On the distribution of sums of two squares

Ofir Gorodetsky, Technion

Asymptotic Counting and L-Functions
Max Planck Institute for Mathematics
May 8, 2025

Based on joint works with Brad Rodgers (Queen's University) and Mo Dick Wong (Durham University).

Definition

This talk will be about sums of two squares – integers that can be expressed as a sum of two perfect squares:

$$1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, \ldots$$

The first part of the talk will concern their asymptotic count.
The second part will concern more refined questions on their distribution.
Throughout we shall compare their behavior to primes.

Motivation

Sums of two squares are studied from various angles:

1. Representation of integers in terms of values of a quadratic form.
2. Norms of elements from number fields.
3. Multiplicative structure: $b(n) = \mathbf{1}_{n=\square+\square}$ is a multiplicative function.
4. Mathematical physics.

Characterization

Let $b\colon \mathbb{N} \to \{0,1\}$ be the indicator of sums of two squares. It is known that b is multiplicative (Fermat, Euler).
Moreover, if $p \equiv 1 \mod 4$ or $p = 2$ then $b(p^k) = 1$ for all k. If $p \equiv 3 \mod 4$ then $b(p^k) = 1$ if and only if k is even.
Proof consists of three facts:

1. A product of sums of two squares is a sum of two squares: $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$.
2. If $p \equiv 3 \mod 4$ divides a sum of two squares then it divides it exactly an even number of times.
3. $p \equiv 1 \mod 4$ implies p is a sum of two squares – Geometry of numbers.

Asymptotics (I)

Landau (1908): $\sum_{n \le x} b(n) \sim K \frac{x}{\sqrt{\log x}}$ as $x \to \infty$. Here

$$K = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \bmod 4} \left(1 - \frac{1}{p^2}\right)^{-1/2} \approx 0.764$$

Landau established an asymptotic expansion in powers of $1/\log x$. In 1913, Ramanujan independently discovered this asymptotic formula ('Landau–Ramanujan constant'). Landau's proof uses complex analysis, zero-free region of $\zeta(s)$ and $L(s, \chi_{-4})$ and Hankel contours.

Asymptotics (II)

Different proofs of $\sum_{n \le x} b(n) \sim K \frac{x}{\sqrt{\log x}}$:

1. Wirsing (1961): main term under $\sum_{p \le x} b(p) \sim \frac{1}{2} \frac{x}{\log x}$.
2. Wirsing (1967): main term under $\sum_{p \le x} \frac{b(p)}{p} \sim \frac{1}{2} \log \log x$.
3. Selberg (1969): main term.
4. Iwaniec (1976): results in short intervals ($H = x^{1-o(1)}$) and arithmetic progressions ($q = x^{o(1)}$) using the half-dimensional sieve.

Accurate main term (I)

Let $F(s) = \sum_n b(n)/n^s$. It has an Euler product:

$$F(s) = (1-2^{-s})^{-1} \prod_{p \equiv 1 \bmod 4} (1-p^{-s})^{-1} \prod_{p \equiv 3 \bmod 4} (1-p^{-2s})^{-1}.$$

Identity (Shanks, 1964):

$$F(s) = \sqrt{\zeta(s) L(s,\chi_{-4})(1-2^{-s})^{-1}}\, G(s)$$

for

$$G(s) = \prod_{k \geq 1} \left(\frac{(1-2^{-2^k s})\zeta(2^k s)}{L(2^k s, \chi_{-4})} \right)^{2^{-k-1}}.$$

Note that G converges absolutely for $\Re s > 1/2$. In this notation,

$$K = \frac{G(1)}{\sqrt{2}}.$$

Accurate main term (II)

By Perron's formula,

$$\sum_{n\le x} b(n) = \frac{1}{2\pi i}\int_{(2)} F(s)\frac{x^s}{s}\mathrm{d}s.$$

Since F has essential singularity in $s=1$ due to $\sqrt{\zeta(s)}$, main term does not come from a residue, but rather from an integral:

$$M(x) = \frac{1}{\pi}\int_{1/2}^{1}\frac{x^s}{(1-s)^{1/2}s}f(s)\mathrm{d}s, \qquad f(s) = F(s)(s-1)^{1/2}.$$

For this main term,

$$\sum_{n\le x} b(n) = M(x) + O(x\exp(-C\sqrt{\log x})).$$

Accurate main term (III)

With the last main term, M. Radziejewski proved (2014):

$$\sum_{n\leq x} b(n) - M(x)$$

oscillates (takes negative and positive values of order $x^{1/2}/(\log x)^2$ infinitely often). Similar to the classical results on the error term

$$\sum_{p\leq x} 1 - \int_2^x \frac{\mathrm{d}t}{\log t}$$

which changes sign infinitely often. Under GRH,

$$\sum_{n\leq x} b(n) - M(x) = O(x^{1/2+\varepsilon}),$$

similarly to the RH result $\sum_{p\leq x} 1 = \int_2^x \frac{\mathrm{d}t}{\log t} + O(x^{1/2+\varepsilon})$.

Definition

Let q be an odd prime power, and let $\mathbb{F}_q$ be the finite field of size q.

The polynomial ring $\mathbb{F}_q[T]$ shares many properties with the ring of integers $\mathbb{Z}$. An analogue of sums of two squares of integers is $A^2 + TB^2$:

$$\begin{aligned} a^2 + b^2 &= \mathrm{Nm}_{\mathbb{Q}(i)/\mathbb{Q}}(a + ib), \\ A^2 + TB^2 &= \mathrm{Nm}_{\mathbb{F}_q(\sqrt{-T})/\mathbb{F}_q(T)}(A + \sqrt{-T}B) \end{aligned}$$

Let $b_q \colon \mathbb{F}_q[T] \to \{0, 1\}$ be the indicator of $A^2 + TB^2$, and set

$$B_q(n) = \sum_{f \in \mathbb{F}_q[T],\, f \text{ monic},\, \deg f = n} b_q(f).$$

Large-q, or large-n

Theorem (Bary-Soroker, Smilansky and Wolf, 2015)

We have

$$B_q(n) = q^n \frac{\binom{2n}{n}}{4^n} + O_n(q^{n-1}), \qquad q \to \infty.$$

$$B_q(n) = K_q \frac{q^n}{\sqrt{\pi n}} + O_q\left(\frac{q^n}{n^{3/2}}\right), \qquad n \to \infty,$$

where

$$K_q = (1 - q^{-1})^{-\frac{1}{2}} \prod_{P\colon (P/T)=-1} (1 - |P|^{-2})^{-\frac{1}{2}}.$$

Results are consistent:

$$\lim_{n\to\infty} \lim_{q\to\infty} \frac{B_q(n)}{q^n/\sqrt{\pi n}} = \lim_{q\to\infty} \lim_{n\to\infty} \frac{B_q(n)}{q^n/\sqrt{\pi n}} = 1.$$

Uniform theorem

Theorem 1 (G., 2016)

We have

$$B_q(n) = K_q \cdot q^n \cdot \frac{\binom{2n}{n}}{4^n}\left(1 + O\left(\frac{1}{qn}\right)\right)$$

with an absolute implied constant.
Moreover, B_q is a polynomial in q of degree n, and K_q is an analytic function of $1/q$.

Proof avoids complex analysis.

Twisted sums

- **Q1**: Fix a nonprincipal Dirichlet character χ mod q. What can one say about the distribution of

$$\sum_{n \le x} b(n)\chi(n)$$

for 'random' x?

- **Q2**: Let χ be a Dirichlet character chosen uniformly at random from the group of $\phi(q)$ Dirichlet characters modulo q. What can one say about the distribution of

$$\sum_{n \le x} b(n)\chi(n)\,?$$

One may ask similar questions replacing $\chi(n)$ with n^{it} (with either t fixed, or random $t \in [1, T]$).

Short sums

- **Q3**: What can be said about the distribution of

$$\sum_{n\leq x,\, n\equiv a \bmod q} b(n)$$

for random $a \in (\mathbb{Z}/q\mathbb{Z})^\times$? Or

$$\sum_{x\leq n<x+H} b(n)$$

for random $x \in [X, 2X]$?

Here q and H should be thought of as functions of x, e.g. $q \asymp x^{1-\delta}$ or $H \asymp x^\delta$.

It will be instructive to consider these questions for b replaced by the indicator of primes $\mathbf{1}_P$, or the von Mangoldt function Λ.

Von Mangoldt and primes

Suppose we want to understand the difference

$$\pi(x;4,3)-\pi(x;4,1).$$

It is the same as

$$-\sum_{p\le x}\chi_{-4}(p).$$

We have

$$\sum_{n\le x}\Lambda(n)\chi_{-4}(n)=-\sum_{\rho:\, L(\rho,\chi_{-4})=0}\frac{x^\rho}{\rho}.$$

By integration by parts,

$$\begin{aligned}\sum_{p\le x}\chi_{-4}(p)&=\sum_{n\le x}\chi_{-4}(n)\frac{\Lambda(n)}{\log n}-\sum_{p^2\le x}\frac{\chi_{-4}(p^2)}{2}+O(x^{1/3})\\&\approx\frac{1}{\log x}\sum_{n\le x}\Lambda(n)\chi_{-4}(n)-\frac{1}{2}\pi(\sqrt{x}).\end{aligned}$$

Almost-periodic functions

Under GRH, if we combine last formulas then

$$(\pi(e^t;4,3)-\pi(e^t;4,1))\frac{t}{e^{t/2}} \approx \sum_{L(1/2+i\gamma,\chi_{-4})=0} \frac{e^{it\gamma}}{1/2+i\gamma}+1.$$

The left-hand side is a *almost periodic function*, meaning: it lives in the closure of the space of trigonometric polynomials. Ultimately, bias comes from squares of primes.

Linear Independence Hypothesis (LI):
$\{\gamma>0 : L(1/2+i\gamma,\chi_{-4})=0\}$ are linearly independent over $\mathbb{Q}$.

Rubinstein–Sarnak

Theorem (Rubinstein–Sarnak, 1993)

Assume GRH and LI for $L(s, \chi_{-4})$. Then for any nice function f,

$$\frac{1}{\log X} \int_1^X f\left((\pi(t; 4, 3) - \pi(t; 4, 1)) \frac{\log t}{\sqrt{t}} \right) \frac{\mathrm{d}t}{t} \to \int_{\mathbb{R}} f \,\mathrm{d}\mu$$

for some absolutely continuous, symmetric measure μ. Moreover, $\mu((0, \infty)) = 0.9959\ldots$. Limit can also be written as

$$\frac{1}{\log X} \int_0^{\log X} f\left((\pi(e^v; 4, 3) - \pi(e^v; 4, 1)) \frac{v}{e^{v/2}} \right) \mathrm{d}v \to \int_{\mathbb{R}} f \,\mathrm{d}\mu$$

Sums of squares bias - integers

Theorem 2 (G., 2023)

Assume GRH. We have

$$\sum_{\substack{n\le x\\ n\equiv 1 \bmod 3}} b(n) - \sum_{\substack{n\le x\\ n\equiv 2 \bmod 3}} b(n) = M(x) + E(x),$$

$$M(x) \sim A\frac{\sqrt{x}}{\log^{3/4} x}, \qquad \frac{1}{X}\int_X^{2X} E^2(x)\mathrm{d}x \ll \frac{X}{\log^{5/2} X}$$

for some positive $A > 0$. In particular, we almost always have

$$\sum_{\substack{n\le x\\ n\equiv 1 \bmod 3}} b(n) > \sum_{\substack{n\le x\\ n\equiv 2 \bmod 3}} b(n).$$

Sums of squares bias - polynomials

Assume q is odd and let S_q be the set of monic polynomials of the shape $A^2 + TB^2$.

Theorem 3 (G., 2025+)

We have

$$\sum_{\substack{f \in S_q \\ \deg f = n}} \chi(f) \ll_\chi \frac{q^{n/2}}{n^{5/4}}$$

if χ is a complex character. If χ is real,

$$\sum_{\substack{f \in S_q \\ \deg f = n}} \chi(f) = \frac{q^{n/2}}{n^{3/4}}(C_{\chi, n \bmod 2} + o(1)).$$

Main idea

Let $F(s,\chi) = \sum_n b(n)\chi(n)/n^s$. One has

$$F(s,\chi) \approx \sqrt{L(s,\chi)L(s,\chi\chi_{-4})}\sqrt[4]{\frac{L(2s,\chi^2)}{L(2s,\chi^2\chi_{-4})}}.$$

Different behavior at $s = 1/2$, depending on χ being real or not.

Primes

Let q be a prime. For a random Dirichlet character χ mod q,

$$\mathbb{E}_\chi \Big|\sum_{p \le x} \chi(p)\Big|^{2k}$$

$$\#\{(p_1, \ldots, p_k, q_1, \ldots, q_k) : \prod p_i \equiv \prod q_j \bmod q,\ q \ne p_i, q_j \le x\}.$$

If $q > x^k$ this is easy to evaluate:

$$\mathbb{E}_\chi \Big|\sum_{p \le x} \chi(p)\Big|^{2k} \sim k!\pi(x)^k.$$

In particular,

$$\frac{\sum_{p \le x} \chi(p)}{\sqrt{\pi(x)}} \xrightarrow[x \to \infty]{d} CN(0,1)$$

if $\log q / \log x \to \infty$, where χ is random modulo q.

Random multiplicative functions

Understanding $\sum_{p\le x}\chi(p)$ becomes easier if we replace the random χ with a random multiplicative function:

$$n=\prod p_i^{e_i} \implies \alpha(n)=\prod \alpha(p_i)^{e_i}$$

and

$(\alpha(p))_p$ are i.i.d random variables, uniformly distributed on S^1.

We have the following orthogonality relation:

$$\mathbb{E}\alpha(n)\overline{\alpha}(m)=\delta_{n,m}.$$

With this set-up:

- $\mathbb{E}|\sum_{p\le x}\alpha(p)|^{2k}=\#\{(p_1,\dots,p_k,q_1,\dots,q_k):\prod p_i=\prod q_j,\ p_i,q_j\le x\}\sim \pi_k(x)x^k$ as $x\to\infty$,
- By CLT,

$$\frac{\sum_{p\le x}\alpha(p)}{\sqrt{\pi(x)}}\xrightarrow[x\to\infty]{d} CN(0,1).$$

Back to sums of squares

Consider

$$S_x = \frac{\sum_{n \le x} b(n)\alpha(n)}{\sqrt{\sum_{n \le x} b(n)}}.$$

Theorem 4 (G.–Mo Dick Wong, 2025)

We have

$$S_x \xrightarrow[x \to \infty]{d} G \cdot \sqrt{V},$$

where $G \sim CN(0,1)$ and V is independent of G. Moreover, V is almost surely positive and finite, and satisfies

$$\mathbb{E}V^p < \infty \longleftrightarrow p < 2.$$

Now let's get back to the prime sum with a random character. Recall

$$\frac{\sum_{p\le x}\chi(p)}{\sqrt{\pi(x)}} \xrightarrow[x\to\infty]{d} CN(0,1)$$

if $\log q/\log x \to \infty$, where χ is random character modulo q. Conjecture based on random matrix theory and function fields:

$$(\star)\,\mathbb{E}_{\chi_0\neq\chi \bmod q}\Big|\sum_{p\le x}\chi(p)\Big|^2 \sim \pi(x)\frac{\log\min\{x,q\}}{\log x}$$

for $q \ge x^{\varepsilon}$. $(\star)$ lies extremely deep: it is morally equivalent to *Pair Correlation Conjecture for Dirichlet L-functions*.

What about distribution of

$$\frac{\sum_{n\le x} b(n)\chi(n)}{\sqrt{\sum_{n\le x} b(n)}}$$

for random $\chi \bmod q$? Currently only solved if χ is replaced by a random multiplicative function. Leads to the following question:

$$\mathbb{E}_{\chi_0\neq\chi \bmod q}\left|\frac{\sum_{n\le x} b(n)\chi(n)}{\sqrt{\sum_{n\le x} b(n)}}\right|^2 \sim ???$$

May conjecture: if $q = x^c$,

$$\frac{\sum_{n\le x} b(n)\chi(n)}{\sqrt{\sum_{n\le x} b(n)}} \xrightarrow[x\to\infty]{d} G\cdot\sqrt{V_c}$$

for $G \sim CN(0,1)$. No guess for V_c.

More motivation for variance

By orthogonality,

$$\frac{1}{(q-1)^2}\sum_{\chi_0\neq\chi \bmod q}\Big|\sum_{p\leq x}\chi(p)\Big|^2=\frac{1}{q-1}\sum_{a=1}^{q-1}\Big(\sum_{\substack{p\leq x\\ p\equiv a \bmod q}}1-\frac{1}{q-1}\mathrm{Li}(x)\Big)^2.$$

RHS is known as *variance of primes in APs*. So $(\star)$ is equivalent to:

$$\mathrm{Var}(\pi(x;\bullet,q))\sim\frac{\pi(x)}{q-1}\frac{\log q}{\log x}$$

for $x\geq q\geq x^{\varepsilon}$. Related to *Hooley's conjecture*. Consistent with Barban–Davenport–Halberstam(–Montgomery–Hooley) Theorem.

Variance in function fields

Similarly,

$$\frac{1}{(q-1)^2}\sum_{\chi_0\neq\chi \bmod q}\Big|\sum_{n\leq x} b(n)\chi(n)\Big|^2$$
$$=\frac{1}{q-1}\sum_{a=1}^{q-1}\Big(\sum_{\substack{n\leq x\\ n\equiv a \bmod q}} b(n)-\frac{\sum_{n\leq x,\,(n,q)=1} b(n)}{q-1}\Big)^2.$$

Theorem 5 (G.-Rodgers, 2020)

Informal statement: in function fields, exists positive G s.t.

$$\Big(\sum_{n\leq x} b(n)\Big)^{-1}\mathbb{E}_{\chi_0\neq\chi \bmod q}\Big|\sum_{n\leq x} b(n)\chi(n)\Big|^2\sim G(\log q/\log x).$$

Leads to a precise conjecture in integers.

Short sums for primes

The sum $\sum_{p \le x,\, p \equiv a \bmod q} 1 - \mathrm{Li}(x)/(q-1)$ for random $(a, q) = 1$ is expected to tend to Gaussian after normalization by standard deviation, for $q = o(x/\log x)$.
Computing variance is equivalent to computing $\sum_{\chi_0 \neq \chi \bmod q} |\sum_{p \le x} \chi(p)|^2$.
Similarly, $\sum_{x < p \le x+H} 1 - \int_x^{x+H} \frac{\mathrm{d}t}{\log t}$ expected to tend to Gaussian after normalization, for $H/\log x \to \infty$; established via moments by Montgomery–Soundararajan (conditionally).

Short sums for sums of two squares

The distribution of $\sum_{n\leq x,\, n\equiv a \bmod q} b(n) - \frac{1}{q-1}\sum_{n\leq x,\, (n,q)=1} b(n)$ for random $(a,q)=1$ is expected to tend to Gaussian if $q = o(x/\sqrt{\log x})$, after normalization by standard deviation.
Computing variance is equivalent to computing $\sum_{\chi_0\neq\chi \bmod q} |\sum_{n\leq x} b(n)\chi(n)|^2$ for which Brad and I gave a conjecture.
Same story expected for $\sum_{x<n\leq x+H} b(n) - (M(x+H) - M(x))$ if $H/\sqrt{\log x} \to \infty$.
Freiberg–Kurlberg–Rosenzweig (2017) proved Poisson behavior for $\sum_{x<n\leq x+H} b(n)$ when $H \sim \lambda\sqrt{\log x}$ via moments (conditionally).

Happy Birthday Pieter!

$$60 + 1 = 5^2 + 6^2$$