EUCLIDEAN ALGORITHM (elementary proof of uniqueness)

Use induction.

Suppose $m = p_1 r_1 \cdots = p'_1 r'_1 \cdots$

where no prime on the left occurs on the right

(otherwise cancel and use induction hypothesis)

May assume:

- $p$ smallest among $p, z, z', \ldots$.
- $z$ smallest among $p', z', \ldots$.
- $p < p'$
- more than one term

Then $m > p^2$ and $m \geq p^2 \Rightarrow m^2 > (pp')^2 \Rightarrow m > pp'$
PERFECT NUMBERS

**Definition:** A number \( m \) is called perfect if \( m = \sigma(m) \) where \( \sigma \) is the sum of divisors.

**Example:** \( \sigma(6) = 1 + 2 + 3 + 6 = 12 \)

**Proof:**

Let \( m = \prod p_i^{k_i} \) be the prime decomposition of \( m \), where \( p_i \) are prime numbers. Then

\[
\sigma(m) = \sum_{i=1}^{n} \frac{p_i^{k_i+1} - 1}{p_i - 1}
\]

For a prime \( p \) and \( k \), \( \sigma(p^k) = \frac{p^{k+1} - 1}{p - 1} \)

So if \( m \) is perfect, then

\[
\sum_{i=1}^{n} \frac{p_i^{k_i+1} - 1}{p_i - 1} = m
\]

Then \( m - p\sigma(p) = 0 \) for \( p \mid m \) which implies that \( m = p\sigma(p) \) for each prime \( p \) dividing \( m \). Thus \( m \) is perfect.

**Contradiction:**

Consider a perfect number \( m \) with \( m > 1 \) and \( m \) not divisible by \( 2 \). Assume \( m \) is the smallest such perfect number.

Then \( 2^k \) divides \( m \) for some \( k \), and \( \sigma(2^k) = 2^{k+1} - 2 \)

Thus \( \sigma(2^k) > 2^k \) if \( k > 1 \), contradicting the assumption that \( m \) is perfect.
So \( \frac{2a+1}{m} \) is a proper divisor of \( m \). But \( \delta(m) < m \) if \( \frac{2a+1}{m} = 1 \). Therefore, \( m = \frac{2a+1}{1+1} \).

\[ h = \frac{2a+1}{1+1} = \frac{2a-1}{2} (2a^2) \]

And \( m = \frac{2a+1}{1+1} = \frac{2a-1}{2} (2a^2) \) is odd. So \( \delta(m) = 2 \) if \( m = 2n \) is even.

Conversely: Say \( m \) is a proper divisor of \( n \). Then, \( \frac{n}{m} = 2. \) Then, \( \delta(n) = (2a+1) \) is a prime divisor of \( n \). Therefore, \( n = 2n = 2^{2a+1} \).
Not known if there are so many.

$p = 2^k - 1$ is called a Mersenne prime.

So $m = 2^k - 1$ is a prime.

Here are the only five divisors of $m$.