$$N = \square + \square + \square$$

Paul Pollack

University of Illinois at
Urbana-Champaign

May 27, 2010

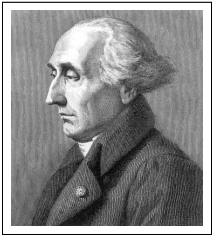
Characterizing sums of squares

The study of sums of squares goes back at least to the dawn of modern number theory.

Let $\square$ stand for a generic member of the set $\{n^2 : n = 0, 1, 2, \dots\}$.

Theorem (Fermat–Euler)

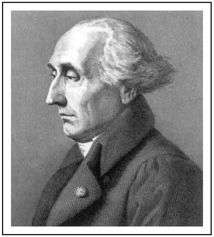
Let n be a natural number. Then $n = \square + \square$ if and only if every prime p dividing n with $p \equiv 3 \pmod 4$ shows up to an even power.



Theorem (Lagrange)

Every natural number is of the form $\square + \square + \square + \square$.

We teach both results in courses on elementary number theory. But what about 3 squares?



Theorem (Lagrange)

Every natural number is of the form $\square + \square + \square + \square$.

We teach both results in courses on elementary number theory. But what about 3 squares?

Theorem (Legendre)

Let n *be a natural number. Then* n *has the form* $\square + \square + \square$ *unless* $n = 4^k(8l + 7)$ *for some nonnegative integers* k *and* l.

How is the three-squares theorem proved?

First, change the problem. Ask about three *rational squares*.
By Hasse-Minkowski,

$$N = \square + \square + \square \text{ in } \mathbb{Q} \iff N = \square + \square + \square \text{ in each } \mathbb{Q}_p.$$

Lemma
If $N = \square + \square + \square$ in $\mathbb{Q}$, then $N = \square + \square + \square$ in $\mathbb{Z}$.

For details, see
Serre's *Course in Arithmetic*, appendix to Chapter 4.

Counting sums of squares

Theorem (I. M. Trivial)

$$\#\{n \leq x : n = \square\} = \sqrt{x} + O(1).$$

Theorem (Landau–Ramanujan)

As $x \to \infty$,

$$\#\{n \leq x : n = \square + \square\} \sim C \frac{x}{\sqrt{\log x}},$$

where

$$C = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod 4} \left(1 - \frac{1}{p^2}\right)^{-1/2}.$$

Theorem

For $x \geq 2$, we have

$$\#\{n \leq x : n = \Box + \Box + \Box\} = \frac{5}{6}x + O(\log x).$$

Proof.

Let's count exceptions.

$$\#\{n \leq x : n \equiv 7 \pmod 8\} = \frac{x}{8} + O(1).$$

$$\#\{n \leq x : n = 4m, m \equiv 7 \pmod 8\} = \frac{x}{8 \cdot 4} + O(1),$$

etc. Notice that $1/8 + 1/(8 \cdot 4) + 1/(8 \cdot 4^2) + \cdots = 1/6$.

Was that too easy?

Let $\Delta(x)$ denote the remainder term in the counting problem for three squares.

Theorem (Osbaldestin and Shiu)

There is a continuous, nowhere differentiable function F with period 1 such that for $N \geq 1$,

$$\frac{1}{N}\sum_{0\leq n<N}\Delta(n) = \frac{3}{8}\frac{\log N}{\log 4} + F\left(\frac{\log N}{\log 4}\right) + \frac{\delta(N)}{N},$$

where

$$\delta(N) = \begin{cases} \frac{1}{8} & \text{if } N \text{ is odd,} \\ 0 & \text{if } N \text{ is even.} \end{cases}$$

A sampling of probabilistic number theory

Let f be an arithmetic function. The mean value of f is

$$\mathcal{M}(f) := \lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} f(n),$$

if the limit exists.

A sampling of probabilistic number theory

Let f be an arithmetic function. The mean value of f is

$$\mathcal{M}(f) := \lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} f(n),$$

if the limit exists.

Examples

- If $f \equiv c$ is constant, then f has mean value c.

A sampling of probabilistic number theory

Let f be an arithmetic function. The mean value of f is

$$\mathcal{M}(f) := \lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} f(n),$$

if the limit exists.

Examples

- If $f \equiv c$ is constant, then f has mean value c.
- If $f(n) = d(n)$, the number of divisors of n, then f does not have a mean value. The average up to x is about $\log x$.

A sampling of probabilistic number theory

Let f be an arithmetic function. The mean value of f is

$$\mathcal{M}(f) := \lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} f(n),$$

if the limit exists.

Examples

- If $f \equiv c$ is constant, then f has mean value c.
- If $f(n) = d(n)$, the number of divisors of n, then f does not have a mean value. The average up to x is about $\log x$.
- If $f(n) = \mathbf{1}_S$, then $\mathcal{M}(f)$ is the asymptotic density of S.

A sampling of probabilistic number theory

Let f be an arithmetic function. The mean value of f is

$$\mathcal{M}(f) := \lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} f(n),$$

if the limit exists.

Examples

- If $f \equiv c$ is constant, then f has mean value c.
- If $f(n) = d(n)$, the number of divisors of n, then f does not have a mean value. The average up to x is about $\log x$.
- If $f(n) = \mathbf{1}_S$, then $\mathcal{M}(f)$ is the asymptotic density of S.
- If $f(n) = \mu(n)$, then f has mean value 0. This is equivalent to the PNT.

Which f have mean values?

For this to be a reasonable question, we should impose some conditions on f. We will assume:

1. f is multiplicative,
2. f is real-valued,
3. f takes values in $[-1, 1]$.

What can we say about $\mathcal{M}(f)$?

Which f have mean values?

For this to be a reasonable question, we should impose some conditions on f. We will assume:

1. f is multiplicative,
2. f is real-valued,
3. f takes values in $[-1, 1]$.

What can we say about $\mathcal{M}(f)$?

Starting point: Write $f(n) = \sum_{d|n} g(d)$ for some arithmetic function g. Then

$$\sum_{n \le x} f(n) = \sum_{n \le x} \sum_{d|n} g(d) = \sum_{d \le x} g(d) \sum_{\substack{n \le x \\ d|n}} 1.$$

A good guess?

This suggests that

$$\frac{1}{x}\sum_{n\le x} f(n) \approx \sum_{d\le x}\frac{g(d)}{d}.$$

So taking the limit, we might expect

$$\begin{aligned}\mathcal{M}(f) &= \sum_{d}\frac{g(d)}{d}\\ &= \prod_{p}\left(1+\frac{g(p)}{p}+\frac{g(p^2)}{p^2}+\dots\right).\end{aligned}$$

Also, g is multiplicative and $g(p^k) = f(p^k) - f(p^{k-1})$.

Conjecture

Under our hypotheses on f, we have

$$\mathcal{M}(f) = \prod_p \left(1 - \frac{1}{p}\right) \left(1 + \sum_{m=1}^{\infty} f(p^m) p^{-m}\right)$$

Theorem (Wintner)

The conjecture holds if

$$\sum_p \frac{1 - f(p)}{p}$$

converges.

Example

The function $f(n) = \phi(n)/n$ has a mean value.

Conjecture (Erdős, Wintner)

Assume f is as before. If

$$\sum_p \frac{1-f(p)}{p}$$

diverges, then $\mathcal{M}(f) = 0$.

Because of the case $f = \mu$, this include the prime number theorem.

From Elliott's *Probabilistic Number Theory, vol. 1*:

> *As was his wont, when giving lectures during the course of his travels, Professor Erdős will advise that certain of the problems which he has posed or recorded, carry prizes. Usually they lie in the range U.S. $50 to $500, but in the case of the Erdős–Wintner conjecture, fearing that he would not see a solution before he left, he offered a prize of* $10^{10}!$.

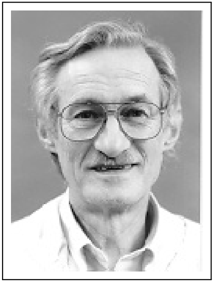
From Elliott's *Probabilistic Number Theory, vol. 1*:

> *As was his wont, when giving lectures during the course of his travels, Professor Erdős will advise that certain of the problems which he has posed or recorded, carry prizes. Usually they lie in the range U.S. \$50 to \$500, but in the case of the Erdős–Wintner conjecture, fearing that he would not see a solution before he left, he offered a prize of* $10^{10}!$.

From the errata:

> *The prize should read* $10^{10!}$.

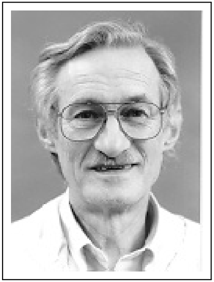
Truth and consequences



Theorem (Wirsing)

The Erdős–Wintner conjecture is correct.

Truth and consequences

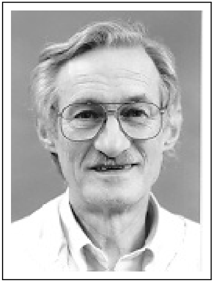


Theorem (Wirsing)

The Erdős–Wintner conjecture is correct.

. . . being a gentleman, he [Wirsing] forgot the prize.

Truth and consequences



Theorem (Wirsing)

The Erdős–Wintner conjecture is correct.

. . . being a gentleman, he [Wirsing] forgot the prize.

But what is this theorem good for, besides earning prize money?

Return to sums of three squares

Let ϕ denote Euler's totient function, so that

$$\phi(n) = \#\{1 \le k \le n : \gcd(k, n) = 1\}.$$

Question: How often is $\phi(n)$ a sum of squares?

Return to sums of three squares

Let ϕ denote Euler's totient function, so that

$$\phi(n) = \#\{1 \leq k \leq n : \gcd(k,n) = 1\}.$$

Question: How often is $\phi(n)$ a sum of squares?

Theorem (Banks, Friedlander, Pomerance, Shparlinski)

For large x,

$$\#\{n \leq x : \phi(n) = \square\} \geq x^{0.7038}.$$

Return to sums of three squares

Let ϕ denote Euler's totient function, so that

$$\phi(n) = \#\{1 \leq k \leq n : \gcd(k, n) = 1\}.$$

Question: How often is $\phi(n)$ a sum of squares?

Theorem (Banks, Friedlander, Pomerance, Shparlinski)

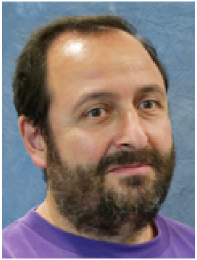
For large x,

$$\#\{n \leq x : \phi(n) = \square\} \geq x^{0.7038}.$$

Theorem (Banks, Luca, Saidak Shparlinski)

For large x,

$$\#\{n \leq x : \phi(n) = \square + \square\} \asymp \frac{x}{(\log x)^{3/2}}.$$

Bill Banks, Igor Shparlinski, Filip Saidak, and John Friedlander

Three squares?

Theorem (P.)

The set of n for which $\phi(n)$ is a sum of three squares has density $7/8$.

Three squares?

Theorem (P.)

The set of n for which $\phi(n)$ is a sum of three squares has density $7/8$.

Let $v_2(m)$ be the power of 2 sitting inside m, and let $u(m)$ be the odd part of m, so that

$$m = 2^{v_2(m)} u(m).$$

According to Legendre,

$$\begin{aligned}\phi(n) \neq \square + \square + \square &\iff \phi(n) = 4^k(8l+7) \text{ for some } k, l \\ &\iff 2 \mid v_2(\phi(n)), \quad u(\phi(n)) \equiv 7 \pmod 8\end{aligned}$$

Let G be the group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})^{\times}$. Define a map $r\colon \mathbb{N} \to G$ by

$$m \mapsto (v_2(m) \bmod 2, u(m) \bmod 8).$$

Then r is a homomorphism (of semigroups).
Now define a map $f\colon \mathbb{N} \to G$ by

$$n \mapsto r(\phi(n)).$$

Then f is a G-valued multiplicative function, in the sense that whenever a and b are relatively prime,

$$f(ab) = f(a) \circ f(b).$$

Also, Legendre says

$$\phi(n) \neq \Box + \Box + \Box \iff f(n) = (0 \bmod 2, 7 \bmod 8).$$

We will show that as n ranges over $\mathbb{N}$, the elements $f(n) \in G$ become equidistributed. In other words, for each fixed $g \in G$, the set $f^{-1}(g) \subset \mathbb{N}$ has asymptotic density $1/8$.

Lemma

Let $g_1, g_2, g_3, \ldots$ be an infinite sequence of elements of a finite abelian group G. Then $\{g_i\}_{i=1}^{\infty}$ is uniformly distributed precisely when

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n \leq x} \chi(g_n) = 0$$

for each nontrivial $\chi \in \hat{G}$.

So let χ be a nontrivial character of $G = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})^{\times}$.
Every element of G squares to be the identity, so the image of χ belongs to $\{1, -1\}$.
We have to show that

$$\lim_{x \to \infty} \frac{1}{x} \sum_{n \le x} \chi(f(n)) = 0.$$

In other words, we want that the function $\chi \circ f$ has mean value zero.
We can apply Wirsing, because:

- $\chi \circ f$ is multiplicative,
- $\chi \circ f$ is real-valued,
- $\chi \circ f$ assumes only the values -1 and 1.

Wirsing says we should look at

$$\sum_{p} \frac{1-\chi(f(p))}{p} = 2 \sum_{p\colon\, \chi(f(p))=-1} \frac{1}{p}.$$

To show this diverges, we want many primes p for which $\chi(f(p)) = -1$.
The characters of $G = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})^{\times}$ have the form $\chi_1\chi_2$:

Characters χ_1 of $\mathbb{Z}/2\mathbb{Z}$: $\{\mathbf{1}, (-1)^n\}$
Characters χ_2 of $(\mathbb{Z}/8\mathbb{Z})^{\times}$: Dirichlet characters mod 8

So for our χ, we have

$$(\chi \circ f)(n) = \zeta^{v_2(\phi(n))}\chi_2(u(n)),$$

where $\zeta \in \{1, -1\}$ and χ_2 is a Dirichlet character mod 8.
Also either $\zeta \neq 1$ or $\chi_2 \neq \mathbf{1}$.

So for our χ, we have

$$(\chi \circ f)(n) = \zeta^{v_2(\phi(n))}\chi_2(u(n)),$$

where $\zeta \in \{1, -1\}$ and χ_2 is a Dirichlet character mod 8.
Also either $\zeta \neq 1$ or $\chi_2 \neq \mathbf{1}$.

Suppose first $\chi_2 = \mathbf{1}$. Then $\zeta = -1$, and

$$\chi(f(p)) = (-1)^{v_2(p-1)}.$$

So if $p \equiv 3 \pmod 4$, then $\chi(f(p)) = -1$. So

$$\sum_{p\colon\ \chi(f(p))=-1} \frac{1}{p} = \infty.$$

This proves $\chi \circ f$ has mean value zero.

Now suppose $\chi_2 \neq \mathbf{1}$. Take a prime $p \equiv 5 \pmod 8$. We have $v_2(p-1) = 2$, and so

$$\begin{aligned} \chi(f(p)) &= \zeta^{v_2(p-1)} \chi_2(u(p-1)) \\ &= \chi_2(u(p-1)). \end{aligned}$$

Either $\chi_2(3) = -1$ or $\chi_2(5) = -1$. In the former case, choose p so that

$$\frac{p-1}{4} \equiv 3 \pmod 8, \qquad \text{i.e.,} \qquad p \equiv 13 \pmod{32}$$

and in the latter choose p so that

$$\frac{p-1}{4} \equiv 5 \pmod 8, \qquad \text{i.e.,} \qquad p \equiv 21 \pmod{32}.$$

Then $\chi(f(p)) = -1$. And the sum of the reciprocals of these p diverges. So $\chi \circ f$ has mean value zero in this case also.

What about other arithmetic functions?

A theorem of Ruzsa says that if G is any finite abelian group, and $f : \mathbb{N} \to G$ is a multiplicative function, then the sets $f^{-1}(g)$, with $g \in G$, all possess asymptotic densities.

Corollary

Let h be any positive-integer valued multiplicative function. Then all three of the sets

$$\{n : h(n) = \Box\}, \quad \{n : h(n) = \Box + \Box\}, \quad \{n : h(n) = \Box + \Box + \Box\}$$

have asymptotic densities.

A parting shot

Let $\lambda(n)$ denote the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^\times$.

Theorem (P.)

The set of n for which $\lambda(n)$ is a sum of three squares has lower density > 0 and upper density < 1.

A parting shot

Let $\lambda(n)$ denote the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^\times$.

Theorem (P.)

The set of n for which $\lambda(n)$ is a sum of three squares has lower density > 0 and upper density < 1.

Conjecture

The set of n for which $\lambda(n)$ is a sum of three squares does not have an asymptotic density.