Sums of 2 squares.

Method of descent:

If $p \equiv 1 \pmod 4$ is prime

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: · $a^2 + b^2 = mp$

· $u \equiv a \bmod m \qquad v \equiv b \bmod m$

$$-\frac{m}{2} < u, v \leq \frac{m}{2}.$$

· $(u - iv)(a + bi) = c + di$

$$N(c + di) = c^2 + d^2 = N(u - iv)N(a + bi) = m^2 r p$$

$r \leq \frac{m}{2}$.

$$a' = \frac{c}{m} \qquad b' = \frac{d}{m}$$

$N(a' + b'i) = (a')^2 + (b')^2 = rp$, a', b' are both integers.

Do Ex 1, parts (2) - (3) now! (2) $11^2 + 1^2 = 2 \cdot 61$

Example: $\overset{a}{11}^2 + \overset{b}{1}^2 = \overset{m}{2} \cdot \overset{p}{61}$

So take $u \equiv 11 \mod 2$ $\quad v \equiv 1 \mod 2$

$-1 < u, v \leq 1 \quad (1 = \frac{m}{2}$

$\Rightarrow u = 1 \qquad v = 1$

$(1 - i)(11 + i) = 12 - 10i$

$$\frac{12-10i}{2} = 6-5i$$

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

$$\overset{a}{84}^2 + \overset{b}{89}^2 = \overset{m}{17} \cdot \overset{p}{881}$$

$$u \equiv 84 \pmod{17} \qquad v \equiv 89 \pmod{17}$$

$$-\frac{m}{2} < u, v \leq \frac{m}{2} \qquad \frac{m}{2} = 8.5$$

$$\Rightarrow u = -1 \qquad v = 4 \qquad (5 \cdot 17 = 85)$$

$$(\overset{u}{-1} - \overset{vi}{4i})(\overset{a}{84} + \overset{bi}{89i}) = (-84 + 4 \cdot 89) + (-89 - 4 \cdot 84)i$$

$$= 272 + (-425)i$$

$\sqrt{17}$ gives $16-25i$

$16^2 + (-25)^2 = 881$ ✓

Announcement: Next week (12, 14) is the last material for the final.

- The final will be cumulative
- On April 26th review in class (April 28th)

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 $a^2 + b^2 = np$.

Suffices to find a s.t. $a^2 \equiv -1 \bmod p$

Then $a^2 + 1^2 \equiv 0 \bmod p$ $(a^2 + 1^2 = np)$.

So can take $b = 1$.

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

how to find it?

① Guess till you find it.

② If you know primitive root $g \bmod p$.

Then FACT: $g^{\frac{p-1}{4}}$ is a square root of $-1 \bmod p$.

1.(4) – justify this fact.

1.(5) – use this in a specific case to find $a^2+b^2 = np$.
$(a^2+1^2 \equiv np)$

---

(5)-(a) $5^{13} \sim$ compute it mod 73.
the cube has
i.e. take a s.t. be the smallest integer
$\equiv 5^{19}$ and 73.

(4) In a field, to check

$\alpha = -1$, it suffices to

check that $\alpha^2 = 1$ and $\alpha \neq 1$.

Apply to $\alpha = a^2$. $a = g^{\frac{p-1}{4}}$.

To check $a^2 \neq 1$ need to use

that g is a <u>primitive root</u>.

.