Introduction to Number Theory Chapter 6 Sums of squares

Robert C. Vaughan

February 18, 2025

1	0^2+1^2	$0^2+0^2+0^2+1^2$	13	2^2+3^2	$0^2+0^2+2^2+$
2	1^2+1^2	$0^2+0^2+1^2+1^2$	17	1^2+4^2	$0^2+0^2+1^2+$
3		$0^2+1^2+1^2+1^2$	19		$1^2+1^2+1^2+$
4	0^2+2^2	$0^2+0^2+0^2+2^2$	23		$1^2+2^2+3^2+$
5	1^2+2^2	$0^2+0^2+1^2+2^2$	29	2^2+5^2	$0^2+0^2+2^2+$
6		$0^2+1^2+1^2+2^2$	31		$1^2+1^2+2^2+$
7		$1^2+1^2+1^2+2^2$	37	1^2+6^2	$1^2+1^2+1^2+$
8	2^2+2^2	$0^2+0^2+2^2+2^2$	41	4^2+5^2	$0^2+0^2+4^2+$
9	0^2+3^2	$0^2+1^2+2^2+2^2$	43		$1^2+1^2+4^2+$
10	1^2+3^2	$0^2+0^2+1^2+3^2$	47		$1^2+1^2+3^2+$
11		$0^2+1^2+1^2+3^2$	53	2^2+7^2	$0^2+0^2+2^2+$
12		$1^2+1^2+1^2+3^2$	59		$0^2+1^2+3^2+$

Sums of Two Squares

- The basic results on sums of squares depend on the theory of quadratic residues, so this chapter is a natural continuation of the previous one.

Sums of Two Squares

- The basic results on sums of squares depend on the theory of quadratic residues, so this chapter is a natural continuation of the previous one.
- Let us start by considering the solubility of $p = x^2 + y^2$ where p is an odd prime and x and y are integers.

Sums of Two Squares

- The basic results on sums of squares depend on the theory of quadratic residues, so this chapter is a natural continuation of the previous one.
- Let us start by considering the solubility of $p = x^2 + y^2$ where p is an odd prime and x and y are integers.
- If we had $p|y$, then we would have to have $p|x$, but then the right hand side would be divisible by p^2, which is obvious nonsense.

Sums of Two Squares

- The basic results on sums of squares depend on the theory of quadratic residues, so this chapter is a natural continuation of the previous one.
- Let us start by considering the solubility of $p = x^2 + y^2$ where p is an odd prime and x and y are integers.
- If we had $p|y$, then we would have to have $p|x$, but then the right hand side would be divisible by p^2, which is obvious nonsense.
- Thus we may assume that $p \nmid y$.

- If we rewrite the equation as $x^2 = p - y^2$, then we have $x^2 \equiv -y^2 \pmod{p}$.

- If we rewrite the equation as $x^2 = p - y^2$, then we have $x^2 \equiv -y^2 \pmod{p}$.
- Thus $-y^2$ has to be a QR modulo p. Hence

$$1 = \left(\frac{-y^2}{p}\right)_L = \left(\frac{-1}{p}\right)_L = (-1)^{\frac{p-1}{2}}$$

by Euler's criterion.

- If we rewrite the equation as $x^2 = p - y^2$, then we have $x^2 \equiv -y^2 \pmod{p}$.
- Thus $-y^2$ has to be a QR modulo p. Hence

$$1 = \left(\frac{-y^2}{p}\right)_L = \left(\frac{-1}{p}\right)_L = (-1)^{\frac{p-1}{2}}$$

  by Euler's criterion.
- Thus $p \equiv 1 \pmod{4}$, and we have proved one half of the following theorem.

Theorem 1 (Fermat/Girard)

An odd prime p is the sum of two squares if and only if $p \equiv 1 \pmod{4}$.

- **Theorem (Fermat/Girard).** *An odd prime p is the sum of two squares if and only if $p \equiv 1 \pmod 4$.*

- **Theorem (Fermat/Girard).** *An odd prime p is the sum of two squares if and only if $p \equiv 1 \pmod 4$.*
- It remains to prove if $p \equiv 1 \pmod 4$, then p is the sum of two squares. We give a proof due to Thue.

- **Theorem (Fermat/Girard).** *An odd prime p is the sum of two squares if and only if $p \equiv 1 \pmod 4$.*
- It remains to prove if $p \equiv 1 \pmod 4$, then p is the sum of two squares. We give a proof due to Thue.
- -1 is a QR. Choose Z so that $Z^2 \equiv -1 \pmod p$ and consider the numbers $xZ + y$ with $0 \le x < \sqrt{p}$ and $0 \le y < \sqrt{p}$ (since a prime is not a perfect square).

- **Theorem (Fermat/Girard).** *An odd prime p is the sum of two squares if and only if $p \equiv 1 \pmod 4$.*
- It remains to prove if $p \equiv 1 \pmod 4$, then p is the sum of two squares. We give a proof due to Thue.
- -1 is a QR. Choose Z so that $Z^2 \equiv -1 \pmod p$ and consider the numbers $xZ + y$ with $0 \le x < \sqrt{p}$ and $0 \le y < \sqrt{p}$ (since a prime is not a perfect square).
- There are $\left(1 + \left\lfloor \sqrt{p} \right\rfloor\right)^2 > \left(\sqrt{p}\right)^2 = p$ of them.

- **Theorem (Fermat/Girard).** *An odd prime p is the sum of two squares if and only if $p \equiv 1 \pmod 4$.*
- It remains to prove if $p \equiv 1 \pmod 4$, then p is the sum of two squares. We give a proof due to Thue.
- -1 is a QR. Choose Z so that $Z^2 \equiv -1 \pmod p$ and consider the numbers $xZ + y$ with $0 \le x < \sqrt{p}$ and $0 \le y < \sqrt{p}$ (since a prime is not a perfect square).
- There are $\left(1 + \lfloor\sqrt{p}\rfloor\right)^2 > \left(\sqrt{p}\right)^2 = p$ of them.
- Since there are more than p of them, there must be a residue class modulo p which contains at least two of them (the Dirichlet Box Principle).

- **Theorem (Fermat/Girard).** *An odd prime p is the sum of two squares if and only if $p \equiv 1 \pmod 4$.*
- It remains to prove if $p \equiv 1 \pmod 4$, then p is the sum of two squares. We give a proof due to Thue.
- -1 is a QR. Choose Z so that $Z^2 \equiv -1 \pmod p$ and consider the numbers $xZ + y$ with $0 \le x < \sqrt{p}$ and $0 \le y < \sqrt{p}$ (since a prime is not a perfect square).
- There are $\left(1 + \lfloor \sqrt{p} \rfloor\right)^2 > \left(\sqrt{p}\right)^2 = p$ of them.
- Since there are more than p of them, there must be a residue class modulo p which contains at least two of them (the Dirichlet Box Principle).
- That is, we have $x_1 Z + y_1 \equiv x_2 Z + y_2 \pmod p$, and since the pairs x_1, y_1 and x_2, y_2 are different we have $xZ + y \equiv 0 \pmod p$ with $|x| = |x_1 - x_2| < \sqrt{p}$, $|y| = |y_1 - y_2| < \sqrt{p}$ and x and y not both 0.

- **Theorem (Fermat/Girard).** *An odd prime p is the sum of two squares if and only if $p \equiv 1 \pmod 4$.*
- It remains to prove if $p \equiv 1 \pmod 4$, then p is the sum of two squares. We give a proof due to Thue.
- -1 is a QR. Choose Z so that $Z^2 \equiv -1 \pmod p$ and consider the numbers $xZ + y$ with $0 \le x < \sqrt{p}$ and $0 \le y < \sqrt{p}$ (since a prime is not a perfect square).
- There are $\left(1 + \lfloor \sqrt{p} \rfloor\right)^2 > \left(\sqrt{p}\right)^2 = p$ of them.
- Since there are more than p of them, there must be a residue class modulo p which contains at least two of them (the Dirichlet Box Principle).
- That is, we have $x_1 Z + y_1 \equiv x_2 Z + y_2 \pmod p$, and since the pairs x_1, y_1 and x_2, y_2 are different we have $xZ + y \equiv 0 \pmod p$ with $|x| = |x_1 - x_2| < \sqrt{p}$, $|y| = |y_1 - y_2| < \sqrt{p}$ and x and y not both 0.
- Now $x^2 + y^2 \equiv x^2 + (-xZ)^2 = x^2(Z^2 + 1) \equiv 0 \pmod p$. Moreover $0 < x^2 + y^2 < p + p = 2p$. Hence $x^2 + y^2 = p$.

- **Example 6.4.** *Sums of two squares have a remarkable multiplicative property. Consider the following table.*

- **Example 6.4.** *Sums of two squares have a remarkable multiplicative property. Consider the following table.*

2	1^2+1^2	26	1^2+5^2	68	2^2+8^2	100	6^2+8^2
4	0^2+2^2	29	2^2+5^2	72	6^2+6^2	104	2^2+10^2
5	1^2+2^2	34	3^2+5^2	74	5^2+7^2	106	5^2+9^2
8	2^2+2^2	40	2^2+6^2	80	4^2+8^2	116	4^2+10^2
9	0^2+3^2	45	3^2+6^2	81	0^2+9^2	117	6^2+9^2
10	1^2+3^2	50	5^2+5^2	82	1^2+9^2	122	1^2+11^2
13	2^2+3^2	52	4^2+6^2	85	2^2+9^2	125	5^2+10^2
20	2^2+4^2	58	3^2+7^2	90	3^2+9^2	128	8^2+8^2
25	0^2+5^2	65	1^2+8^2	98	7^2+7^2	130	3^2+11^2

- **Example 6.4.** *Sums of two squares have a remarkable multiplicative property. Consider the following table.*

2	1^2+1^2	26	1^2+5^2	68	2^2+8^2	100	6^2+8^2
4	0^2+2^2	29	2^2+5^2	72	6^2+6^2	104	2^2+10^2
5	1^2+2^2	34	3^2+5^2	74	5^2+7^2	106	5^2+9^2
8	2^2+2^2	40	2^2+6^2	80	4^2+8^2	116	4^2+10^2
9	0^2+3^2	45	3^2+6^2	81	0^2+9^2	117	6^2+9^2
10	1^2+3^2	50	5^2+5^2	82	1^2+9^2	122	1^2+11^2
13	2^2+3^2	52	4^2+6^2	85	2^2+9^2	125	5^2+10^2
20	2^2+4^2	58	3^2+7^2	90	3^2+9^2	128	8^2+8^2
25	0^2+5^2	65	1^2+8^2	98	7^2+7^2	130	3^2+11^2

- This looks as though, if a number n has a factorisation ab with both a and b being sums of two squares, then n is also the sum of two squares.

- **Example 6.4.** *Sums of two squares have a remarkable multiplicative property. Consider the following table.*

-

2	1^2+1^2	26	1^2+5^2	68	2^2+8^2	100	6^2+8^2
4	0^2+2^2	29	2^2+5^2	72	6^2+6^2	104	2^2+10^2
5	1^2+2^2	34	3^2+5^2	74	5^2+7^2	106	5^2+9^2
8	2^2+2^2	40	2^2+6^2	80	4^2+8^2	116	4^2+10^2
9	0^2+3^2	45	3^2+6^2	81	0^2+9^2	117	6^2+9^2
10	1^2+3^2	50	5^2+5^2	82	1^2+9^2	122	1^2+11^2
13	2^2+3^2	52	4^2+6^2	85	2^2+9^2	125	5^2+10^2
20	2^2+4^2	58	3^2+7^2	90	3^2+9^2	128	8^2+8^2
25	0^2+5^2	65	1^2+8^2	98	7^2+7^2	130	3^2+11^2

- This looks as though, if a number n has a factorisation ab with both a and b being sums of two squares, then n is also the sum of two squares.
- For example $130 = 2 \times 4 \times 13$ and both 2, 5 and 13 are sums of two squares.

- **Example 6.5.** *It turns out that there is a neat identity which proves this.*

- **Example 6.5.** *It turns out that there is a neat identity which proves this.*
- *Given x, y, X and Y we have*

$$(x^2+y^2)(X^2+Y^2)=(xX-yY)^2+(xY+yX)^2.$$

- **Example 6.5.** *It turns out that there is a neat identity which proves this.*
- *Given x, y, X and Y we have*

$$(x^2+y^2)(X^2+Y^2)=(xX-yY)^2+(xY+yX)^2.$$

- *The simplest proof is to multiply out both sides*

$$x^2X^2+x^2Y^2+y^2X^2+y^2Y^2,$$

$$x^2X^2-2xXyY+y^2Y^2+x^2Y^2+2xYyX+y^2X^2$$

and observe that the cross product terms on the right cancel and then the two sides are equal.

- **Example 6.5.** *It turns out that there is a neat identity which proves this.*
- *Given* x, y, X *and* Y *we have*

$$(x^2+y^2)(X^2+Y^2)=(xX-yY)^2+(xY+yX)^2.$$

- *The simplest proof is to multiply out both sides*

$$x^2X^2+x^2Y^2+y^2X^2+y^2Y^2,$$

$$x^2X^2-2xXyY+y^2Y^2+x^2Y^2+2xYyX+y^2X^2$$

and observe that the cross product terms on the right cancel and then the two sides are equal.
- *Another way of seeing this identity is to write it as* $(x^2+y^2)(X^2+Y^2)=|x+iy|^2|X+iY|^2=|(x+iy)(X+iY)|^2=|xX-yY+i(xY+yX)|^2=(xX-yY)^2+(xY+yX)^2.$

- Now we can prove Fermat's theorem

Theorem 2 (Fermat)

Let n have the canonical decomposition $n = p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$ where the q_j are the primes in the factorisation with $q_j \equiv 3 \pmod 4$ and the p_j are the prime 2 (if n is even) and the primes $p_j \equiv 1 \pmod 4$. Then n is the sum of two squares if and only if all the exponents b_j are even.

- Now we can prove Fermat's theorem

Theorem 2 (Fermat)

Let n have the canonical decomposition $n = p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$ where the q_j are the primes in the factorisation with $q_j \equiv 3 \pmod 4$ and the p_j are the prime 2 (if n is even) and the primes $p_j \equiv 1 \pmod 4$. Then n is the sum of two squares if and only if all the exponents b_j are even.

- **Proof.** If n satisfies the necessary condition, then the result follows by repeated use of the identity and the special cases $p = 2$, $p \equiv 1 \pmod 4$ and q^2.

- Now we can prove Fermat's theorem

Theorem 2 (Fermat)

Let n have the canonical decomposition $n = p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$ where the q_j are the primes in the factorisation with $q_j \equiv 3 \pmod 4$ and the p_j are the prime 2 (if n is even) and the primes $p_j \equiv 1 \pmod 4$. Then n is the sum of two squares if and only if all the exponents b_j are even.

- **Proof.** If n satisfies the necessary condition, then the result follows by repeated use of the identity and the special cases $p = 2$, $p \equiv 1 \pmod 4$ and q^2.
- To prove the converse observe that if q is a prime with $q \equiv 3 \pmod 4$ and $n = x^2 + y^2 \equiv 0 \pmod q$, then we have $q|x$ and $q|y$, for if not, then we have nonsense;

$$1 = \left(\frac{-y^2}{q}\right)_L = \left(\frac{-1}{q}\right)_L = -1.$$

- Now we can prove Fermat's theorem

Theorem 2 (Fermat)

Let n have the canonical decomposition $n = p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$ where the q_j are the primes in the factorisation with $q_j \equiv 3 \pmod 4$ and the p_j are the prime 2 (if n is even) and the primes $p_j \equiv 1 \pmod 4$. Then n is the sum of two squares if and only if all the exponents b_j are even.

- **Proof.** If n satisfies the necessary condition, then the result follows by repeated use of the identity and the special cases $p = 2$, $p \equiv 1 \pmod 4$ and q^2.
- To prove the converse observe that if q is a prime with $q \equiv 3 \pmod 4$ and $n = x^2 + y^2 \equiv 0 \pmod q$, then we have $q|x$ and $q|y$, for if not, then we have nonsense;

$$1 = \left(\frac{-y^2}{q}\right)_L = \left(\frac{-1}{q}\right)_L = -1.$$

- Thus n/q^2 is a sum of two squares and we can use an inductive argument.

- It is also possible to show a similar result for numbers of the form $x^2 + 2y^2$ and likewise for $x^2 + 3y^2$.

- It is also possible to show a similar result for numbers of the form x^2+2y^2 and likewise for x^2+3y^2.
- The general rule here is that if -2 (or -3 in the second case) is a QR modulo p, then p can be represented and there is an identity $(x^2+\lambda y^2)(X^2+\lambda Y^2)=(xX-\lambda yY)^2+\lambda(xY+yX)^2$ which works in both cases.

- It is also possible to show a similar result for numbers of the form $x^2 + 2y^2$ and likewise for $x^2 + 3y^2$.
- The general rule here is that if -2 (or -3 in the second case) is a QR modulo p, then p can be represented and there is an identity $(x^2 + \lambda y^2)(X^2 + \lambda Y^2) = (xX - \lambda yY)^2 + \lambda(xY + yX)^2$ which works in both cases.
- In the case of $x^2 + 2y^2$ Thue's argument shows that if $p \equiv 1 \text{ or } 3 \pmod 8$, then there are x and y such that $x^2 + 2y^2 = mp$ with $m = 1$ or 2.

- It is also possible to show a similar result for numbers of the form $x^2 + 2y^2$ and likewise for $x^2 + 3y^2$.
- The general rule here is that if -2 (or -3 in the second case) is a QR modulo p, then p can be represented and there is an identity $(x^2 + \lambda y^2)(X^2 + \lambda Y^2) = (xX - \lambda yY)^2 + \lambda(xY + yX)^2$ which works in both cases.
- In the case of $x^2 + 2y^2$ Thue's argument shows that if $p \equiv 1 \text{ or } 3 \pmod 8$, then there are x and y such that $x^2 + 2y^2 = mp$ with $m = 1$ or 2.
- If $m = 2$, then $2|x$ and the equation reduces to $2(x/2)^2 + y^2 = p$.

- It is also possible to show a similar result for numbers of the form $x^2 + 2y^2$ and likewise for $x^2 + 3y^2$.
- The general rule here is that if -2 (or -3 in the second case) is a QR modulo p, then p can be represented and there is an identity
$(x^2 + \lambda y^2)(X^2 + \lambda Y^2) = (xX - \lambda yY)^2 + \lambda(xY + yX)^2$
which works in both cases.
- In the case of $x^2 + 2y^2$ Thue's argument shows that if $p \equiv 1$ or $3 \pmod 8$, then there are x and y such that $x^2 + 2y^2 = mp$ with $m = 1$ or 2.
- If $m = 2$, then $2|x$ and the equation reduces to $2(x/2)^2 + y^2 = p$.
- For the form $x^2 + 3y^2$, when $p \equiv 1 \pmod 3$, Thue reduces to $x^2 + 3y^2 = mp$ with $m = 1, 2$ or 3.

- It is also possible to show a similar result for numbers of the form $x^2 + 2y^2$ and likewise for $x^2 + 3y^2$.
- The general rule here is that if -2 (or -3 in the second case) is a QR modulo p, then p can be represented and there is an identity $(x^2 + \lambda y^2)(X^2 + \lambda Y^2) = (xX - \lambda yY)^2 + \lambda(xY + yX)^2$ which works in both cases.
- In the case of $x^2 + 2y^2$ Thue's argument shows that if $p \equiv 1 \text{ or } 3 \pmod 8$, then there are x and y such that $x^2 + 2y^2 = mp$ with $m = 1$ or 2.
- If $m = 2$, then $2|x$ and the equation reduces to $2(x/2)^2 + y^2 = p$.
- For the form $x^2 + 3y^2$, when $p \equiv 1 \pmod 3$, Thue reduces to $x^2 + 3y^2 = mp$ with $m = 1, 2$ or 3.
- Then $m = 3$ can be dealt with as before.

- It is also possible to show a similar result for numbers of the form x^2+2y^2 and likewise for x^2+3y^2.
- The general rule here is that if -2 (or -3 in the second case) is a QR modulo p, then p can be represented and there is an identity
  $(x^2+\lambda y^2)(X^2+\lambda Y^2)=(xX-\lambda yY)^2+\lambda(xY+yX)^2$
  which works in both cases.
- In the case of x^2+2y^2 Thue's argument shows that if $p\equiv 1$ or $3 \pmod 8$, then there are x and y such that $x^2+2y^2=mp$ with $m=1$ or 2.
- If $m=2$, then $2|x$ and the equation reduces to $2(x/2)^2+y^2=p$.
- For the form x^2+3y^2, when $p\equiv 1 \pmod 3$, Thue reduces to $x^2+3y^2=mp$ with $m=1,2$ or 3.
- Then $m=3$ can be dealt with as before.
- The possibility $m=2$ cannot happen because when $p>2$ one cannot have $2|xy$, so the left hand side is $\equiv 1+3\equiv 4 \pmod 8$ and 4 does not divide $2p$.

- This phenomenon does not occur for more general binary quadratic forms
$$ax^2 + bxy + cy^2$$
because it is possible in most cases that $D = b^2 - 4ac$ is a QR modulo p, but the form does not represent p.

- This phenomenon does not occur for more general binary quadratic forms
$$ax^2 + bxy + cy^2$$
because it is possible in most cases that $D = b^2 - 4ac$ is a QR modulo p, but the form does not represent p.
- It turns out there is a different form with the same value of discriminant D which represents p.

- This phenomenon does not occur for more general binary quadratic forms
$$ax^2 + bxy + cy^2$$
because it is possible in most cases that $D = b^2 - 4ac$ is a QR modulo p, but the form does not represent p.
- It turns out there is a different form with the same value of discriminant D which represents p.
- **Example 6.6.** *In the case when $D = -20$, there are basically two forms, (everything else with that discriminant can be reduced to them) $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$. The discriminant -20 is a QR for $p = 7$ and $p = 29$, but only the second form represents 7 and only the first one represents 29.*
This is related to the "class number problem", and the fact that the quadratic number field $\mathbb{Q}(\sqrt{-5})$ fails to have uniqueness of factorisation.

- This phenomenon does not occur for more general binary quadratic forms

$$ax^2 + bxy + cy^2$$

because it is possible in most cases that $D = b^2 - 4ac$ is a QR modulo p, but the form does not represent p.
- It turns out there is a different form with the same value of discriminant D which represents p.
- **Example 6.6.** *In the case when $D = -20$, there are basically two forms, (everything else with that discriminant can be reduced to them) $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$. The discriminant -20 is a QR for $p = 7$ and $p = 29$, but only the second form represents 7 and only the first one represents 29.*

  This is related to the "class number problem", and the fact that the quadratic number field $\mathbb{Q}(\sqrt{-5})$ fails to have uniqueness of factorisation.
- This phenomenon was extensively studied by Gauss in *Disquisitiones Arithmeticæ* in 1798 (he was 21). It is a very elegant theory.

- First, in modern notation, one can write

$$ax_1^2 + bx_1x_2 + cx_2^2 = \mathbf{x}A\mathbf{x}^T$$

where $\mathbf{x}$ denotes the vector (x_1, x_2), $\mathbf{x}^T$ its transpose and A is the matrix

$$A = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

- First, in modern notation, one can write

$$ax_1^2 + bx_1x_2 + cx_2^2 = \mathbf{x}A\mathbf{x}^T$$

where $\mathbf{x}$ denotes the vector (x_1, x_2), $\mathbf{x}^T$ its transpose and A is the matrix

$$A = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

- If the 2×2 matrix U has integer entries and $\det U = \pm 1$, then it is invertible and the inverse has integer entries.

- First, in modern notation, one can write

$$ax_1^2 + bx_1x_2 + cx_2^2 = \mathbf{x}A\mathbf{x}^T$$

where $\mathbf{x}$ denotes the vector (x_1, x_2), $\mathbf{x}^T$ its transpose and A is the matrix

$$A = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

- If the 2×2 matrix U has integer entries and $\det U = \pm 1$, then it is invertible and the inverse has integer entries.
- Thus $\mathbf{x}UAU^T\mathbf{x}^T$ will represent the same integers as $\mathbf{x}A\mathbf{x}^T$.

- First, in modern notation, one can write

$$ax_1^2 + bx_1x_2 + cx_2^2 = \mathbf{x}A\mathbf{x}^T$$

where $\mathbf{x}$ denotes the vector (x_1, x_2), $\mathbf{x}^T$ its transpose and A is the matrix

$$A = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

- If the 2×2 matrix U has integer entries and $\det U = \pm 1$, then it is invertible and the inverse has integer entries.
- Thus $\mathbf{x}UAU^T\mathbf{x}^T$ will represent the same integers as $\mathbf{x}A\mathbf{x}^T$.
- Hence one can divide the forms $ax_1^2 + bx_1x_2 + cx_2^2$, i.e. matrices A, with a given discriminant $D = -4\det A$, into "equivalence classes".

- First, in modern notation, one can write
$$ax_1^2 + bx_1x_2 + cx_2^2 = \mathbf{x}A\mathbf{x}^T$$
where $\mathbf{x}$ denotes the vector (x_1, x_2), $\mathbf{x}^T$ its transpose and A is the matrix
$$A = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$
- If the 2×2 matrix U has integer entries and $\det U = \pm 1$, then it is invertible and the inverse has integer entries.
- Thus $\mathbf{x}UAU^T\mathbf{x}^T$ will represent the same integers as $\mathbf{x}A\mathbf{x}^T$.
- Hence one can divide the forms $ax_1^2 + bx_1x_2 + cx_2^2$, i.e. matrices A, with a given discriminant $D = -4\det A$, into "equivalence classes".
- The number of different equivalence classes is called the class number $h(D)$.

- First, in modern notation, one can write

$$ax_1^2 + bx_1x_2 + cx_2^2 = \mathbf{x}A\mathbf{x}^T$$

where $\mathbf{x}$ denotes the vector (x_1, x_2), $\mathbf{x}^T$ its transpose and A is the matrix

$$A = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

- If the 2×2 matrix U has integer entries and $\det U = \pm 1$, then it is invertible and the inverse has integer entries.
- Thus $\mathbf{x}UAU^T\mathbf{x}^T$ will represent the same integers as $\mathbf{x}A\mathbf{x}^T$.
- Hence one can divide the forms $ax_1^2 + bx_1x_2 + cx_2^2$, i.e. matrices A, with a given discriminant $D = -4\det A$, into "equivalence classes".
- The number of different equivalence classes is called the class number $h(D)$.
- There is a canonical or "reduced" form - in which the coefficients satisfy a certain minimality condition - which is normally taken to be the representative of the class.

- **Example 6.7.** *When* $D = -20$ *the class number* $h(-20) = 2$ *and the two reduced forms are* $x_1^2 + 5y_2^2$ *and* $2x_1^2 + 2x_1x_2 + 3x_2^2$.

- **Example 6.7.** *When* $D = -20$ *the class number* $h(-20) = 2$ *and the two reduced forms are* $x_1^2 + 5y_2^2$ *and* $2x_1^2 + 2x_1x_2 + 3x_2^2$.
- In the modern era the subject of binary quadratic forms is subsumed in the study of quadratic number fields $\mathbb{Q}(\sqrt{D})$.

- The proof of Lagrange's four square theorem is a similar.

- The proof of Lagrange's four square theorem is a similar.
- As for two squares there is an identity, discovered by Euler.

Theorem 3 (Euler's four squares identity)

For any numbers a, b, c, d, w, x, y, z,

$$\begin{aligned}(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2) &= \\ &(ax-by-cz-dw)^2+(ay+bx+cw-dz)^2+ \\ &(az+cx+dy-bw)^2+(aw+dx+bz-cy)^2.\end{aligned}$$

- The proof of Lagrange's four square theorem is a similar.
- As for two squares there is an identity, discovered by Euler.

Theorem 3 (Euler's four squares identity)

For any numbers a, b, c, d, w, x, y, z,

$$\begin{aligned}(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2) = \\ (ax-by-cz-dw)^2+(ay+bx+cw-dz)^2+ \\ (az+cx+dy-bw)^2+(aw+dx+bz-cy)^2.\end{aligned}$$

- One could just multiply it out. Here is an alternative.

- The proof of Lagrange's four square theorem is a similar.
- As for two squares there is an identity, discovered by Euler.

Theorem 3 (Euler's four squares identity)

For any numbers a, b, c, d, w, x, y, z*,*

$$\begin{aligned}(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2) = \\ (ax-by-cz-dw)^2+(ay+bx+cw-dz)^2+ \\ (az+cx+dy-bw)^2+(aw+dx+bz-cy)^2.\end{aligned}$$

- One could just multiply it out. Here is an alternative.
- Think of it as a polynomial in the variable x. The coefficient of x^2 on both sides is $a^2+b^2+c^2+d^2$.

- The proof of Lagrange's four square theorem is a similar.
- As for two squares there is an identity, discovered by Euler.

Theorem 3 (Euler's four squares identity)

For any numbers a, b, c, d, w, x, y, z,

$$\begin{aligned}(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2) = \\ (ax-by-cz-dw)^2+(ay+bx+cw-dz)^2+ \\ (az+cx+dy-bw)^2+(aw+dx+bz-cy)^2.\end{aligned}$$

- One could just multiply it out. Here is an alternative.
- Think of it as a polynomial in the variable x. The coefficient of x^2 on both sides is $a^2+b^2+c^2+d^2$.
- The coefficient of x on the left is obviously 0, and a little checking shows that the x-terms on the right cancel.

- The proof of Lagrange's four square theorem is a similar.
- As for two squares there is an identity, discovered by Euler.

Theorem 3 (Euler's four squares identity)

For any numbers a, b, c, d, w, x, y, z,

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2) = (ax-by-cz-dw)^2+(ay+bx+cw-dz)^2+ (az+cx+dy-bw)^2+(aw+dx+bz-cy)^2.$$

- One could just multiply it out. Here is an alternative.
- Think of it as a polynomial in the variable x. The coefficient of x^2 on both sides is $a^2+b^2+c^2+d^2$.
- The coefficient of x on the left is obviously 0, and a little checking shows that the x-terms on the right cancel.
- That leaves the "constant" term. To check that put $x=0$ and repeat the argument with y. And then z, and then w.

- Now we can prove Lagrange's theorem.

Theorem 4 (Lagrange)

Every natural number is the sum of four squares.

- Now we can prove Lagrange's theorem.

Theorem 4 (Lagrange)

Every natural number is the sum of four squares.

- **Proof.** By the identity and the 2-square theorem it suffices to treat $p \equiv 3 \pmod 4$.

- Now we can prove Lagrange's theorem.

Theorem 4 (Lagrange)

Every natural number is the sum of four squares.

- **Proof.** By the identity and the 2-square theorem it suffices to treat $p \equiv 3 \pmod 4$.
- The following us useful

Lemma 5

If n is even and is a sum of four squares, then so is $\frac{n}{2}$.

- Now we can prove Lagrange's theorem.

Theorem 4 (Lagrange)

Every natural number is the sum of four squares.

- **Proof.** By the identity and the 2-square theorem it suffices to treat $p \equiv 3 \pmod 4$.
- The following us useful

Lemma 5

If n is even and is a sum of four squares, then so is $\frac{n}{2}$.

- **Proof.** When $n = a^2 + b^2 + c^2 + d^2$ is even, the number of odd squares will be even,

- Now we can prove Lagrange's theorem.

Theorem 4 (Lagrange)

Every natural number is the sum of four squares.

- **Proof.** By the identity and the 2-square theorem it suffices to treat $p \equiv 3 \pmod 4$.
- The following us useful

Lemma 5

If n is even and is a sum of four squares, then so is $\frac{n}{2}$.

- **Proof.** When $n = a^2 + b^2 + c^2 + d^2$ is even, the number of odd squares will be even,
- and thus the a, b, c, d can be rearranged so that a, b have the same parity and so do c, d.

- Now we can prove Lagrange's theorem.

Theorem 4 (Lagrange)

Every natural number is the sum of four squares.

- **Proof.** By the identity and the 2-square theorem it suffices to treat $p \equiv 3 \pmod 4$.
- The following us useful

Lemma 5

If n is even and is a sum of four squares, then so is $\frac{n}{2}$.

- **Proof.** When $n = a^2 + b^2 + c^2 + d^2$ is even, the number of odd squares will be even,
- and thus the a, b, c, d can be rearranged so that a, b have the same parity and so do c, d.
- Therefore $\frac{n}{2} = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2$.

- This is the core of the proof.

Lemma 6

If p is an odd prime, then there are integers a, b, c, d and an m so that $0 < a^2 + b^2 + c^2 + d^2 = mp < \frac{p^2}{2}$.

- This is the core of the proof.

Lemma 6

If p is an odd prime, then there are integers a, b, c, d and an m so that $0 < a^2 + b^2 + c^2 + d^2 = mp < \frac{p^2}{2}$.

- **Proof**. The $\frac{p+1}{2}$ numbers $0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are pairwise incongruent modulo p.

- This is the core of the proof.

Lemma 6

If p is an odd prime, then there are integers a, b, c, d and an m so that $0 < a^2 + b^2 + c^2 + d^2 = mp < \frac{p^2}{2}$.

- **Proof**. The $\frac{p+1}{2}$ numbers $0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are pairwise incongruent modulo p.
- Thus the $\frac{p+1}{2}$ numbers u^2 with $0 \le u \le \frac{p-1}{2}$ will lie in separate residue classes modulo p and the $\frac{p+1}{2}$ numbers $-v^2 - 1$ with $0 \le v \le \frac{p-1}{2}$ will lie in separate residue classes modulo p.

- This is the core of the proof.

Lemma 6

If p is an odd prime, then there are integers a, b, c, d and an m so that $0 < a^2 + b^2 + c^2 + d^2 = mp < \frac{p^2}{2}$.

- **Proof**. The $\frac{p+1}{2}$ numbers $0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are pairwise incongruent modulo p.
- Thus the $\frac{p+1}{2}$ numbers u^2 with $0 \le u \le \frac{p-1}{2}$ will lie in separate residue classes modulo p and the $\frac{p+1}{2}$ numbers $-v^2 - 1$ with $0 \le v \le \frac{p-1}{2}$ will lie in separate residue classes modulo p.
- Since $\frac{p+1}{2} + \frac{p+1}{2} = p + 1 > p$ there will be at least one residue class which contains one or more of each.

- This is the core of the proof.

Lemma 6

If p is an odd prime, then there are integers a, b, c, d and an m so that $0 < a^2 + b^2 + c^2 + d^2 = mp < \frac{p^2}{2}$.

- **Proof**. The $\frac{p+1}{2}$ numbers $0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are pairwise incongruent modulo p.
- Thus the $\frac{p+1}{2}$ numbers u^2 with $0 \le u \le \frac{p-1}{2}$ will lie in separate residue classes modulo p and the $\frac{p+1}{2}$ numbers $-v^2 - 1$ with $0 \le v \le \frac{p-1}{2}$ will lie in separate residue classes modulo p.
- Since $\frac{p+1}{2} + \frac{p+1}{2} = p + 1 > p$ there will be at least one residue class which contains one or more of each.
- Hence there are u, v such that $u^2 \equiv -v^2 - 1 \pmod{p}$, and $0 < u^2 + v^2 + 1 \le \frac{p^2-2p+3}{2} < \frac{p^2}{2}$.

- This is the core of the proof.

Lemma 6

If p is an odd prime, then there are integers a, b, c, d and an m so that $0 < a^2 + b^2 + c^2 + d^2 = mp < \frac{p^2}{2}$.

- **Proof**. The $\frac{p+1}{2}$ numbers $0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are pairwise incongruent modulo p.
- Thus the $\frac{p+1}{2}$ numbers u^2 with $0 \le u \le \frac{p-1}{2}$ will lie in separate residue classes modulo p and the $\frac{p+1}{2}$ numbers $-v^2 - 1$ with $0 \le v \le \frac{p-1}{2}$ will lie in separate residue classes modulo p.
- Since $\frac{p+1}{2} + \frac{p+1}{2} = p + 1 > p$ there will be at least one residue class which contains one or more of each.
- Hence there are u, v such that $u^2 \equiv -v^2 - 1 \pmod{p}$, and $0 < u^2 + v^2 + 1 \le \frac{p^2-2p+3}{2} < \frac{p^2}{2}$.
- Now we only have to show that $m = 1$ is possible.

- We just showed that there is an integer m with $0 < m < p$ so that for some a, b, c, d we have $a^2 + b^2 + c^2 + d^2 = mp$.

- We just showed that there is an integer m with $0 < m < p$ so that for some a, b, c, d we have $a^2 + b^2 + c^2 + d^2 = mp$.
- We may suppose that m is chosen minimally and by Lemma 5 that m is odd, and if $m = 1$, then we are done.

- We just showed that there is an integer m with $0 < m < p$ so that for some a, b, c, d we have $a^2 + b^2 + c^2 + d^2 = mp$.
- We may suppose that m is chosen minimally and by Lemma 5 that m is odd, and if $m = 1$, then we are done.
- Suppose $m > 1$. If m were to divide each of a, b, c, d, then we would have $m|p$ contradicting $m < p$.

- We just showed that there is an integer m with $0 < m < p$ so that for some a, b, c, d we have $a^2 + b^2 + c^2 + d^2 = mp$.
- We may suppose that m is chosen minimally and by Lemma 5 that m is odd, and if $m = 1$, then we are done.
- Suppose $m > 1$. If m were to divide each of a, b, c, d, then we would have $m|p$ contradicting $m < p$.
- Choose x, y, z, w so $x \equiv a \pmod{m}$, $|x| \le \frac{m-1}{2}$, $y \equiv -b \pmod{m}$, $|y| \le \frac{m-1}{2}$, $z \equiv -c \pmod{m}$, $|z| \le \frac{m-1}{2}$, $w \equiv -d \pmod{m}$, $|w| \le \frac{m-1}{2}$. Not all x, y, z, w are 0.

- We just showed that there is an integer m with $0 < m < p$ so that for some a, b, c, d we have $a^2 + b^2 + c^2 + d^2 = mp$.
- We may suppose that m is chosen minimally and by Lemma 5 that m is odd, and if $m = 1$, then we are done.
- Suppose $m > 1$. If m were to divide each of a, b, c, d, then we would have $m|p$ contradicting $m < p$.
- Choose x, y, z, w so $x \equiv a \pmod{m}$, $|x| \le \frac{m-1}{2}$, $y \equiv -b \pmod{m}$, $|y| \le \frac{m-1}{2}$, $z \equiv -c \pmod{m}$, $|z| \le \frac{m-1}{2}$, $w \equiv -d \pmod{m}$, $|w| \le \frac{m-1}{2}$. Not all x, y, z, w are 0.
- Moreover $x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{m}$ and so $0 < x^2 + y^2 + z^2 + w^2 = mn \le 4\left(\frac{m-1}{2}\right)^2 = (m-1)^2$.

- We just showed that there is an integer m with $0 < m < p$ so that for some a, b, c, d we have $a^2 + b^2 + c^2 + d^2 = mp$.
- We may suppose that m is chosen minimally and by Lemma 5 that m is odd, and if $m = 1$, then we are done.
- Suppose $m > 1$. If m were to divide each of a, b, c, d, then we would have $m|p$ contradicting $m < p$.
- Choose x, y, z, w so $x \equiv a \pmod{m}$, $|x| \le \frac{m-1}{2}$, $y \equiv -b \pmod{m}$, $|y| \le \frac{m-1}{2}$, $z \equiv -c \pmod{m}$, $|z| \le \frac{m-1}{2}$, $w \equiv -d \pmod{m}$, $|w| \le \frac{m-1}{2}$. Not all x, y, z, w are 0.
- Moreover $x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{m}$ and so $0 < x^2 + y^2 + z^2 + w^2 = mn \le 4\left(\frac{m-1}{2}\right)^2 = (m-1)^2$.
- Thus $0 < n < m$. Now
$ax - by - cz - dw \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m}$,
$ay + bx + cw - dz \equiv -ab + ab - cd + dc \equiv 0 \pmod{m}$,
$az + cx + dy - bw \equiv -ac + ac - db + db \equiv 0 \pmod{m}$,
$aw + dx + bz - cy \equiv -ad + ad - bc + bc \equiv 0 \pmod{m}$.

- We just showed that there is an integer m with $0 < m < p$ so that for some a, b, c, d we have $a^2 + b^2 + c^2 + d^2 = mp$.
- We may suppose that m is chosen minimally and by Lemma 5 that m is odd, and if $m = 1$, then we are done.
- Suppose $m > 1$. If m were to divide each of a, b, c, d, then we would have $m|p$ contradicting $m < p$.
- Choose x, y, z, w so $x \equiv a \pmod{m}$, $|x| \le \frac{m-1}{2}$, $y \equiv -b \pmod{m}$, $|y| \le \frac{m-1}{2}$, $z \equiv -c \pmod{m}$, $|z| \le \frac{m-1}{2}$, $w \equiv -d \pmod{m}$, $|w| \le \frac{m-1}{2}$. Not all x, y, z, w are 0.
- Moreover $x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{m}$ and so $0 < x^2 + y^2 + z^2 + w^2 = mn \le 4\left(\frac{m-1}{2}\right)^2 = (m-1)^2$.
- Thus $0 < n < m$. Now
  $ax - by - cz - dw \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m}$,
  $ay + bx + cw - dz \equiv -ab + ab - cd + dc \equiv 0 \pmod{m}$,
  $az + cx + dy - bw \equiv -ac + ac - db + db \equiv 0 \pmod{m}$,
  $aw + dx + bz - cy \equiv -ad + ad - bc + bc \equiv 0 \pmod{m}$.
- By Euler's identity m^2np is the sum of four squares and each is divisible by m^2. Hence np is the sum of four squares. But $n < m$ contradicting the minimality of m.

- Many numbers are not the sum of two squares and every number is the sum of four, so what about sums of three?

- Many numbers are not the sum of two squares and every number is the sum of four, so what about sums of three?
- This is quite hard and was first solved by Legendre in 1798.

- Many numbers are not the sum of two squares and every number is the sum of four, so what about sums of three?
- This is quite hard and was first solved by Legendre in 1798.
- In the case of two squares we saw that the $p \equiv 3 \pmod 4$, when they occur to an odd power, were excluded by a simple congruence argument.

- Many numbers are not the sum of two squares and every number is the sum of four, so what about sums of three?
- This is quite hard and was first solved by Legendre in 1798.
- In the case of two squares we saw that the $p \equiv 3 \pmod 4$, when they occur to an odd power, were excluded by a simple congruence argument.
- **Example 6.8.** *We know that* $x^2 \equiv 0, 1$ *or* $4 \pmod 8$. *Thus one can check that*

$$x_1^2 + x_2^2 + x_3^2 \equiv 0, 1, 2, 3, 4, 5, 6, \pmod 8$$

but $x_1^2 + x_2^2 + x_3^2 \not\equiv 7 \pmod 8$.

- Many numbers are not the sum of two squares and every number is the sum of four, so what about sums of three?
- This is quite hard and was first solved by Legendre in 1798.
- In the case of two squares we saw that the $p \equiv 3 \pmod 4$, when they occur to an odd power, were excluded by a simple congruence argument.
- **Example 6.8.** *We know that $x^2 \equiv 0$, 1 or 4 $\pmod 8$. Thus one can check that*

$$x_1^2 + x_2^2 + x_3^2 \equiv 0, 1, 2, 3, 4, 5, 6, \pmod 8$$

but $x_1^2 + x_2^2 + x_3^2 \not\equiv 7 \pmod 8$.

- *Thus if $x_1^2 + x_2^2 + x_3^2 = n$, then we have to have $n \equiv 0, 1, 2, 3, 4, 5, 6, \pmod 8$. Moreover if $x_1^2 + x_2^2 + x_3^2 \equiv 0 \pmod 4$, then the variables x_j have to be all even and we can factor out a 4 on both sides and reduce to $(x_1/2)^2 + (x_2/2)^2 + (x_3/2)^2 = n/4$*

- Then we have just proved

Theorem 7

If $n = 4^h(8k+7)$ for some non-negative integers h and k, then n is not the sum of three squares.

- Then we have just proved

Theorem 7

If $n = 4^h(8k+7)$ *for some non-negative integers* h *and* k*, then* n *is not the sum of three squares.*

- Legendre proved that all other n *are* the sum of three squares. The proof is quite complicated and I do not plan to give it here.

- Given a positive integer s, how many ways are there of writing n as the sum of two squares of integers?

- Given a positive integer s, how many ways are there of writing n as the sum of two squares of integers?
- We count $(-x)^2$ separately from x^2 when $x \neq 0$. Suppose $z \in \mathbb{C}$ and $|z| < 1$. Consider the series

$$f(z) = \sum_{n=-\infty}^{\infty} z^{n^2} = 1 + 2\sum_{n=1}^{\infty} z^{n^2}.$$

Then formally

$$f(z)^s = \sum_{n_1} \dots \sum_{n_s} z^{n_1^2+\cdots+n_s^2} = \sum_{n=0}^{\infty} r_s(n) z^n$$

where $r_s(n)$ is the number of ways of writing n as the sum of s squares.

- Given a positive integer s, how many ways are there of writing n as the sum of two squares of integers?
- We count $(-x)^2$ separately from x^2 when $x \neq 0$. Suppose $z \in \mathbb{C}$ and $|z| < 1$. Consider the series

$$f(z) = \sum_{n=-\infty}^{\infty} z^{n^2} = 1 + 2\sum_{n=1}^{\infty} z^{n^2}.$$

Then formally

$$f(z)^s = \sum_{n_1} \dots \sum_{n_s} z^{n_1^2+\cdots+n_s^2} = \sum_{n=0}^{\infty} r_s(n) z^n$$

where $r_s(n)$ is the number of ways of writing n as the sum of s squares.
- The function $f(z)$ has lots of structure and this can be used to find formulas for $r_s(n)$, and was exploited extensively by Jacobi.

- In 1770 Edward Waring stated without proof that "every positive integer is the sum of at most four squares, nine cubes, nineteen biquadrates, and so on".

- In 1770 Edward Waring stated without proof that "every positive integer is the sum of at most four squares, nine cubes, nineteen biquadrates, and so on".
- What we think he meant was that if we define $g(k)$ to be the smallest number s such that every positive integer is the sum of at most s k-th powers, then $g(2) = 4$, $g(3) = 9$, $g(4) = 19$.

- In 1770 Edward Waring stated without proof that "every positive integer is the sum of at most four squares, nine cubes, nineteen biquadrates, and so on".
- What we think he meant was that if we define $g(k)$ to be the smallest number s such that every positive integer is the sum of at most s k-th powers, then $g(2) = 4$, $g(3) = 9$, $g(4) = 19$.
- Many mathematicians have worked on Waring's Problem; Hilbert, Landau, Hardy, Littlewood, Davenport, ...

- In 1770 Edward Waring stated without proof that "every positive integer is the sum of at most four squares, nine cubes, nineteen biquadrates, and so on".
- What we think he meant was that if we define $g(k)$ to be the smallest number s such that every positive integer is the sum of at most s k-th powers, then $g(2)=4$, $g(3)=9$, $g(4)=19$.
- Many mathematicians have worked on Waring's Problem; Hilbert, Landau, Hardy, Littlewood, Davenport, ...
- What we believe is that $g(k)=2^k+\left\lfloor\left(\frac{3}{2}\right)^k\right\rfloor-2$ and we know this is true for all but a finite number of exceptions, and there are none with $k\le 471,600,000$.

- In 1770 Edward Waring stated without proof that "every positive integer is the sum of at most four squares, nine cubes, nineteen biquadrates, and so on".
- What we think he meant was that if we define $g(k)$ to be the smallest number s such that every positive integer is the sum of at most s k-th powers, then $g(2) = 4$, $g(3) = 9$, $g(4) = 19$.
- Many mathematicians have worked on Waring's Problem; Hilbert, Landau, Hardy, Littlewood, Davenport, ...
- What we believe is that $g(k) = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$ and we know this is true for all but a finite number of exceptions, and there are none with $k \le 471{,}600{,}000$.
- The value of $g(k)$ depends on the peculiarities of a few small numbers, and probably the extremal n is

$$2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 = \left(\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 \right) \times 2^k + \left(2^k - 1\right) \times 1^k$$

- A harder problem which avoids the peculiarities of small numbers, is to take $G(k)$ to be the smallest s such that every *sufficiently large* integer is the sum of at most s k-th powers.

- A harder problem which avoids the peculiarities of small numbers, is to take $G(k)$ to be the smallest s such that every *sufficiently large* integer is the sum of at most s k-th powers.
- This has only been solved in two cases,

- A harder problem which avoids the peculiarities of small numbers, is to take $G(k)$ to be the smallest s such that every *sufficiently large* integer is the sum of at most s k-th powers.
- This has only been solved in two cases,
- $G(2) = 4$ (Lagrange) and

- A harder problem which avoids the peculiarities of small numbers, is to take $G(k)$ to be the smallest s such that every *sufficiently large* integer is the sum of at most s k-th powers.
- This has only been solved in two cases,
- $G(2) = 4$ (Lagrange) and
- $G(4) = 16$ (Davenport).

- A harder problem which avoids the peculiarities of small numbers, is to take $G(k)$ to be the smallest s such that every *sufficiently large* integer is the sum of at most s k-th powers.
- This has only been solved in two cases,
- $G(2) = 4$ (Lagrange) and
- $G(4) = 16$ (Davenport).
- For example we only know that $4 \le G(3) \le 7$ (Linnik) and

- A harder problem which avoids the peculiarities of small numbers, is to take $G(k)$ to be the smallest s such that every *sufficiently large* integer is the sum of at most s k-th powers.
- This has only been solved in two cases,
- $G(2) = 4$ (Lagrange) and
- $G(4) = 16$ (Davenport).
- For example we only know that $4 \le G(3) \le 7$ (Linnik) and
- $6 \le G(5) \le 17$ (RCV and Wooley).