Section 13.3

$x^2 + y^2 = z^2$ ✓ ?

↳ which squares are the sum of two other squares?

nonzero

↳ A. all of them : $9^2 = 9^2 + 0^2$

Q: which numbers are the sum of two squares?

A: $1 = 1^2 + 0^2$

$2 = 1^2 + 1^2$

$3 = \dots$ ✗

Solve Diophantine equ. $x^2 + y^2 = n$

1. For which n are there solns?

Note: this is additive number theory

But...

Thm: If m and n are sums of two squares, then mn is a sum of two squares.

Pf: Suppose $m = a^2 + b^2$, $n = c^2 + d^2$

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

Ex: $5 = 2^2 + 1^2$ $\quad 13 = 2^2 + 3^2$

So $5^k \, 13^l$ is a sum of two squares for any k, l

Q: which primes are the sum of two squares?

Thm: If $p \equiv 3 \mod 4$, then p is not a sum of two squares

Pf: squares mod 4 : 0, 1

Sums of 2 squares mod 4: 0, 1, 2

3 mod 4 is not sum of two squares

Surprise: Converse is true

Thm: If $p \equiv 1, 2 \mod 4$ is prime, then $p = a^2 + b^2$ for

Some $a, b \in \mathbb{Z}$

Pf techniques varied, long

Ex: Find a number which is not (just) the prod. of primes $\equiv 1, 2 \mod 4$ which can be written as the sum of two sqs.

A: $9 = 3^2 + 0^2$

$18 = 3^2 + 3^2$

Thm: $n > 0$ is a sum of two squares if and only if each prime factor of n which is $\equiv 3 \mod 4$ appears to an even power in the prime fact. of n.

Ex. $9 = 3^2$, $18 = 2^1 \cdot 3^2$

$49 = 7^2$, $245 = 5 \cdot 7^2$

can be written as sum of two squares

pf: Suppose each prime $\equiv 3 \mod 4$ appears to an even power in the prime factorization of n.

Then write $n = t^2 u$ where

- every prime $p \mid n$ s.t. $p \equiv 3 \mod 4$ has $p \mid t$
- u is a product of primes $p \equiv 1, 2 \mod 4$ or $u = 1$

B/c u is the product of primes $\equiv 1, 2 \mod 4$ or $u=1$, $u = m^2 + n^2$ for some m, n

Then $n = t^2 u = t^2(m^2 + n^2) = (tm)^2 + (tn)^2$

Spose by contradiction, for the converse, that $n = x^2 + y^2$ and $n = p^{2j+1} r$ for p prime, $p \equiv 3 \bmod 4$, $p \nmid r$

Let $d = (x, y)$, $a = \frac{x}{d}$, $b = \frac{y}{d}$

Then $n = x^2 + y^2 = (da)^2 + (db)^2 = d^2(a^2 + b^2)$

Set $m = \frac{n}{d^2} = a^2 + b^2$ ← odd many ps

Note $(a, b) = 1$ ← evenly many ps

Since and odd power of p divided n, an odd power of p divides m

So $p \mid m$.

Next $p \nmid a$ b/c if it did, then $p \mid m - a^2 = b^2 \longrightarrow p \mid b \rightarrow p \mid (a, b) = 1$ ↯

So $\exists z$ s.t. $az \equiv b \bmod p$

$$0 \equiv m = a^2 + b^2 \equiv a^2 + (az)^2$$
$$= a^2(1 + z^2) \mod p$$

$p \nmid a$ so $0 \equiv 1 + z^2 \mod p$

$$-1 \equiv z^2 \mod p$$

so -1 is quadratic residue mod $p \equiv 3 \mod 4$ $\lightning$

Q: What if we look at 3 squares?

$1 = 1^2 + 0^2 + 0^2$

$2 = 1^2 + 1^2 + 0^2$

$3 = 1^2 + 1^2 + 1^2$

$\vdots$

$6 = 2^2 + 1^2 + 1^2$

$7 = ???$ ✗

Q: What about 4 squares?

Thm (Lagrange): Every positive integer is the sum of 4 squares

Idea of pf:

- show that if m, n are sums of 4 sqs. then mn is the sum of 4 sqs. with arithmetic identity
- show that every prime is the sum of 4 sqs.