Math 4400
Week 11 - Thursday
Mersenne primes

Recall:

Def'n: For l a prime, the corresponding Mersenne number is

$$M_l = 2^l - 1$$

When is M_l prime? (Mersenne primes)

The Lucas-Lehmer test (Week 7) gives a simple way to check.

Today: we give an equivalent statement (see Ex. 3 on worksheet)

Theorem: Let $\alpha = 2+\sqrt{3}$ in $\mathbb{Z}[\sqrt{3}]$.

M_ℓ is prime $\iff$ $\alpha^{2^{\ell-1}} \equiv -1 \bmod M_\ell$
$(\ell > 2)$ (Note $2^{\ell-1} = \frac{M_\ell+1}{2}$)

(Recall Pepin ~ F_n is prime $\iff$ $3^{\frac{F_n-1}{2}} \equiv -1 \bmod F_n$).

Example: $M_3 = 7$. $(2+\sqrt{3})^4 = \left((2+\sqrt{3})^2\right)^2$ ... $7+4\sqrt{3}$

$\equiv (4\sqrt{3})^2 \bmod 7$

$\equiv 48 \bmod 7$

$\equiv -1 \bmod 7$ ... $48 = 7\cdot 7 - 1$ ✓

So 7 is prime! !!

Recall: Proof of Pepin used essentially:

① $F_n - 1$ a power of 2

② $3^{\frac{F_n-1}{2}} = -1$ in $\mathbb{F}_{F_n}^\times$ if F_n prime by quad. recip

+ Lemma that gives $3^{2^{k-1}} = -1 \iff 3$ has order 2^k.

Cannot make similar argument in $\mathbb{F}_{M_\ell}^\times$

$|\mathbb{F}_{M_\ell}^\times| = M_\ell - 1 = 2^\ell - 2$ not a power of 2!

Idea: $|\mathbb{F}_{p^2}^\times| = p^2-1 = (p-1)(p+1)$

If $p = M_\ell$, $p+1 = 2^\ell$ is a power of 2.

Can use this to imitate Pepin argument!
(Construct an element of order 2^ℓ in $\mathbb{F}_{p^2}^\times$).

Claim 1: For M_ℓ a Mersenne prime, $\ell > 2$,
3 is not a square mod M_ℓ.
Thus

$a+b\sqrt{3}$ $\quad \mathbb{F}_{M_\ell}[\sqrt{3}] = \mathbb{Z}[\sqrt{3}]/M_\ell$ or
$a, b \in \mathbb{F}_{M_\ell}$ $\quad \mathbb{F}_{M_\ell}[x]/x^2-3$
is a field of order M_ℓ^2.

Justification of Claim 1:

$4 \mid 2^\ell$ $\ell > 2$

- $M_\ell \equiv 3 \bmod 4$ $\quad M_\ell = 2^\ell - 1 = -1 \bmod 4$
- $M_\ell \equiv 1 \bmod 3$ $\quad M_\ell = 2^\ell - 1 \equiv \left(2^{\frac{\ell-1}{2}}\right)^2 \cdot 2 - 1$
$\equiv 2 - 1 \equiv 1 \bmod 3.$

So $\left(\frac{3}{M_\ell}\right) = -\left(\frac{M_\ell}{3}\right) = -1$ ✓

A computation in $\mathbb{F}_p[\sqrt{3}]$ $\left[\text{assume } \left(\frac{3}{p}\right) = -1\right]$

$$(a + b\sqrt{3})^p = a^p + (b\sqrt{3})^p$$
$$= a + b^p(\sqrt{3})^p$$
$$= a + b \cdot 3^{\frac{p-1}{2}} \cdot \sqrt{3}$$
$$= a + b \cdot \left(\frac{3}{p}\right)\sqrt{3}$$
$$= a - b\sqrt{3}$$

$(\sqrt{3})^p = \sqrt{3}^{p-1}\sqrt{3} = (3^{\frac{p-1}{2}})\sqrt{3}$

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

$$= (2+\sqrt{3})(2-\sqrt{3})$$
$$= 4 - 3 = 1 \mod p.$$

Justification of main theorem

Suppose $p = M_l$ is prime

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

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

- $(2+\sqrt{3})^{\frac{p+1}{2}} \equiv \pm 1 \mod p$
- $(2+\sqrt{3})^{\frac{p+1}{2}} \equiv 1 \iff$ $I(2+\sqrt{3})$ multiple of $2p+1$. in $\mathbb{Z}[\sqrt{3}]$

discrete log for $\mathbb{F}_p[\sqrt{3}]$

$\text{ind}(2+\sqrt{3}) = 2(p-1)k$

$(g^{k(p-1)})^2 = 2+\sqrt{3}$ $\Leftrightarrow$ $2+\sqrt{3} = (a+b\sqrt{3})^2 \mod p$

$(g^{k\cdot(p-1)})^{p+1} = 1$ where $(a+b\sqrt{3})^{p+1} = a^2 - 3b^2 = 1 \mod p$

$p^2-1 = \frac{p+1}{2} \cdot 2(p-1)$

Get $a^2 + 3b^2 \equiv 2$, $a^2 - 3b^2 \equiv 1$, so

$$2a^2 \equiv 3 \mod p.$$

$$\left(\frac{2}{p}\right)\left(\frac{a^2}{p}\right) = \left(\frac{3}{p}\right)$$

$$\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) \quad \text{by assumption}$$

$\ell > 2$

$p = M_\ell = 2^\ell - 1$

$\equiv -1 \mod 8$

$\equiv 7 \mod 8$

$1 = -1$ Contradiction!

Conversely, assume $(2+\sqrt{3})^{2^{\ell-1}} \equiv -1 \mod M_\ell$.

Claim 2: There is a prime $p \mid M_\ell$ s.t. $\left(\frac{3}{p}\right) = -1$.

Taking p as in claim 2,

$$(2+\sqrt{3})^{2^{\ell-1}} \equiv -1 \mod p \quad \text{in } \mathbb{F}_p[\sqrt{3}]^\times$$

so order of $2+\sqrt{3}$ is 2^ℓ ← same lemma as Tuesday's

Since $(2+\sqrt{3})^{p+1} = 1$, $2^\ell \mid p+1$

by example. for Pepin

so $2^\ell - 1 \le p \le M_\ell = 2^\ell - 1$,

i.e. $p = M_\ell$. ✓

Justification of claim 2:

$M_\ell = n^2 p_1 \cdots p_K$ (n odd, p_i distinct odd primes)

$\equiv 1 \bmod 3$ $\equiv 1 \bmod 4$ n, p_i not div by 3, 2.

$1 \equiv M_\ell \equiv p_1 \cdots p_K \bmod 3$ $\quad -1 \equiv M_\ell \equiv p_1 \cdots p_K \bmod 4$.

each p_i is $\equiv 1$ or $-1 \bmod 4$

s of them $\equiv -1 \bmod 4$

s odd.

So $1 = \left(\frac{M_\ell}{3}\right) = \left(\frac{p_1}{3}\right) \cdots \left(\frac{p_K}{3}\right)$

$= (-1)^s \cdot \left(\frac{3}{p_1}\right) \cdots \left(\frac{3}{p_K}\right)$

$= -\left(\frac{3}{p_1}\right) \cdots \left(\frac{3}{p_K}\right)$

one has to be -1.