Math 4400
Week 11 - Tuesday
Fermat Primes

This week: 2 applications of quadratic reciprocity

- Thursday - The Lucas-Lehmer test
  (When is $2^\ell - 1$ prime?
  See Week 7, exercise 3).
- Today - Fermat primes
  (Similar ideas to Lucas-Lehmer,
  but simpler).

In both we will only use quadratic reciprocity for $p=3$ — this case was justified completely in the Week 10, Thursday video!

Definition: The Fermat numbers are $F_n = 2^{2^n}+1$.

Example: $F_0 = 3 \quad F_1 = 5 \quad F_2 = 17$

$F_3 = 257 \quad F_4 = 65537$

$F_5 = 4294967297$

F_0, F_1, F_2, F_3, and F_4 are prime.

Fermat conjectured F_n is always prime,

BUT IN FACT,

$$F_5 = 4294967297 = 641 \cdot 6700417$$

(Euler, 100 years after Fermat)

In fact, now we think that most likely F_n is not prime for any $n > 4$.

regular 5-gon

An interesting Fact: The regular n-gon

is constructible with straight edge and compass if and only if

$n = 2^k p_1 p_2 \cdots p_r$ with p_i distinct Fermat primes.

(Asked by ancient Greeks, answered by Gauss + Wantzel, modern perspective via Galois theory).

Hard to check if F_n is prime by brute force, because F_n is very big.

F_n has $\sim 0.3 \cdot 2^n$ digits.

Theorem (Pepin's Test):

For $n \geq 1$,
F_n is prime if and only if $3^{\frac{F_n - 1}{2}} \equiv -1 \bmod F_n$.

Example: $F_3 = 257 = 2^{2^3} + 1$

To use test, need to compute

$128 = \frac{F_3 - 1}{2}$ $\quad 3^{128} \bmod 257.$

Successive squares

$3^2 = 9 \quad \bmod 257$ \ will need to

$$3^4 = 81 \mod 257$$
$$3^8 = 136 \mod 257$$
$$3^{16} = -8 \mod 257$$
$$3^{32} = 64 \mod 257$$
$$3^{64} = -16 \mod 257$$
$$3^{128} = -1 \mod 257$$

square $2^n - 1$ times to check F_n.

So $F_3 = 257$ is prime.

Justification for Pepin's test:

First half - if F_n is prime, then $3^{\frac{F_n-1}{2}} \equiv -1 \mod F_n$.

$$3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \mod F_n$$ (Euler's formula for the Legendre symbol)

$$\left(\frac{3}{F_n}\right) \overset{\text{q.r.}}{=} \left(\frac{F_n}{3}\right) = -1$$

$F_n = 2^{2^n}+1$

$4 \mid 2^{2^n}$ when $n \geq 1$

$F_n \equiv 1 \mod 4$

$F_n = 2^{2^n}+1$

$F_n = (2^{2^{n-1}})^2 + 1$

Any square in $\mathbb{F}_3^\times$ is 1.

$F_n \equiv 1 + 1 \mod 3$

$\equiv 2 \mod 3$ ✓

Second half: If $3^{\frac{F_n-1}{2}} \equiv -1 \mod F_n$,
then F_n is prime.

Let p be a prime dividing F_n.
So $p \le F_n$. We will show $p \ge F_n$
$\Rightarrow p = F_n$.

Since $p \mid F_n$, $3^{\frac{F_n-1}{2}} \equiv -1 \bmod p$.

So $3^{\frac{F_n-1}{2}} = 3^{2^{2^n}/2} = \underline{3^{2^{(2^n-1)}}} \equiv \underline{-1} \bmod p$.

square $\quad 3^{2^{2^n}} \equiv 1 \bmod p$

Claim: In any group G, if $g \in G$ is such that

$$g^{2^k} = e \quad \text{and} \quad g^{2^{k-1}} \neq e,$$

then g has order 2^k and in particular $|G| \ge 2^k$. By Lagrange.

Applied to $G = \mathbb{F}_p^\times$, $g = 3$, $k = 2^n$ raising to 2^{2^n} power.

we find $p-1 = |\mathbb{F}_p^\times| \ge 2^{2^n}$
so $p \ge 2^{2^n}+1 = F_n$, as desired.

Justification of claim:

① If $g^m = e$, then $\mathrm{ord}(g) \mid m$.

So $\operatorname{ord}(g) \mid 2^K$. Only divisors are 2^a for $a \leq K$. But if $g^{2^a} = e$ for $a < K$, then $\underbrace{\left(g^{2^a}\right)^{2^{K-a-1}}}_{= e^{2^{K-a-1}}} = g^{2^{K-1}} = e$, but we have assumed this is not the case!