Euclid-Euler theorem

Recall that a *Mersenne prime* is a prime of the form $2^n - 1$.

Lemma 2.8.1

If $2^n - 1$ *is a prime, then so is* n.

Mersenne primes

Recall that a *Mersenne prime* is a prime of the form $2^n - 1$.

Lemma 2.8.1

If $2^n - 1$ is a prime, then so is n.

Proof. Suppose, for the sake of contradiction, $n = ab$. Then

$$2^{ab} - 1 = (\underbrace{2^a}_{x})^b - 1 = (2^a - 1)(1 + 2^a + \cdots + (2^a)^{b-1}).$$

Here the last equality follows by applying lemma 2.7.3 to $x = 2^a$. □

$$1 + x + x^2 + \cdots + x^e = \frac{x^{e+1} - 1}{x - 1}$$

Recall that a *Mersenne prime* is a prime of the form $2^n - 1$.

Lemma 2.8.1

If $2^n - 1$ is a prime, then so is n.

Note that the converse is not true. For example,

$$2^{11} - 1 = 2047 = 23 \cdot 89.$$

We will use M_p to denote the candidate of Mersenne prime $2^p - 1$.

We are going to prove the following theorem.

Theorem 2.8.2 (Euclid-Euler)

An even natural number N is perfect if and only if it has the form $N_p := 2^{p-1}M_p$, where M_p is a Mersenne prime.

First, recall that a positive number N is *perfect* iff $\sigma_1(N) = 2N$.

Euclid-Euler theorem

Proof. ($\Longleftarrow$) Suppose M_p is a Mersenne prime. Then we have

$$
\begin{aligned}
\sigma_1(N_p) &= \sigma_1(2^{p-1})\sigma_1(M_p) && \text{by the multiplicativity of } \sigma_1(\cdot) \\
&= \frac{2^p - 1}{2 - 1}(1 + M_p) && \text{by theorem 2.7.2} \\
&= (2^p - 1) \cdot 2^p && M_p := 2^p - 1 \\
&= \boxed{M_p \cdot 2^{p-1}} \cdot 2 = 2N_p.
\end{aligned}
$$

$(\implies)$ Suppose N is an even perfect number. Let $p = v_2(N) + 1$. Note that $p \geqslant 2$ and hence $M_p \geqslant 3$.

($\implies$) Suppose N is an even perfect number. Let $p = v_2(N) + 1$. Note that $p \geqslant 2$ and hence $M_p \geqslant 3$.

Let $q = \frac{N}{2^{p-1}}$. By the prime factorization of N, it is coprime to 2^{p-1}. Hence, by the multiplicativity of $\sigma_1(\cdot)$,

$$\sigma_1(N) = \sigma_1(2^{p-1})\sigma_1(q) = (2^p - 1)\sigma_1(q) = M_p\sigma_1(q).$$

$(\implies)$ Suppose N is an even perfect number. Let $p = v_2(N) + 1$. Note that $p \geqslant 2$ and hence $M_p \geqslant 3$.

Let $q = \frac{N}{2^{p-1}}$. By the prime factorization of N, it is coprime to 2^{p-1}. Hence, by the multiplicativity of $\sigma_1(\cdot)$,

$$\sigma_1(N) = \sigma_1(2^{p-1})\sigma_1(q) = (2^p - 1)\sigma_1(q) = M_p\sigma_1(q).$$

On the other hand, by perfectness of N, we have

$$\sigma_1(N) = 2N = 2^p q = (1 + M_p)q.$$

Combine previous equalities, we obtain

$$M_p \sigma_1(q) = (1 + M_p) q.$$

Let's simplify it:

$$\sigma_1(q) = q + \frac{q}{M_p}.$$

Note that $\frac{q}{M_p}$ is a proper divisor of q since $M_p \geqslant 3$. Hence, the right-hand side is the sum of two distinct divisors of q.

Combine previous equalities, we obtain

$$M_p\sigma_1(q) = (1 + M_p)q.$$

Let's simplify it:

$$\sigma_1(q) = q + \frac{q}{M_p}.$$

Note that $\frac{q}{M_p}$ is a proper divisor of q since $M_p \geqslant 3$. Hence, the right-hand side is the sum of two distinct divisors of q.

However, by definition, $\sigma_1(q)$ is the sum of ALL divisors of q. Therefore, $\frac{q}{M_p}$ and q are all the divisors of q. Consequently, we must have $q = M_p$, and it has to be a prime since it has only two distinct divisors. $\square$