Fermat Numbers

The **Fermat numbers** are numbers of the form

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

Fermat thought that all the F_n were prime. The first five are:

$$F_0 = 3, \quad f_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

However, it turns out that $641 \mid F_5 = 2^{32} + 1$. Note that

$$641 = 2^4 + 5^4 \quad \text{and} \quad 641 = 2^7 \cdot 5 + 1.$$

Therefore,

$$2^7 \cdot 5 = 641 - 1, \quad \text{so} \quad 2^{28} \cdot 5^4 = (641 - 1)^4 = 641 \cdot x + 1.$$

Here x is an integer.
On the other hand, $5^4 = 641 - 2^4$, so

$$2^{28} \cdot (641 - 2^4) = 641 \cdot x + 1,$$

$$641 \cdot 2^{28} - 2^{32} = 641 \cdot x + 1,$$

$$2^{32} + 1 = 641 \left(2^{28} - x\right).$$

This proves that $641 \mid 2^{32} + 1$.

A **Fermat prime** is a Fermat number which is prime. It is an open question as to whether there are infinitely many Fermat primes.

Surprisingly, Fermat primes arise in deciding whether a regular n-gon (a convex polygon with n equal sides) can be constructed with a compass and a straightedge. Gauss showed that a regular n-gon is contructible with a compass and a straightedge if and only if n is a power of 2 times a product of distinct Fermat primes.

Here are some properties of the Fermat numbers.

Proposition. If p is prime and $p \mid F_n$, then $p = k \cdot 2^{n+2} + 1$ for some k. □

I won't prove this result, since the proof requires results about quadratic residues which I won't discuss for a while. Here's how it can be used.

Example. Check $F_4 = 2^{2^4} + 1 = 65537$ for primality.

Here $n = 4$, so all prime divisors must have the form $k \cdot 2^6 + 1 = 64k + 1$. There are around 1024 numbers less than 65537 of this form, but I only need to check numbers up to the square root $\sqrt{65537} \approx 256$. (For if a number has a prime factor, it must have a prime factor less than its square root.)

k	$64k + 1$	Conclusion
1	65	Not prime
2	129	Not prime
3	193	Prime, but doesn't divide 65537

(The next value of $64k + 1$ is 257, which is larger than $\sqrt{65537}$.) Conclusion: 65537 must be prime! □

Proposition. $F_0F_1\cdots F_{n-1} = F_n - 2$ for $n > 0$.

Proof. $F_0 = 3$ and $F_1 = 5$, so $F_0 = F_1 - 2$. The result is true for $n = 1$.

Take $n > 0$, and assume the result is true for n; I'll try to prove it for $n+1$. By assumption,

$$F_0F_1\cdots F_{n-1} = F_n - 2, \quad \text{so} \quad F_0F_1\cdots F_{n-1}F_n = (F_n - 2)F_n.$$

Now

$$(F_n - 2)F_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2\cdot 2^n} - 1 = 2^{2^{n+1}} - 1 = 2^{2^{n+1}} + 1 - 2 = F_{n+1} - 2.$$

That is,

$$F_0F_1\cdots F_{n-1}F_n = F_{n+1} - 2.$$

This is the statement for $n+1$, so the proof is complete, by induction. □

Proposition. If $m \neq n$, $(F_m, F_n) = 1$.

Proof. Assume $m < n$ (if not, switch m and n). Suppose p is prime and $p \mid F_m$ and $p \mid F_n$. Also, $p \mid F_0F_1\cdots F_{n-1}$ since $m < n$ implies that F_m occurs in this product. But

$$F_n - 2 = F_0F_1\cdots F_{n-1}, \quad \text{so} \quad 2 = F_n - F_0F_1\cdots F_{n-1}.$$

Since p divides both of the terms on the right, $p \mid 2$, so $p = 2$. This is impossible, since all the F_n's are odd.

Therefore, there is no prime dividing both F_m and F_n, and hence $(F_m, F_n) = 1$. □