Sums of Squares

Some integers are the sum of two squares, for example:

$58=3^2+7^2$ and $64=0^2+8^2$

Some integers are not the sum of two squares, for example:

7 and 15

We want to know which integers are the sum of two squares and which are not.

Theorem

If m and n are both the sum of two squares then mn is the sum of two squares.

Proof

$m=a^2+b^2$ and $n^2=c^2+d^2$

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

This also means that if m is the sum of two squares then any positive power of m is the sum of two squares.

Theorem

2 is the sum of two squares

Proof

$2=1^2+1^2$

Theorem

No integer of the form $4k+3$ is the sum of two squares

Proof

mod 4:

$x=0,1,2,3$ so $x^2=0,1$ and $y=0,1,2,3$ so $y^2=0,1$

so $x^2+y^2=0,1,2$ so $x^2+y^2\neq 3$

end of mod 4

So an integer of the form $4k+3$ cannot be the sum of two squares.

All primes (except 2) are of the form $4k+1$ or $4k+3$

We have just proved that no prime of the form $4k+3$ is the sum of two squares.

Fermat proved that every prime of the form $4k+1$ is the sum of two squares.

Theorem

Every even power of an integer is the sum of two squares

Proof

$6^{10}=(6^5)^2+0^2$ etc

We can write any integer n in the form:

$n=(2^a)(3^b)(5^c)(7^d)(11^e)(...)$

2 is the sum of two squares

So $(2)^a$ is the sum of two squares.

$5,13,17,...$ are all of the form $4k+1$

So $5,13,17,...$ are all the sum of two squares.

So $(5)^c,(13)^f,(17)^g,...$ are all the sum of two squares.

$3,7,11,...$ are all of the form $4k+3$

So $3,7,11,...$ are not the sum of two squares.

But $(3)^b,(7)^d,(11)^e,...$ are all the sum of two squares if $b,d,e,...$ are all even.

So n is the sum of two squares if all the powers of all the $4k+3$ primes are even.

So $(2^5)(3^{10})(5^{14})(7^2)(11^{24})(13^3)(17^1)$ is the sum of two squares

It turns out that:

n is the sum of two squares if and only if all the powers of all the $4k+3$ primes are even.

So $(2^1)(3^4)(5^0)(7^3)(11^0)(13^0)(17^8)(19^{20})$ is not the sum of two squares

Difference of two squares

Theorem

No integer of the form $4k+2$ is the difference of two squares.

Proof

mod 4:

$x=0,1,2,3$ so $x^2=0,1$ and $y=0,1,2,3$ so $y^2=0,1$

so $x^2-y^2=0,1,-1$ so $x^2-y^2=0,1,3$ so $x^2-y^2\neq 2$

end of mod 4

So an integer of the form $4k+2$ cannot be the difference of two squares.

We can easily verify that:

Theorem

Every integer of the form 4k is the difference of two squares

Proof

$$4k=(k+1)^2-(k-1)^2$$

Also

$$4k+1=(2k+1)^2-(2k)^2$$

And

$$4k+3=(2k+2)^2-(2k+1)^2$$

So n is the difference of two squares if and only if n is not of the form $4k+2$

see Exercise

Theorem

Every odd prime can be written as the difference of two squares in just one way.

Proof

If:

$$p=n^2-m^2=(n-m)(n+m)$$

then:

p can be factorised and is therefore not a prime unless $(n-m)=1$ and $p=(n+m)$

Which means we must have:

$$n=\frac{p+1}{2} \quad \text{and} \quad m=\frac{p-1}{2}$$

It can be proved that:

Every integer is the sum of:

- 4 squares
- 9 cubes
- 19 fourth powers
- 37 fifth powers

etc

EXERCISE

Show that no integer of the form $8k+7$ is the sum of three squares.

SOLUTION

mod 8

$x=0,1,2,3,4,5,6,7$ so $x^2=0,1,4$

$y=0,1,2,3,4,5,6,7$ so $y^2=0,1,4$

$z=0,1,2,3,4,5,6,7$ so $z^2=0,1,4$

So $x^2+y^2+z^2=0,1,2,3,4,5,6$

end of mod 8