# Euler's function and sums of squares

Paul Pollack

University of Illinois

July 16, 2010

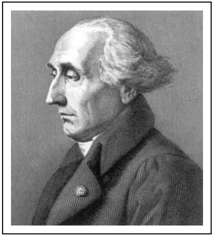
# Characterizing sums of squares

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

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

**Theorem (Fermat–Euler)**

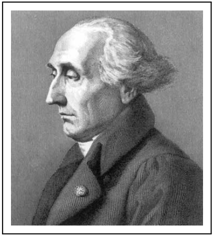
*Let $n$ be a natural number. Then $n = \Box + \Box$ if and only if every prime $p$ dividing $n$ with $p \equiv 3 \pmod 4$ shows up to an even power.*



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* $l$.

# 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*

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

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

# Enter Euler

Let $\phi$ denote Euler's totient function, so that

$$\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^{\times}.$$

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

# Enter Euler

Let $\phi$ denote Euler's totient function, so that

$$\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^{\times}.$$

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

Theorem (Banks, Friedlander, Pomerance, Shparlinski)

*For large $x$,*

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

# Enter Euler

Let $\phi$ denote Euler's totient function, so that

$$\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times.$$

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

Theorem (Banks, Friedlander, Pomerance, Shparlinski)

*For large $x$,*

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

Theorem (Banks, Luca, Saidak, Shparlinski)

*For $x \ge 3$,*

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

# 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 $7/8$.*

**Proof:** Let $v_2(m)$ be the exponent on 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,

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

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.

Also,

$$m \neq \square + \square + \square \iff r(m) = (0 \bmod 2, 7 \bmod 8).$$

So we want to know how often $r(\phi(n)) = (0 \bmod 2, 7 \bmod 8)$.

We will show that as $n$ ranges over $\mathbb{N}$, the elements $r(\phi(n)) \in G$ become equidistributed.

### Theorem

*For each $g \in G$, the set of $n \in \mathbb{N}$ for which $r(\phi(n)) = g$ has asymptotic density $1/8$.*

Recall the following elementary equidistribution criterion:

### Lemma

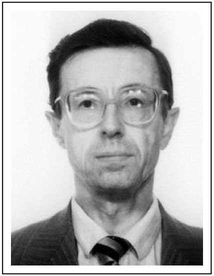
*Let $g_1, g_2, g_3, \ldots$ be an infinite sequence of elements of a finite abelian group $G$. Then $\{g_i\}_{i=1}^{\infty}$ is uniformly distributed precisely when*

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

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

Let $\chi$ be a nontrivial character of $G = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})^\times$. Then $f(n) := \chi(r(\phi(n)))$ is a multiplicative function. We want to know that $f$ has mean value zero.

Let $\mathcal{M}_k$ denote the class of multiplicative functions $f\colon \mathbb{N} \to \mathbb{C}$ with $f(n)^k = 1$ for each $n$.



### Theorem (Halász)

*Let $f$ be an arithmetic function with the property that $f \in \mathcal{M}_k$ and*

$$\sum_{p\colon\ f(p)\neq 1} \frac{1}{p}$$

*diverges. Then $f$ has mean value zero.*

For our functions $f(n) = \chi(r(\phi(n)))$, we have $f(p) \neq 1$ for an entire congruence class of primes $p$ modulo 32.

Thank you!

# 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.*