

Perfect Numbers

Definition. A number $n > 0$ is **perfect** if $\sigma(n) = 2n$. Equivalently, n is perfect if it is equal to the sum of its divisors other than itself.

Example. 6 is perfect, because

$$6 = 1 + 2 + 3, \quad \text{or} \quad 2 \cdot 6 = 1 + 2 + 3 + 6. \quad \square$$

It is not known whether there are any odd perfect numbers, or whether there are infinitely many even perfect numbers. The existence of infinitely many even perfect numbers is related to the existence of infinitely many Mersenne primes by the following result.

Proposition. n is an even perfect number if and only if $n = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is a Mersenne prime.

Proof. First, suppose $2^k - 1$ is prime. Then $n = 2^{k-1}(2^k - 1)$ is even; I want to show that it's perfect. Since $2^k - 1$ is an odd prime, it is relatively prime to 2^{k-1} . Hence,

$$\begin{aligned} \sigma(n) &= \sigma(2^{k-1}(2^k - 1)) = \sigma(2^{k-1}) \sigma(2^k - 1) = \left(\frac{2^k - 1}{2 - 1}\right) \left(\frac{(2^k - 1)^2 - 1}{(2^k - 1) - 1}\right) = \\ &= (2^k - 1)((2^k - 1) + 1) = (2^k - 1)2^k = 2 \cdot 2^{k-1}(2^k - 1) = 2n. \end{aligned}$$

Therefore, n is perfect.

Conversely, suppose n is an even perfect number. I want to show $n = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is a Mersenne prime.

Since n is even, I can write $n = 2^i m$, where $i \geq 1$ and m is odd. Then

$$2^{i+1}m = 2n = \sigma(n) = \sigma(2^i m) = \sigma(2^i)\sigma(m) = (2^{i+1} - 1)\sigma(m).$$

Since 2^{i+1} divides the left side, it divides the right side. But $2^{i+1} - 1$ is odd, so I must have $2^{i+1} \mid \sigma(m)$. I claim further that 2^{i+1} is the *highest* power of 2 which divides $\sigma(m)$. For if $2^{i+2} \mid \sigma(m)$, then

$$2^{i+1}m = (2^{i+1} - 1)\sigma(m) = (2^{i+1} - 1) \cdot 2^{i+2} \cdot \text{junk}.$$

Hence, $m = (2^{i+1} - 1) \cdot 2 \cdot \text{junk}$, which contradicts the fact that m is odd.

Since I now know that 2^{i+1} is the *highest* power of 2 which divides $\sigma(m)$, I can write $\sigma(m) = 2^{i+1}s$, where s is odd. Then

$$2^{i+1}m = (2^{i+1} - 1)\sigma(m) = (2^{i+1} - 1) \cdot 2^{i+1}s, \quad \text{so} \quad m = (2^{i+1} - 1)s.$$

Hence,

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

If I can show $s = 1$, then I will have gotten n to have the right form.

To do this, start with $m = (2^{i+1} - 1)s$. Add s to both sides to get

$$m + s = 2^{i+1}s = \sigma(m).$$

m is divisible by 1, by itself, and by s (because $m = (2^{i+1} - 1)s$). If $s = m$, then

$$n = 2^i m = 2^i (2^{i+1} - 1)s = 2^i (2^{i+1} - 1)m, \quad \text{so} \quad 1 = 2^{i+1} - 1.$$

This implies $i = 0$, which is a contradiction. So $s \neq m$. If in addition $s > 1$, then 1, s , and m are three *distinct* divisors of m , so

$$\sigma(m) \geq m + s + 1.$$

This contradicts $m + s = \sigma(m)$, derived above. Therefore, $s = 1$.

At this point, I know $n = 2^i(2^{i+1} - 1)$. I only need to show that $2^{i+1} - 1$ is prime. Since 1 and $2^{i+1} - 1$ are distinct factors of $2^{i+1} - 1$, I have

$$2^{i+1} = \sigma(m) = \sigma(2^{i+1} - 1) \geq 1 + (2^{i+1} - 1) = 2^{i+1}.$$

Therefore, $\sigma(2^{i+1} - 1) = 2^{i+1}$. But this means that 1 and $2^{i+1} - 1$ are the *only* factors of $2^{i+1} - 1$, i.e. $2^{i+1} - 1$ is prime. \square

Example. $2^7 - 1 = 127$ is prime, so

$$2^6(2^7 - 1) = 8128$$

is perfect. \square

I now know that finding even perfect numbers is equivalent to finding Mersenne primes — primes of the form $2^n - 1$. I showed earlier that $2^n - 1$ is prime implies that n is prime. So to look for Mersenne primes, I only need to look at $2^n - 1$ for n prime. Next, I'll derive a result which simplifies checking that $2^n - 1$ is prime. First, here's an amusing lemma.

Lemma. $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$.

Proof. Assume without loss of generality that $a \geq b$. The greatest common divisor of two numbers doesn't change if I subtract the smaller from the larger, so

$$(2^a - 1, 2^b - 1) = ((2^a - 1) - (2^b - 1), 2^b - 1) = (2^a - 2^b, 2^b - 1) = (2^b(2^{a-b} - 1), 2^b - 1).$$

Since $2^b - 1$ is odd, it has no factors in common with the 2^b in the first term. So

$$(2^b(2^{a-b} - 1), 2^b - 1) = (2^{a-b} - 1, 2^b - 1).$$

Now I see that the “ $2^{(\cdot)} - 1$ ” in each slot is just along for the ride: All the action is taking place in the exponents. And what is happening is that the subtraction algorithm for computing greatest common divisors is operating in the exponents! — the original pair a, b , was replaced by $a - b, b$.

It follows that the exponents will “converge” to (a, b) , because this is what the subtraction algorithm does. And when the algorithm terminates, I'll have $(2^{(a,b)} - 1, 0) = 2^{(a,b)} - 1$, proving the result. \square

Example. $(42, 54) = 6$, so

$$(2^{42} - 1, 2^{54} - 1) = 2^6 - 1 = 63.$$

This is surely not obvious, especially when you consider that $2^{42} - 1 = 4398046511103$ and $2^{54} - 1 = 18014398509481983$! \square

Theorem. Let p be an odd prime. Every factor of $2^p - 1$ has the form $2kp + 1$ for some $k \geq 0$.

Proof. It suffices to prove that the result holds for *prime* factors of $2^p - 1$. For

$$(2ap + 1)(2bp + 1) = 2(2abp + a + b)p + 1,$$

so products of numbers of the form $2kp + 1$ also have that form.

Suppose then that q is a prime factor of $2^p - 1$. Little Fermat says $q \mid 2^{q-1} - 1$. The preceding lemma implies that

$$(2^p - 1, 2^{q-1} - 1) = 2^{(p, q-1)} - 1.$$

Now $q \mid 2^p - 1$ and $q \mid 2^{q-1} - 1$ implies $q \mid 2^{(p, q-1)} - 1$. In particular, $2^{(p, q-1)} - 1 > 1$, since it's divisible by the prime q . This in turn implies that $(p, q-1) > 1$. Now p is prime, so this is only possible if $(p, q-1) = p$. In particular, $p \mid q-1$.

Write $q-1 = tp$, so $q = tp + 1$. q is odd, so $q-1$ is even, and tp is even. Since p is odd, t must be even: $t = 2k$ for some k . Then $q = 2kp + 1$, which is what I wanted to show. \square

Example. Is $2^{17} - 1 = 131071$ prime? $\sqrt{131071} \approx 362$. If $2^{17} - 1$ has a proper prime factor, it must have one less than 362, and the prime factor must have the form $2k \cdot 17 + 1 = 34k + 1$. So I need to check the primes less than 362 to see if they divide 131071.

k	$34k + 1$	
1	35	Not prime
2	69	Not prime
3	103	103 \nmid 131071
4	137	137 \nmid 131071
5	171	Not prime
6	205	Not prime
7	239	239 \nmid 131071
8	273	Not prime
9	307	307 \nmid 131071
10	341	Not prime

Therefore, $2^{17} - 1$ is prime. \square