Lecture 10.2

Last time:

- A prime p is of the form

$$p = x^2 + y^2$$

if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

- For $p \equiv 1 \pmod 4$, to write p as a sum of two squares,

  * Solve $x^2 + 1 = pm$ for some $1 \leq m < p$.

  * If $m > 1$, descend to a solution to $x_1^2 + y_1^2 = pm_1$ for $1 \leq m_1 < m$.

  * Stop when $x^2 + y^2$

* Stop when $x_k + y_k = p$.

We've answered the question of when a prime is a sum of two squares.

Let's tackle composite numbers now.

By Exercise 2 from lecture 10.1,

- if $n = x^2 + y^2$ the some prime dividing n is $p \equiv 1 \pmod 4$

- the product of sums of squares is again a sum of squares

- if $n = x^2 + y^2$ then $d^2 n$ is also a sum of two squares.

Can anything else happen?

It turns out, no.

Theorem For $n = d^2 p_1 \cdots p_r$ where $p_1, \ldots, p_r$ are distinct primes and $d \in \mathbb{N}$ is not divisible by any p_i, then

(1) $n = x^2 + y^2$ for some $x, y \in \mathbb{Z}$ if and only if for each $1 \le i \le r$, $p_i = 2$ or $p_i \equiv 1 \pmod 4$.

(2) $n = x^2 + y^2$ for relatively prime $x, y \in \mathbb{Z}$

(2) $n = x^2 + y^2$ for relatively prime $x, y \in \mathbb{Z}$

if and only if n is a product of odd primes $p \equiv 1 \pmod 4$ or n is 2 times such a product.

Pf: (1) If each $p_i = 2$ or $p_i \equiv 1 \pmod 4$, the second and third comments above imply n is a sum of squares.

Conversely, if some $p_i \equiv 3 \pmod 4$, then

$$x^2 + y^2 = n \equiv 0 \pmod{p_i}$$

$$\Longrightarrow x^2 \equiv -y^2 \pmod{p_i}$$

$$\Longrightarrow \left(\frac{-1}{p_i}\right) = 1 \quad \text{or} \quad x \equiv y \equiv 0 \pmod{p_i}$$

$\left(\frac{\ }{p_i}\right)$ ... $x^2 \equiv y^2 \equiv 0 \pmod{p_i}$.

But $\left(\frac{-1}{p_i}\right) = -1$ so p_i must divide x and y, meaning p_i^2 divides x^2, y^2 and $n = x^2 + y^2$, a contradiction.

Therefore none of the p_i are 3 mod 4. $\square$

Exercise 1: Prove (2).

$\boxed{\text{Ex}}$ $n = 1105 = 5 \cdot 13 \cdot 17$ and all three prime divisors are 1 mod 4, so $1105 = x^2 + y^2$ for some x, y.

We have:

We have:

$$5 = 1^2 + 2^2, \qquad 13 = 2^2 + 3^2,$$

$$17 = 1^2 + 4^2.$$

So $$5.13 = (1^2 + 2^2)(2^2 + 3^2)$$

$$= (1.2 + 2.3)^2 + (1.3 - 2.2)^2$$

$$= 8^2 + (-1)^2$$

and $$(5.13).17 = (1^2 + 8^2)(1^2 + 4^2)$$

$$= (1.1 + 8.4)^2 + (1.4 - 8.1)^2$$

$$= 33^2 + (-4)^2.$$

$\boxed{\text{Ex}}$ $n = 252000 = 2^5 . 3^2 . 5^3 . 7$

$$= 60^2 \cdot 2 \cdot 5 \cdot 7$$

but $7 \equiv 3 \pmod 4$, so n is not a sum of two squares.

$\boxed{\text{Ex}}$ $n = 11169 = 3^2 \cdot 17 \cdot 73$ and $17 \equiv 73 \equiv 1 \pmod 4$, so n is a sum of two squares. We have $17 = 1^2 + 4^2$ and from Lecture 10.1,

$$73 = 3^2 + 8^2.$$

So $11169 = 3^2(1^2+4^2)(3^2+8^2)$

$$= 3^2\left((1\cdot 3 + 4\cdot 8)^2 + (1\cdot 8 - 4\cdot 3)^2\right)$$

$$= 3^2\left(35^2 + (-4)^2\right)$$

$$= 105^2 + 12^2.$$

Exercise 2: Write each n as a sum of two squares, or show that this is not possible.

(a) 2000 (b) 2022 (c) 4645

(d) 166465 (e) 1214596

Recall: the set of primitive Pythagorean triples (a,b,c) can be parametrized

by

$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2}$$

for odd, relatively prime $s, t \in \mathbb{N}$.

Q: Which integers n can appear as c

in some Pythagorean triple (a,b,c)?

Theorem The hypotenuse c in a primitive

Pythagorean triple (a,b,c) is a product

of primes $p \equiv 1 \pmod 4$.

Pf: By the above, $2c = s^2 + t^2$ for some relatively prime $s, t \in \mathbb{Z}$ so by our characterization of sums of two squares, c is a product of primes $p \equiv 1 \pmod 4$. $\square$

Ex Let $c = 2210 = 2 \cdot 1105$.

By an example above,

$$1105 = 33^2 + 4^2$$

so $$2210 = (1^2 + 1^2)(4^2 + 33^2)$$

$$= (1 \cdot 4 + 1 \cdot 33)^2 + (1 \cdot 33 - 1 \cdot 4)^2$$

$$= \underbrace{37}_{s}{}^2 + \underbrace{29}_{t}{}^2 .$$

Then $1105 = \dfrac{37^2 + 29^2}{2}$ is the hypotenuse in the triple

$$(a,b,c) = \left(37 \cdot 29,\ \frac{37^2 - 29^2}{2},\ \frac{37^2+29^2}{2}\right)$$

$$= (1073,\ 264,\ 1105).$$

Next time: sums of divisors.