7. MERSENNE AND FERMAT PRIMES

§7.1. Mersenne Primes

A **Mersenne prime** is one of the form $M_n = 2^n - 1$ for some n. The first 12 Mersenne primes are given in the following table.

n	M_n	value	discovered
2	$2^2 - 1$	3	antiquity
3	$2^3 - 1$	7	
5	$2^5 - 1$	31	
7	$2^7 - 1$	127	
13	$2^{13} - 1$	8191	before 1461
17	$2^{17} - 1$	131071	1588
19	$2^{19} - 1$	524287	1588
31	$2^{31} - 1$	2147483647	1772
61	$2^{61} - 1$	about 2×10^{18}	1883
89	$2^{89} - 1$	about 6×10^{26}	1911
107	$2^{107} - 1$	about 2×10^{32}	1914
127	$2^{127} - 1$	about 2×10^{38}	1876

You'll notice that in all these cases n is prime. This is always the case.

Theorem 1: If $M_n = 2^n - 1$ is prime then so is n.
Proof: Suppose $n = ab$ where $1 < a, b < n$.
Then $2^n - 1 = 2^{ab} - 1$.
Since $x^b - 1 = (x - 1)(x^{b-1} + x^{b-2} + ... + x + 1)$ for all x, $2^a - 1$ is a factor of $2^{ab} - 1$.
Hence M_n is composite.


Marin Mersenne

As can be seen from the above table the converse doesn't hold.
For example:
$M_{11} = 2047 = 23 \times 89$.

Mersenne numbers get very large, very quickly. In fact, as of January 2016, only 51 Mersenne primes are known, the largest being $2^{82,589,933} - 1$. Most of the larger ones have been found with the aid of a computer, or in the more recent cases, by an army of computers in what is known as distributed computing. Thousands of volunteers are allocated a portion of the work in testing a single M_p and they let their computers work on the problem when it's otherwise idle.

7.2. Perfect Numbers

We define **$\sigma(n)$** to be the **sum of the divisors** of n (including 1, and n itself). A **perfect number** is one that is equal to the sum of its *proper* divisors, that is, where $\sigma(n) = 2n$.

Example 1: $\sigma(24) = 1 + 2 + 3 + 4 + 6 + 8 + 12 + 24 = 60$.
The number 28 is perfect because $28 = 1 + 2 + 4 + 7 + 14$, or in other words, $\sigma(28) = 56$.
The perfect numbers 6, 28, 496 and 8128 were known to Euclid. The next was 33,550,336, mentioned in a 1456 manuscript. All known perfect numbers are even, though it's not known whether there are any odd ones.

Theorem 2: If m, n are coprime then $\sigma(mn) = \sigma(m)\sigma(n)$.
Proof: The divisors of mn are precisely the products ab where $a \mid m$ and $b \mid n$.
So if the divisors of m are $a_1, a_2, ..., a_r$ and the divisors of n are $b_1, b_2, ..., b_s$ then the divisors of mn are the $a_i b_j$. Hence $\sigma(mn) = (a_1 + a_2 + ... + a_r)(b_1 + b_2 + ... + b_s) = \sigma(m)\sigma(n)$.

Theorem 3: $\sigma(p^n) = \dfrac{p^{n+1} - 1}{p - 1}$.

Proof: $\sigma(p^n) = 1 + p + p^2 + ... + p^n$.

The above two theorems enable us to easily compute $\sigma(n)$ for any n.

Example 2: Find $\sigma(600)$.
Solution: $\sigma(600) = \sigma(2^3.3.5^2) = \sigma(2^3)\sigma(3)\sigma(5^2) = 15.4.31 = 1860$.

Perfect numbers are closely related to Mersenne primes. Every time a new Mersenne prime is announced we have a new perfect number.

Theorem 4: The even perfect numbers are precisely those numbers of the form $2^{n-1}(2^n - 1)$ where $2^n - 1$ is a Mersenne prime.
Proof: We firstly prove that if $2^n - 1$ is prime then $2^{n-1}(2^n - 1)$ is perfect.
Let $p = 2^n - 1$ be a Mersenne prime and let $N = 2^{n-1}p$.

$$\begin{aligned}\sigma(N) &= 1 + 2 + 2^2 + ... + 2^{n-1} + p + 2p + 2^2p + ... + 2^{n-1}p \\ &= (1 + 2 + 2^2 + ... + 2^{n-1})(p + 1) \\ &= (2^n - 1)(p + 1) \\ &= (2^n - 1)(2^n) \\ &= 2N.\end{aligned}$$

Now suppose that N is an even perfect number.
Write $N = 2^mP$ where $m \geq 1$ and P is odd.

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

Therefore $\frac{P}{\sigma(P)} = \frac{2^{m+1} - 1}{2^{m+1}}$.

Since the numerator and denominator on the right hand side are coprime we must have

$P = k(2^{m+1} - 1)$ and $\sigma(P) = 2^{m+1}k$ for some positive integer k.

If $k > 1$ then $\sigma(P) \geq (2^{m+1}k - k) + k + (2^{m+1} - 1) + 1 = 2^{m+1}(k + 1) > 2^{m+1}k = \sigma(P)$.

This is a contradiction.

Hence $k = 1$ and so $P = 2^{m+1} - 1$ and $\sigma(P) = 2^{m+1} = P + 1$.

If P isn't prime $\sigma(P) > P + 1$, giving a contradiction.

Hence $N = 2^m P$ where P is a Mersenne prime.

No odd perfect numbers are known and it's considered likely that there are none. However a proof has not yet been found.

7.3. Fermat Primes

A **Fermat number** is one of the form $F_N = 2^N + 1$. A **Fermat prime** is a Fermat number that is prime. Fermat proved that for F_N to be prime N itself must be a power of 2, so we could define a Fermat prime to be a prime of the form $2^{2^n} + 1$.

Theorem 5: Every Fermat prime has the form $2^{2^n} + 1$ for some n.

Proof: Suppose $P = 2^N + 1$ is a Fermat prime.

Suppose p is an odd prime divisor of N. Write $N = pQ$.

Then since $x^n + 1 = (x + 1)(x^{n-1} - x^{n-2} + ... - x + 1)$ for odd n, $2^N + 1 = 2^{pQ} + 1$ is divisible by $2^Q + 1$, which is a contradiction.

Hence the only prime divisor of N is 2 and so N is a power of 2.

Example 3: The first five Fermat numbers are:

n	$\mathbf{2^{2^n} + 1}$
0	3
1	5
2	17
3	257
4	65537

Pierre de Fermat

These were known to Fermat, who rashly predicted that $2^{2^n} + 1$ is prime for all n, though he admitted he didn't have a proof. In fact despite a huge amount of computing effort since, no larger Fermat prime has ever been discovered.

Euler pointed out that $F_5 = 4294967297 = 641 \times 6700417$. Since then it has been shown that for all n with $5 \le n \le 32$ the number $2^{2^n} + 1$ is composite.

There's a connection between Fermat primes and constructible polygons, that is, regular polygons that can be constructed by ruler and compass. Everyone knows that an equilateral triangle can be constructed by ruler and compass. This is because 3 is a Fermat prime. There are ruler and compass constructions for a regular pentagon and even a regular polygon with 17 sides. Such constructions are possible because 5 and 17 are Fermat primes. However there's no way of constructing a regular 7 sided polygon by ruler and compass because 7 is not a Fermat prime.

Constructing a regular n-gon is equivalent to constructing an angle of $(360/n)°$. Of course it's possible to bisect any angle, so the fact that we can construct a regular pentagon means that we can construct regular polygons with 10, 20, 40, ... sides.

Theorem 6: A regular n-sided polygon is constructible by ruler and compass if and only if n is a power of 2 times a product of distinct Fermat primes (including powers of 2 alone).

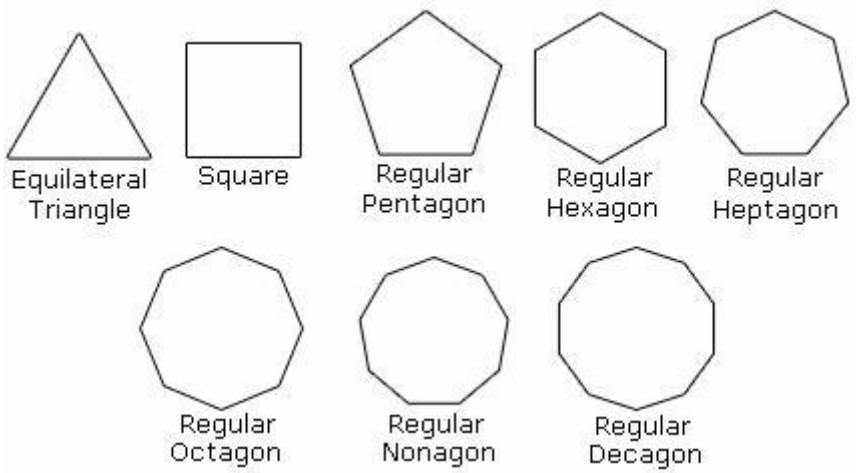
Proof: We'll only present a small portion of the proof. Suppose a regular p-sided polygon can be constructed, where p is prime. This means that we can construct the point in the complex plane that represents $\alpha = e^{2\pi i/p}$, which is a zero of the polynomial $x^p - 1$.

This factorises as $(x - 1)(x^{p-1} + x^{p-2} + ... + x + 1)$ and of course α is a zero of the second factor. This polynomial, of degree $p - 1$, can be shown to be prime

over $\mathbb{Q}$, that is, it can't factorise further into polynomials with rational coefficients. This polynomial is what's called the **minimum polynomial** of α, the monic polynomial of lowest degree that has α as a zero. It can be shown (see my notes on Galois Theory) that a complex number is constructible if and only if the degree of its minimum polynomial over $\mathbb{Q}$ is a power of 2. Thus $p - 1 = 2^n$ for some n and hence p is a Fermat prime.

Example 4: The values of n up to 256, for which a regular n-sided polygon can be constructed by ruler and compass are:

3	4	5	6	8	10	12	16	17	20	24	32
34	40	48	64	68	80	96	128	160	176	192	256



The construction for the regular heptadecagon (17 sides) is extremely complicated.