Sums of 2 squares.

Method of descent:

If \( p = 1 \mod 4 \) is prime, we want to write \( p = a^2 + b^2 \).

**Step 1:** Find \( a^2 + b^2 = mp \).

**Step 2:** Descent - an algorithm to
find \( (a')^2 + (b')^2 = m'p \)

\[ m' \leq \frac{m}{2}. \]
Repeat until you find $p = x^2 + y^2$.

Exercise 1 - (2) - (3): follow method of descent, given a starting equation.

To do this: $a^2 + b^2 = mp$

\[ u \equiv a \mod m \quad v \equiv b \mod m \]

\[-\frac{m}{2} < u, v \leq \frac{m}{2} \]

\[ (u - iv)(a + bi) = c + di \]

\[ N(c + di) = c^2 + d^2 = N(u - iv)N(a + bi) = m^2 \sqrt[p]{p} \]
\[ a' = \frac{c}{m}, \quad b' = \frac{p}{m} \]

\[ N(a' + b'i) = (a')^2 + (b')^2 = r \quad \text{for } a', b' \text{ are both integers} \]

Do Ex 1, part (2) - (5) now!

(2) \[ 11^2 + 1^2 = 2.61 \]

**Example:** \[ 11^2 + 1^2 = 2.61 \]

So take \( u = 11 \mod 2 \quad v = 1 \mod 2 \)

\(-1 < u, v < 1 \quad (c = \frac{m}{2}) \]

\[ \Rightarrow u = 1, \quad v = 1 \]

\[ (1 - i)(11 + i) = 12 - 10i \]
\[
\frac{12 - 10i}{i} = 6 - 5i
\]

\[
6^2 + (-5)^2 = 61 \quad \checkmark
\]

\[
a^2 + b^2 = 17 \cdot 881
\]

\[
u = \frac{a}{\sqrt{2}} \equiv 17 \quad v = \frac{b}{\sqrt{2}} \equiv 17
\]

\[-\frac{\sqrt{2}}{2} < u, v \leq \frac{\sqrt{2}}{2} \quad \frac{\sqrt{2}}{2} = 8.5
\]

\[
\Rightarrow \quad u = -1 \quad v = 4
\]

\[
(-1 - 4i)(84 + 89i) = (-84 + 4 \cdot 89) + (-89 - 4 \cdot 89)i
\]

\[= 272 + (425)i \]

Given: 16 - 25i
\[ 16^2 + (-25)^2 = 881 \]  

**Announcement:** Next week \((12, 14)\) is the last material for the final. The final will be cumulative. On April 26th, review in class. Before then, I'll post template/info like for midterm.

April 19, 21 we'll cover an optional topic (Elliptic curve cryptography). Quizzes and assignment -- bonus points.
To find $a^2 + b^2 = n_0$.

Suffice to find $a$ s.t. $a^2 = -1 \mod p$,

then $a^2 + 1^2 \equiv 0 \mod p$ ($a^2 + 1^2 = n_0$).

So we can take $b = 1$.

Since $p \equiv 1 \mod 4$, we know there exists a square root of $-1 \mod p$.

How to find it?

① Guess till you find it.

② If you know primitive root $g$ mod $p$. 
Then FACT: \( g^{\frac{p-1}{4}} \) is a square root of \(-1 \mod p\).

1. (a) - justify this fact.

1. (b) - use this in a specific case to find \( a^2 + b^2 = \pm p \). 
\[
\begin{align*}
(a^2 + 1^2 & = \pm p) \\
(5^2 + 1^2 & = \pm 63)
\end{align*}
\]

(5) - (a) \( 5^{18} \) - compute it \( \mod 73 \). The whole thing,

i.e., take \( a^2 \) to be the smallest integer
In a field, to check 

\[ \alpha = -1, \text{ if sufficient to check that } \alpha^2 = 1 \text{ and } \alpha \neq 1. \]

Apply to \( \alpha = \alpha^2 \). \( a = y^{p-1} \).

To check \( \alpha^2 \neq 1 \) need to use that \( \alpha \) is a primitive root.
\[ \alpha = q^2 + 1 \]

\[ N(2) = n \]

\[ M(2i) \leq M(2) \Rightarrow \frac{N(2)}{2} = 2. \]

Draw circles of radius \( \sqrt{2} \) at each pink point. You cover everything.
This doesn't work in \( \mathbb{Z} \) [W.S.].

Suppose \( a^2 + b^2 = mp \), \( p \equiv 1 \mod 4 \), suppose \( p \neq m \).

\[
N(\alpha + \beta i) = mp.
\]

\[
(a + bi)(a - bi) = mp.
\]

\[
p = (x + yi)(x - yi)
\]

\[
x^2 + y^2 = p.
\]

So, \( x + bi \) (resp. \( x - yi \)) has to be factor of one of the LHS.