Recall: $n = x^2 - xy + y^2 = N(x + \omega y)$.

Which n are represented?

Lemma: If $n \equiv 2 \pmod 3$, then $n \neq x^2 - xy + y^2$.

Pf: Look mod 3 at all values / as x & y range.

Theorem: If $p \equiv 1 (3)$ is prime, then $\exists\, x, y \in \mathbb{Z}$ s.t. $p = x^2 - xy + y^2$.

Not only do x & y exist, but they can be determined efficiently.

Step 1: Find $z \neq 1$ s.t. $z^3 \equiv 1 \pmod p$.

How to find z? Look at $a^{\frac{p-1}{3}}$. If $\neq 1$,

then $z = a^{\frac{p-1}{3}}$ satisfies $z^3 = \left(a^{\frac{p-1}{3}}\right)^3 = a^{p-1} \equiv 1 (p)$.

$z^3 - 1 = 0 \iff z^3 = 1$ Maybe there should be 3 roots,

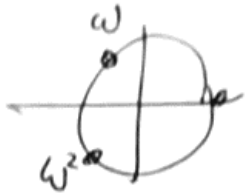
Last time: Looked at tables of $a^{\frac{p-1}{3}} \pmod p$ as a ranges mod p.

Π

Ex: $p = 43$. $\frac{p-1}{3} = 14$

a	1	2	3	4	5	6	7	8	9	10	11
a^{14}	1	1	36	1	36	36	6	1	6	36	1

$36 \equiv -7 \bmod 43$ z.



If $a^{\frac{p-1}{3}} = z \neq 1$, then $z^3 = 1$.

There are 3 solutions to $z^3 = 1$, $z = 1, 6, 36$.

$(36)^3 = (6^2)^3 = (6^3)^2 \equiv 1$.

How likely is it to find such an a with $a^{\frac{p-1}{3}} \equiv 6$ or 36?

I.e. $\#\{a \neq 0 \bmod p \mid a^{\frac{p-1}{3}} \neq 1 \ (p)\} = \frac{2}{3}(p-1)$.

Why? When $p = 43$ & $\frac{p-1}{3} = 14$, how many a's have $a^{14} - 6 \equiv 0 \pmod p$?

Answer: 14 values of a.

$\{a : a^{14} \equiv 6 \bmod 43\} = \{7, 9, 13, 14, 15, 17, 18, 25, 26, 28, 29, 30, 34, 36\}$

$\# \uparrow = 14$.

How many a's have $a^{14} \equiv 36 \bmod 43$?

Again we will have 14 such values of a.

So total $14+14 = 28$ values out $42 = p-1$

($\frac{2}{3}$ of the a's) have $a^{\frac{p-1}{3}} \equiv 6$ or 36 $\not\equiv 1$.

$z^3 \equiv 1$ has 3 roots

---

once we have such a $z_1 \equiv 6$.

Know: $z^3 - 1 \equiv 0 \bmod p$.

$\Rightarrow z^3 - 1 = p \cdot k$ for some $k \in \mathbb{Z}$.

(Ex: $6^3 - 1 = 215 = 43 \cdot 5$)

over $\mathbb{Z}[\omega]$ polynomial $z^3 - 1 = (z-1)(z^2+z+1)$

$= (z-1)(z-\omega)(z-\bar{\omega})$.

$\rightarrow 6^3 - 1 = (6-1)(6^2+6+1)$.

$= 5 \cdot (43)$

In general, $z^3 - 1 = (z-1)(z-\omega)(z-\bar{\omega}) = p \cdot k$.

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

& $z \neq 1 \pmod p$, & in $\mathbb{Z}$, p is prime.

So $z-1 \mid k$. $\Rightarrow (z-1)(z^2+z+1) = p \cdot k$.

Say. $k = (z-1) \cdot \ell$ $\Rightarrow z^2+z+1 = p \cdot \ell$ in $\mathbb{Z}$.

k: 5, $z-1$: 6, ℓ: 1, p: 43, ℓ: 1.

In $\mathbb{Z}[\omega]$, $(z-\omega)(z-\bar{\omega}) = p \cdot \ell$.

Does $p \mid z-\omega$ or $p \mid z-\bar{\omega}$? No

If $p \mid z-\omega$, then $z-\omega = (c+d\omega) \cdot p$.

$= p \cdot c + p \cdot d\omega$

$\Rightarrow p \cdot c = z$, & $p \cdot d = -1$.

But $p \mid (z-\omega)(z-\bar{\omega}) \Rightarrow p$ is not prime,

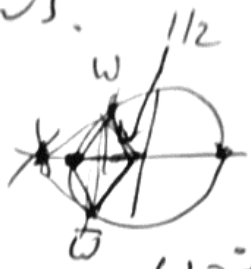
If $p = (x+y\omega)(x+y\bar{\omega}) = x^2 - xy + y^2$.

So the components $x+y\omega$ must divide one of $z-\omega$ or $z-\bar{\omega}$.

Last Step (Step 2): $GCD_{\mathbb{Z}[\omega]} = (p, z-\omega)$.

Ex: $GCD(\mathbb{Z}_{43}, 6-\omega)$.

Recall: $n = qm + r$, $\frac{n}{m} \sim q \in \mathbb{Z}[\omega]$.



$\omega = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$

For us $43 = q(6-\omega) + r$.

$$\frac{n}{m} = \frac{43}{(6-\omega)} \frac{(6-\bar{\omega})}{(6-\bar{\omega})} = \frac{43\cdot(6-\bar{\omega})}{36 - 6\omega - 6\bar{\omega} + 1}$$

$\omega + \bar{\omega} = -1$

$$= \frac{43\cdot(6-\bar{\omega})}{43} = q. \quad \begin{matrix} -6(\omega+\bar{\omega}) \\ +6 \end{matrix}$$

So $q = 6 - \bar{\omega}$ & $r = 0$.

$\Rightarrow$ $m = GCD = 6-\omega = \gcd(43, 6-\omega)$

So $43 = x^2 - xy + y^2$ where $\boxed{\begin{matrix} x = 6 \\ y = -1 \end{matrix}}$

$p = (x+y\omega)(x+y\bar{\omega})$.

New example: $p = 97$. $\frac{p-1}{3} = 32$

a	1	2	3	4	
a^{32}	1	35	35	61	

How many $a \not\equiv 0 \bmod p$ have $a^{32} \equiv 35 \pmod{97}$?

Ans: 32 a's with $a^{32} \equiv 35$

& how many a's with $a^{32} \equiv 61 \bmod 97$?

again 32,

So total # a's with $a^{32} \neq 1 \ (\equiv 35, 61)$

is: $64 = \frac{2}{3} \cdot 96 = \frac{2}{3}(p-1)$.

Step 1: Find a s.t. $a^{\frac{p-1}{3}} \neq 1$, say

$a = 2$, set $z = a^{\frac{p-1}{3}} = 35$. (in $\mathbb{Z}/p$).

Then $z^3 \equiv 1 \ (p)$. $\Rightarrow$ $z^3 - 1 \equiv 0 (p)$.

$(z^3-1) = (z-1)(z^2+z+1) = p \cdot k$.

$\|$ 4087 $\quad$ 34 $\cdot (\quad) = 97 \cdot 442$.

$\Rightarrow$ divide out $z-1$ from LHS & k on RHS.

$(z^2+z+1) = 97 \cdot 13$ (in $\mathbb{Z}$).

in $\mathbb{Z}[\omega]$: $(z-\omega)(z-\bar{\omega}) = 97 \cdot 13$.

Step 2: Find GCD of $p = 97$ & $35-\omega$.

$n = qm + r$.

$97 = q_1(35-\omega) + r_1$.

Look at $\dfrac{(97)}{(35-\omega)}\dfrac{(35-\bar{\omega})}{(35-\bar{\omega})} = \dfrac{3395 - 97\bar{\omega}}{35^2+35+1}$.

$= \dfrac{3395 - 97\bar{\omega}}{1261} \approx 3 = q$.

$\omega^2+\omega+1=0$.

$\bar{\omega} = \omega^2 = -\omega - 1$.

$\Rightarrow 97 = 3(35-\omega) + r$.

$r_1 = -8 + 3\omega$.

$N(x+y\omega) = x^2 - xy + y^2$.

$35 - \omega = q_2(-8+3\omega) + r_2$

$\dfrac{(35-\omega)(-8+3\bar{\omega})}{(-8+3\omega)(-8+3\bar{\omega})} = \dfrac{-280 + 105(-\omega-1) + 8\omega - 3}{64 - (-8)\cdot 3 + 9}$

$= \dfrac{-388 - 97\omega}{97} = -4 - \omega = q_2$.

$r_2 = 0$.

$\Rightarrow GCD(97, 35-\omega) = -8+3\omega$

$\Rightarrow$ $\boxed{97 = x^2 - xy + y^2 = N(x+y\omega)}$

where $x = -8$

$y = 3$.

Recap: To solve $p = N(x+y\omega) = x^2 - xy + y^2$:

Step 1: Go to $\mathbb{Z}/p$ & find a s.t.

$a^{\frac{p-1}{3}} \neq 1$ (66% chance).

& set $z \equiv a^{\frac{p-1}{3}} \pmod{p}$.

Step 2: $GCD_{\mathbb{Z}[\omega]}(p, z-\omega) = x + y\omega$.

Then $x^2 - xy + y^2 = p$.

Next set of ideas: Worked great for

$x^2 + y^2$, $x^2 - xy + y^2$

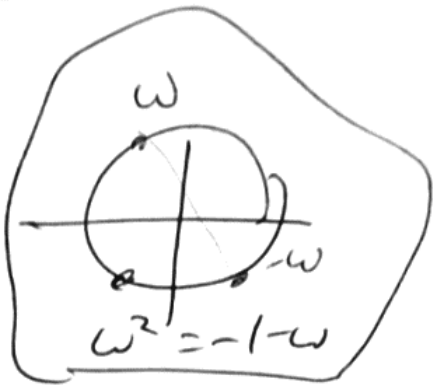
Know: $37 = (6-\omega)(6-\bar{\omega})$

& $97 = (-8+3\omega)(-8+3\bar{\omega})$.

What if $n = 43 \cdot 97 = 3589.4171$

Can we find x & y s.t.

$4171 = 3589 = x^2 - xy + y^2$?



$4337 \cdot 97 = (6-\omega)(6-\bar{\omega})$
$\cdot (-8+3\omega)(-8+3\bar{\omega})$

$= [(6-\omega)(-8+3\omega)][\quad]$

$-48+26\omega-3\omega^2(-1-\omega)$.

$(\underbrace{-45}_{x} + \underbrace{29}_{y}\omega) \mid 3589$

$x^2 - xy + y^2 = 45^2 + 45 \cdot 29 + 29^2 = 4171$.

For general $n = p_1 \cdots p_k$, $p_j \equiv 1 \pmod 3$,
just find representation of each & multiply Eisenstein integers.