The Euler Phi Function

- An **arithmetic function** takes positive integers as inputs and produces real or complex numbers as outputs.
- If f is an arithmetic function, the **divisor sum** $Df(n)$ is the sum of the values of f at the positive divisors of n.
- $\tau(n)$ is the number of positive divisors of n; $\sigma(n)$ is the sum of the positive divisors of n.
- The **Möbius function** $\mu(n)$ is 1 if $n = 1$ and 0 if n has a repeated prime factor. Otherwise, it is $(-1)^k$, where k is the number of (distinct) prime factors.
- The **Dirichlet product** of arithmetic functions f and g is $(f * g)(n) = \displaystyle\sum_{d|n} f(d)g\left(\frac{n}{d}\right)$.
- The **Möbius inversion formula** says that $\mu * Df = f$.
- $D\phi(n) = n$.
- $\phi(n) = n \cdot \displaystyle\prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$.
- The Euler phi function is **multiplicative**: If $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

I'm going to describe a formula for computing $\phi(n)$ which uses the prime factorization of n. This will require some preliminaries on **divisor sums**.

Definition. An **arithmetic function** is a function defined on the positive integers which takes values in the real or complex numbers.

Examples. (a) Define $f : \mathbb{Z}^+ \to \mathbb{R}$ by $f(n) = \sin n$. Then f is an arithmetic function.

(b) The Euler phi function ϕ is an arithmetic function.

(c) Define $\tau : \mathbb{Z}^+ \to \mathbb{Z}^+$ by

$$\tau(n) = (\text{the number of positive divisors of } n).$$

For example, $\tau(12) = 6$, since there are 6 positive divisors of 12 — 1, 2, 3, 4, 6, and 12. τ is an arithmetic function.

(d) Define $\sigma : \mathbb{Z}^+ \to \mathbb{Z}^+$ by

$$\sigma(n) = (\text{the sum of the positive divisors of } n).$$

Since 1, 2, 3, 6, 9, and 18 are the positive divisors of 18,

$$\sigma(18) = 1 + 2 + 3 + 6 + 9 + 18 = 39.$$

σ is an arithmetic function. □

Definition. The **Möbius function** is the arithmetic function defined by $\mu(1) = 1$, and for $n > 1$,

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_i \cdots p_k,\ p_i \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases}.$$

Thus, $\mu(n) = 0$ if n is divisible by a square.

Example. $\mu(6) = 1$, since $6 = 2 \cdot 3$. Likewise, $\mu(30) = -1$, since $30 = 2 \cdot 3 \cdot 5$. But $\mu(12) = 0$ and $\mu(250 = 0$. □

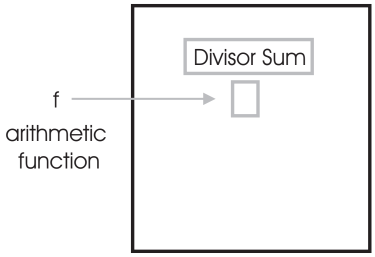
Definition. If f is an arithmetic function, the **divisor sum** of f is

$$[D(f)](n) = \sum_{d|n} f(d).$$

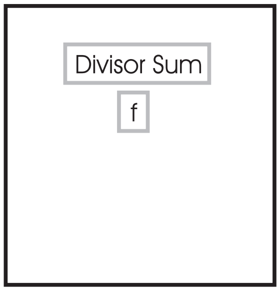
To save writing, I'll make the convention that when I write "$\sum_{d|n}$", I mean to sum over all the *positive* divisors of a positive integer n. Thus, the divisor sum of f evaluated at a positive integer n takes the positive divisors of n, plugs them into f, and adds up the results.

Notice that the divisor sum is a function *which takes an arithmetic function as input and produces an arithmetic function as output*.

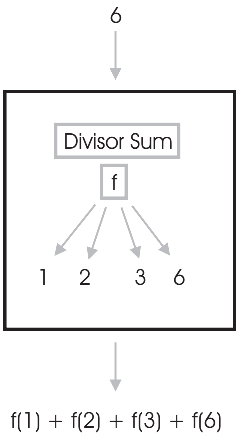
The divisor sum machine takes in an arithmetic function f.



With f installed in the divisor sum machine, you get a new arithmetic function: D(f).



D(f) works by taking a number, applying f to each divisor of the sum, and adding up the results.



Example. Suppose $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ is defined by $f(n) = n^2$. Then

$$[D(f)](n) = \sum_{d|n} d^2.$$

For example,

$$[D(f)](12) = \sum_{d|12} d^2 = 1^2 + 2^2 + 3^2 + 4^2 + 6^2 + 12^2 = 210.$$

Lemma.

$$[D(\mu)](n) = \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Proof. The formula for $n = 1$ is obvious.

Suppose $n > 1$. Let

$$n = p_1^{r_1} \cdots p_k^{r_k}$$

be the factorization of n into distinct primes. What are the nonzero terms in the sum $\sum_{d|n} \mu(d)$? They will come from d's which are products of single powers of $p_1, \ldots p_k$, and also $d = 1$.

For example, $\mu(p_1 p_2 p_7)$ and $\mu(p_2 p_4)$ would give rise to nonzero terms in the sum, but $\mu(p_3^3 p_8) = 0$.

So

$$\sum_{d|n} \mu(d) = 1 + (\mu(p_1) + \cdots + \mu(p_k)) + (\mu(p_1 p_2) + \mu(p_1 p_3) + \cdots + \mu(p_{k-1} p_k)) + \cdots + \mu(p_1 p_2 \cdots p_k) =$$

$$1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k = (1-1)^k = 0. \quad \square$$

Example. Suppose $n = 24$. The divisor sum is

$$\sum_{d|24} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12) + \mu(24) = 1 + (-1) + (-1) + 0 + 1 + 0 + 0 = 0. \quad \square$$

Definition. If f and g are arithmetic functions, their **Dirichlet product** is

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Example. If f and g are arithmetic functions,

$$(f * g)(12) = f(1)g(12) + f(2)g(6) + f(3)g(4) + f(4)(g(3) + f(6)g(2) + f(12)(g(1). \quad \square$$

I'll need two helper functions in what follows. Define

$$I(n) = 1 \quad \text{for all} \quad n \in \mathbb{Z}^+,$$

$$e(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases} \quad \text{for all} \quad n \in \mathbb{Z}^+.$$

Properties of the Dirichlet product.

Let f, g, and h be arithmetic functions.

1. $f * g = g * f$.
2. $(f * g) * h = f * (g * h)$.
3. $f * e = f = e * f$.
4. $f * I = Df = I * f$.
5. $\mu * I = e$.

Proof. For property 1, note that divisors of n come in pairs $\left\{d, \dfrac{n}{d}\right\}$, and that if $\left\{d, \dfrac{n}{d}\right\}$ is a divisor pair, so is $\left\{\dfrac{n}{d}, d\right\}$. This means that the same terms occur in both

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) \quad \text{and} \quad (g * f)(n) = \sum_{d|n} g(d)f\left(\frac{n}{d}\right),$$

so they're equal.

Associativity is a little tedious, so I'll just note that $[(f * g) * h](n)$ and $[f * (g * h)](n)$ are equal to

$$\sum_{\{d,e,f\}} f(d)g(e)h(f),$$

where the sum runs over all triples of positive numbers d, e, f such that $def = n$. You can fill in the details.

For property 3, note that

$$(f * e)(n) = \sum_{d|n} f(d)e\left(\frac{n}{d}\right) = f(n)e(1) = f(n).$$

($e\left(\dfrac{n}{d}\right)$ is 0 except when $\dfrac{n}{d} = 1$, i.e. when $d = n$.)

For property 4,

$$(f * I)(n) = \sum_{d|n} f(d)I\left(\frac{n}{d}\right) = \sum_{d|n} f(d) \cdot 1 = \sum_{d|n} f(d) = (Df)(n).$$

For property 5, start with $n = 1$:

$$(\mu * I)(1) = \mu(1)I(1) = 1 \cdot 1 = 1 = e(1).$$

Now suppose $n > 0$. Then

$$(\mu * I)(n) = (D\mu)(n) = 0 = e(n).$$

Therefore, the formula holds for all n. □

The next result is very powerful, but the proof will look easy with all the machinery I've collected.

Theorem. (**Möbius Inversion Formula**) If f is an arithmetic function, then $f = \mu * Df$.

Proof.

$$\mu * Df = \mu * I * f = e * f = f. \quad \square$$

Next, I'll compute the divisor sum of the Euler phi function.

Lemma.

$$[D(\phi)](n) = \sum_{d|n} \phi(d) = n.$$

Proof. Let n be a positive integer. Construct the fractions

$$\frac{1}{n}, \quad \frac{2}{n}, \ldots, \frac{n-1}{n}, \quad \frac{n}{n}.$$

Reduce them all to lowest terms. Consider a typical lowest-term fraction $\dfrac{a}{d}$. Here $d \mid n$ (because it came from a fraction whose denominator was n, $a < d$ (because the original fraction was less than 1), and $(a, d) = 1$ (because it's in lowest terms).

Notice that (going the other way) if $\dfrac{a}{d}$ is a fraction with positive top and bottom which satisfies $d \mid n$, $a < d$, and $(a, d) = 1$, then it *is* one of the lowest-terms fractions. For $dk = n$ for some k, and then $\dfrac{a}{d} = \dfrac{ka}{kd} = \dfrac{ka}{n}$ — and the last fraction is one of the original fractions.

How many of the lowest-terms fractions have "d" on the bottom? Since the "a" on top is a positive number relatively prime to d, there are $\phi(d)$ such fractions. Summing over all d's which divide n gives $\displaystyle\sum_{d|n} \phi(d)$. But since every lowest-terms fraction has *some such* "d" on the bottom, this sum accounts for all the fractions — and there are n of them. Therefore, $\displaystyle\sum_{d|n} \phi(d) = n$. □

Example. Suppose $n = 6$. Then

$$\sum_{d|6} \phi(d) = \phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2 = 6. \quad \square$$

Lemma. Let $n \ge 1$.

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Proof. By Möbius inversion and the previous result,

$$\phi(n) = (\mu * D\phi)(n) = \sum_{d|n} \mu(d) D\phi\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \frac{n}{d}. \quad \square$$

Example. Take $n = 6$, so $\phi(6) = 2$.

$$\sum_{d|6} \mu(d) \frac{6}{d} = \mu(1) \cdot \frac{6}{1} + \mu(2) \cdot \frac{6}{2} + \mu(3) \cdot \frac{6}{3} + \mu(6) \cdot \frac{6}{6} =$$

$$(1)(6) + (-1)(3) + (-1)(2) + (1)(1) = 2. \quad \square$$

Theorem. Let $n \ge 1$.

$$\phi(n) = n \cdot \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

(By convention, the empty product — the product with no terms — equals 1.)

Proof. If $n = 1$, the result is immediate by convention.

If $n > 1$, let $p_1, \ldots, p_k$ be the distinct prime factors of n. Then

$$\prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) =$$

$$1 - \sum_i \frac{1}{p_i} + \sum_{i \neq j} \frac{1}{p_i p_j} - \cdots + (-1)^k \frac{1}{p_1 p_2 \cdots p_k}.$$

Each term is $\pm\dfrac{1}{d}$, where d is 1 (the first term) or a product of *distinct* primes. The $(-1)^i$ in front of each term alternates signs according to the number of p's — which is exactly what the Möbius function does. So the expression above is

$$\sum_{d \mid n} \frac{\mu(d)}{d}.$$

(I can run the sum over *all* divisors, because $\mu(d) = 0$ if d has a repeated prime factor.) Now simply multiply by n:

$$n \cdot \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) = \sum_{d \mid n} \mu(d) \frac{n}{d} = \phi(n). \quad \square$$

Example. $40 = 2^3 \cdot 5$, so

$$\phi(40) = 40\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 16.$$

Likewise, $81 = 3^4$, so

$$\phi(81) = 81 \cdot \left(1 - \frac{1}{3}\right) = 54.$$

More generally, if p is prime and $k \geq 1$, then

$$\phi(p^k) = p^k - p^{k-1}.$$

For

$$\phi(p^k) = p^k \cdot \left(1 - \frac{1}{p}\right) = p^k - p^{k-1}. \quad \square$$

Definition. An arithmetic function f is **multiplicative** if $(m, n) = 1$ implies

$$f(mn) = f(m)f(n).$$

Lemma. ϕ is multiplicative — that is, if $(m, n) = 1$, then

$$\phi(mn) = \phi(m)\phi(n).$$

Proof. Suppose $(m, n) = 1$. Now

$$\phi(m) = m \cdot \prod_{\substack{p \mid m \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) \quad \text{and} \quad \phi(n) = n \cdot \prod_{\substack{q \mid n \\ q \text{ prime}}} \left(1 - \frac{1}{q}\right).$$

So

$$\frac{\phi(m)\phi(n)}{mn} = \left(\prod_{\substack{p \mid m \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)\right) \left(\prod_{\substack{q \mid n \\ q \text{ prime}}} \left(1 - \frac{1}{q}\right)\right).$$

Since $(m, n) = 1$, the two products have no primes in common. Moreover, the primes that appear in *either* of the products are exactly the prime factors of mn. So

$$\frac{\phi(m)\phi(n)}{mn} = \prod_{\substack{r \mid mn \\ r \text{ prime}}} \left(1 - \frac{1}{r}\right).$$

Hence,

$$\phi(m)\phi(n) = (mn) \cdot \prod_{\substack{r \mid mn \\ r \text{ prime}}} \left(1 - \frac{1}{r}\right) = \phi(mn). \quad \square$$

Example. If $n \geq 3$, then $\phi(n)$ is even. In fact, if n has k odd prime factors, then $2^k \mid \phi(n)$.

To see this, observe first that

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

This is even if $2^k \geq 4$.

So suppose that n has k odd prime factors. Then

$$\phi(n) = n \cdot \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) = \phi(n) = n \cdot \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(\frac{p-1}{p}\right) = \frac{n}{\displaystyle\prod_{\substack{p \mid n \\ p \text{ prime}}} p} \prod_{\substack{p \mid n \\ p \text{ prime}}} (p-1).$$

The denominator of the fraction is the product of primes dividing n, so the fraction is actually an integer. The second term has at least one even factor for each odd prime dividing n, because if p is an odd prime then $p - 1$ is even. Hence, the second term — and therefore $\phi(n)$ — is divisible by 2^k.

For example, consider $7623 = 3^2 \cdot 7 \cdot 11^2$. There are 3 odd prime factors, so $\phi(7623)$ should be divisible by 8. And in fact, $\phi(7623) = 3960 = 8 \cdot 495$. $\square$

The Sum and Number of Divisors

Definition. The **sum of divisors** function is given by

$$\sigma(n) = \sum_{d \mid n} d.$$

The **number of divisors** function is given by

$$\tau(n) = \sum_{d \mid n} 1.$$

Example. Recall that a number is **perfect** if it's equal to the sum of its divisors other than itself. It follows that a number n is perfect if $\sigma(n) = 2n$. □

Example.

$$\sigma(15) = 1 + 3 + 5 + 15 = 24 \quad \text{and} \quad \tau(15) = 4. \quad \square$$

I want to show that σ and τ are multiplicative. I can do most of the work in the following lemma.

Lemma. The divisor sum of a multiplicative function is multiplicative.

Proof. Suppose f is multiplicative, and let $D(f)$ be the divisor sum of f. Suppose $(m, n) = 1$. Then

$$[D(f)](m) = \sum_{a \mid m} f(a) \quad \text{and} \quad [D(f)](n) = \sum_{b \mid n} f(b).$$

Then

$$[D(f)](m) \cdot [D(f)](n) = \left(\sum_{a \mid m} f(a)\right) \left(\sum_{b \mid n} f(b)\right) = \sum_{a \mid m} \sum_{b \mid n} f(a) f(b).$$

Now $(m, n) = 1$, so if $a \mid m$ and $b \mid n$, then $(a, b) = 1$. Therefore, multiplicativity of f implies

$$[D(f)](m) \cdot [D(f)](n) = \sum_{a \mid m} \sum_{b \mid n} f(ab).$$

Now every divisor d of mn can be written as $d = ab$, where $a \mid m$ and $b \mid n$. Going the other way, if $a \mid m$ and $b \mid n$ then $ab \mid mn$. So I may set $d = ab$, where $d \mid mn$, and replace the double sum with a single sum:

$$[D(f)](m) \cdot [D(f)](n) = \sum_{d \mid mn} f(ab) = [D(f)](mn).$$

This proves that $D(f)$ is multiplicative. □

Example. The identity function $\text{id}(x) = x$ is multiplicative: $\text{id}(mn) = mn = \text{id}(m) \cdot \text{id}(n)$ for *all* m, n (so *a fortiori* for $(m, n) = 1$). Therefore, the divisor sum of id is multiplicative. But

$$[D(\text{id})](n) = \sum_{d \mid n} \text{id}(d) = \sum_{d \mid n} d = \sigma(n).$$

Hence, the sum of divisors function σ is multiplicative. □

Example. The constant function $I(n) = 1$ is multiplicative: $I(mn) = mn = I(m) \cdot I(n)$ for *all* m, n (so *a fortiori* for $(m, n) = 1$). Therefore, the divisor sum of I is multiplicative. But

$$[D(I)](n) = \sum_{d|n} I(d) = \sum_{d|n} 1 = \tau(n).$$

Hence, the number of divisors function τ is multiplicative. □

I'll use multiplicativity to obtain formulas for $\sigma(n)$ and $\tau(n)$ in terms of their prime factorizations (as I did with ϕ). First, I'll get the formulas in the case where n is a power of a prime.

Lemma. Let p be prime. Then:

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$$

$$\tau(p^k) = k + 1$$

Proof. The divisors of p^k are 1, p, p^2, ..., p^k. So the sum of the divisors is

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

And since the divisors of p^k are 1, p, p^2, ..., p^k, there are $k + 1$ of them, and

$$\tau(p^k) = k + 1. \quad □$$

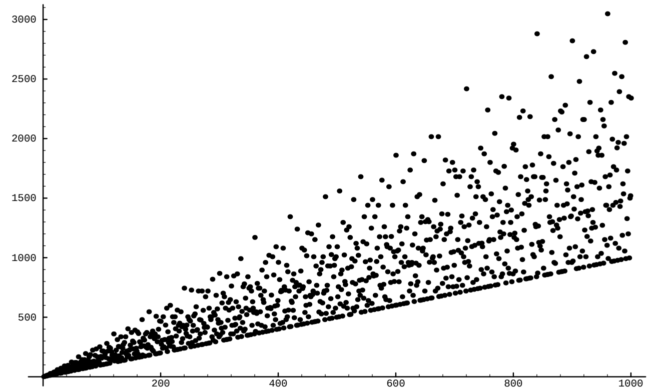
Theorem. Let $n = p_1^{r_1} \cdots p_k^{r_k}$, where the p's are distinct primes and $r_i \geq 1$ for all i. Then:

$$\sigma(n) = \left(\frac{p_1^{r_1+1} - 1}{p_1 - 1}\right) \cdots \left(\frac{p_k^{r_k+1} - 1}{p_k - 1}\right)$$

$$\tau(n) = (r_1 + 1) \cdots (r_k + 1)$$

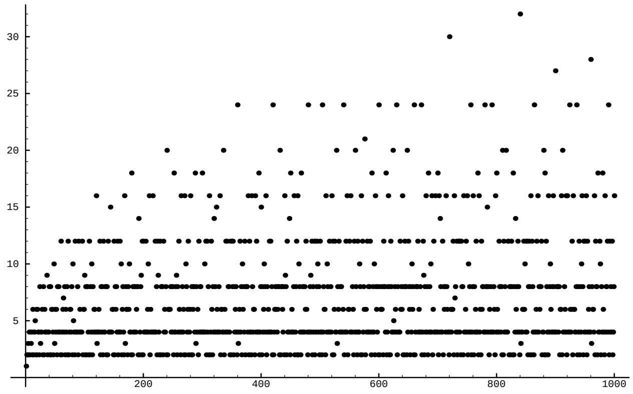
Proof. These results follow from the preceding lemma, the fact that σ and τ are multiplicative, and the fact that the prime power factors $p_i^{r_i}$ are pairwise relatively prime. □

Here is a graph of $\sigma(n)$ for $1 \leq n \leq 1000$.



Note that if p is prime, $\sigma p = p+1$. This gives the point $(p, p+1)$, which lies on the line $y = x+1$. This is the line that you see bounding the dots below.

Here is a graph of $\tau(n)$ for $1 \le n \le 1000$.



If p is prime, $\tau(p) = 2$. Thus, τ repeatedly returns to the horizontal line $y = 2$, which you can see bounding the dots below.

Example. $720 = 2^4 \cdot 3^2 \cdot 5$, so

$$\sigma(720) = \left(\frac{2^5-1}{2-1}\right)\left(\frac{3^3-1}{3-1}\right)\left(\frac{5^2-1}{5-1}\right) = 2418,$$

$$\tau(720) = (4+1)(2+1)(1+1) = 30. \quad \square$$

Example. For each n, there are only finitely many numbers k whose divisors sum to n: $\sigma(k) = n$. For k divides itself, so

$$n = \sigma(k) = (\text{junk}) + k > k.$$

This says that k must be less than n. So if I'm looking for numbers whose divisors sum to n, I only need to look at numbers less than n. For example, if I want to find all numbers whose divisors sum to 42, I only need to look at $\{1, 2, \ldots, 41\}$. $\square$

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,

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

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

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 $i \ge 1$ 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 $i = 0$ ⤫. 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. □

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

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

is perfect. □

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

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

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. □

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 $2^{54} - 1 = 18014398509481983$! □

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. □

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	$103 \not\mid 131071$
4	137	$137 \not\mid 131071$
5	171	Not prime
6	205	Not prime
7	239	$239 \not\mid 131071$
8	273	Not prime
9	307	$307 \not\mid 131071$
10	341	Not prime

Therefore, $2^{17} - 1$ is prime. □