 \le \nu \le \kappa - 1 \end{cases}$$

$$\lim_{q\to\infty} \frac{\mathrm{Var}(\mathcal{N}_{k,\nu})}{N/K} \sim \begin{cases} 2\dfrac{\log_q K}{\log_q N} + \ldots, & \log_q K < \dfrac{1}{2}\log_q N \\ 1 + \ldots, & \dfrac{1}{2}\log_q N < \log_q K \end{cases}$$

Summary

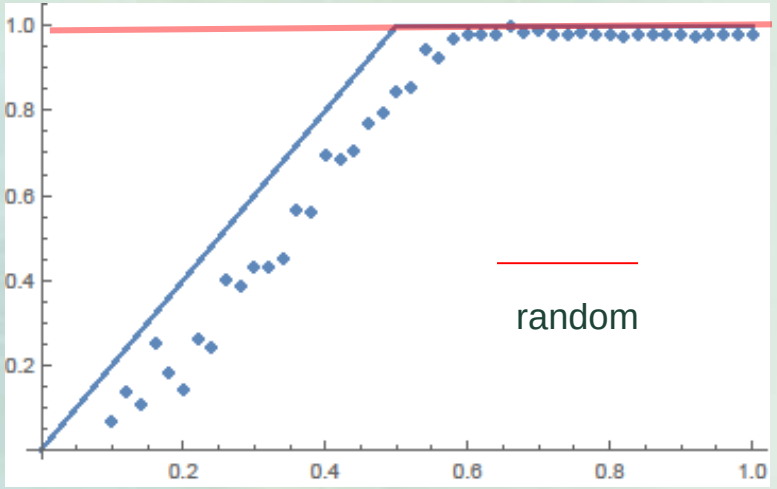
The angles associated to representations of primes as $p = a^2 + b^2$ exhibit randomness on global scale, but deviations on shorter scales.

In particular we predict that the number variance in short arcs exhibits:

- Poissonian statistics for very short arcs,

- Random Matrix Theory statistics for medium-sized arcs

We develop a function field analogue where we **prove** the corresponding statements in the large finite field limit



$$\frac{\mathrm{Var}(\mathcal{N}_{K,N})}{N/K} \quad \text{vs} \quad \log K / \log \mathrm{N}$$