Recall:

Tuesday video – Pepin's test for Fermat primes

Thursday video – A version of Lucas-Lehmer

$$M_\ell \text{ is prime} \iff (2+\sqrt{3})^{2^{\ell-1}} \equiv -1 \bmod M_\ell$$

↑ in $\mathbb{Z}[\sqrt{3}]$.

means $= a + b\sqrt{3}$ where

$a \equiv -1 \bmod M_\ell$

$b \equiv 0 \bmod M_\ell$

Exercise 3 explains how to go from this version to the week 7 version.

(Just a computation)

Focus on Exercise 2 for today.

Idea of Ex 2 - do some examples/computations that might help understand ideas in proof for today / last Thursday

---

On Tuesday we did part (1) $p \equiv 3 \bmod 4$

Find a primitive root in $\mathbb{F}_3[i]$ nine elements $\mathbb{F}_p[i]$ field with p^2 elements.

compute discrete log.

Fact: If $\mathbb{F}$ is a field with n elements

then $|\mathbb{F}^\times| = n-1$ $\mathbb{F}^\times$ is a group

So by Lagrange, $a^{n-1}=1$ for any $a \in \mathbb{F}^\times$.

i.e any $a \in \mathbb{F}^\times$ is an $(n-1)$st root of unity. A "primitive root in $\mathbb{F}$" is shorthand for a primitive $(n-1)$st root of unity in $\mathbb{F}$. (i.e $n-1$ is smallest power that gives 1)

Lagrange: If G is a finite group and $a \in G$ then $a^{|G|} = e$ (identity in G)
↑ size of G

Can also say $\operatorname{ord}(a) \mid |G|$

$\operatorname{ord}(a)$ = smallest power s.t. $a^k = e$.

Idea of discrete log: if $\zeta \in \mathbb{F}^\times$ is a primitive root, then any other element of $\mathbb{F}^\times$ is a power of ζ. $a = \zeta^{I(a)} \leftarrow I$ is the discrete log.

$I: \mathbb{F}^\times \to \mathbb{Z}/(n-1)\mathbb{Z}$.

Fact: Any finite field has a primitive root.

$$\{j+k(n-1)\} = \{j\}^{k(n-1)} = \{j\}^{(n-1)^k} = \{j\}$$

---

(2). Show and d in $\mathbb{F}_p$ has a square root in $\mathbb{F}_p[i]$.

($p \equiv 3 \pmod 4$)

$$(a+bi)^2 = (a^2-b^2) + \underline{(2ab)}i$$

To be in $\mathbb{F}_p$ need $2ab = 0$.

So $a=0$ or $b=0$

In (7) "Deduce from (4)" should be S...

a^2 or $(bi)^2 = -b^2$

So elements in $\mathbb{F}_p$ that are squares of elements in $\mathbb{F}_p(i)$ are a^2 or $-a^2$ for a in $\mathbb{F}_p$.

Need to check that for any $c \in \mathbb{F}_p$, either c or $-c$ is a square in $\mathbb{F}_p$

i.e. either $\left(\frac{c}{p}\right) = 1$ or $\left(\frac{-c}{p}\right) = 1$.

Exercises (3) – (7).

The key idea in Pepin's test, and Lucas Lehmer was to use simple criterion for an element in a group to have a order power of 2.

e.g. in Pepin $p = 2^{2^n} + 1$

$$|\mathbb{F}_p^\times| = 2^{2^n}.$$

and you can show 3 has order

$$3^{2^{2^n}-1} \equiv -1 \text{ in } \mathbb{F}_p^\times.$$

LL - $p = M_l = 2^l - 1$ $\quad |\mathbb{F}_p^\times| = 2^l - 2$ not div. by a big power of 2.

$|F_{p^2}^{\times}| = p^2 - 1 = (p+1)(p-1) = 2^k(2^k - 2).$

$p = 2^k - 1$

$(2+\sqrt{3})^{p+1} = 1.$

Can find a "subgroup" of size $p+1$.

(3) – (7) explain how to cut down to a group of size $p+1$.

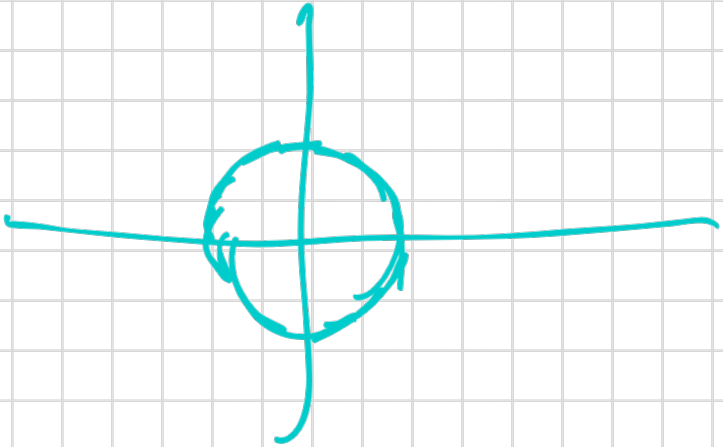
In $\mathbb{C}$ — $N(z) = z\bar{z} = (x+yi)(x-yi) = x^2+y^2$

$z = x + yi$

$N(z) = 1 \iff x^2 + y^2 = 1$

$\iff$ z is on the circle of radius 1 around 0

$e^{i\theta} = \cos\theta + i\sin\theta$



The circle $N(z)=1$ is a subgroup of $\mathbb{C}^\times$.

Euler: $\mathbb{R}/2\pi\mathbb{Z} \xrightarrow{\theta \mapsto e^{2\pi i\theta}} N(z)=1$ ↪ Like discrete log.