Perfect Numbers and Mersenne Primes

Definition: Let $n \in \mathbb{Z}^+$. If $\sigma(n) = 2n$, then n is called a perfect number.

Ex: $\sigma(6) = 1+2+3+6 = 12 = 2 \times 6$

$\therefore$ 6 is a perfect number.

$\sigma(28) = \sigma(2^2 \cdot 7) = \frac{2^3-1}{2-1} \cdot \frac{7^2-1}{7-1} = 56 = 2 \times 28$

$\therefore$ 28 is a perfect number.

Theorem 7.10: Let $n \in \mathbb{Z}^+$. Then,

n is an even perfect number

$\Longleftrightarrow$

$n = 2^{m-1}(2^m - 1)$ where $m \geq 2$ and $2^m - 1$ is prime.

Proof: Assume that $n = 2^{m-1}(2^m-1)$ where $m \geq 2$ and $2^m - 1$ is prime.

We wish to show that n is an even perfect number.

Since $m \geq 2$, 2^{m-1} is even and hence n is even.

Also, in this case, $2^m - 1$ is odd.

$\therefore \gcd(2^{m-1}, 2^m-1) = 1.$

Hence, as σ is multiplicative, we get

$$\sigma(n) = \sigma(2^{m-1}(2^m-1)) = \sigma(2^{m-1})\,\sigma(2^m-1)$$

By Lemm 7.1,

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

and

$$\sigma(2^m-1) = 2^m-1+1 \quad (\text{as } 2^m-1 \text{ is prime}) = 2^m$$

$$\therefore \sigma(n) = (2^m-1)2^m = 2(2^{m-1}(2^m-1)) = 2n$$

$\therefore n$ is an even perfect number.

To prove the converse, assume that n is an even perfect number.

We can always write n in the form

$$n = 2^s t$$

where $s \geq 1$ ($\because n$ is even) and t is odd.

Since $\gcd(2^s, t) = 1$, by Lemma 7.1,

$$\sigma(n) = \sigma(2^s)\,\sigma(t)$$

$$= \left(\frac{2^{s+1}-1}{2-1}\right)\sigma(t)$$

$$\therefore \sigma(n) = (2^{s+1}-1)\,\sigma(t) \quad \text{—} (1)$$

On the other hand, since n is perfect, we've

$$\sigma(n) = 2n.$$
$$= 2 \cdot 2^s \cdot t$$
$$\sigma(n) = 2^{s+1} t \quad \text{—} (2)$$

$$(1) \text{ and } (2) \implies (2^{s+1}-1)\sigma(t) = 2^{s+1} t \quad \text{—} (3)$$

$$\therefore 2^{s+1} \mid (2^{s+1}-1)\,\sigma(t)$$

Since $\gcd(2^{s+1}, 2^{s+1}-1) = 1$, we've

$$2^{s+1} \mid \sigma(t)$$

$$\therefore \sigma(t) = 2^{s+1} q \text{ for some } q \in \mathbb{Z}.$$

Substitute this in (3) to get

$$(2^{s+1}-1)\, 2^{s+1} q = 2^{s+1} t$$

$$\therefore (2^{s+1}-1) q = t \quad \text{—} (4)$$

$$\therefore q \mid t.$$

Also, $q < t$ since $2^{s+1}-1 > 1$.

$$(4) \implies t + q = 2^{s+1} q$$

$$\therefore t + q = \sigma(t) \quad \text{—} (5)$$

We show that $q = 1$.
Suppose $q > 1$. Then, since $1 < q < t$, we conclude that t has at least three distinct divisors, namely 1, q and t.

$$\therefore \sigma(t) \geq 1 + q + t$$

This contradicts (5).

$$\therefore q = 1$$

$$\therefore t = 2^{s+1} - 1 \quad (\text{by } (4)) \quad (6)$$

Also, $\sigma(t) = t + 1$ (by (5))

$\therefore t \,(>1)$ has only t and 1 as positive divisors.

$\therefore t$ is prime.

$$\therefore n = 2^s t = 2^s(2^{s+1} - 1) \quad (\text{by } (6))$$
with $s \geq 1$

$$= 2^{m-1}(2^m - 1) \text{ where } m = s+1 \geq 2$$
and $2^m - 1$ is prime.

It follows that, in order to find the even perfect numbers, we need to find primes of the form $2^m - 1$.
Following theorem is useful.

Theorem 7.11: Let $m \in \mathbb{Z}^+$. If $2^n - 1$ is prime then n is prime.

Proof: Exercise (This is actually a problem done in the class.)

The contrapositive of the above theorem says

"if n is composite then $2^n - 1$ is composite".

Therefore, in search of the primes of the form $2^n - 1$, we should consider integers n that are prime.

Ex: $2^{35} - 1$ cannot be prime because 35 is not prime.

* The converse of Theorem 7.11 is not true. For example, $2^{11} - 1 = 2047 = 23 \cdot 89$ is composite but 11 is prime.

Definition: Let $m \in \mathbb{Z}^+$.

1. $M_m = 2^m - 1$ is called the m^{th} Mersenne number

2. If $M_p = 2^p - 1$ is prime, where p is prime, then M_p is called a Mersenne prime.

Ex: $M_2 = 2^2 - 1 = 3$ is a Mersenne prime.

$M_3 = 2^3 - 1 = 7$ " " " "

$M_5 = 2^5 - 1 = 31$ " " " "

$M_7 = 2^7 - 1 = 127$ " " " "

$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ is not a Mersenne prime.