**MATH 324 Summer 2012**
**Elementary Number Theory**

**Notes on the Fermat Numbers**

## *Fermat Numbers*

The *Fermat numbers* $\{\Phi_n\}_{n\geq 0}$ are defined to be the positive integers

$$\Phi_n = 2^{2^n} + 1,$$

for $n \geq 0$.

The first five Fermat numbers

$$\Phi_0 = 3, \quad \Phi_1 = 5, \quad \Phi_2 = 17, \quad \Phi_3 = 257, \quad \Phi_4 = 65537$$

are all primes, and this led Fermat to conjecture that every Fermat number $\Phi_n$ is a prime.

Almost 100 years later, in 1732, Euler showed that this conjecture was false, and he gave the following counterexample:

$$\Phi_5 = 4294967297 = 641 \cdot 6700417.$$

The Fermat numbers that are prime are called *Fermat primes*, and to this day, it is not known if there are infinitely many Fermat primes. No fermat primes beyond $\Phi_4$ have been found. However, as of 2010, the largest known composite Fermat number is $\Phi_{2478782}$. Not all the intermediate Fermat numbers are known to be composite, for example, $\Phi_{33}$ is the smallest Fermat number that has not yet been shown to be composite.

The mathematician G. Bennet gave an elementary proof of the fact that $\Phi_5$ is composite without doing any division! His proof is as follows: First note that

$$641 = 5 \cdot 2^7 + 1.$$

Now,

$$\begin{aligned}
\Phi_5 &= 2^{2^5} + 1 = 2^{32} + 1 = 2^4 \cdot 2^{28} + 1 = 16 \cdot 2^{28} + 1 \\
&= (641 - 625) \cdot 2^{28} + 1 = (641 - 5^4) \cdot 2^{28} + 1 \\
&= 641 \cdot 2^{28} - \left(5 \cdot 2^7\right)^4 + 1 = 641 \cdot 2^{28} - (641 - 1)^4 + 1 \\
&= 641 \cdot 2^{28} - \left(641^4 - 4 \cdot 641^3 + 6 \cdot 641^2 - 4 \cdot 641 + 1\right) + 1 \\
&= 641 \cdot \left(2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4\right)
\end{aligned}$$

so that $641 \,\big|\, \Phi_5$.

There is a lot known about the Fermat numbers, but probably the most important is the connection, found by Gauss in 1796, between the Fermat primes and the straight-edge and compass construction of regular polygons. His result is as follows:

**Theorem.** A regular polygon with $n$ sides is constructible using only a straight edge and compass if and only if

$$n = 2^{r+2} \qquad \text{or} \qquad n = 2^r \cdot F_1 F_2 \cdots F_k,$$

where $r \geq 0$ and $F_1$, $F_2$, $\ldots$, $F_k$ are distinct Fermat primes.

The early Greeks knew how to construct regular polygons with $2^k$, $3 \cdot 2^k$, $5 \cdot 2^k$, and $15 \cdot 2^k = 2^k \cdot 3 \cdot 5$ sides. They also knew how to construct regular polygons with

$$3,\ 4,\ 5,\ 6,\ 8,\ 10,\ 12,\ 15, \text{ and } 16$$

sides, but did not know how to construct a regular polygon with 17 sides. This was done by Gauss when he was 19 years of age, and (so the story goes) he decided to devote the rest of his life to mathematics. He also requested that a 17-sided regular polygon be engraved on his tombstone (it is not there).

Now we give a recurrence relation satisfied by the Fermat numbers and use this to prove some interesting results.

**Theorem.** For every integer $n \geq 0$, we have

$$\Phi_{n+1} - 2 = \Phi_0 \cdot \Phi_1 \cdot \Phi_2 \cdots \Phi_n$$

**Proof.** Since $2^{2^0} - 1 = 1$, then we have

$$\begin{aligned}
\Phi_0 \cdot \Phi_1 \cdot \Phi_2 \cdot \Phi_3 \cdots \Phi_n &= 1 \cdot \Phi_0 \cdot \Phi_1 \cdot \Phi_2 \cdot \Phi_3 \cdots \Phi_n \\
&= \left(2^{2^0} - 1\right)\left(2^{2^0} + 1\right)\left(2^{2^1} + 1\right)\left(2^{2^2} + 1\right)\left(2^{2^3} + 1\right)\cdots\left(2^{2^n} + 1\right) \\
&= \left(2^{2^1} - 1\right)\left(2^{2^1} + 1\right)\left(2^{2^2} + 1\right)\left(2^{2^3} + 1\right)\cdots\left(2^{2^n} + 1\right) \\
&= \left(2^{2^2} - 1\right)\left(2^{2^2} + 1\right)\left(2^{2^3} + 1\right)\cdots\left(2^{2^n} + 1\right) \\
&= \left(2^{2^3} - 1\right)\left(2^{2^3} + 1\right)\cdots\left(2^{2^n} + 1\right) \\
&\quad\vdots \\
&= \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) \\
&= 2^{2^{n+1}} - 1 \\
&= 2^{2^{n+1}} + 1 - 2 \\
&= \Phi_{n+1} - 2.
\end{aligned}$$

□

**Theorem.** Any two distinct Fermat numbers $\Phi_m$ and $\Phi_n$ with $m > n$ are relatively prime.

**Proof.** Let $\Phi_m$ and $\Phi_n$ be distinct Fermat numbers with $m > n$, and suppose that $d > 0$ is a common divisor of $\Phi_m$ and $\Phi_n$, then $d$ divides $2 = \Phi_m - \Phi_0 \cdot \Phi_1 \cdots \Phi_n \cdots \Phi_{m-1}$. Therefore, $d = 1$ or $d = 2$, but $\Phi_m$ and $\Phi_n$ are odd, so we must have $d = 1$. Therefore, for $m > n$, the Fermat numbers $\Phi_m$ and $\Phi_n$ are relatively prime. □

And now we give G. Polya's elementary proof that there are infinitely many primes, that is, there is no largest prime.

**Theorem.** There are infinitely many primes.

**Proof.** There are infinitely many distinct Fermat numbers, each of which is divisible by an odd prime, and since any two Fermat numbers are relatively prime, these odd primes must all be distinct. Thus, there are infinitely many primes. □

Finally, we can show the following:

**Theorem.** For every integer $n \geq 0$, the positive integer

$$N = 2^{2^n} - 1$$

is divisible by at least $n$ different primes.

**Proof.** Note that for each $n \geq 0$ we have

$$2^{2^n} - 1 = 2^{2^n} + 1 - 2 = \Phi_n - 2 = \Phi_0 \cdot \Phi_1 \cdot \Phi_2 \cdot \Phi_3 \cdots \Phi_{n-1},$$

and all of the $\Phi_k$'s are pairwise relatively prime. □

Recall that a positive integer $n$ is a **triangular number** if and only if

$$n = \frac{k(k+1)}{2}$$

for some positive integer $k$. As an exercise, prove the following result:

**Theorem.** Among the Fermat numbers $\Phi_n$, there are no squares, no cubes, and no triangular numbers (except $\Phi_0 = 3 = \frac{2 \cdot 3}{2}$).