Sums of squares

Nashville Math Club

September 22, 2020

Squares of integers

Question

How many numbers are perfect squares?

Squares of integers

Question

How many numbers are perfect squares?

- Of course, there are infinitely many: $1, 4, 9, 16, 25, 36, \ldots$.

Squares of integers

Question

How many numbers are perfect squares?

- Of course, there are infinitely many: $1, 4, 9, 16, 25, 36, \ldots$.

Question

But how **common** *are they?*

Squares of integers

Question

How many numbers are perfect squares?

- Of course, there are infinitely many: $1, 4, 9, 16, 25, 36, \ldots$.

Question

But how **common** *are they?*

- Look at the whole numbers from 1 to X. about $\sqrt{X}$ of them are perfect squares.

Squares of integers

Question

How many numbers are perfect squares?

- Of course, there are infinitely many: $1, 4, 9, 16, 25, 36, \ldots$.

Question

But how **common** *are they?*

- Look at the whole numbers from 1 to X. about $\sqrt{X}$ of them are perfect squares.
- So about $\frac{\sqrt{X}}{X} = \frac{1}{\sqrt{X}}$ are.

Squares of integers

Question

How many numbers are perfect squares?

- Of course, there are infinitely many: $1, 4, 9, 16, 25, 36, \ldots$.

Question

But how **common** *are they?*

- Look at the whole numbers from 1 to X. about $\sqrt{X}$ of them are perfect squares.
- So about $\frac{\sqrt{X}}{X} = \frac{1}{\sqrt{X}}$ are.
- So up to a million, about 0.1% are, up to a trillion, about 1 in a million are.

Squares of integers

Question

How many numbers are perfect squares?

- Of course, there are infinitely many: $1, 4, 9, 16, 25, 36, \ldots$.

Question

But how **common** *are they?*

- Look at the whole numbers from 1 to X. about $\sqrt{X}$ of them are perfect squares.
- So about $\frac{\sqrt{X}}{X} = \frac{1}{\sqrt{X}}$ are.
- So up to a million, about 0.1% are, up to a trillion, about 1 in a million are. So 0% of numbers are perfect squares.

Sums of squares

- The question gets more interesting if we ask about sums of squares.

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$.

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 to 10 are sums of two squares?

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 to 10 are sums of two squares?

- $1 = 1^2 + 0^2$,

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 to 10 are sums of two squares?

- $1 = 1^2 + 0^2$,$2 = 1^2 + 1^2$,

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 to 10 are sums of two squares?

- $1 = 1^2 + 0^2$,$2 = 1^2 + 1^2$, $\cancel{3}$,

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 to 10 are sums of two squares?

- $1 = 1^2 + 0^2$,$2 = 1^2 + 1^2$, $\cancel{3}$, $4 = 2^2 + 0^2$,

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 to 10 are sums of two squares?

- $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$, $\cancel{3}$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$,

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 to 10 are sums of two squares?

- $1 = 1^2 + 0^2$,$2 = 1^2 + 1^2$, $\cancel{3}$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $\cancel{6}$,

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 to 10 are sums of two squares?

- $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$, $\cancel{3}$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $\cancel{6}$, $\cancel{7}$,

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 to 10 are sums of two squares?

- $1 = 1^2 + 0^2$,$2 = 1^2 + 1^2$, $\cancel{3}$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $\cancel{6}$, $\cancel{7}$, $8 = 2^2 + 2^2$,

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 to 10 are sums of two squares?

- $1 = 1^2 + 0^2$,$2 = 1^2 + 1^2$, $\cancel{3}$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $\cancel{6}$, $\cancel{7}$, $8 = 2^2 + 2^2$, $9 = 3^2 + 0^2$,

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 to 10 are sums of two squares?

- $1 = 1^2 + 0^2$,$2 = 1^2 + 1^2$, $\cancel{3}$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $\cancel{6}$, $\cancel{7}$, $8 = 2^2 + 2^2$, $9 = 3^2 + 0^2$, $10 = 3^2 + 1^2$.

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 *to* 10 *are sums of two squares?*

- $1 = 1^2 + 0^2$,$2 = 1^2 + 1^2$, $\cancel{3}$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $\cancel{6}$, $\cancel{7}$, $8 = 2^2 + 2^2$, $9 = 3^2 + 0^2$, $10 = 3^2 + 1^2$.
- So 70% of them are.

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 to 10 are sums of two squares?

- $1 = 1^2 + 0^2$,$2 = 1^2 + 1^2$, $\cancel{3}$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $\cancel{6}$, $\cancel{7}$, $8 = 2^2 + 2^2$, $9 = 3^2 + 0^2$, $10 = 3^2 + 1^2$.
- So 70% of them are. What is special about the numbers $3, 6, 7$?

Sums of squares

- The question gets more interesting if we ask about sums of squares.
- 20 is a sum of two squares as $20 = 2^2 + 4^2$. So is $16 = 4^2 + 0^2$.

Question

Which numbers from 1 to 10 are sums of two squares?

- $1 = 1^2 + 0^2$,$2 = 1^2 + 1^2$, $\cancel{3}$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $\cancel{6}$, $\cancel{7}$, $8 = 2^2 + 2^2$, $9 = 3^2 + 0^2$, $10 = 3^2 + 1^2$.
- So 70% of them are. What is special about the numbers $3, 6, 7$? How can you test?

Basic Facts

- Look at the first squares $1, 4, 9, 16, 25, \ldots$ and divide by 4 with remainder. What do you notice?

Basic Facts

- Look at the first squares $1, 4, 9, 16, 25, \ldots$ and divide by 4 with remainder. What do you notice?
- If we look **modulo** 4, the remainders are $1, 0, 1, 0, 1, \ldots$. So squares look like they're 0 or 1 mod 4.

Basic Facts

- Look at the first squares $1, 4, 9, 16, 25, \ldots$ and divide by 4 with remainder. What do you notice?
- If we look **modulo** 4, the remainders are $1, 0, 1, 0, 1, \ldots$. So squares look like they're 0 or 1 mod 4. Can you explain this?

Basic Facts

- Look at the first squares $1, 4, 9, 16, 25, \ldots$ and divide by 4 with remainder. What do you notice?
- If we look **modulo** 4, the remainders are $1, 0, 1, 0, 1, \ldots$. So squares look like they're 0 or 1 mod 4. Can you explain this?
- Explanation: Every number is even or odd. So its of the form $x = 2n$ or $x = 2n + 1$.

Basic Facts

- Look at the first squares $1, 4, 9, 16, 25, \ldots$ and divide by 4 with remainder. What do you notice?
- If we look **modulo** 4, the remainders are $1, 0, 1, 0, 1, \ldots$. So squares look like they're 0 or 1 mod 4. Can you explain this?
- Explanation: Every number is even or odd. So its of the form $x = 2n$ or $x = 2n + 1$.
- Now $(2n)^2 = 4n^2$ is a multiple of 4, and $(2n + 1)^2 = 4(n^2 + n) + 1$ is a multiple of 4 plus 1.

Basic Facts

- Look at the first squares $1, 4, 9, 16, 25, \ldots$ and divide by 4 with remainder. What do you notice?
- If we look **modulo** 4, the remainders are $1, 0, 1, 0, 1, \ldots$. So squares look like they're 0 or 1 mod 4. Can you explain this?
- Explanation: Every number is even or odd. So its of the form $x = 2n$ or $x = 2n + 1$.
- Now $(2n)^2 = 4n^2$ is a multiple of 4, and $(2n + 1)^2 = 4(n^2 + n) + 1$ is a multiple of 4 plus 1.
- What about a sum of two squares?

Basic Facts

- Look at the first squares $1, 4, 9, 16, 25, \ldots$ and divide by 4 with remainder. What do you notice?
- If we look **modulo** 4, the remainders are $1, 0, 1, 0, 1, \ldots$. So squares look like they're 0 or 1 mod 4. Can you explain this?
- Explanation: Every number is even or odd. So its of the form $x = 2n$ or $x = 2n + 1$.
- Now $(2n)^2 = 4n^2$ is a multiple of 4, and $(2n + 1)^2 = 4(n^2 + n) + 1$ is a multiple of 4 plus 1.
- What about a sum of two squares? (0 or 1) plus (0 or 1) equals $0, 1, 2$.

Basic Facts

- Look at the first squares $1, 4, 9, 16, 25, \ldots$ and divide by 4 with remainder. What do you notice?
- If we look **modulo** 4, the remainders are $1, 0, 1, 0, 1, \ldots$. So squares look like they're 0 or 1 mod 4. Can you explain this?
- Explanation: Every number is even or odd. So its of the form $x = 2n$ or $x = 2n + 1$.
- Now $(2n)^2 = 4n^2$ is a multiple of 4, and $(2n + 1)^2 = 4(n^2 + n) + 1$ is a multiple of 4 plus 1.
- What about a sum of two squares? (0 or 1) plus (0 or 1) equals $0, 1, 2$.
- So a number that's $4n + 3$ (its 3 mod 4) can **never** be a sum of two squares.

Basic Facts

- Look at the first squares $1, 4, 9, 16, 25, \ldots$ and divide by 4 with remainder. What do you notice?
- If we look **modulo** 4, the remainders are $1, 0, 1, 0, 1, \ldots$. So squares look like they're 0 or 1 mod 4. Can you explain this?
- Explanation: Every number is even or odd. So its of the form $x = 2n$ or $x = 2n + 1$.
- Now $(2n)^2 = 4n^2$ is a multiple of 4, and $(2n + 1)^2 = 4(n^2 + n) + 1$ is a multiple of 4 plus 1.
- What about a sum of two squares? (0 or 1) plus (0 or 1) equals $0, 1, 2$.
- So a number that's $4n + 3$ (its 3 mod 4) can **never** be a sum of two squares.
- This explains 3 and 7. What about 6? The answer has to do with **prime factorizations**.

A Crazy Formula

- A product of sums of two squares is a sum of two squares.

A Crazy Formula

- A product of sums of two squares is a sum of two squares.

Fact (Brahmagupta–Fibonacci identity)

We have

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

A Crazy Formula

- A product of sums of two squares is a sum of two squares.

Fact (Brahmagupta–Fibonacci identity)

We have

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

- Its just algebra!

A Crazy Formula

- A product of sums of two squares is a sum of two squares.

Fact (Brahmagupta–Fibonacci identity)

We have

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

- Its just algebra! But its the first hint of a long story... and new identities have been made famous by Fields Medalist Manjul Bhargava.

A Crazy Formula

- A product of sums of two squares is a sum of two squares.

Fact (Brahmagupta–Fibonacci identity)

We have

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2.$$

- Its just algebra! But its the first hint of a long story... and new identities have been made famous by Fields Medalist Manjul Bhargava. Its even related to black holes!

A Crazy Formula

- A product of sums of two squares is a sum of two squares.

Fact (Brahmagupta–Fibonacci identity)

We have

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

- Its just algebra! But its the first hint of a long story... and new identities have been made famous by Fields Medalist Manjul Bhargava. Its even related to black holes!
- Example: $8 = 2^2 + 2^2$, $10 = 3^2 + 1^2$, so $80 = (6 - 2)^2 + (2 + 6)^2 = 16 + 64$ is a sum of two squares.

A Crazy Formula

- A product of sums of two squares is a sum of two squares.

Fact (Brahmagupta–Fibonacci identity)

We have

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

- Its just algebra! But its the first hint of a long story... and new identities have been made famous by Fields Medalist Manjul Bhargava. Its even related to black holes!
- Example: $8 = 2^2 + 2^2$, $10 = 3^2 + 1^2$, so $80 = (6 - 2)^2 + (2 + 6)^2 = 16 + 64$ is a sum of two squares.
- Natural first step: which **prime numbers** are $\square + \square$?

The key result

- Fermat, the prince of amateur mathematicians, proved:

The key result

- Fermat, the prince of amateur mathematicians, proved:

Theorem (Fermat's Two Squares Theorem)

A prime $p > 2$ is a sum of two squares if and only if p is 1 mod 4.

The key result

- Fermat, the prince of amateur mathematicians, proved:

Theorem (Fermat's Two Squares Theorem)

A prime $p > 2$ is a sum of two squares if and only if p is $1 \bmod 4$.

- $p = 2 = 1^2 + 1^2$; all other primes are 1 or 3 mod 4.

The key result

- Fermat, the prince of amateur mathematicians, proved:

Theorem (Fermat's Two Squares Theorem)

A prime $p > 2$ is a sum of two squares if and only if p is $1 \bmod 4$.

- $p = 2 = 1^2 + 1^2$; all other primes are 1 or 3 mod 4.
- If something is 3 mod 4, then its not a sum of two squares.

The key result

- Fermat, the prince of amateur mathematicians, proved:

Theorem (Fermat's Two Squares Theorem)

A prime $p > 2$ is a sum of two squares if and only if p is 1 mod 4.

- $p = 2 = 1^2 + 1^2$; all other primes are 1 or 3 mod 4.
- If something is 3 mod 4, then its not a sum of two squares.
- So we just have to show primes of the form $4n + 1$ are.

The key result

- Fermat, the prince of amateur mathematicians, proved:

Theorem (Fermat's Two Squares Theorem)

A prime $p > 2$ is a sum of two squares if and only if p is 1 mod 4.

- $p = 2 = 1^2 + 1^2$; all other primes are 1 or 3 mod 4.
- If something is 3 mod 4, then its not a sum of two squares.
- So we just have to show primes of the form $4n + 1$ are.
- Any ideas about how to do this?

World record

- Shockingly short (but not easy!) proof:

World record

- Shockingly short (but not easy!) proof:

A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares

D. Zagier
Department of Mathematics, University of Maryland, College Park, MD 20742

The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

$$(x,y,z) \mapsto \begin{cases} (x + 2z,\ z,\ y - x - z) & \text{if } x < y - z \\ (2y - x,\ y,\ x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y,\ x - y + z,\ y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \mapsto (x, z, y)$ also has a fixed point. $\square$

World record

- Shockingly short (but not easy!) proof:

A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares

D. ZAGIER
Department of Mathematics, University of Maryland, College Park, MD 20742

The involution on the finite set $S = \{(x,y,z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

$$(x,y,z) \mapsto \begin{cases} (x+2z,\ z,\ y-x-z) & \text{if } x < y-z \\ (2y-x,\ y,\ x-y+z) & \text{if } y-z < x < 2y \\ (x-2y,\ x-y+z,\ y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x,y,z) \mapsto (x,z,y)$ also has a fixed point. $\square$

- We will try to discover our own proof.

Moving to algebra

- Mantra: Always use algebra when you can.

Moving to algebra

- Mantra: Always use algebra when you can.
- We want to solve $n = x^2 + y^2$.

Moving to algebra

- Mantra: Always use algebra when you can.
- We want to solve $n = x^2 + y^2$.
- Main algebra trick: Factor!

Moving to algebra

- Mantra: Always use algebra when you can.
- We want to solve $n = x^2 + y^2$.
- Main algebra trick: Factor!
- If instead we wanted to study **differences** of two squares, we'd have $n = x^2 - y^2 = (x+y)(x-y)$.

Moving to algebra

- Mantra: Always use algebra when you can.
- We want to solve $n = x^2 + y^2$.
- Main algebra trick: Factor!
- If instead we wanted to study **differences** of two squares, we'd have $n = x^2 - y^2 = (x+y)(x-y)$.
- For example, any odd number $2n+1$ is a difference of two squares.

Moving to algebra

- Mantra: Always use algebra when you can.
- We want to solve $n = x^2 + y^2$.
- Main algebra trick: Factor!
- If instead we wanted to study **differences** of two squares, we'd have $n = x^2 - y^2 = (x + y)(x - y)$.
- For example, any odd number $2n + 1$ is a difference of two squares. Solve $x + y = 2n + 1$, $x - y = 1$ to get $x = n + 1$, $y = n$.

Moving to algebra

- Mantra: Always use algebra when you can.
- We want to solve $n = x^2 + y^2$.
- Main algebra trick: Factor!
- If instead we wanted to study **differences** of two squares, we'd have $n = x^2 - y^2 = (x + y)(x - y)$.
- For example, any odd number $2n + 1$ is a difference of two squares. Solve $x + y = 2n + 1$, $x - y = 1$ to get $x = n + 1$, $y = n$. Thus, $2n + 1 = (x + y)(x - y) = (n + 1)^2 - n^2$.

Moving to algebra

- Mantra: Always use algebra when you can.
- We want to solve $n = x^2 + y^2$.
- Main algebra trick: Factor!
- If instead we wanted to study **differences** of two squares, we'd have $n = x^2 - y^2 = (x+y)(x-y)$.
- For example, any odd number $2n+1$ is a difference of two squares. Solve $x + y = 2n + 1$, $x - y = 1$ to get $x = n + 1$, $y = n$. Thus, $2n + 1 = (x+y)(x-y) = (n+1)^2 - n^2$.
- This doesn't seem to work for us. We need a **bigger number system**.

Complex Numbers

- You may have seen the **imaginary unit** i defined by $i^2 = -1$.

Complex Numbers

- You may have seen the **imaginary unit** i defined by $i^2 = -1$.
- This allows us to solve quadratic equations.

Complex Numbers

- You may have seen the **imaginary unit** i defined by $i^2 = -1$.
- This allows us to solve quadratic equations. But we can say something much better:

Complex Numbers

- You may have seen the **imaginary unit** i defined by $i^2 = -1$.
- This allows us to solve quadratic equations. But we can say something much better:
- A **complex number** is a number $x + iy$ where x, y are real numbers.

Complex Numbers

- You may have seen the **imaginary unit** i defined by $i^2 = -1$.
- This allows us to solve quadratic equations. But we can say something much better:
- A **complex number** is a number $x + iy$ where x, y are real numbers.

Theorem (The Fundamental Theorem of Algebra)

Every polynomial factors into degree one factors if you allow complex numbers.

Complex Numbers

- You may have seen the **imaginary unit** i defined by $i^2 = -1$.
- This allows us to solve quadratic equations. But we can say something much better:
- A **complex number** is a number $x + iy$ where x, y are real numbers.

Theorem (The Fundamental Theorem of Algebra)

Every polynomial factors into degree one factors if you allow complex numbers.

- This is completely crazy! You throw in one extra number to solve quadratic equations, and suddenly you can solve polynomials of **any** degree.

Complex Numbers

- You may have seen the **imaginary unit** i defined by $i^2 = -1$.
- This allows us to solve quadratic equations. But we can say something much better:
- A **complex number** is a number $x + iy$ where x, y are real numbers.

Theorem (The Fundamental Theorem of Algebra)

Every polynomial factors into degree one factors if you allow complex numbers.

- This is completely crazy! You throw in one extra number to solve quadratic equations, and suddenly you can solve polynomials of **any** degree.
- Really great article giving pictures to explain this: "The Fundamental Theorem of Algebra for Artists".

Practicing with complex numbers

- Try computing some complex numbers yourself! Do the following:

Practicing with complex numbers

- Try computing some complex numbers yourself! Do the following:
- Compute $(3 + 5i) - (7 - 2i)$.

Practicing with complex numbers

- Try computing some complex numbers yourself! Do the following:
- Compute $(3 + 5i) - (7 - 2i)$. Answer: Add **real and imaginary parts**: $(3 - 7) + (5 + 2)i = -4 + 7i$.

Practicing with complex numbers

- Try computing some complex numbers yourself! Do the following:
- Compute $(3+5i)-(7-2i)$. Answer: Add **real and imaginary parts**: $(3-7)+(5+2)i = -4+7i$.
- What is $(3+5i)(7-2i)$?

Practicing with complex numbers

- Try computing some complex numbers yourself! Do the following:
- Compute $(3+5i)-(7-2i)$. Answer: Add **real and imaginary parts**: $(3-7)+(5+2)i=-4+7i$.
- What is $(3+5i)(7-2i)$? Answer: Expand out $(3+5i)(7-2i)=21+35i-6i-10i^2=(21+10)+29i=31+29i$.

Practicing with complex numbers

- Try computing some complex numbers yourself! Do the following:
- Compute $(3+5i)-(7-2i)$. Answer: Add **real and imaginary parts**: $(3-7)+(5+2)i = -4+7i$.
- What is $(3+5i)(7-2i)$? Answer: Expand out $(3+5i)(7-2i) = 21+35i-6i-10i^2 = (21+10)+29i = 31+29i$.
- What about i^3?

Practicing with complex numbers

- Try computing some complex numbers yourself! Do the following:
- Compute $(3+5i)-(7-2i)$. Answer: Add **real and imaginary parts**: $(3-7)+(5+2)i = -4+7i$.
- What is $(3+5i)(7-2i)$? Answer: Expand out $(3+5i)(7-2i) = 21+35i-6i-10i^2 = (21+10)+29i = 31+29i$.
- What about i^3? Answer: $i^3 = i^2 \cdot i = -i$.

Practicing with complex numbers

- Try computing some complex numbers yourself! Do the following:
- Compute $(3+5i)-(7-2i)$. Answer: Add **real and imaginary parts**: $(3-7)+(5+2)i = -4+7i$.
- What is $(3+5i)(7-2i)$? Answer: Expand out $(3+5i)(7-2i) = 21+35i-6i-10i^2 = (21+10)+29i = 31+29i$.
- What about i^3? Answer: $i^3 = i^2 \cdot i = -i$.
- What is $\frac{3+5i}{7-2i}$?

Practicing with complex numbers

- Try computing some complex numbers yourself! Do the following:
- Compute $(3+5i)-(7-2i)$. Answer: Add **real and imaginary parts**: $(3-7)+(5+2)i=-4+7i$.
- What is $(3+5i)(7-2i)$? Answer: Expand out $(3+5i)(7-2i)=21+35i-6i-10i^2=(21+10)+29i=31+29i$.
- What about i^3? Answer: $i^3=i^2\cdot i=-i$.
- What is $\frac{3+5i}{7-2i}$? Answer: Trick: Multiply top and bottom by the **conjugate** $7+2i$ to get a difference of squares

Practicing with complex numbers

- Try computing some complex numbers yourself! Do the following:
- Compute $(3+5i)-(7-2i)$. Answer: Add **real and imaginary parts**: $(3-7)+(5+2)i=-4+7i$.
- What is $(3+5i)(7-2i)$? Answer: Expand out $(3+5i)(7-2i)=21+35i-6i-10i^2=(21+10)+29i=31+29i$.
- What about i^3? Answer: $i^3=i^2\cdot i=-i$.
- What is $\frac{3+5i}{7-2i}$? Answer: Trick: Multiply top and bottom by the **conjugate** $7+2i$ to get a difference of squares

$$\frac{3+5i}{7-2i}=\frac{(3+5i)(7+2i)}{(7-2i)(7+2i)}=\frac{21+35i+6i+10i^2}{49-4i^2}=\frac{11+41i}{53}$$

$$=\frac{11}{53}+\frac{41}{53}i.$$

Complex numbers for our problem

- For us: $p = (x^2 + y^2)$ factors as $p = (x + iy)(x - iy)$.

Complex numbers for our problem

- For us: $p = (x^2 + y^2)$ factors as $p = (x + iy)(x - iy)$.
- For example: $5 = 2^2 + 1^2 = (2 + i)(2 - i)$.

Complex numbers for our problem

- For us: $p = (x^2 + y^2)$ factors as $p = (x + iy)(x - iy)$.
- For example: $5 = 2^2 + 1^2 = (2 + i)(2 - i)$.
- Prime numbers are numbers that can't be split up into products of smaller numbers (except for 1 and p).

Complex numbers for our problem

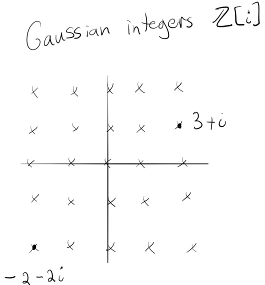
- For us: $p = (x^2 + y^2)$ factors as $p = (x + iy)(x - iy)$.
- For example: $5 = 2^2 + 1^2 = (2 + i)(2 - i)$.
- Prime numbers are numbers that can't be split up into products of smaller numbers (except for 1 and p).
- What we are asking: Do primes split up or not over the set of **Gaussian integers** $\mathbb{Z}[i] = \{x + iy \mid x, y \text{ are integers}\}$.

Complex numbers for our problem

- For us: $p = (x^2 + y^2)$ factors as $p = (x + iy)(x - iy)$.
- For example: $5 = 2^2 + 1^2 = (2 + i)(2 - i)$.
- Prime numbers are numbers that can't be split up into products of smaller numbers (except for 1 and p).
- What we are asking: Do primes split up or not over the set of **Gaussian integers** $\mathbb{Z}[i] = \{x + iy \mid x, y \text{ are integers}\}$.
- These form a **lattice**: they are the points (x, y) with whole number coordinates: (note: the point $3 + i$ should say $2 + i$)

Complex numbers for our problem

- For us: $p = (x^2 + y^2)$ factors as $p = (x + iy)(x - iy)$.
- For example: $5 = 2^2 + 1^2 = (2 + i)(2 - i)$.
- Prime numbers are numbers that can't be split up into products of smaller numbers (except for 1 and p).
- What we are asking: Do primes split up or not over the set of **Gaussian integers** $\mathbb{Z}[i] = \{x + iy \mid x, y \text{ are integers}\}$.
- These form a **lattice**: they are the points (x, y) with whole number coordinates: (note: the point $3 + i$ should say $2 + i$)



Properties of $\mathbb{Z}[i]$

- Gaussian integers have a lot of similar properties to the number system of ordinary integers $\mathbb{Z}$.

Properties of $\mathbb{Z}[i]$

- Gaussian integers have a lot of similar properties to the number system of ordinary integers $\mathbb{Z}$.
- You can add, subtract, and multiply, them.

Properties of $\mathbb{Z}[i]$

- Gaussian integers have a lot of similar properties to the number system of ordinary integers $\mathbb{Z}$.
- You can add, subtract, and multiply, them.
- There are **prime numbers** here. What should a prime be?

Properties of $\mathbb{Z}[i]$

- Gaussian integers have a lot of similar properties to the number system of ordinary integers $\mathbb{Z}$.
- You can add, subtract, and multiply, them.
- There are **prime numbers** here. What should a prime be? p in $\mathbb{Z}$ is prime if $p = ab$ with a, b in $\mathbb{Z}$ means a or b is ± 1.

Properties of $\mathbb{Z}[i]$

- Gaussian integers have a lot of similar properties to the number system of ordinary integers $\mathbb{Z}$.
- You can add, subtract, and multiply, them.
- There are **prime numbers** here. What should a prime be? p in $\mathbb{Z}$ is prime if $p = ab$ with a, b in $\mathbb{Z}$ means a or b is ± 1.
- What is special about ± 1?

Properties of $\mathbb{Z}[i]$

- Gaussian integers have a lot of similar properties to the number system of ordinary integers $\mathbb{Z}$.
- You can add, subtract, and multiply, them.
- There are **prime numbers** here. What should a prime be? p in $\mathbb{Z}$ is prime if $p = ab$ with a, b in $\mathbb{Z}$ means a or b is ± 1.
- What is special about ± 1? Answer: They are the only integers a with $1/a$ still an integer; you can solve $ab = 1$ in $\mathbb{Z}$.

Properties of $\mathbb{Z}[i]$

- Gaussian integers have a lot of similar properties to the number system of ordinary integers $\mathbb{Z}$.
- You can add, subtract, and multiply, them.
- There are **prime numbers** here. What should a prime be? p in $\mathbb{Z}$ is prime if $p = ab$ with a, b in $\mathbb{Z}$ means a or b is ± 1.
- What is special about ± 1? Answer: They are the only integers a with $1/a$ still an integer; you can solve $ab = 1$ in $\mathbb{Z}$. These are called **units**.

Properties of $\mathbb{Z}[i]$

- Gaussian integers have a lot of similar properties to the number system of ordinary integers $\mathbb{Z}$.
- You can add, subtract, and multiply, them.
- There are **prime numbers** here. What should a prime be? p in $\mathbb{Z}$ is prime if $p = ab$ with a, b in $\mathbb{Z}$ means a or b is ± 1.
- What is special about ± 1? Answer: They are the only integers a with $1/a$ still an integer; you can solve $ab = 1$ in $\mathbb{Z}$. These are called **units**.
- What are the units in $\mathbb{Z}[i]$?

A special function

- The size of an integer is $|a|$. If you multiply integers together, they usually get bigger (except when you multiply by 0 or ± 1).

A special function

- The size of an integer is $|a|$. If you multiply integers together, they usually get bigger (except when you multiply by 0 or ± 1).
- The units are **exactly** the integers with $|a| = 1$.

A special function

- The size of an integer is $|a|$. If you multiply integers together, they usually get bigger (except when you multiply by 0 or ± 1).
- The units are **exactly** the integers with $|a| = 1$.
- The **norm** of a Gaussian integer is $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$.

A special function

- The size of an integer is $|a|$. If you multiply integers together, they usually get bigger (except when you multiply by 0 or ± 1).
- The units are **exactly** the integers with $|a| = 1$.
- The **norm** of a Gaussian integer is $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$. So $N(2 + i) = 2^2 + 1^2 = 5$.

A special function

- The size of an integer is $|a|$. If you multiply integers together, they usually get bigger (except when you multiply by 0 or ± 1).
- The units are **exactly** the integers with $|a| = 1$.
- The **norm** of a Gaussian integer is $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$. So $N(2 + i) = 2^2 + 1^2 = 5$.
- Why is this useful? Its **multiplicative**: $N(xy) = N(x)N(y)$. Check this in the next few minutes.

A special function

- The size of an integer is $|a|$. If you multiply integers together, they usually get bigger (except when you multiply by 0 or ± 1).
- The units are **exactly** the integers with $|a| = 1$.
- The **norm** of a Gaussian integer is $N(a+bi) = (a+bi)(a-bi) = a^2 + b^2$. So $N(2+i) = 2^2 + 1^2 = 5$.
- Why is this useful? Its **multiplicative**: $N(xy) = N(x)N(y)$. Check this in the next few minutes.
- Ok, let's check: Its the secret behind our strange identity!

$$N((a+bi)(c+di)) = N((ac-bd) + (ad+bc)i)$$

$$= (ac-bd)^2 + (ad+bc)^2$$

$$= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 = (a^2+b^2)(c^2+d^2) = N(a+bi)N(c+di).$$

Using norms to discover units

- Since we can divide with complex numbers, we are asking: for which x is there a y with $xy = 1$.

Using norms to discover units

- Since we can divide with complex numbers, we are asking: for which x is there a y with $xy = 1$. Thus, $N(x)N(y) = 1$.

Using norms to discover units

- Since we can divide with complex numbers, we are asking: for which x is there a y with $xy = 1$. Thus, $N(x)N(y) = 1$.
- But the only units in $\mathbb{Z}$ are ± 1!

Using norms to discover units

- Since we can divide with complex numbers, we are asking: for which x is there a y with $xy = 1$. Thus, $N(x)N(y) = 1$.
- But the only units in $\mathbb{Z}$ are ± 1! So we have to have $N(x) = 1$.

Using norms to discover units

- Since we can divide with complex numbers, we are asking: for which x is there a y with $xy = 1$. Thus, $N(x)N(y) = 1$.
- But the only units in $\mathbb{Z}$ are ± 1! So we have to have $N(x) = 1$. What numbers satisfy this?

Using norms to discover units

- Since we can divide with complex numbers, we are asking: for which x is there a y with $xy = 1$. Thus, $N(x)N(y) = 1$.
- But the only units in $\mathbb{Z}$ are ± 1! So we have to have $N(x) = 1$. What numbers satisfy this?
- If $a^2 + b^2 = 1$, we have a, b are $0, \pm 1$.

Using norms to discover units

- Since we can divide with complex numbers, we are asking: for which x is there a y with $xy = 1$. Thus, $N(x)N(y) = 1$.
- But the only units in $\mathbb{Z}$ are ± 1! So we have to have $N(x) = 1$. What numbers satisfy this?
- If $a^2 + b^2 = 1$, we have a, b are $0, \pm 1$. Only possibilities: $\pm 1, \pm i$. That's it!

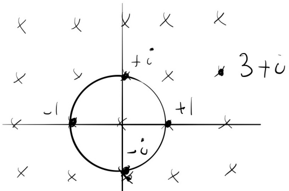
Using norms to discover units

- Since we can divide with complex numbers, we are asking: for which x is there a y with $xy = 1$. Thus, $N(x)N(y) = 1$.
- But the only units in $\mathbb{Z}$ are ± 1! So we have to have $N(x) = 1$. What numbers satisfy this?
- If $a^2 + b^2 = 1$, we have a, b are $0, \pm 1$. Only possibilities: $\pm 1, \pm i$. That's it!
- These are the Gaussian integers on the **unit circle** (note: the point $3 + i$ should say $2 + i$)

Using norms to discover units

- Since we can divide with complex numbers, we are asking: for which x is there a y with $xy = 1$. Thus, $N(x)N(y) = 1$.
- But the only units in $\mathbb{Z}$ are ± 1! So we have to have $N(x) = 1$. What numbers satisfy this?
- If $a^2 + b^2 = 1$, we have a, b are $0, \pm 1$. Only possibilities: $\pm 1, \pm i$. That's it!
- These are the Gaussian integers on the **unit circle** (note: the point $3 + i$ should say $2 + i$)

Gaussian integer units



Primes in $\mathbb{Z}[i]$

- We can finally define primes.

Primes in $\mathbb{Z}[i]$

- We can finally define primes. A **prime Gaussian integer** is a number x such that if $x = ab$, then one of a or b is $\pm 1, \pm i$.

Primes in $\mathbb{Z}[i]$

- We can finally define primes. A **prime Gaussian integer** is a number x such that if $x = ab$, then one of a or b is $\pm 1, \pm i$.

Theorem (Fundamental Theorem of Arithmetic)

Every Gaussian integer factors **uniquely** *as a product of primes.*

Primes in $\mathbb{Z}[i]$

- We can finally define primes. A **prime Gaussian integer** is a number x such that if $x = ab$, then one of a or b is $\pm 1, \pm i$.

Theorem (Fundamental Theorem of Arithmetic)

Every Gaussian integer factors **uniquely** *as a product of primes.*

- The main reason: You can do long division: Given a, b, solve $a = bq + r$ with $0 \leq N(r) < N(b)$.

Primes in $\mathbb{Z}[i]$

- We can finally define primes. A **prime Gaussian integer** is a number x such that if $x = ab$, then one of a or b is $\pm 1, \pm i$.

Theorem (Fundamental Theorem of Arithmetic)

Every Gaussian integer factors **uniquely** *as a product of primes.*

- The main reason: You can do long division: Given a, b, solve $a = bq + r$ with $0 \leq N(r) < N(b)$. Why: solve $\frac{a}{b} = q + \frac{r}{b}$ with $N(\frac{r}{b}) < 1$.

Primes in $\mathbb{Z}[i]$

- We can finally define primes. A **prime Gaussian integer** is a number x such that if $x = ab$, then one of a or b is $\pm 1, \pm i$.

Theorem (Fundamental Theorem of Arithmetic)

Every Gaussian integer factors **uniquely** *as a product of primes.*

- The main reason: You can do long division: Given a, b, solve $a = bq + r$ with $0 \leq N(r) < N(b)$. Why: solve $\frac{a}{b} = q + \frac{r}{b}$ with $N(\frac{r}{b}) < 1$.
- But lattice you are always at distance less than 1 from a lattice point! Maximal distance is diagonal of square: $\sqrt{2}/2 < 1$.

Primes in $\mathbb{Z}[i]$

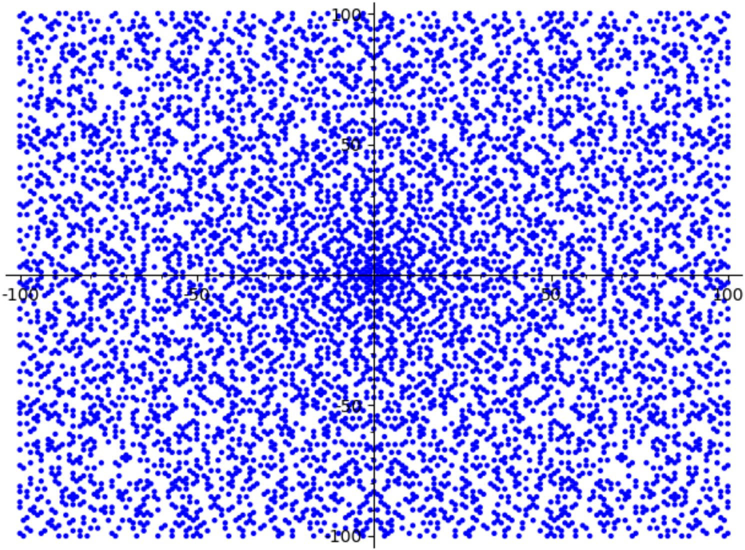
- We can finally define primes. A **prime Gaussian integer** is a number x such that if $x = ab$, then one of a or b is $\pm 1, \pm i$.

Theorem (Fundamental Theorem of Arithmetic)

Every Gaussian integer factors **uniquely** *as a product of primes.*

- The main reason: You can do long division: Given a, b, solve $a = bq + r$ with $0 \leq N(r) < N(b)$. Why: solve $\frac{a}{b} = q + \frac{r}{b}$ with $N(\frac{r}{b}) < 1$.
- But lattice you are always at distance less than 1 from a lattice point! Maximal distance is diagonal of square: $\sqrt{2}/2 < 1$.
- This is extremely special! For example, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ means that the theorem is false for $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

A picture of the Gaussian primes



Final basic facts

Theorem (Wilson's Theorem)

If p is a prime integer, then $(p-1)! \equiv -1 \pmod{p}$.

Final basic facts

Theorem (Wilson's Theorem)

If p is a prime integer, then $(p-1)! \equiv -1 \pmod{p}$.

if $ab \equiv 1 \pmod{p}$

$p = 13$ $\quad (p-1)! = 12!$

$= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12$

$\equiv 1 \cdot (1)^5 \cdot (-1) \equiv -1 \pmod{13}$

Final basic facts

Theorem (Wilson's Theorem)

If p is a prime integer, then $(p-1)! \equiv -1 \pmod{p}$.

$p = 13 \qquad (p-1)! = 12!$

$a \qquad b \qquad$ if $ab \equiv 1 \pmod{p}$

$= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12$

$\equiv 1 \cdot (1)^5 \cdot (-1) \equiv -1 \pmod{13}$

Lemma (Lagrange)

If p is prime of the form $4n+1$, then $-1 \equiv m^2 \pmod{p}$ for an m.

Final basic facts

Theorem (Wilson's Theorem)

If p is a prime integer, then $(p-1)! \equiv -1 \pmod{p}$.

if $ab \equiv 1 \pmod{p}$

$p = 13$ $\quad (p-1)! = 12!$

$= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12$

$\equiv 1 \cdot (1)^5 \cdot (-1) \equiv -1 \pmod{13}$

Lemma (Lagrange)

If p is prime of the form $4n+1$, then $-1 \equiv m^2 \pmod{p}$ for an m.

$$-1 \equiv 12! \equiv (1\cdot 12)(2\cdot 11)(3\cdot 10)\ldots(6\cdot 7) \equiv (-1)^6(6!)^2 \equiv (6!)^2 \pmod{13}$$

Finally, our proof!

- Claim: If $p \equiv 1 \pmod 4$, then $p = x^2 + y^2$ is solvable.

Finally, our proof!

- Claim: If $p \equiv 1 \pmod 4$, then $p = x^2 + y^2$ is solvable.
- Pick the m with $p | (m^2 + 1)$ by Lagrange.

Finally, our proof!

- Claim: If $p \equiv 1 \pmod 4$, then $p = x^2 + y^2$ is solvable.
- Pick the m with $p | (m^2 + 1)$ by Lagrange.
- Factor $m^2 + 1 = (m + i)(m - i)$.

Finally, our proof!

- Claim: If $p \equiv 1 \pmod 4$, then $p = x^2 + y^2$ is solvable.
- Pick the m with $p|(m^2+1)$ by Lagrange.
- Factor $m^2 + 1 = (m+i)(m-i)$.
- As $m/p \pm i/p$ is not a Gaussian integer, p doesn't divide $m+i$ or $m-i$.

Finally, our proof!

- Claim: If $p \equiv 1 \pmod 4$, then $p = x^2 + y^2$ is solvable.
- Pick the m with $p|(m^2 + 1)$ by Lagrange.
- Factor $m^2 + 1 = (m + i)(m - i)$.
- As $m/p \pm i/p$ is not a Gaussian integer, p doesn't divide $m + i$ or $m - i$.
- So p divides a product of two numbers, but neither of those two numbers by themselves! This implies that p is a **Gaussian prime** (the same is true for integer primes).

Finally, our proof!

- Claim: If $p \equiv 1 \pmod 4$, then $p = x^2 + y^2$ is solvable.
- Pick the m with $p | (m^2 + 1)$ by Lagrange.
- Factor $m^2 + 1 = (m + i)(m - i)$.
- As $m/p \pm i/p$ is not a Gaussian integer, p doesn't divide $m + i$ or $m - i$.
- So p divides a product of two numbers, but neither of those two numbers by themselves! This implies that p is a **Gaussian prime** (the same is true for integer primes).
- Thus, p has a non-trivial factorization

$$p = (a + bi)(c + di).$$

Finally, our proof!

- Claim: If $p \equiv 1 \pmod 4$, then $p = x^2 + y^2$ is solvable.
- Pick the m with $p | (m^2 + 1)$ by Lagrange.
- Factor $m^2 + 1 = (m + i)(m - i)$.
- As $m/p \pm i/p$ is not a Gaussian integer, p doesn't divide $m + i$ or $m - i$.
- So p divides a product of two numbers, but neither of those two numbers by themselves! This implies that p is a **Gaussian prime** (the same is true for integer primes).
- Thus, p has a non-trivial factorization

$$p = (a + bi)(c + di).$$

- Take norms:

Finally, our proof!

- Claim: If $p \equiv 1 \pmod 4$, then $p = x^2 + y^2$ is solvable.
- Pick the m with $p|(m^2+1)$ by Lagrange.
- Factor $m^2 + 1 = (m+i)(m-i)$.
- As $m/p \pm i/p$ is not a Gaussian integer, p doesn't divide $m+i$ or $m-i$.
- So p divides a product of two numbers, but neither of those two numbers by themselves! This implies that p is a **Gaussian prime** (the same is true for integer primes).
- Thus, p has a non-trivial factorization

$$p = (a+bi)(c+di).$$

- Take norms:

$$N(p) = p^2 = (a^2+b^2)(c^2+d^2).$$

Wrapping up

Wrapping up

- So $a^2 + b^2 = p = c^2 + d^2$!

Wrapping up

- So $a^2 + b^2 = p = c^2 + d^2$!
- For example, $13 | ((6!)^2 + 1) = (720 + i)(720 - i)$.

Wrapping up

- So $a^2 + b^2 = p = c^2 + d^2$!
- For example, $13 | ((6!)^2 + 1) = (720 + i)(720 - i)$.
- 13 splits up as $13 = (3 + 2i)(3 - 2i)$. So $13^2 = 3^2 + 2^2$.

Any numbers

- What about non-prime numbers?

Any numbers

- What about non-prime numbers? By combining what we learned, you can show:

Any numbers

- What about non-prime numbers? By combining what we learned, you can show:

Theorem

An integer $n > 1$ is a sum of two squares if and only if the exponents of any prime that's $3 \pmod 4$ in the prime factorization of n is **even** *(note: zero is an even number).*

Any numbers

- What about non-prime numbers? By combining what we learned, you can show:

Theorem

An integer $n > 1$ is a sum of two squares if and only if the exponents of any prime that's $3 \pmod 4$ in the prime factorization of n is **even** *(note: zero is an even number).*

Example

$5096 = 2^3 \cdot 13^1 \cdot 7^2$ is a sum of two squares (14^2 and 70^2), but $35672 = 2^3 \cdot 13^1 \cdot 7^3$ is **not**.

Final thoughts

- What about sums of three squares? Four squares? A famous theorem of Lagrange says **every** number is a sum of 4 squares.

Final thoughts

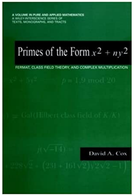
- What about sums of three squares? Four squares? A famous theorem of Lagrange says **every** number is a sum of 4 squares.
- How many ways can you write a number as a sum of two squares?

Final thoughts

- What about sums of three squares? Four squares? A famous theorem of Lagrange says **every** number is a sum of 4 squares.
- How many ways can you write a number as a sum of two squares?
- How many primes of the form $x^2 + ny^2$ are there?

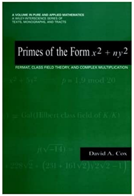
Final thoughts

- What about sums of three squares? Four squares? A famous theorem of Lagrange says **every** number is a sum of 4 squares.
- How many ways can you write a number as a sum of two squares?
- How many primes of the form $x^2 + ny^2$ are there?



Final thoughts

- What about sums of three squares? Four squares? A famous theorem of Lagrange says **every** number is a sum of 4 squares.
- How many ways can you write a number as a sum of two squares?
- How many primes of the form $x^2 + ny^2$ are there?



- What other questions can you think of?