Lecture 10.1

Last time:

- We can decide whether $x^2 \equiv a \pmod{p}$ has solutions using the symbol

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \equiv \begin{cases} 1, & \text{if solutions exist} \\ -1, & \text{if no solution exists} \end{cases}$$

and the following laws of quadratic reciprocity.

- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}$

- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv \pm 1 \pmod 8 \\ -1, & p \equiv \pm 3 \pmod 8 \end{cases}$

- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv 1, 7 \pmod 8 \\ -1, & p \equiv 3, 5 \pmod 8 \end{cases}$

- For any distinct odd primes p and q,

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

Sums of Squares

Question: Which numbers n are of the form $n = x^2 + y^2$ for $x, y \in \mathbb{Z}$?

How do you think we can approach this

question using what we've developed so far?

One strategy is to list the numbers $n - x^2$ for $x = 0, 1, 2, \ldots$ until you get a perfect square or $n - x^2 < 0$.

Exercise 1: Explain why it's enough to check if $n - x^2$ is a square for $0 \leq x \leq \sqrt{\frac{n}{2}}$.

Here's some data to help us formulate some guesses:

$1 = 1^2 + 0^2$	11 NO	21 NO	31 NO	$41 = 4^2 + 5^2$
$2 = 1^2 + 1^2$	12 NO	22 NO	$32 = 4^2 + 4^2$	42 NO
3 NO	$13 = 2^2 + 3^2$	23 NO	33 NO	43 NO
$4 = 0^2 + 2^2$	14 NO	24 NO	$34 = 3^2 + 5^2$	44 NO
$5 = 1^2 + 2^2$	15 NO	$25 = 3^2 + 4^2$	35 NO	$45 = 3^2 + 6^2$
6 NO	$16 = 0^2 + 4^2$	$26 = 1^2 + 5^2$	$36 = 0^2 + 6^2$	46 NO
7 NO	$17 = 1^2 + 4^2$	27 NO	$37 = 1^2 + 6^2$	47 NO
$8 = 2^2 + 2^2$	$18 = 3^2 + 3^2$	28 NO	38 NO	48 NO
$9 = 0^2 + 3^2$	19 NO	$29 = 2^2 + 5^2$	39 NO	$49 = 0^2 + 7^2$
$10 = 1^2 + 3^2$	$20 = 2^2 + 4^2$	30 NO	$40 = 2^2 + 6^2$	$50 = 5^2 + 5^2$

What patterns do you spot?

Among the primes, it appears that

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

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

Here's a larger table with primes only:

$2 = 1^2 + 1^2$	31 NO	$73 = 3^2 + 8^2$	127 NO	179 NO
3 NO	$37 = 1^2 + 6^2$	79 NO	131 NO	$181 = 9^2 + 10^2$
$5 = 1^2 + 2^2$	$41 = 4^2 + 5^2$	83 NO	$137 = 4^2 + 11^2$	191 NO
7 NO	43 NO	$89 = 5^2 + 8^2$	139 NO	$193 = 7^2 + 12^2$
11 NO	47 NO	$97 = 4^2 + 9^2$	$149 = 7^2 + 10^2$	$197 = 1^2 + 14^2$
$13 = 2^2 + 3^2$	$53 = 2^2 + 7^2$	$101 = 1^2 + 10^2$	151 NO	199 NO
$17 = 1^2 + 4^2$	59 NO	103 NO	$157 = 6^2 + 11^2$	211 NO

17	$= 1^2 + 4^2$	59	NO	103	NO	157	$= 6^2 + 11^2$	211	NO
19	NO	61	$= 5^2 + 6^2$	107	NO	163	NO	223	NO
23	NO	67	NO	109	$= 3^2 + 10^2$	167	NO	227	NO
29	$= 2^2 + 5^2$	71	NO	113	$= 7^2 + 8^2$	173	$= 2^2 + 13^2$	229	$= 2^2 + 15^2$

Let's prove it.

Theorem For an odd prime p, $p = x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$.

Pf: ($\Rightarrow$) Suppose $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

Since p is odd, one of x, y must be odd and the other even, say $x = 2j$ and $y = 2k+1$.

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

$$= (2j)^2 + (2k+1)^2$$

$$= 4j^2 + 4k^2 + 4k + 1$$

$$\equiv 1 \pmod 4. \quad \square$$

Alternative proof: If $p = x^2 + y^2$ then

$x^2 \equiv -y^2 \pmod p$, so

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

This implies $p \equiv 1 \pmod 4$. $\square$

Why doesn't the reciprocity law for $\left(\frac{-1}{p}\right)$ give a proof of ($\Leftarrow$)? Let's see.

Pf: ($\Leftarrow$) Let $p \equiv 1 \pmod 4$ be prime. By the reciprocity law for $\left(\frac{-1}{p}\right)$, we know -1 is a square mod p, say $x^2 \equiv -1 \pmod p$.

Unfortunately, all this says is that

$$pm = x^2 + 1 \text{ for some } m \in \mathbb{N},$$

but maybe this is a step in the right direction.

Notice that

$$m = \frac{x^2+1}{p} \leq \frac{(p-1)^2+1}{p} = \frac{p^2-2p+2}{p}$$

$$= p - \frac{2p-2}{p} < p.$$

Claim: given $x^2 + y^2 = pm$ for some $x, y, m \in \mathbb{N}$, if $1 < m < p$, then we can find $x_1, y_1, m_1 \in \mathbb{Z}$ with $1 \leq m_1 < m$ and $x_1^2 + y_1^2 = pm_1$.

Exercise 2: How would you discover this pattern for yourself? Here are a couple things to investigate to get you on the right track:

(a) If $p = x^2 + y^2$, then any square times p is also a sum of squares.

(b) If $m = x^2 + y^2$ and $n = z^2 + w^2$, then mn is also a sum of squares, namely

$$mn = (xu + yb)^2 + (xv - yu)^2.$$

(c) If $n = x^2 + y^2$ then <u>some</u> prime dividing n is congruent to $1 \bmod 4$.

Notice that we already have a solution $x^2 + 1^2 = pm$ for some m, so we need only "descend" this by

$$x_1^2 + y_1^2 = pm_1 \qquad m_1 < m$$

$$x_2^2 + y_2^2 = pm_2 \qquad m_2 < m_1$$

$$\vdots$$

$$x_k^2 + y_k^2 = p \qquad 1 < m_{k-1}$$

to obtain a solution.

This turns out to be rather involved,

so let's go through slowly.

Starting with $x^2 + y^2 = pm$, $m > 1$,

choose $-\frac{m}{2} \leq u, v \leq \frac{m}{2}$ satisfying

$$u \equiv x \pmod{m}, \quad v \equiv y \pmod{m}.$$

Then $u^2 + v^2 \equiv x^2 + y^2 \pmod{m}$, so

$$x^2 + y^2 \equiv pm$$

and $$u^2 + v^2 = mr$$

with $0 \leq r < m$. (Why?)

Next, let's multiply these two sums of squares to get a new sum of squares (by Exercise 2(b) above):

$$pm^2 r = (x^2 + y^2)(u^2 + v^2)$$

$$= (xu + yv)^2 + (xv - yu)^2,$$

Notice that

$$xu + yv \equiv x^2 + y^2 \equiv 0 \pmod{m}$$

$$xv - yu \equiv xy - yx \equiv 0 \pmod{m}.$$

So we can divide through by m^2 to get

$$pr = \left(\frac{xu+yv}{m}\right)^2 + \left(\frac{xv-yu}{m}\right)^2.$$

Set $x_1 = \frac{xu+yv}{m}$, $y_1 = \frac{xv-yu}{m}$

and $m_1 = r$.

We finish by showing $m_1 > 0$.

If $r = m_1 = 0$, then $u^2 + v^2 = 0$,

forcing $u = 0$ and $v = 0$, and

$x \equiv 0 \pmod{m}$ and $y \equiv 0 \pmod{m}$

$x \equiv 0 \pmod{m}$ and $y \equiv 0 \pmod{m}$.

Then m^2 divides $x^2 + y^2 = pm$, which means m divides p.

But we started with $1 < m < p$, so this is impossible.

Therefore $1 \leq r = m_1 < m$ and we're done. □

Ex $p = 17$ is a sum of squares:

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

Ex $p = 19$ is not a sum of squares.

Ex $p = 73$ is a sum of squares;

let's use descent to find

$$x^2 + y^2 = 73.$$

First, $x^2 \equiv -1 \pmod{73}$ has a solution, $x = 27$.

Note: you can find this in a few ways:

- brute force, i.e. check x^2 for $x \equiv 0, 1, \ldots, 36$
- find the first $x^2 + 1$ divisible

by 73

- find the first multiple of 73 which is 1 more than a square

- compute $a^{\frac{p-1}{4}} \pmod p$ until you find one $\equiv -1 \pmod p$, then take $x \equiv a^{\frac{p-1}{8}}$.

This gives us

$$27^2 + 1 = 730 = 73 \cdot 10$$

so we want $-5 \leq u, v \leq 5$ which satisfy $u \equiv 27 \pmod{10}$

$$v \equiv 1 \pmod{10}$$

$\rightsquigarrow$ use $u = -3, v = 1.$

By the descent algorithm, we should have $x_1^2 + y_1^2 = 73m_1$ for $m_1 < 10$,

where $$x_1 = \frac{27(-3) + 1 \cdot 1}{10} = -8$$

$$y_1 = \frac{27 \cdot 1 - 1(-3)}{10} = 3$$

Indeed, $(-8)^2 + 3^2 = 73$ so we got it after one descent step!

Exercise 3: Express each of the following as a sum of two squares, if possible:

(a) 59 (b) 61 (c) 89

(d) 373 (e) 657

hint: factor it first

Next time: composite sums of squares.