

Sums of Squares & r -gonal numbers

Swastika Dey, Anderson Hao, Jeffrey Xu, Jessie Wang, Yuanrui Zhao

PROMYS

October 9, 2026

When was the first time you saw a sum of squares?

When was the first time you saw a sum of squares?

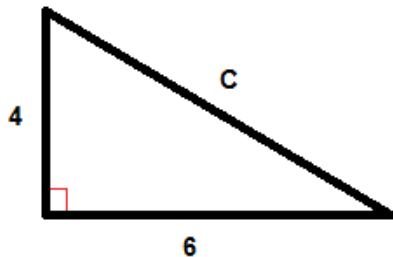


Figure: Right triangles! Pythagorean theorem!

When was the next time you saw a sum of squares?

When was the next time you saw a sum of squares?

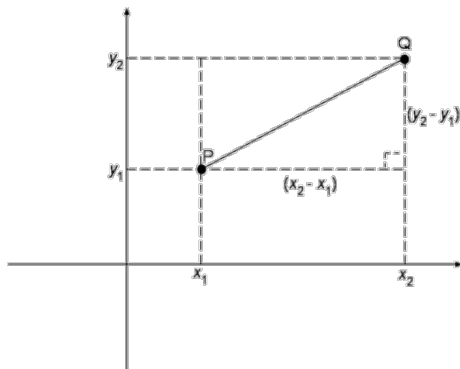


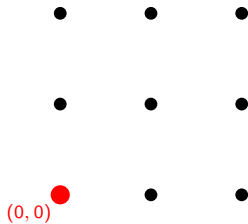
Figure: Distance between two lattice points! $PQ = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$

An interesting extension of these problems is to ask...

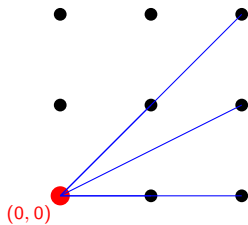
An interesting extension of these problems is to ask...

How many distinct distances are there between pairs of lattice points (a_1, b_1) and (a_2, b_2) in the $n \times n$ grid defined by $0 \leq a_i, b_i \leq n$?

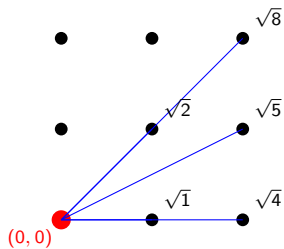
All distinct distances from $(0, 0)$ in a 2×2 grid



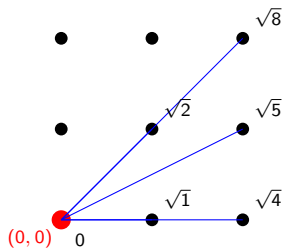
All distinct distances from $(0, 0)$ in a 2×2 grid



All distinct distances from $(0, 0)$ in a 2×2 grid

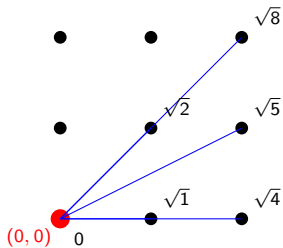


All distinct distances from $(0, 0)$ in a 2×2 grid

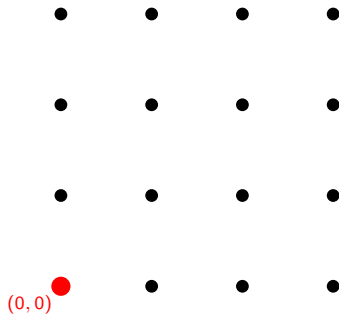


All distinct distances from $(0,0)$ in a 2×2 grid

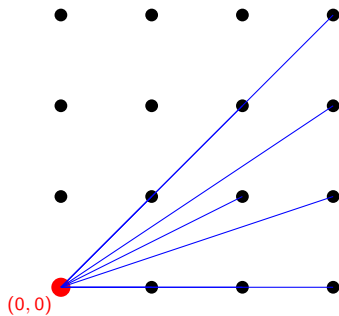
Total distinct distances: 6



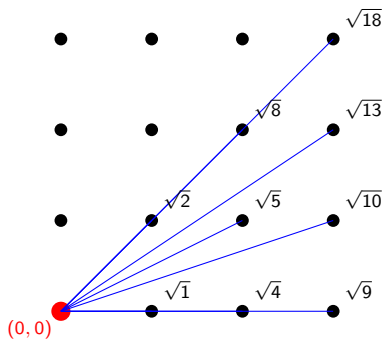
All distinct distances from $(0,0)$ in a 3×3 grid



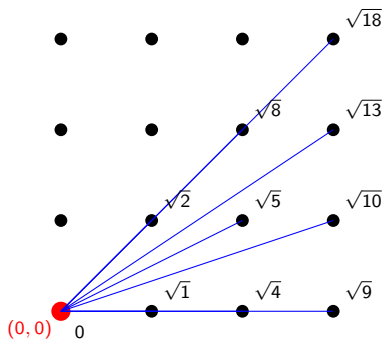
All distinct distances from $(0,0)$ in a 3×3 grid



All distinct distances from $(0,0)$ in a 3×3 grid

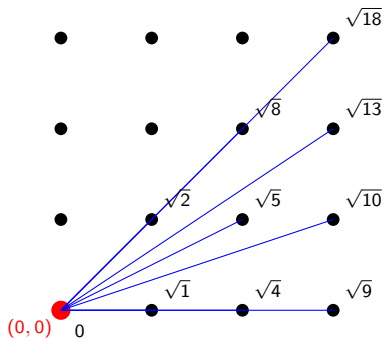


All distinct distances from $(0,0)$ in a 3×3 grid

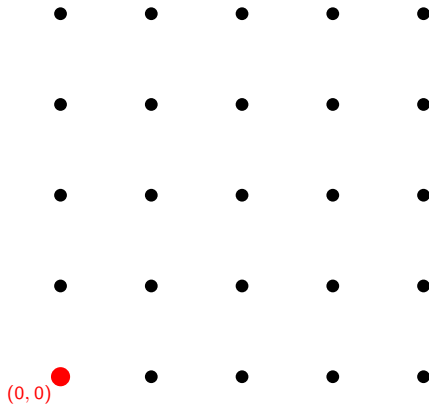


All distinct distances from $(0,0)$ in a 3×3 grid

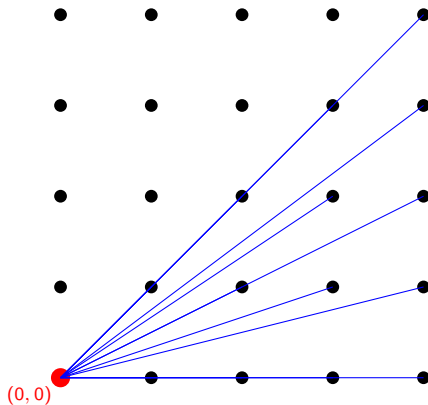
Total distinct distances: 10



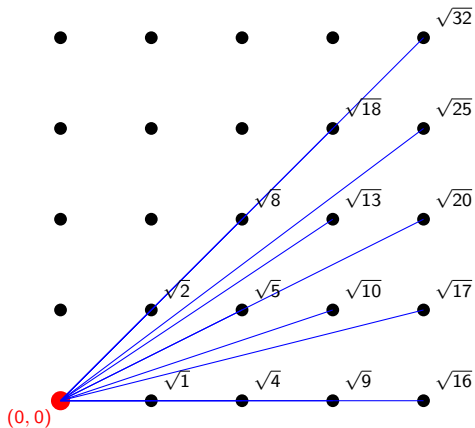
All distinct distances from $(0, 0)$ in a 4×4 grid



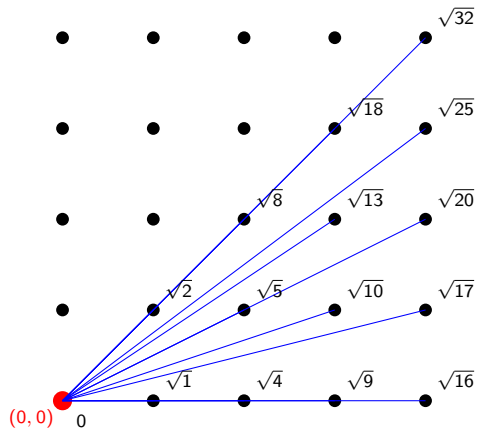
All distinct distances from $(0,0)$ in a 4×4 grid



All distinct distances from $(0,0)$ in a 4×4 grid

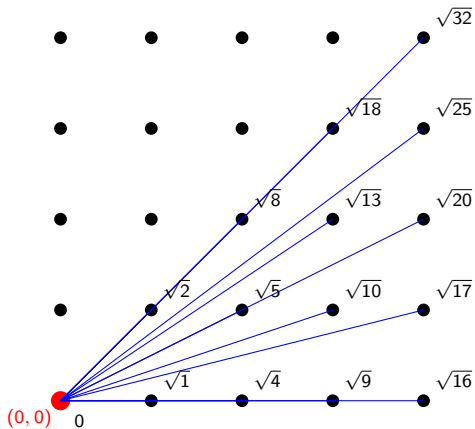


All distinct distances from $(0,0)$ in a 4×4 grid



All distinct distances from $(0,0)$ in a 4×4 grid

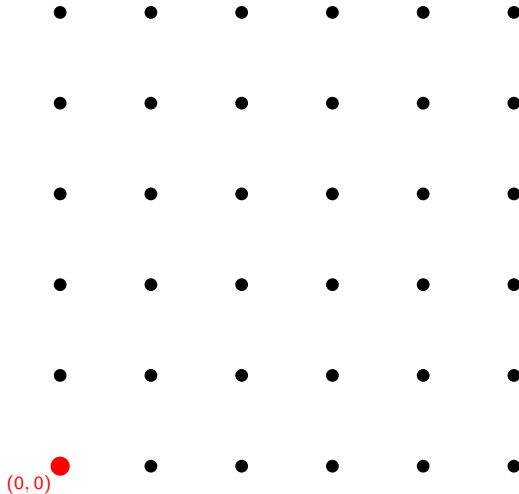
Total distinct distances: 15



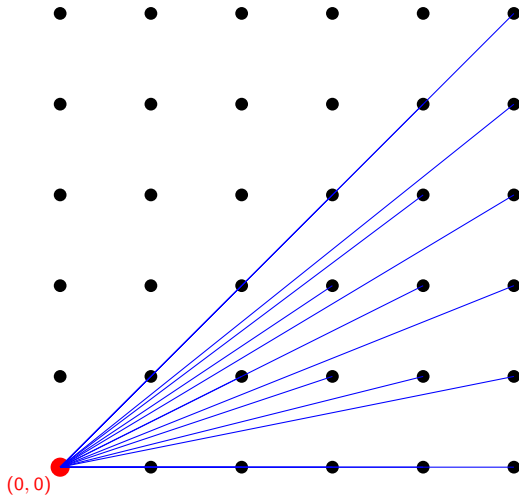
Distinct Distances Table

Grid Size n	Distinct Distances
2	6
3	10
4	15

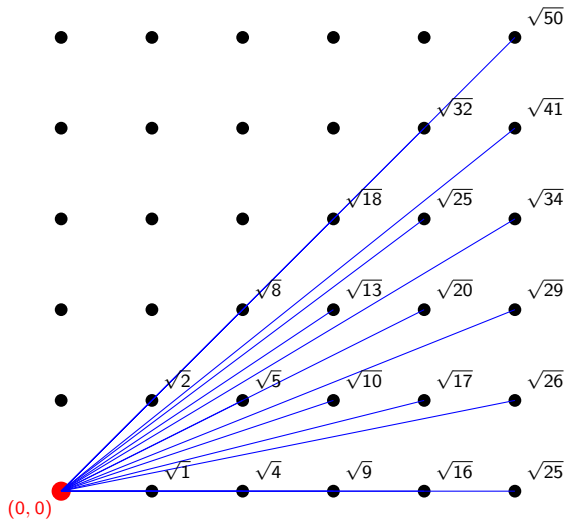
All distinct distances from $(0, 0)$ in a 5×5 grid



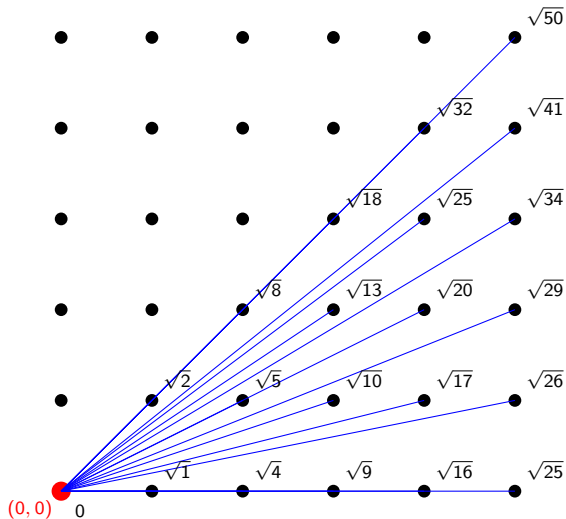
All distinct distances from $(0, 0)$ in a 5×5 grid



All distinct distances from $(0, 0)$ in a 5×5 grid

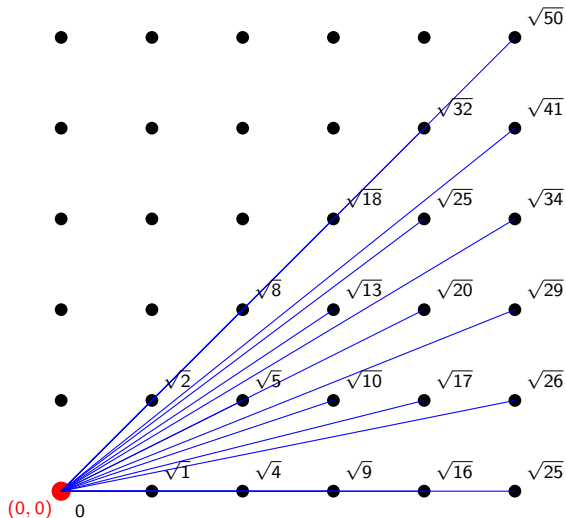


All distinct distances from $(0, 0)$ in a 5×5 grid



All distinct distances from $(0,0)$ in a 5×5 grid

Total distinct distances: 20



Distinct Distances Table

Grid Size n	Distinct Distances
2	6
3	10
4	15
5	20

Can we find a general formula for this count for an $n \times n$ grid?

Can we find a general formula for this count for an $n \times n$ grid?

Neither can we!

Can we find a general formula for this count for an $n \times n$ grid?

Neither can we!

We bound by: $n + 1 + \binom{n+1}{2}$.

To answer this question, we must determine the number of ways to express a number as the sum of two squares...

Let's try some examples.

- 5 can be written as the sum of two squares...

To answer this question, we must determine the number of ways to express a number as the sum of two squares...

Let's try some examples.

- 5 can be written as the sum of two squares in 8 ways:

$$(\pm 1)^2 + (\pm 2)^2 \text{ and } (\pm 2)^2 + (\pm 1)^2$$

To answer this question, we must determine the number of ways to express a number as the sum of two squares...

Let's try some examples.

- 5 can be written as the sum of two squares in 8 ways:

$$(\pm 1)^2 + (\pm 2)^2 \text{ and } (\pm 2)^2 + (\pm 1)^2$$

- 50 can be written as the sum of two squares...

To answer this question, we must determine the number of ways to express a number as the sum of two squares...

Let's try some examples.

- 5 can be written as the sum of two squares in 8 ways:

$$(\pm 1)^2 + (\pm 2)^2 \text{ and } (\pm 2)^2 + (\pm 1)^2$$

- 50 can be written as the sum of two squares in 12 ways:

$$(\pm 1)^2 + (\pm 7)^2; (\pm 7)^2 + (\pm 1)^2; \text{ and } (\pm 5)^2 + (\pm 5)^2.$$

To answer this question, we must determine the number of ways to express a number as the sum of two squares...

Let's try some examples.

- 5 can be written as the sum of two squares in 8 ways:

$$(\pm 1)^2 + (\pm 2)^2 \text{ and } (\pm 2)^2 + (\pm 1)^2$$

- 50 can be written as the sum of two squares in 12 ways:

$$(\pm 1)^2 + (\pm 7)^2; (\pm 7)^2 + (\pm 1)^2; \text{ and } (\pm 5)^2 + (\pm 5)^2.$$

- 11 can be written as the sum of two squares...

To answer this question, we must determine the number of ways to express a number as the sum of two squares...

Let's try some examples.

- 5 can be written as the sum of two squares in 8 ways:

$$(\pm 1)^2 + (\pm 2)^2 \text{ and } (\pm 2)^2 + (\pm 1)^2$$

- 50 can be written as the sum of two squares in 12 ways:

$$(\pm 1)^2 + (\pm 7)^2; (\pm 7)^2 + (\pm 1)^2; \text{ and } (\pm 5)^2 + (\pm 5)^2.$$

- 11 can be written as the sum of two squares in 0 ways:

$$9 + 4 > 11; 9 + 1 < 11; \text{ and } 4 + 4 < 11$$

To answer this question, we must determine the number of ways to express a number as the sum of two squares...

Let's try some examples.

- 5 can be written as the sum of two squares in 8 ways:

$$(\pm 1)^2 + (\pm 2)^2 \text{ and } (\pm 2)^2 + (\pm 1)^2$$

- 50 can be written as the sum of two squares in 12 ways:

$$(\pm 1)^2 + (\pm 7)^2; (\pm 7)^2 + (\pm 1)^2; \text{ and } (\pm 5)^2 + (\pm 5)^2.$$

- 11 can be written as the sum of two squares in 0 ways:

$$9 + 4 > 11; 9 + 1 < 11; \text{ and } 4 + 4 < 11$$

- 11234567800004 can be written as the sum of two squares...

To answer this question, we must determine the number of ways to express a number as the sum of two squares...

Let's try some examples.

- 5 can be written as the sum of two squares in 8 ways:

$$(\pm 1)^2 + (\pm 2)^2 \text{ and } (\pm 2^2) + (\pm 1)^2$$

- 50 can be written as the sum of two squares in 12 ways:

$$(\pm 1)^2 + (\pm 7)^2; (\pm 7) + (\pm 1)^2; \text{ and } (\pm 5)^2 + (\pm 5)^2.$$

- 11 can be written as the sum of two squares in 0 ways:

$$9 + 4 > 11; 9 + 1 < 11; \text{ and } 4 + 4 < 11$$

- 11234567800004 can be written as the sum of two squares in 32 ways:

$$\begin{aligned} &(\pm 3337550)^2 + (\pm 308752)^2; (\pm 3274510)^2 + (\pm 715648)^2; \\ &(\pm 2799602)^2 + (\pm 1843040)^2; \text{ and } (\pm 2552498)^2 + (\pm 2172400)^2, \\ &\text{as well as their reverses.} \end{aligned}$$

To answer this question, we must determine the number of ways to express a number as the sum of two squares...

Let's try some examples.

- 5 can be written as the sum of two squares in 8 ways:

$$(\pm 1)^2 + (\pm 2)^2 \text{ and } (\pm 2)^2 + (\pm 1)^2$$

- 50 can be written as the sum of two squares in 12 ways:

$$(\pm 1)^2 + (\pm 7)^2; (\pm 7)^2 + (\pm 1)^2; \text{ and } (\pm 5)^2 + (\pm 5)^2.$$

- 11 can be written as the sum of two squares in 0 ways:

$$9 + 4 > 11; 9 + 1 < 11; \text{ and } 4 + 4 < 11$$

- 11234567800004 can be written as the sum of two squares in 32 ways:

$$\begin{aligned} &(\pm 3337550)^2 + (\pm 308752)^2; (\pm 3274510)^2 + (\pm 715648)^2; \\ &(\pm 2799602)^2 + (\pm 1843040)^2; \text{ and } (\pm 2552498)^2 + (\pm 2172400)^2, \\ &\text{as well as their reverses.} \end{aligned}$$

- 11234567800001 can be written as the sum of two squares...

To answer this question, we must determine the number of ways to express a number as the sum of two squares...

Let's try some examples.

- 5 can be written as the sum of two squares in 8 ways:

$$(\pm 1)^2 + (\pm 2)^2 \text{ and } (\pm 2)^2 + (\pm 1)^2$$

- 50 can be written as the sum of two squares in 12 ways:

$$(\pm 1)^2 + (\pm 7)^2; (\pm 7)^2 + (\pm 1)^2; \text{ and } (\pm 5)^2 + (\pm 5)^2.$$

- 11 can be written as the sum of two squares in 0 ways:

$$9 + 4 > 11; 9 + 1 < 11; \text{ and } 4 + 4 < 11$$

- 11234567800004 can be written as the sum of two squares in 32 ways:

$$\begin{aligned} &(\pm 3337550)^2 + (\pm 308752)^2; (\pm 3274510)^2 + (\pm 715648)^2; \\ &(\pm 2799602)^2 + (\pm 1843040)^2; \text{ and } (\pm 2552498)^2 + (\pm 2172400)^2, \\ &\text{as well as their reverses.} \end{aligned}$$

- 112345678000001 can be written as the sum of two squares in 0 ways:

What's going on?

Four is a magic number

It turns out that looking at squares modulo 4 reveals a lot

Lemma

Any number that is 3 mod 4 cannot be written as the sum of two squares.

- $n^2 = 0 \text{ or } 1 \pmod{4}$

Four is a magic number

It turns out that looking at squares modulo 4 reveals a lot

Lemma

Any number that is 3 mod 4 cannot be written as the sum of two squares.

- $n^2 = 0$ or $1 \pmod{4}$
- What about 21?
- Or $11234567800001 = 7 \cdot 13 \cdot 123456789011$?

The Diophantus-Brahmagupta-Fibonacci-Kertzer Identity

The Diophantus-Brahmagupta-Fibonacci-Kertzer Identity

Lemma

Let $n, m \in \mathbb{N}$. If n and m are the sum of two squares, we have that mn is a sum of two squares as well.

$$\begin{aligned} mn &= (a^2 + b^2)(c^2 + d)^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2 \\ &= (ac + bd)^2 + (ad - bc)^2 \end{aligned}$$

The Diophantus-Brahmagupta-Fibonacci-Kertzer Identity

Lemma

Let $n, m \in \mathbb{N}$. If n and m are the sum of two squares, we have that mn is a sum of two squares as well.

$$\begin{aligned} mn &= (a^2 + b^2)(c^2 + d^2) \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2 \\ &= (ac + bd)^2 + (ad - bc)^2 \end{aligned}$$

- Is the converse true?
- What if we're dealing with a prime, which can't be split up into two smaller factors?

Prime Time

Let's see which primes can be written as the sum of two squares.

Prime Time

Let's see which primes can be written as the sum of two squares.

- 2 can be, as $1^2 + 1^2 = 2$.

Prime Time

Let's see which primes can be written as the sum of two squares.

- 2 can be, as $1^2 + 1^2 = 2$.
- Primes that are 3 modulo 4 can't be, as shown previously.

Prime Time

Let's see which primes can be written as the sum of two squares.

- 2 can be, as $1^2 + 1^2 = 2$.
- Primes that are 3 modulo 4 can't be, as shown previously.
- What about primes that are 1 modulo 4?

Prime Time

Let's see which primes can be written as the sum of two squares.

- 2 can be, as $1^2 + 1^2 = 2$.
- Primes that are 3 modulo 4 can't be, as shown previously.
- What about primes that are 1 modulo 4?

$$5 = 2^2 + 1^2 \quad 37 = 6^2 + 1^2 \quad 73 = 8^2 + 3^2$$

$$13 = 3^2 + 2^2 \quad 41 = 5^2 + 4^2 \quad 89 = 8^2 + 5^2$$

$$17 = 4^2 + 1^2 \quad 53 = 7^2 + 2^2 \quad 97 = 9^2 + 4^2$$

$$29 = 5^2 + 2^2 \quad 61 = 6^2 + 5^2 \quad 101 = 10^2 + 1^2$$

Prime Time

Let's see which primes can be written as the sum of two squares.

- 2 can be, as $1^2 + 1^2 = 2$.
- Primes that are 3 modulo 4 can't be, as shown previously.
- What about primes that are 1 modulo 4?

$$5 = 2^2 + 1^2 \quad 37 = 6^2 + 1^2 \quad 73 = 8^2 + 3^2$$

$$13 = 3^2 + 2^2 \quad 41 = 5^2 + 4^2 \quad 89 = 8^2 + 5^2$$

$$17 = 4^2 + 1^2 \quad 53 = 7^2 + 2^2 \quad 97 = 9^2 + 4^2$$

$$29 = 5^2 + 2^2 \quad 61 = 6^2 + 5^2 \quad 101 = 10^2 + 1^2$$

Anderson's Heuristic

Because all the 1 mod 4 primes under 100 are representable as the sum of two squares, all primes that are 1 mod 4 are representable as the sum of two squares.

The Real Proof

It turns out that all primes that are 1 modulo 4 actually can be represented as the sum of two squares.

Theorem

Let $p \in \mathbb{N}$ be an odd prime. Then p can be represented as the sum of two squares if and only if $p \equiv 1 \pmod{4}$.

There are two main parts to the proof:

Lemma

Let $p \in \mathbb{N}$ be an odd prime. Then -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{4}$.

Lemma

Let $p \in \mathbb{N}$ be an odd prime. Then p can be represented as the sum of two squares if and only if -1 is a quadratic residue modulo p .

Big Theorem!

Theorem

A natural k can be expressed as the sum of two squares if and only if

$$k = 2^\ell \prod_{q \equiv 3 \pmod{4}} q^2 \prod_{p \equiv 1 \pmod{4}} p,$$

where $\ell \in \mathbb{Z}_{\geq 0}$.

Big Theorem!

Theorem

A natural k can be expressed as the sum of two squares if and only if

$$k = 2^\ell \prod_{q \equiv 3 \pmod{4}} q^2 \prod_{p \equiv 1 \pmod{4}} p,$$

where $\ell \in \mathbb{Z}_{\geq 0}$.

Proof.

Big Theorem!

Theorem

A natural k can be expressed as the sum of two squares if and only if

$$k = 2^\ell \prod_{q \equiv 3 \pmod{4}} q^2 \prod_{p \equiv 1 \pmod{4}} p,$$

where $\ell \in \mathbb{Z}_{\geq 0}$.

Proof. ($\Rightarrow$), all numbers that are products of p , q^2 , and 2 should work.

Big Theorem!

Theorem

A natural k can be expressed as the sum of two squares if and only if

$$k = 2^\ell \prod_{q \equiv 3 \pmod{4}} q^2 \prod_{p \equiv 1 \pmod{4}} p,$$

where $\ell \in \mathbb{Z}_{\geq 0}$.

Proof. ($\Rightarrow$), all numbers that are products of p , q^2 , and 2 should work.

If an odd prime $r \mid \gcd(a, b)$, then $r^2 \mid a^2 + b^2$.

Big Theorem!

Theorem

A natural k can be expressed as the sum of two squares if and only if

$$k = 2^\ell \prod_{q \equiv 3 \pmod{4}} q^2 \prod_{p \equiv 1 \pmod{4}} p,$$

where $\ell \in \mathbb{Z}_{\geq 0}$.

Proof. ($\Rightarrow$), all numbers that are products of p , q^2 , and 2 should work.

If an odd prime $r \mid \gcd(a, b)$, then $r^2 \mid a^2 + b^2$.

If $r \nmid a, r \nmid b$, $a^2 \equiv -b^2 \pmod{r} \implies (ab^{-1})^2 \equiv -1 \pmod{r}$. Then $\text{ord}_r(ab^{-1}) = 4$, so $4 \mid r - 1 \implies r \equiv 1 \pmod{4}$

Let's test this

Can $86632 = 2^3 \cdot 7^2 \cdot 13 \cdot 17$ be written as $a^2 + b^2$?

Let's test this

Can $86632 = 2^3 \cdot 7^2 \cdot 13 \cdot 17$ be written as $a^2 + b^2$? Yes! Because of 7^2 .

Let's test this

Can $86632 = 2^3 \cdot 7^2 \cdot 13 \cdot 17$ be written as $a^2 + b^2$? Yes! Because of 7^2 .

$$(\pm 14)^2 + (\pm 292)^2, \quad (\pm 126)^2 + (\pm 266)^2,$$

and permutations.

Let's test this

Can $86632 = 2^3 \cdot 7^2 \cdot 13 \cdot 17$ be written as $a^2 + b^2$? Yes! Because of 7^2 .

$$(\pm 14)^2 + (\pm 292)^2, \quad (\pm 126)^2 + (\pm 266)^2,$$

and permutations.

Can $2987104 = 2^5 \cdot 17^3 \cdot 19$ be written?

Let's test this

Can $86632 = 2^3 \cdot 7^2 \cdot 13 \cdot 17$ be written as $a^2 + b^2$? Yes! Because of 7^2 .

$$(\pm 14)^2 + (\pm 292)^2, \quad (\pm 126)^2 + (\pm 266)^2,$$

and permutations.

Can $2987104 = 2^5 \cdot 17^3 \cdot 19$ be written? No. Because 19^1 .

Theorem

The number of ordered pairs $(a, b) \in \mathbb{Z}$ that satisfy $a^2 + b^2 = k$, if

$$k = 2^\ell \prod_{q \equiv 3 \pmod{4}} q^2 \prod_{p \equiv 1 \pmod{4}} p,$$

where $\ell \in \mathbb{Z}_{\geq 0}$, is $4\tau(m)$, where m is the $1 \pmod{4}$ part.

Theorem

The number of ordered pairs $(a, b) \in \mathbb{Z}$ that satisfy $a^2 + b^2 = k$, if

$$k = 2^\ell \prod_{q \equiv 3 \pmod{4}} q^2 \prod_{p \equiv 1 \pmod{4}} p,$$

where $\ell \in \mathbb{Z}_{\geq 0}$, is $4\tau(m)$, where m is the $1 \pmod{4}$ part.

- Go into complex numbers: need solutions to $N(\alpha) = k$.

Theorem

The number of ordered pairs $(a, b) \in \mathbb{Z}$ that satisfy $a^2 + b^2 = k$, if

$$k = 2^\ell \prod_{q \equiv 3 \pmod{4}} q^2 \prod_{p \equiv 1 \pmod{4}} p,$$

where $\ell \in \mathbb{Z}_{\geq 0}$, is $4\tau(m)$, where m is the $1 \pmod{4}$ part.

- Go into complex numbers: need solutions to $N(\alpha) = k$.
- Factorize k into Norms of prime factors of α .

Theorem

The number of ordered pairs $(a, b) \in \mathbb{Z}$ that satisfy $a^2 + b^2 = k$, if

$$k = 2^\ell \prod_{q \equiv 3 \pmod{4}} q^2 \prod_{p \equiv 1 \pmod{4}} p,$$

where $\ell \in \mathbb{Z}_{\geq 0}$, is $4\tau(m)$, where m is the $1 \pmod{4}$ part.

- Go into complex numbers: need solutions to $N(\alpha) = k$.
- Factorize k into Norms of prime factors of α .
- For the Norms that are 2 or consist of $q \equiv 3 \pmod{4}$ primes, you can choose the prime factors of α one way.

Theorem

The number of ordered pairs $(a, b) \in \mathbb{Z}$ that satisfy $a^2 + b^2 = k$, if

$$k = 2^\ell \prod_{q \equiv 3 \pmod{4}} q^2 \prod_{p \equiv 1 \pmod{4}} p,$$

where $\ell \in \mathbb{Z}_{\geq 0}$, is $4\tau(m)$, where m is the $1 \pmod{4}$ part.

- Go into complex numbers: need solutions to $N(\alpha) = k$.
- Factorize k into Norms of prime factors of α .
- For the Norms that are 2 or consist of $q \equiv 3 \pmod{4}$ primes, you can choose the prime factors of α one way.
- For the $1 \pmod{4}$ part, there are $\tau(m)$ ways.

Theorem

The number of ordered pairs $(a, b) \in \mathbb{Z}$ that satisfy $a^2 + b^2 = k$, if

$$k = 2^\ell \prod_{q \equiv 3 \pmod{4}} q^2 \prod_{p \equiv 1 \pmod{4}} p,$$

where $\ell \in \mathbb{Z}_{\geq 0}$, is $4\tau(m)$, where m is the $1 \pmod{4}$ part.

- Go into complex numbers: need solutions to $N(\alpha) = k$.
- Factorize k into Norms of prime factors of α .
- For the Norms that are 2 or consist of $q \equiv 3 \pmod{4}$ primes, you can choose the prime factors of α one way.
- For the $1 \pmod{4}$ part, there are $\tau(m)$ ways.
- But we may multiply α by units! So $4\tau(m)$.

Testing

How many ways can $100 = 2^2 \cdot 5^2$ be written as $a^2 + b^2$?

How many ways can $100 = 2^2 \cdot 5^2$ be written as $a^2 + b^2$? $4 \cdot \tau(100) = 12$.

$$(\pm 10)^2 + 0^2, \quad (\pm 6)^2 + (\pm 8)^2,$$

and permutations.

How many ways can $100 = 2^2 \cdot 5^2$ be written as $a^2 + b^2$? $4 \cdot \tau(100) = 12$.

$$(\pm 10)^2 + 0^2, \quad (\pm 6)^2 + (\pm 8)^2,$$

and permutations.

How many ways can $930852 = 2^2 \cdot 3^4 \cdot 13^2 \cdot 17$ be written as $a^2 + b^2$?

Testing

How many ways can $100 = 2^2 \cdot 5^2$ be written as $a^2 + b^2$? $4 \cdot \tau(100) = 12$.

$$(\pm 10)^2 + 0^2, \quad (\pm 6)^2 + (\pm 8)^2,$$

and permutations.

How many ways can $930852 = 2^2 \cdot 3^4 \cdot 13^2 \cdot 17$ be written as $a^2 + b^2$? $4 \cdot \tau(13^2 \cdot 17) = 24$.

$$(\pm 954)^2 + (\pm 144)^2, \quad (\pm 936)^2 + (\pm 234)^2,$$

$$(\pm 774)^2 + (\pm 576)^2,$$

and permutations.

Million Dollar question!

Million Dollar question!

Can you write 6 as sum of three square numbers?

Million Dollar question!

Can you write 6 as sum of three square numbers?

You got it. It's $2^2 + 1^2 + 1^2$.

Million Dollar question!

Can you write 6 as sum of three square numbers?

You got it. It's $2^2 + 1^2 + 1^2$.

Now what about 7?

Million Dollar question!

Can you write 6 as sum of three square numbers?

You got it. It's $2^2 + 1^2 + 1^2$.

Now what about 7?

Yeap, you can't write 7 as sum of three square numbers.

Why?

Lemma

Every integer n with $n \equiv 7 \pmod{8}$ cannot be written as a sum of three integer squares, i.e. there do not exist integers x, y, z such that $n = x^2 + y^2 + z^2$.

Residues are: $r \in \{0, 1, 2, 3, 4, -3, -2, -1\}$, and $x^2 \equiv (-x)^2$, so only consider $x \in \{0, 1, 2, 3, 4\}$.

Why?

Lemma

Every integer n with $n \equiv 7 \pmod{8}$ cannot be written as a sum of three integer squares, i.e. there do not exist integers x, y, z such that $n = x^2 + y^2 + z^2$.

Residues are: $r \in \{0, 1, 2, 3, 4, -3, -2, -1\}$, and $x^2 \equiv (-x)^2$, so only consider $x \in \{0, 1, 2, 3, 4\}$. Their squares mod 8 are:

$$(8k)^2 = 64k^2 \equiv 0 \pmod{8}$$

$$(8k + 1)^2 = 64k^2 + 16k + 1 \equiv 1 \pmod{8}$$

$$(8k + 2)^2 = 64k^2 + 32k + 4 \equiv 4 \pmod{8}$$

$$(8k + 3)^2 = 64k^2 + 48k + 9 \equiv 1 \pmod{8}$$

$$(8k + 4)^2 = 64k^2 + 64k + 16 \equiv 0 \pmod{8}$$

Why?

Lemma

Every integer n with $n \equiv 7 \pmod{8}$ cannot be written as a sum of three integer squares, i.e. there do not exist integers x, y, z such that $n = x^2 + y^2 + z^2$.

Residues are: $r \in \{0, 1, 2, 3, 4, -3, -2, -1\}$, and $x^2 \equiv (-x)^2$, so only consider $x \in \{0, 1, 2, 3, 4\}$. Their squares mod 8 are:

$$(8k)^2 = 64k^2 \equiv 0 \pmod{8}$$

$$(8k + 1)^2 = 64k^2 + 16k + 1 \equiv 1 \pmod{8}$$

$$(8k + 2)^2 = 64k^2 + 32k + 4 \equiv 4 \pmod{8}$$

$$(8k + 3)^2 = 64k^2 + 48k + 9 \equiv 1 \pmod{8}$$

$$(8k + 4)^2 = 64k^2 + 64k + 16 \equiv 0 \pmod{8}$$

So for any integer a , we have:

$$a^2 \equiv 0, 1, 4 \pmod{8}.$$

Can you find any combination of three numbers from the set 0, 1, 4 whose sum is congruent to 7 modulo 8?

Can you find any combination of three numbers from the set 0, 1, 4 whose sum is congruent to 7 modulo 8?

I know you can't.

That's why 7 cannot be written as sum of three square numbers.

Confusing stuffs!

LET'S DO SOME NUMERICALS!

Confusing stuffs!

LET'S DO SOME NUMERICALS!

What is 28 in mod 8?

Confusing stuffs!

LET'S DO SOME NUMERICALS!

What is 28 in mod 8?

YEAH, It's 4 mod 8

Confusing stuffs!

LET'S DO SOME NUMERICALS!

What is 28 in mod 8?

YEAH, It's 4 mod 8

Can you write 28 as sum of three square numbers?

Confusing stuffs!

LET'S DO SOME NUMERICALS!

What is 28 in mod 8?

YEAH, It's 4 mod 8

Can you write 28 as sum of three square numbers?

No, we can't but it's not 7 in mod 8.

What the hell!

What about 112 in mod 8

What the hell!

What about 112 in mod 8

It's 0 in mod 8

What the hell!

What about 112 in mod 8

It's 0 in mod 8

Can you write it sum of three square numbers?

What the hell!

What about 112 in mod 8

It's 0 in mod 8

Can you write it sum of three square numbers?

And we can't write 112 as sum of three square numbers also!!

Let's do some numericals

Numbers that are impossible to write as sum of three square numbers		
7	28	112
15	60	240
23	92	368
31	124	496
39	156	624
⋮	⋮	⋮

Factorization of these interesting numbers!

Numbers that are impossible to write as sum of three square numbers		
7	$28 = 4 \cdot 7$	$112 = 4^2 \cdot 7$
15	$60 = 4 \cdot 15$	$240 = 4^2 \cdot 15$
23	$92 = 4 \cdot 23$	$368 = 4^2 \cdot 23$
31	$124 = 4 \cdot 31$	$496 = 4^2 \cdot 31$
39	$156 = 4 \cdot 39$	$624 = 4^2 \cdot 39$
$\vdots$	$\vdots$	$\vdots$

Interesting!

Numbers that are impossible to write as sum of three square numbers		
$n = 8k + 7$	$n = 4^1 \cdot (8k + 7)$	$n = 4^2 \cdot (8k + 7)$

Interesting!

Numbers that are impossible to write as sum of three square numbers		
$n = 8k + 7$	$n = 4^1 \cdot (8k + 7)$	$n = 4^2 \cdot (8k + 7)$
7	$28 = 4 \cdot 7$	$112 = 4^2 \cdot 7$
15	$60 = 4 \cdot 15$	$240 = 4^2 \cdot 15$
23	$92 = 4 \cdot 23$	$368 = 4^2 \cdot 23$
31	$124 = 4 \cdot 31$	$496 = 4^2 \cdot 31$
39	$156 = 4 \cdot 39$	$624 = 4^2 \cdot 39$
$\vdots$	$\vdots$	$\vdots$

Swastika's Theorem

Theorem (Swastika's Theorem)

Let $n = 4^a(8k + 7)$ be a positive integer, where $a, k \in \mathbb{Z}_{\geq 0}$. Then n cannot be written as the sum of three squares; that is, there do not exist integers x, y, z such that

$$n = x^2 + y^2 + z^2.$$

- (Induction). Base case $a = 0$:

When $a = 0$, we have $n = 8k + 7$, which contradicts our previous lemma

Swastika's Theorem

Theorem (Swastika's Theorem)

Let $n = 4^a(8k + 7)$ be a positive integer, where $a, k \in \mathbb{Z}_{\geq 0}$. Then n cannot be written as the sum of three squares; that is, there do not exist integers x, y, z such that

$$n = x^2 + y^2 + z^2.$$

- (Induction). Base case $a = 0$:
When $a = 0$, we have $n = 8k + 7$, which contradicts our previous lemma
- (Induction Hypothesis) For all $a \geq 1$, no integer of the form $4^a(8k + 7)$ can be written as the sum of three squares.

Swastika's Theorem

Theorem (Swastika's Theorem)

Let $n = 4^a(8k + 7)$ be a positive integer, where $a, k \in \mathbb{Z}_{\geq 0}$. Then n cannot be written as the sum of three squares; that is, there do not exist integers x, y, z such that

$$n = x^2 + y^2 + z^2.$$

- (Induction). Base case $a = 0$:
When $a = 0$, we have $n = 8k + 7$, which contradicts our previous lemma
- (Induction Hypothesis) For all $a \geq 1$, no integer of the form $4^a(8k + 7)$ can be written as the sum of three squares.
- If $x^2 + y^2 + z^2$ is divisible by 4, then x, y, z are all even.

Swastika's Theorem

Theorem (Swastika's Theorem)

Let $n = 4^a(8k + 7)$ be a positive integer, where $a, k \in \mathbb{Z}_{\geq 0}$. Then n cannot be written as the sum of three squares; that is, there do not exist integers x, y, z such that

$$n = x^2 + y^2 + z^2.$$

- (Induction). Base case $a = 0$:
When $a = 0$, we have $n = 8k + 7$, which contradicts our previous lemma
- (Induction Hypothesis) For all $a \geq 1$, no integer of the form $4^a(8k + 7)$ can be written as the sum of three squares.
- If $x^2 + y^2 + z^2$ is divisible by 4, then x, y, z are all even.
- (Inductive step) Write $x = 2x_0, y = 2y_0, z = 2z_0$. SFTSOC, Substituting, we obtain

$$4^{a+1}(8k + 7) = 4(x_0^2 + y_0^2 + z_0^2),$$

Swastika's Theorem

Theorem (Swastika's Theorem)

Let $n = 4^a(8k + 7)$ be a positive integer, where $a, k \in \mathbb{Z}_{\geq 0}$. Then n cannot be written as the sum of three squares; that is, there do not exist integers x, y, z such that

$$n = x^2 + y^2 + z^2.$$

- (Induction). Base case $a = 0$:
When $a = 0$, we have $n = 8k + 7$, which contradicts our previous lemma
- (Induction Hypothesis) For all $a \geq 1$, no integer of the form $4^a(8k + 7)$ can be written as the sum of three squares.
- If $x^2 + y^2 + z^2$ is divisible by 4, then x, y, z are all even.
- (Inductive step) Write $x = 2x_0, y = 2y_0, z = 2z_0$. SFTSOC, Substituting, we obtain

$$4^{a+1}(8k + 7) = 4(x_0^2 + y_0^2 + z_0^2),$$

and dividing through by 4 gives

$$4^a(8k + 7) = x_0^2 + y_0^2 + z_0^2$$

which contradicts our induction hypothesis.

Four really is a magic number

It turns out that three squares are not enough to write every number. How about four?

Four really is a magic number

It turns out that three squares are not enough to write every number. How about four?

Theorem

Every natural number can be written as the sum of four squares.

Four really is a magic number

It turns out that three squares are not enough to write every number. How about four?

Theorem

Every natural number can be written as the sum of four squares.

Proof.

I have discovered a truly marvelous truth of this theorem, but the margins of this slideshow and the length of the time I have are too small to properly explain it. □

Wait but I don't like squares... How about triangles?

Wait but I don't like squares... How about triangles?

Triangular numbers



1

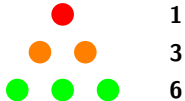
Wait but I don't like squares... How about triangles?

Triangular numbers



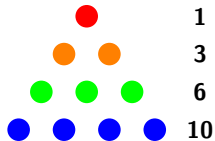
Wait but I don't like squares... How about triangles?

Triangular numbers

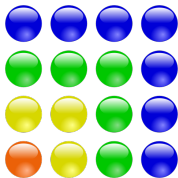


Wait but I don't like squares... How about triangles?

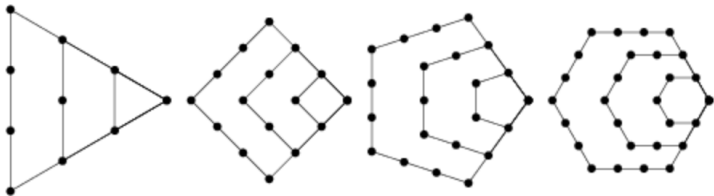
Triangular numbers



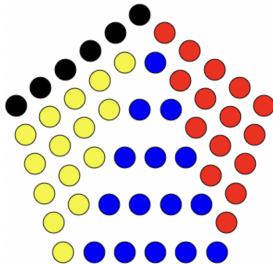
4-gons and 4-gonal numbers



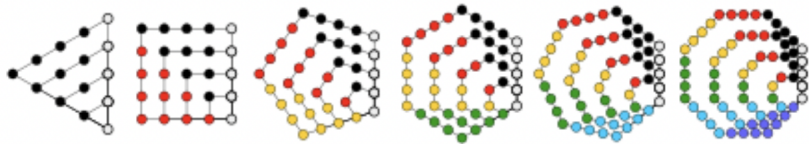
r -gons and r -gonal numbers



$(n-1)$ th r -gonal number to n th r -gonal number



(n-1)th r-gonal number to nth r-gonal number



$$f(n, r) = f(n - 1, r) + (1 + (n - 1)(r - 2))$$

What is the nth r-gonal number?

$$\begin{aligned}f(n, r) &= f(n-1, r) + (1 + (n-1)(r-2)) \\&= f(r, 0) + \sum_{k=0}^{n-1} (1 + k(r-2)) \\&= 0 + \sum_{k=0}^{n-1} (1 + k(r-2)) \\&= \frac{n(1 + (1 + (n-1)(r-2)))}{2} \\&= \frac{n(2 + (n-1)(r-2))}{2}\end{aligned}$$

What numbers could be expressed as a sum of r-gonal numbers?

Can a number be both r_1 -gonal and r_2 -gonal?

Thank you :)))

Happy Birthday Clyde!!!

