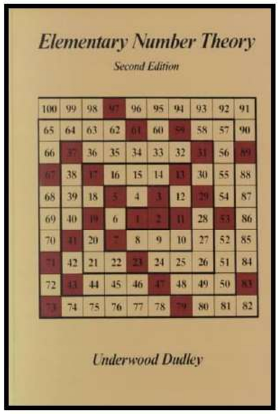
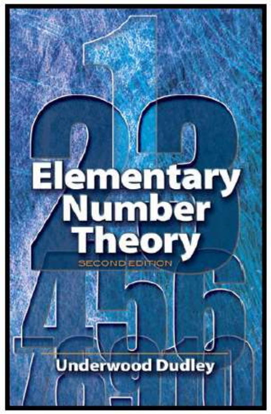
Elementary Number Theory

Section 8. Perfect Numbers—Proofs of Theorems





Theorem 8.1 (Euclid)

Theorem 8.1 (Euclid). If $2^k - 1$ is prime, then $2^{k-1}(2^k - 1)$ is perfect.

Proof. Let $n = 2^{k-1}(2^k - 1)$. Since $2^k - 1$ is prime by hypothesis, then $\sigma(2^k - 1) = (2^k - 1) + 1 = 2^k$ by Note 7.A. Also, $\sigma(p^n) = (p^{n+1} - 1)/(p - 1)$ for prime p by Exercise 7.8, so $\sigma(2^{k-1}) = (2^{(k-1)+1} - 1)/((2) - 1) = 2^k - 1$. Now 2^{k-1} and $2^k - 1$ are relatively prime so, since σ is multiplicative (by Theorem 7.4), we have

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

$$= (2^k - 1) \cdot 2^k = 2 \cdot 2^{k-1}(2^k - 1) = 2n.$$

Thus n is perfect (by definition), as claimed. □

Theorem 8.2 (Euler)

Theorem 8.2 (Euler). If n is an even perfect number, then $n = 2^{p-1}(2^p - 1)$ for some prime p, and $2^p - 1$ is also prime.

Proof. In n is even then $n = 2^e m$ where m is odd and $e \geq 1$. Since $\sigma(m) > m$ (because 1 and m are divisors of m), then we have $\sigma(m) = m + s$ for some $s > 0$. Now $\sigma(2^{e+1}) = 2^{e+2} - 1$ by Exercise 7.8. Since n is perfect, then $\sigma(n) = 2n$ and so by Theorem 7.4

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

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

Thus $m = (2^{e+1} - 1)s$, so that s is a divisor of m, and $s < m$ because $e \geq 1$. But $\sigma(m) = m + s$, so s is the sum of all the divisors of m that are less than m. That is, s is the sum of a group of (positive) numbers that includes s. This is possible only if the group consists of one number. Now 1 is a divisor of m and so this one number must be $s = 1$. That is, the only divisors of $m = (2^{e+1} - 1)s = 2^{e+1} - 1$ are 1 and m itself. Hence, $m = 2^{e+1} - 1$ is prime.

Theorem 8.2 (Euler, continued)

Theorem 8.2 (Euler). If n is an even perfect number, then $n = 2^{p-1}(2^p - 1)$ for some prime p, and $2^p - 1$ is also prime.

Proof (continued). We have that $\sigma(m) = m + s = m + 1$, so that $m = 2^{e+1} - 1$ is prime. By Theorem 8.1 (of Euclid), this implies that $p = e + 1$ is prime. Hence $m = 2^p - 1$ for some prime p, $e = p - 1$, and hence $n = 2^e m = 2^{p-1}(2^p - 1)$, as claimed. □