Fermat Primes, Quadratic Reciprocity I

Theorem (Pépin's Test)

$F_n = 2^{2^n} + 1$ is prime if and only if
$3^{\frac{F_n - 1}{2}} = 3^{2^{2^n} - 1} \equiv -1 \pmod{F_n}$.

Fermat Primes, Quadratic Reciprocity II

Proof.

Assume $\mathbf{F_n}$ is prime. By quadratic reciprocity, $3^{\frac{F_n-1}{2}} = \left(\frac{F_n}{3}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$. This is because $F_n = 2^{2^n} + 1 \equiv (-1)^{2^n} + 1 \equiv 1 + 1 \equiv 2 \ (mod 3)$

Assume $\mathbf{3^{\frac{F_n-1}{2}} \equiv -1 \ (mod \ F_n)}$. The order of 3 modulo F_n is $F_n - 1 = 2^{2^n}$. If $p \mid F_n$, the same is true for the order of 3 modulo p. The order divides $(p-1)$. So $2^{2^n} \mid (p-1)$. Therefore $p - 1 = k2^{2^n}$, and therefore $p = 1 + k \cdot 2^{2^n} \geq 1 + 2^{2^n} = F_n$. So $F_n \leq p \leq F_n$, which implies $F_n = p$ is prime. □

Some Numerology I

There are only five known Fermat primes primes. There are only 5 known Fermat primes. They are:

n	F_n
0	3
1	5
2	17
3	257
4	65537

The known Fermat primes are precisely the first 5 Fermat numbers. Fermat claimed that the next number $F_5 = 2^{2^5} + 1 = 4294967297$ is also prime. However, about 100 years after Fermat, Euler found the following factorization $4294967297 = 641 \cdot 6700417$. By 2003 it was known that F_n is composite for $5 \leq n \leq 32$.

Some Numerology II

If $n = 7$, the number of steps needed to determine that F_7 is composite, is equal to 127. This number pales in comparison to the actual prime factors of
$F_7 = 59649589127497217 \cdot 5704689200685129054721$.

Lucas-Lehmer Test I

Recall the Mersenne numbers $M_\ell = 2^\ell - 1$. They are composite if ℓ is composite. So they can be prime only if ℓ is prime.

Theorem (Lucas-Lehmer)

Define recursively a sequence s_n of integers by $s_1 = 4$ and $s_{n+1} = s_n^2 - 2$. Let ℓ be an odd prime. Then $M_\ell = 2^\ell - 1$ is prime if and only if $s_{\ell-1} \equiv 0 \pmod{M_\ell}$.

Lucas-Lehmer Test II

Example

s_1	4
s_2	14
s_3	194
s_4	37634
s_5	1416317954
s_6	$2005 \ldots 6114$

For $M_7 = 127$ you replace $s_3 \equiv -60$ and continue $s_4 = (-60)^2 - 2 \equiv 42$, $s_5 \equiv 42^2 - 2 = -16$, $s_6 \equiv (-16)^2 - 2 = 0$.