This week: 2 applications of quadratic reciprocity

- Thursday - The Lucas-Lehmer test
  (When is $2^p-1$ 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
Definition: The Fermat numbers are $F_n = 2^{2^n} + 1$.

Example: $F_0 = 3, F_1 = 5, F_2 = 17$

$F_3 = 257, F_4 = 65537$

$F_5 = 4294967299$

$F_0, F_1, F_2, F_3, \text{ and } F_4$ are prime.

Fermat conjectured $F_n$ is always prime,

BUT IN FACT,

$F_5 = 4294967299 = 641 \cdot 6700417$

(Euler, 100 years after Fermat)

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

An interesting fact: The regular $n$-gon is constructible if $n$ is a power of 2, or a product of distinct Fermat primes.
is constructible with straight edge and compass if and only if
\[ n = 2^k p_1 p_2 \ldots p_r \] 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.

\[ F_n \text{ has } \sim 0.3 \cdot 2^n \text{ digits.} \]

**Theorem (Pepin’s Test):**

\[ \text{For } n \geq 1, \]
\[ F_n \text{ is prime if and only if } 3^{\frac{F_n - 1}{2}} \equiv -1 \mod F_n. \]

**Example:** \( F_3 = 257 = 2^8 + 1 \)

To use test, need to compute
\[ 128 = \frac{F_3 - 1}{2} \]
\[ 3^{128} \mod 257. \]

Successive squares
\[ 3^2 = 9 \mod 257 \]
\[ \text{will need to} \]
\[3^2 = 8 \quad \text{mod 257}\]
\[3^3 = 136 \quad \text{mod 257}\]
\[3^4 = -8 \quad \text{mod 257}\]
\[3^{16} = 64 \quad \text{mod 257}\]
\[3^{32} = -16 \quad \text{mod 257}\]
\[3^{64} = -1 \quad \text{mod 257}\]

So \(F_3 = 257\) is prime.

Justification for Pepin's test:

First half— if \(F_n\) is prime, then \(3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}\).

\[
3^{\frac{F_n-1}{2}} \equiv \left(3\right)^{\frac{F_n}{2}} \equiv \left(\frac{3}{F_n}\right) \pmod{F_n} \quad \text{(Euler's formula for the Legendre symbol)}
\]

\[
\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = -1
\]

\[
F_n = 2^{2^n} + 1
\]
\[F_n = 1 \quad \text{mod } 4\]
\[F_n = 1 + 1 \quad \text{mod } 3
\]
\[\equiv 2 \quad \text{mod } 3\]

Any square in \(\mathbb{F}_3^*\) is 1.

Second half: If \(3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}\), then \(F_n\) is prime.
Let $p$ be a prime dividing $F_n$. So $p \leq F_n$. We will show $p \geq F_n$.

So $p = F_n$.

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

So $3^{\frac{F_n-1}{2}} = 3^{\frac{2^{2^n}-2}{2}} = 3^{2^{2^n} \bmod (q^2-1)}$

Square $3^{2^{2^n}} \equiv 1 \bmod p$.

Claim: In any group $G$, if $g \in G$ is such that $g^{2^k} = e$ and $g^{2^{k-1}} \neq e$,

then $g$ has order $2^k$ and

in particular $|G| \geq 2^k$. By Lagrange.

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

we find $p - 1 = 1|\mathbb{F}_p^x| \geq 2^{2^n}$

so $p \geq 2^{2^n} + 1 = F_n$, as desired.

Justification of claim:

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

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