Math 4400
Week 12 - Tuesday
Sums of two squares and descent.

Question: which integers n can be written as sums of 2 squares?

$$n = a^2 + b^2, \quad a, b \in \mathbb{Z}?$$

Example: $10 = 3^2 + 1^2$ ✓, but there's no way to get 19 x.

We will give a complete answer this week.
— interestingly, it is intimately related to unique factorization in $\mathbb{Z}[i]$.

Simple observations:
If $n = a^2 + b^2$, then
- $n \geq 0$ $(a^2, b^2 \geq 0)$
- $n \equiv 0, 1,$ or $2 \bmod 4$.
  $a^2, b^2 \equiv 0$ or $1 \bmod 4$.

A more interesting observation:

Theorem: If m and n are each sums of 2 squares, then so is their product mn.

Proof: If $m = a^2 + b^2$ $\quad n = c^2 + d^2$

$m = N(a+bi) \quad n = N(c+di)$

$N(x+yi) = x^2 + y^2 = (x+yi)(x-yi)$

$mn = N(a+bi)N(c+di)$

$mn = N((a+bi)(c+di))$

$= N(ac - bd + (ad+bc)i)$

$= (ac-bd)^2 + (ad+bc)^2$

Example: $5 = 2^2 + 1^2 = N(2+i)$

$13 = 3^2 + 2^2 = N(3+2i)$

so $65 = 5 \cdot 13 = N(2+i)N(3+2i)$

$= N((2+i)(3+2i))$

$= N(4+7i) = 4^2 + 7^2.$

Since every n is a product of primes, suggest we should first ask:

Which primes are sums of 2 squares?

Example: Recall – Week 1, Exercise 3

You noticed that for $p < 100$ prime,

$p = a^2 + b^2 \iff \underset{=1^2+1}{p = 2}$ or $p \equiv 1 \bmod 4.$

Theorem: If p is prime then $p = a^2 + b^2$ if and only if $p = 2$ or $p \equiv 1 \mod 4$

Necessity by simple observation above

Hard part: If $p \equiv 1 \mod 4$, then $p = a^2 + b^2$.

We will show this by explaining an algorithm to find a and b.

Step 1: Find a, b s.t. $a^2 + b^2 = mp$

Step 2 (Descent): Modify a, b to get a', b' with $a'^2 + b'^2 = m'p$, $m' < m$.

(Repeat until $m' = 1$)

Step 1: Find a, b s.t. $a^2 + b^2 = mp$

$\Leftrightarrow$ $a^2 + b^2 \equiv 0 \mod p$

Since $p \equiv 1 \mod 4$, there is a square root of -1 in $\mathbb{F}_p$,

i.e. there is an integer a s.t. $a^2 \equiv -1 \mod p$.

So

$$a^2 + 1^2 \equiv 0 \mod p$$

i.e. can take $b = 1$.

Example: $5^2 \equiv -1 \bmod 13$. $5^2 + 1^2 = 2 \cdot 13$.

Step 2 (Descent): Modify a, b to get a', b' with $a'^2 + b'^2 = m'p$, $m' < m$.

Have $a^2 + b^2 = mp$. Want to "factor out m". but need to stay in integers.

Trick: multiply $a+bi$ by a Gaussian integer to get something bigger where can factor out m.

Take $-\frac{m}{2} < u, v \le \frac{m}{2}$ s.t. $u \equiv a \bmod m$
$v \equiv b \bmod m$.

$u^2 + v^2 = m \cdot r$. Note $mr = u^2 + v^2 \le \frac{m^2}{4} + \frac{m^2}{4}$

(i.e. $u^2 + v^2 \equiv 0 \bmod m$
$u^2 + v^2 \equiv a^2 + b^2 \equiv 0 \bmod m$)

$mr \le \frac{m^2}{2}$ divide by m.

so $r \le \frac{m}{2}$.

$$N((u - iv)(a + ib)) = N(u - iv)N(a + ib) = m^2 r p.$$

$$(u - iv)(a + ib) = (au + vb) + (ub - va)i$$

$(au + vb)^2 + (ub - va)^2 = m^2 rp$

$5^2 + 1^2 = 2 \cdot 13$ $m=2$

$u = 1$, $v = 1$ ($-1 < u, v \le 1$ so u, v 0 or 1).

$(1 - i)(5 + i) = 6 - 4i$

$\}$ divide by $m = 2$.

$3 - 2i$

$N(3-2i) = 3^2 + 2^2 = 13$!

In general, set $a' = \dfrac{au+vb}{m}$ $\quad b' = \dfrac{ub-va}{m}$

from above $a'^2 + b'^2 = rp$.

integers because

$$au+vb \equiv a\cdot a + b\cdot b \mod m$$
$$\equiv a^2 + b^2 \mod m.$$
$$\equiv 0 \mod m$$

i.e. $m \mid au+vb$.

$$ub - va \equiv ab - ba$$
$$\equiv 0 \mod m.$$

so $m \mid ub - va$.

Now,

$$a'^2 + b'^2 = N(a'+b'i)$$
$$= N\left(\frac{(u-iv)(a+ib)}{m}\right)$$
$$= \frac{m^2 rp}{m^2} = rp, \quad r < m \checkmark.$$

If $r > 1$, repeat descent to get smaller r till you land at p.

Example: $9^2+7^2=130=10\cdot 13.$

Use to express 13 as a^2+b^2:

$a=9 \quad b=7 \quad p=13.$

$m=10 \qquad -5 < u, v \leq 5$

$u \equiv 9 \bmod 10 \Rightarrow u=-1$

$v \equiv 7 \bmod 10 \Rightarrow v=-3$

$$(u-vi)(a+bi) = (-1+3i)(9+7i)$$
$$= -30+20i$$

$\Big\downarrow$ div by 10

$$= -3+2i \rightsquigarrow (-3)^2+2^2=13.$$

Next time: We'll see this is the Euclidean algorithm in $\mathbb{Z}[i]$, and use that to understand exactly which n are sums of 2 squares.