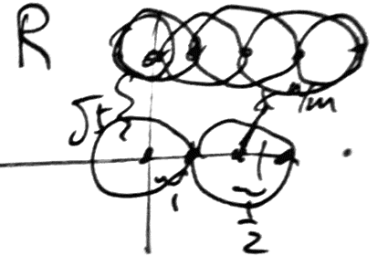
Recall: Know Euclidean algorithm (in $\mathbb{Z}$ & $\mathbb{Z}[i]$ & not in $\mathbb{Z}[\sqrt{-5}]$, $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$ but $2 \nmid (1+\sqrt{-5})$ & $2 \nmid (1-\sqrt{-5})$).

No "good" division algorithm: $\exists\, n = mq + r$. (in $R = \mathbb{Z}[\sqrt{-5}]$).

Given n & $m \neq 0$, try to find q & r with $N(r) < N(m)$.

where $N(x+\sqrt{-5}y) = |x+\sqrt{-5}y|^2 = x^2+5y^2$. In $\mathbb{Z}[i]$, looked at $\frac{n}{m}$, took q to be "nearest" element of R.



$\left|\frac{n}{m} - q\right|$ could be as large as $\sqrt{\frac{1}{2^2} + \left(\frac{\sqrt{5}}{2}\right)^2} = \sqrt{\frac{6}{4}} > 1$.

So if $|r| = |n - mq| = |m| \cdot \underbrace{\left|\frac{n}{m} - q\right|}_{>1}$.

In a general ring R, the group of units $R^\times = \{u \in R \mid \exists v \in R : uv = 1\}$.

Def: An element $r \in R$ is irreducible if $b \mid r \Rightarrow \begin{cases} b = \text{unit} \\ \text{or} \\ b = \text{associate to } r \end{cases}$

Def: Two elements r & $s \in R$ are associates if $\exists\, u \in R^\times$ s.t. $r = us$.

Exercise 1: Prove that $R^\times$ is a group. (Prove $u, v \in R \Rightarrow u \cdot v \in R$ & $u \in R \Rightarrow u^{-1} \in R$.)

Exercise 2: Are $2+i$ & $2-i$ associates in $\mathbb{Z}[i]$?

Def: An element $r \in R$ & $r \notin R^\times$ is prime if: $r \mid s \cdot t \Rightarrow r \mid s$ or $r \mid t$.

So in $R = \mathbb{Z}[\sqrt{-5}]$, 2 is irreducible But 2 is not prime.

All the way back to: Which primes are sums of two squares? Already know: If $p \equiv 3 (4)$, then $p \neq x^2 + y^2$.

Claim: Every $p \equiv 1 (4)$ is a sum of two squares.

Ex: $p = 17 (= 4^2 + 1^2)$.

x	1	2	3	4	5	6	7	8	9	10
$x^2 \pmod{17}$	1	4	9	16	8	2	15	13	13	15

(-8, -7, 11, 11)

So: squares mod 17 are: $1, 2 (=6^2), 4, 8 (=5^2), 9, 13, 15, 16$.

Lemma: Mod any prime, half of the numbers (excluding 0) are "quadratic residues" i.e. $\#\{n \bmod p \mid n \neq 0 \ \& \ \exists x : x^2 \equiv n \pmod p\} = \frac{1}{2}(p-1)$

Ex: $p=7$. Who are the squares? There will be $\frac{7-1}{2} = 3$ squares.

x	1	2	3	4	5	6
x^2	1	4	2	2	4	1

"2 is a quadratic residue mod 7 because $\exists x (=3)$ with $x^2 \equiv 2 \pmod 7$.

We say that 3 is a "quadratic non-residue" mod 7, No solution to $x^2 \equiv 3 \bmod 7$.

---

pf of Lemma: Clear that $(-x)^2 \equiv (x)^2$ so list of squares must be a palindrome. So we can only see at most half the numbers among the squares. But why no other repeats / collisions?. What is a collision? If $x^2 \equiv y^2 \pmod p$, $\Rightarrow x^2 - y^2 \equiv 0 \ (p)$.

Then $(x+y)\cdot(x-y) \equiv 0 \ (p)$. $\Rightarrow p \mid (x+y)\cdot(x-y)$.

$\Rightarrow [p \mid x+y$ or $p \mid x-y.] \Rightarrow [\underbrace{x+y \equiv 0 \ (p)}_{\Downarrow\ x \equiv -y \ (p).}$ OR $\underbrace{x-y \equiv 0 \ (p)}_{\Downarrow\ x \equiv y \ (p).}]$.

So all squares in the first half are distinct!

Remember FLT: If $a \not\equiv 0 \ (p)$, then $a^{p-1} \equiv 1 \ (p)$.

For p odd, $p-1$ is even, so $\frac{p-1}{2} \in \mathbb{Z}$ what is $a^{\frac{p-1}{2}} \pmod p$?.

Ex: Back to $p=7$, Table of x^3:

x	1	2	3	4	5	6
x^3	1	1	−1	1	−1	−1
					" $(-2)^3$	" $(-1)^3$

Since $(-x)^3 = -(x^3)$, this table is anti-palindromic.

Notice: $\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \Rightarrow$ $a^{\frac{p-1}{2}} = 1$ or -1.

$\frac{p-1}{2}$	$p=7$

Which a have $a^{\frac{p-1}{2}} \equiv 1$, not -1. Here: $\{1, 2, 4\}$.

Fact: $a^{\frac{p-1}{2}} \equiv 1 \iff a$ is a quadratic residue.

Exercise 3: Make a table of $\left(p=17,\ \frac{p-1}{2}=8\right)$,

X	1	2	3	...
$(\mathrm{mod}\ 17)\cdot X^8$			-1	

$3,\ 3^2=9,\ 3^4=13,\ 3^8=13^2=-1.$

Back $p\equiv 1\ (4)$, how to write them as sums of $x^2+y^2=p$?

Ex: $p=17$, Step 1: Find quadratic non-residue, e.g. $a=3$.

So $3^{\frac{p-1}{2}}=-1$. so let $z=3^{\frac{p-1}{4}}=13$. Then.

$z^2=\left(a^{\frac{p-1}{4}}\right)^2=a^{\frac{p-1}{2}}\equiv -1\ (\mathrm{mod}\ p)$. I.e. $z^2+1\equiv 0\ (\mathrm{mod}\ p)$.

So $z^2+1=p\cdot k$. in $\mathbb{Z}$. But in $\mathbb{Z}[i]$, $(z+i)(z-i)=p\cdot k$.

To find common factor; Apply Euclidean Algorithm to $(z+i)$ and p.

__Ex:__ $p=17$, $a=3$, $z=13$, $13^2+1=170=p\cdot 10$.

Use Euclidean Alg on $(13+i)$ & 17. $\quad n = m q_1 + r_1$, $n = 17$, $m = 13+i$

$$\frac{(17)(13-i)}{(13+i)(13-i)} = \frac{221-17i}{170} \approx 1 = q_1. \qquad 17 = (13+i)\cdot 1 + r_1.$$

$r_1 = \boxed{4-i}$, $\quad 13+i = (4-i)q_2 + r_2$, $r_2 = 0$.

$$\frac{(13+i)(4+i)}{(4-i)(4+i)} = \frac{52-1+17i}{17} = 3+i = q_2.$$

$r_1 = \gcd(13+i, 17)$.

So $4-i \mid 17 \Rightarrow 17 = (4+i)(4-i) = 4^2+1^2$.

So step 2: let $z = a^{\frac{p-1}{4}}$ & find $\gcd(z+i, p)$. DONE.

Take $p = 55{,}497{,}159{,}953$. Let $a = 21{,}345$. So that $a^{\frac{p-1}{2}} \equiv -1 \ (p)$. Let $z = a^{\frac{p-1}{4}} = 4{,}334{,}787{,}849$.

$\gcd(z+i, p) = 235{,}532 + i\,4673$. & $235532^2 + 4673^2 = p$!!!