Chapter 4

Fermat and Mersenne Primes

4.1 Fermat primes

Theorem 4.1. *Suppose $a, n > 1$. If*

$$a^n + 1$$

is prime then a is even and

$$n = 2^e$$

for some e.

Proof. If a is odd then $a^n + 1$ is even; and since it is ≥ 5 it is composite.

Suppose n has an odd factor r, say

$$n = rs.$$

We have

$$x^r + 1 = (x + 1)(x^{r-1} - x^{r-2} + x^{r-3} - \cdots + 1).$$

On substituting $x = a^s$,

$$a^s + 1 \mid a^n + 1,$$

and so $a^n + 1$ is composite.

Thus n has no odd factor, and so

$$a = 2^e.$$

□

Definition 4.1. *The number*

$$F(n) = 2^{2^n} + 1$$

is called a Fermat number; and if it is prime it is called a Fermat prime.

Thus

$$F(0) = 3,\ F(1) = 5,\ F(2) = 17,\ F(3) = 257,\ F(4) = 65537,\ F(5) = 4,294,967,297, \ldots$$

Fermat conjectured that the Fermat numbers are all prime. Sadly this has proved untrue.

$F(0)$ to $F(4)$ are indeed prime, but $F(5)$ is composite.

How do I know? There is a standard `Unix` program `factor` for factorizing numbers. Here is what I get:

```
tim@boole:~> /usr/games/factor 65537
65537: 65537
tim@boole:~> /usr/games/factor 4294967297
4294967297: 641 6700417
```

There is a sister program `primes` which will print all the primes in a given range:

```
tim@boole:~> /usr/games/primes 1000 1020
1009
1013
1019
```

No further Fermat primes have been found, and a heuristic argumnent suggests there probably are no more. (A *heuristic argument* is one that suggests a result is true, but does not prove it.)

The probability that

$$F(n) = 2^{2^n}$$

is prime is

$$\frac{1}{\ln(F(n))} \approx \frac{1}{2^n \ln 2}.$$

Thus the expected number of Fermat primes $F(n$ with $n \geq 5$ is

$$\frac{1}{\ln 2} \sum_{n \geq 5} \frac{1}{2^n} = \frac{1}{\ln 2} \frac{1}{16} \approx$$

So one could wager that there are no more Fermat primes after $F(4)$.

4.2 Mersenne primes

Theorem 4.2. *Suppose $a, n > 1$. If*

$$a^n - 1$$

is prime then $a = 2$ and n is prime.

Proof. We have

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + 1).$$

Thus

$$a - 1 \mid a^n - 1,$$

and so $a^n - 1$ is composite if $a > 2$.

Now suppose n is composite, say

$$n = rs,$$

with $r, s > 1$. We have

$$x^r + 1 = (x + 1)(x^{n-1} - x^{n-2} + x^{n-3} - \cdots + 1).$$

Substituting $x = a^s$,

$$a^s - 1 \mid a^n - 1,$$

and so $a^n - 1$ is composite.

Hence n is prime. □

Definition 4.2. *For each prime p the number*

$$M(p) = 2^p - 1$$

is called a Mersenne number; and if it is prime it is called a Mersenne prime.

We have

$$M(2) = 3,\ M(3) = 8,\ M(5) = 31,\ M(7) = 63,\ M(11) = 2047, \dots$$

The following heuristic argument suggests that there are an infinity of Mersenne primes.

The probability that $M(p)$ is prime is

$$\frac{1}{\ln(2^p - 1)} \approx \frac{1}{p \ln 2}.$$

Thus the expected number of Mersenne primes is

$$\frac{1}{\ln 2} \sum \frac{1}{p},$$

where the sum runs over all primes.

But we have seen that

$$\sum \frac{1}{p}$$

is divergent. So this suggests (strongly) that the number of Mersenne primes is infinite.

We shall see later that there is a subtle test — the Lucas-Lehmer test — for the primality of the Mersenne number $M(p)$. This allows the primality of very large Mersenne numbers to be tested on the computer much more quickly than other numbers of the same size.

For this reason, the largest known prime is invariably a Mersenne prime; and the search for the next Mersenne prime is a popular pastime.

The Great Internet Mersenne Prime Search, or GIMPS (`http://www.mersenne.org/`), is a communal effort — which anyone can join — to find the next Mersenne prime. The record to date, the 47th known Mersenne prime, is

$$2^{43,112,609} - 1.$$

This was discovered in 2008, and has over 10 million digits.

We shall join the search, and possibly win a large prize!

4.3 Perfect numbers

Definition 4.3. *We denote the sum of the divisors of $n > 0$ by $\sigma(n)$*

Note that we include 1 and n in the factors of n. Thus

$$\sigma(1) = 1,\ \sigma(2) = 3,\ \sigma(3) = 4,\ \sigma(4) = 7,\ \sigma(5) = 6,\ \sigma(6) = 12, \ldots$$

Definition 4.4. *The integer $n > 0$ is said to be perfect if it is the sum of its proper divisors, ie if*

$$\sigma(n) = 2n.$$

Thus 6 is the first perfect number.

Theorem 4.3. *If $M(p) = 2^p - 1$ is a Mersenne prime then*

$$n = 2^{p-1}(2^p - 1)$$

is perfect; and every even perfect number is of this form.

Proof. The number n above has factors

$$2^r \text{ and } 2^r M(p)$$

for $r = 0, 1, \ldots, p - 1$, with sum

$$\sigma(n) = \left(1 + 2 + 2^2 + \cdots + 2^{p-1}\right)(1 + M(p)) = (2^p - 1)2^p = 2n.$$

Lemma 4.1. *The function $\sigma(n)$ is* multiplicative in the number-theoretic sense*, ie*

$$\gcd(m, n) = 1 \implies \sigma(mn) = \sigma(m)\sigma(n).$$

Proof. If $\gcd(m, n) = 1$ then the factors of mn are the numbers rs, where r is a factor of m, and s is a factor of n. The result follows at once from this. □

Now suppose n is an even perfect number. Let

$$n = 2^e m,$$

where m is odd. Then

$$\sigma(n) = (2^{e+1} - 1)\sigma(m).$$

But $\sigma(n) = 2n$. Thus

$$2^{e+1} m = (2^{e+1} - 1)\sigma(m).$$

It follows that

$$2^{e+1} - 1 \mid m,$$

say

$$m = (2^{e+1} - 1)q.$$

Then

$$\sigma(m) = 2^{e+1} q = m + q.$$

But m and q are both factors of m. It follows that they are the *only* factors of m. Hence $q = 1$ and

$$m = 2^{e+1} - 1$$

is prime. □

It is not known if there are any odd perfect numbers. If there are, then the first one is $> 10^{500}$.