Chapter 1

Number of special form

1.1 Introduction (Marin Mersenne)

See the book.

1.2 The perfect number

Definition 1.2.1. A positive integer $n$ is said to be perfect if $n$ is equal to the sum of all its positive divisors, excluding $n$ itself.

Example 1.2.1. $n = 6$

all divisors are 1, 2, 3, 6

$6 = 1 + 2 + 3$, $\sigma(n) = 1 + 2 + 3 + 6 = 12 \Rightarrow \sigma(6) = 2 \cdot 6$

so 6 is a perfect number.

Remark 1.2.1. A number $n$ is perfect if $\sigma(n) = 2n$

Example 1.2.2. $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$

$= 2 \cdot 28$

so 28 is a perfect number.

Theorem 1.2.1. If $2^k - 1$ is prime ($k > 1$), then $n = 2^{k-1}(2^k - 1)$ is perfect and every even perfect number is of this form.

Proof. Let $2^k - 1 = p$, $p$ is prime $\Rightarrow$ $gcd(p, 2^{k-1}) = 1 \Rightarrow n = 2^{k-1}p$

so $\sigma(n) = \sigma(2^{k-1}p) = \sigma(2^{k-1})\sigma(p)$

$= \frac{2^k - 1}{2-1}(p + 1) = (2^k - 1)2^k = 2 \cdot 2^{k-1}(2^k - 1)$

$= 2 \cdot n$

so $n$ perfect number.
We will now show that an even integer is perfect number then it is of the form \(2^{k-1}(2^k - 1)\) where \(2^k - 1\) is prime.

Let \(n\) be an even perfect number
\[\Rightarrow \exists \ k \in \mathbb{N}, \ k \geq 2 \ \exists \ n = 2^{k-1}m, \text{ where } m \in \mathbb{N} \text{ and } m \text{ is odd.}\]

\[\Rightarrow \gcd(2^{k-1}, m) = 1, \text{ and } \sigma(n) = \sigma(2^{k-1}m) = \sigma(2^{k-1})\sigma(m)\]

but \(\sigma(n) = 2n = \sigma(2^{k-1})\sigma(m)\)

so \(2 \cdot 2^{k-1}m = (2^k - 1)\sigma(m)\)
\[\Rightarrow \quad 2^km = (2^k - 1)\sigma(m) \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots (1)\]
\[\Rightarrow \quad (2^k - 1)|2^km, \text{ but } (2^k - 1)|m, \text{ because } \gcd(2^k - 1, 2^k) = 1.\]

So \(\exists \ M \in \mathbb{Z} \ \exists \ m = (2^k - 1)M \ldots \ldots \ldots \ldots (2)\)

substitute equation (2) in (1)
\[2^k \cdot (2^k - 1)M = (2^k - 1)\sigma(m)\]
\[\Rightarrow \quad 2^kM = \sigma(m)\]

since \(m\) and \(M\) are both divisors of \(m\) with \(M < m\)
\[\Rightarrow \quad \sigma(m) \geq m + M\]

\[2^kM = \sigma(m) \geq m + M = (2^k - 1)M + M\]

\[2^kM = \sigma(m) \geq 2^kM - M + M\]

\[2^kM = \sigma(m) \geq 2^kM\]
\[\Rightarrow \quad \sigma(m) = m + M\]
\[\Rightarrow \quad m \ \text{ has only two positive divisors, which are } m \text{ and } M\]

so \(m\) is a prime and \(M = 1\)
\[\Rightarrow \quad m = (2^k - 1)M = (2^k - 1) \cdot 1 \quad \text{is a prime number}\]
\[\Rightarrow \quad \text{any perfect number } n \ \text{has the form}\]
\[n = (2^{k-1})m = 2^{k-1}(2^k - 1), \text{ where } 2^k - 1 \text{ is prime.} \quad \square\]

**Lemma 1.2.1.** If a number \(a^k - 1\) is prime, \(a > 0, \ k \geq 2, \) then \(a = 2\) and \(k\) is also prime.

**Proof.** (1) first we will show \(a = 2\)
\[a^k - 1 = \left(a - 1\right)\frac{a^k - 1}{a - 1} = \left(a - 1\right)(a^{k-1} + a^{k-2} + \ldots + a + 1)\]
\[= \left(a - 1\right)(\sum_{i=0}^{k-1} a^i)\]

since \(a^{k-1} + a^{k-2} + \ldots + a + 1 \geq a + 1 > 1 \text{ and } a^k - 1 \text{ is prime number}\)

so the other factor must be 1, that is \(a - 1 = 1 \quad \Rightarrow \quad a = 2.\)
(2) second we will show $k$ is prime
Let $k$ be composite number, $r$ and $s \in N \ni k = r \cdot s$
\[a^k - 1 = a^{rs} - 1 = (a^r - 1)^{a^{s-1}}\]
\[= (a^r - 1)\left(\sum_{i=0}^{s-1} a^{ri}\right)\]
\[= (a^r - 1)(1 + a^r + a^{2r} + \ldots + a^{r(s-1)})\]
\[\Rightarrow a^k - 1 \text{ is composite number (contradiction)}\]
\[\Rightarrow k \text{ is prime}.\]

**Theorem 1.2.2.** Prove that $16^m$, $m \in N$ ends in 6.

*Proof. 16 = 10 + 6*

\[16^m = (10 + 6)^m = \sum_{i=0}^{m} \binom{m}{i} 10^{m-i}6^i\]
\[= \left(\sum_{i=0}^{m-1} 10^{m-i}6^i\right) + 6^m\]
\[= 10v + 6^m\]
but $6^m = 6 + 10w$
\[\Rightarrow 16^m = 6 + 10k \equiv 6(mod\ 10)\]

**Theorem 1.2.3.** Every even perfect number $n$ ends in 6 or 8. That is $n \equiv 6(mod\ 10)$ or $n \equiv 8(mod\ 10)$

*Proof. Since $n$ is even perfect number*

\[\exists k \text{ prime } \ni n = 2^{k-1}(2^k - 1), 2^k - 1 \text{ is prime}\]
If $k = 2$ \implies $n = 2(2^2 - 1) = 2 \cdot 3 = 6$ (done)
If $k > 2$, since any prime number $k$ is either of the form $k = 4m + 1$ or of the form $k = 4m + 3$
If $k = 4m + 1$
\[\Rightarrow n = 2^{4m+1-1}(2^{4m+1} - 1)\]
\[= (2^4)^m(2(2^4)^m - 1)\]
\[= (16)^m(2(16)^m - 1)\]
Since $(16)^m \text{ ends in } 6 \implies 2(16)^m \text{ ends in } 2$
\[\Rightarrow 2(16)^m - 1 \text{ ends in } 1 \implies (16)^m(2(16)^m - 1) \text{ ends in } 6\]
\[\Rightarrow n \equiv 6(mod\ 10)\]
If $k = 4m + 3$

$\Rightarrow n = 2^{4m+3-1}(2^{4m+3} - 1)$

$= 4(16)^m(8(16)^m - 1)$

Since $(16)^m$ ends in 6 $\Rightarrow 4(16)^m$ ends in 4,

$8(16)^m$ ends in 8 $\Rightarrow 8(16)^m - 1$ ends in 7,

$4(16)^m(8(16)^m - 1)$ ends in 8.

$\Rightarrow$ every even perfect number $n$ ends in 6 or 8
1.3 Mersenne primes and amicable number

**Definition 1.3.1.** The numbers of the form \( M_n = 2^n - 1 \), \( (n > 1) \) are called Mersenne numbers.

If \( M_n \) is prime it is called Mersenne prime number.

**Example 1.3.1.**

\[
\begin{align*}
M_2 &= 2^2 - 1 = 3 \\
M_3 &= 2^3 - 1 = 7 \\
M_5 &= 2^5 - 1 = 11
\end{align*}
\]

are Mersenne prime numbers.

\[
\begin{align*}
M_4 &= 2^4 - 1 = 15 \\
M_{11} &= 2^{11} - 1 = 2047
\end{align*}
\]

are Mersenne numbers not Mersenne prime.

**Remark 1.3.1.** If \( n \) is prime it is not necessarily true that \( M_n = 2^n - 1 \) is a prime.

**Theorem 1.3.1.** If \( p \) and \( q = 2p+1 \) are primes, then either \( q|M_p \) or \( q|(M_p+2) \), but not both.

**Proof.** By Fermats theorem, we know that
\[
2^{p-1} - 1 \equiv 0 \pmod{q}
\]
\[
(2^{\frac{p-1}{2}} - 1)(2^{\frac{p-1}{2}} + 1) = (2^p - 1)(2^p + 1) \equiv 0 \pmod{q}
\]
let \( M_p = 2^p - 1 \)
\[
\Rightarrow M_p + 2 = 2^p + 1
\]
\[
\Rightarrow M_p(M_p + 2) \equiv 0 \pmod{q}
\]
\[
\Rightarrow q|M_p \text{ or } q|(M_p+2)
\]
Now if \( q|M_p \) and \( q|(M_p+2) \Rightarrow q|2 \) (contradiction)

**Example 1.3.2.** If \( p = 23 \) then \( q = 2p+1 = 47 \) is prime whether \( 47|M_{23} \) or not, or whether \( 2^{23} \equiv 1 \pmod{47} \)

we have \( 2^{23} = 2^3(2^5)^4 \equiv 2^3(-15)^4 \pmod{47} \)

but \( (-15)^4 = (225)^2 \equiv (-10)^2 \equiv 6 \pmod{47} \)

So \( 2^{23} = 2^36 \equiv 48 \equiv 1 \pmod{47} \)
\[
\Rightarrow 47|(2^{23} - 1) = M_{23}
\]

So \( M_{23} \) is composite.

The previous Theorem does not help us to test the primality of \( M_{29} \), say \( 59 \nmid M_{29} \) but \( 59|(M_{29} + 2) \).
What condition on \( q \) will ensure that \( q | M_p \)?
The answer is to be found in the following theorem

**Theorem 1.3.2.** If \( q = 2n + 1 \) is prime, then

(1) \( q | M_n \), provided that \( q \equiv 1(mod\ 8) \) or \( q \equiv 7(mod\ 8) \).
(2) \( q | (M_n + 2) \), provided that \( q \equiv 3(mod\ 8) \) or \( q \equiv 5(mod\ 8) \).

**Example 1.3.3.** 1) Let \( n = 23 \Rightarrow q = 47 \)
since \( 47 \equiv 7(mod\ 8) \) \( \Rightarrow 47 | M_{23} \).
2) Let \( n = 29 \)
since \( q = 59 \) and \( 59 \equiv 3(mod\ 8) \) \( \Rightarrow 59 | (M_{29} + 2) \).

**Corollary 1.3.1.** If \( p \) and \( q = 2p + 1 \) are both odd primes, with \( p \equiv 3(mod\ 4) \), then \( q | M_p \).

**Proof.** An odd prime is of the form \( 4k + 1 \) or \( 4k + 3 \).
If \( p = 4k + 3 \), then \( q = 8k + 7 \) and \( q \equiv 7(mod\ 8) \) \( \Rightarrow q | M_p \).
In case \( p = 4k + 1 \), then \( q = 8k + 3 \) so \( q | M_p \) but \( q | (M_p + 2) \) (because \( q \equiv 3(mod\ 8) \)).

**Example 1.3.4.** All of the following \( p \) primes, \( p \equiv 3(mod\ 4) \) for which \( q = 2p + 1 \) is also prime \( p = 11, 23, 83, 131, 179, 181, 239, 251 \Rightarrow q | M_p \) in this case \( M_p \) is composite Mersene number.

**Theorem 1.3.3.** If \( p \) is an odd prime, then any divisor of \( M_p \) is of the form \( 2pk + 1 \).

**Theorem 1.3.4.** If \( p \) is an odd prime, then any prime divisor \( q \) of \( M_p \) is of the form \( q \equiv \pm 1(mod\ 8) \).

**Proof.** Suppose that \( q = 2p + 1 \) is a prime divisor of \( M_p \) if \( a = 2^{\frac{p+1}{2}} \), then
\[
a^2 - 2 = 2^{p+1} - 2 = 2M_p \equiv 0(mod\ q)
\Rightarrow a^2 \equiv 2(mod\ q)
\]
since \( p = \frac{q-1}{2} \) \( \Rightarrow (a^2)^p = a^{q-1} \equiv 2^p(mod\ q) \) \( \cdot \cdot \cdot (1) \)
since \( q \) is an odd integer \( \Rightarrow \ gcd(a, q) = 1 \) and so \( a^{q-1} \equiv 1(mod\ q) \)
(from \( 1 ) \) \( \Rightarrow 2^p \equiv 1(mod\ q) \) \( \Rightarrow q | (2^p - 1) = M_p \).
by theorem 1.3.2 provided that \( q \equiv 1(mod\ 8) \) or \( q \equiv 7(mod\ 8) \)
\( \Rightarrow q \equiv -1(mod\ 8) \)
Example 1.3.5. Consider $M_{17} = 2^{17} - 1$, $p = 17$
we will show that $M_{17}$ is a prime, consider the integers of the form $2kp + 1 = 34k + 1$ which are less than $362 < \sqrt{M_{17}}$, are $35, 69, 103, 137, 171, 205, 239, 273, 307, 341$.

Since the smallest nontrivial divisor of $M_{17}$ must be prime, we need only consider the primes among the foregoing ten numbers, namely, $103, 137, 239, 307$.

Example 1.3.6. If $n$ is an odd perfect number, then $n = p^k m^2$ where $p$ is a prime $p \nmid m$, and $p \equiv k \equiv 1(\text{mod } 4)$; in particular, $n \equiv 1(\text{mod } 4)$.

Corollary 1.3.2. If $n$ is an odd perfect number, then $n$ is of the form $n = p^{k_1}m^2$ where the $p_i$ are distinct odd primes and $p_1 \equiv k_1 \equiv 1(\text{mod } 4)$.

Definition 1.3.2. A positive integer $n$ is said to be deficient number if $\sigma(n) < 2n$, and an abundant number if $\sigma(n) > 2n$.

Example 1.3.7. Let $n = 20 = 4 \cdot 5$ $\sigma(20) = \sigma(2^2)\sigma(5) = \frac{2^3-1}{2-1} \cdot \frac{5^2-1}{5-1} = 7 \cdot 6 = 42$
$\Rightarrow \sigma(20) > 2(20)$
$\Rightarrow 42 > 40$
so $n$ is a bundent number.
$\sigma(4) = 1 + 2 + 4 = 7 < 2 \cdot 4$
so $4$ is deficient number.

Definition 1.3.3. Amicable numbers (friendly numbers):
Amicable pair of numbers $m$ and $n$ are positive integers if each number is equal to the sum of all positive divisors of the other, not counting the number itself, that is $\sigma(m) - m = n$ and $\sigma(n) - n = m$ or $\sigma(m) = m + n = \sigma(n)$.

Example 1.3.8. $m = 220$ and $n = 284$ are amicable pair, because the sum of divisors of $220$ is equal $1 + 2 + 4 + 5 + 10 + 11 + 22 + 55 + 110 = 284$ and the sum of divisors of $284$ is $1 + 2 + 4 + 71 + 142 = 220$. Or $\sigma(220) = 220 + 284 = \sigma(284) = 504$.

Remark 1.3.2. In 9th century the arabian mathematician Thabit ibn Qurra finds rules for amicable pairs:
If $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$, and $r = 9 \cdot 2^{2n-1} - 1$ are all prime numbers,
where $n \geq 2$, then $2^n pq$ and $2^n r$ are an amicable pair of numbers. This rule produces amicable numbers for $n = 2, 4$ and 7, but for no other $n \leq 20000$. 

7
Proof. \( \sigma(2^n pq) = \frac{2^{n+1} - 1}{2 - 1}(p + 1)(q + 1) = (2^{n+1} - 1)(3 \cdot 2^{n-1})(3 \cdot 2^n) = (2^{n+1} - 1)(9 \cdot 2^{2n-1}) \ldots \) (1)

And \( \sigma(2^n r) = (2^{n+1} - 1)(r + 1) = (2^{n+1} - 1)(9 \cdot 2^{2n-1}) \ldots \) (2).

So from (1) and (2) we have \( \sigma(2^n pq) = \sigma(2^n r) \), so the numbers \( 2^n pq \) and \( 2^n r \) are amicable pairs.

\[ \square \]

1.4 Fermat numbers

Definition 1.4.1. A Fermat number is an integer of the form \( F_n = 2^{2^n} + 1 \), for \( n \geq 0 \).

If \( F_n \) is primes it is said to be a Fermat prime.

Example 1.4.1. \( F_0 = 3, \ F_1 = 5, \ F_2 = 17, \ F_3 = 257, \ F_4 = 65537 \) are all primes. But \( F_5 = 429496797 \) is composite number (discovered by Euler) and \( F_5 \) is divisible by 641.

Theorem 1.4.1. The Fermat number \( F_5 \) is divisible by 641.

Proof. Let \( a = 2^7, \ b = 5 \), so \( 1 + ab = 1 + 2^7 \cdot 5 = 641 \).

Since \( 1 + ab - b^4 = 1 + (a - b^3)b = 1 + (128 - 125)b = 1 + 3b = 2^4 \).

But this implies that

\[ F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 2^4(2^7)^4 + 1 = 2^4a^4 + 1 \]

\[ = (1 + ab - b^4)a^4 + 1 = (1 + ab)a^4 + (1 - a^4b^4) = (1 + ab)a^4 + (1 - a^2b^2)(1 + a^2b^2) = (1 + ab)a^4 + (1 - ab)(1 + ab)(1 + a^2b^2) \]

\[ = (1 + ab)[a^4 + (1 - ab)(1 + a^2b^2)] = 641[a^4 + (1 - ab)(1 + a^2b^2)], \] which gives \( 641 | F_5 \), so \( F_5 \) is composite number.

\[ \square \]

Theorem 1.4.2. For Fermat numbers \( F_m \) and \( F_n \), where \( m > n \geq 0 \), \( \gcd(F_m, F_n) = 1 \).

Proof. Put \( d = \gcd(F_m, F_n) \). Since Fermat numbers are odd integers, \( d \) must be odd. If we set \( x = 2^n \) and \( k = 2^{m-n} \), then

\[ \frac{F_m - 2}{F_n} = \frac{(2^x)^{2^{m-n}} - 1}{2^x + 1} = \frac{x^k - 1}{x + 1} = x^{k-1} - x^{k-2} + \cdots - 1 = t \in \mathbb{Z}, \]

hence \( F_n | F_m - 2 \). From \( d | F_n \) it follows that \( d | (F_m - 2) \). But \( d | F_m \implies d | 2 \) but \( d \) is an odd integer, and so \( d = 1 \implies d = 1 = \gcd(F_m, F_n) \).

\[ \square \]