Mersenne Primes

From Chapter 14 of *A Friendly Introduction to Number Theory*, Fourth Edition. Joseph H. Silverman.
Copyright © 2013 by Pearson Education, Inc. All rights reserved.

Mersenne Primes

In this chapter we will study primes that can be written in the form $a^n - 1$ with $n \geq 2$. For example, 31 is such a prime, since $31 = 2^5 - 1$. The first step is to look at some data.

$2^2 - 1 = 3$	$2^3 - 1 = 7$	$2^4 - 1 = 3 \cdot 5$	$2^5 - 1 = 31$
$3^2 - 1 = 2^3$	$3^3 - 1 = 2 \cdot 13$	$3^4 - 1 = 2^4 \cdot 5$	$3^5 - 1 = 2 \cdot 11^2$
$4^2 - 1 = 3 \cdot 5$	$4^3 - 1 = 3^2 \cdot 7$	$4^4 - 1 = 3 \cdot 5 \cdot 17$	$4^5 - 1 = 3 \cdot 11 \cdot 31$
$5^2 - 1 = 2^3 \cdot 3$	$5^3 - 1 = 2^2 \cdot 31$	$5^4 - 1 = 2^4 \cdot 3 \cdot 13$	$5^5 - 1 = 2^2 \cdot 11 \cdot 71$
$6^2 - 1 = 5 \cdot 7$	$6^3 - 1 = 5 \cdot 43$	$6^4 - 1 = 5 \cdot 7 \cdot 37$	$6^5 - 1 = 5^2 \cdot 311$
$7^2 - 1 = 2^4 \cdot 3$	$7^3 - 1 = 2 \cdot 3^2 \cdot 19$	$7^4 - 1 = 2^5 \cdot 3 \cdot 5^2$	$7^5 - 1 = 2 \cdot 3 \cdot 2801$
$8^2 - 1 = 3^2 \cdot 7$	$8^3 - 1 = 7 \cdot 73$	$8^4 - 1 = 3^2 \cdot 5 \cdot 7 \cdot 13$	$8^5 - 1 = 7 \cdot 31 \cdot 151$

An easy observation is that if a is odd then $a^n - 1$ is even, so it cannot be prime. Looking at the table, we also see that it appears that $a^n - 1$ is always divisible by $a - 1$. This observation is indeed true. We can prove that it is true by using the famous formula for the sum of a geometric series:

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1). \qquad \textbf{Geometric Series}$$

To check this Geometric Series formula, we multiply out the product on the right. Thus,

$$\begin{aligned}(x-1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1) \\ &= x \cdot (x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1) \\ &\quad - 1 \cdot (x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1)\end{aligned}$$

$$\begin{aligned} &= (x^n + x^{n-1} + \cdots + x^3 + x^2 + x) \\ &\qquad - (x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1) \\ &= x^n - 1, \end{aligned}$$

since all the other terms cancel.

Using the Geometric Series formula with $x = a$, we see immediately that $a^n - 1$ is always divisible by $a - 1$. So $a^n - 1$ will be composite unless $a - 1 = 1$, that is, unless $a = 2$.

However, even if $a = 2$, the number $2^n - 1$ is frequently composite. Again we look at some data:

n	2	3	4	5	6	7	8	9	10
$2^n - 1$	3	7	$3 \cdot 5$	31	$3^2 \cdot 7$	127	$3 \cdot 5 \cdot 17$	$7 \cdot 73$	$3 \cdot 11 \cdot 31$

Even this short table suggests the following:

When n is even, $2^n - 1$ is divisible by $3 = 2^2 - 1$.
When n is divisible by 3, $2^n - 1$ is divisible by $7 = 2^3 - 1$.
When n is divisible by 5, $2^n - 1$ is divisible by $31 = 2^5 - 1$.

So we suspect that if n is divisible by m, then $2^n - 1$ will be divisible by $2^m - 1$.

Having made this observation, it is easy to verify that it is true. So suppose that n factors as $n = mk$. Then $2^n = 2^{mk} = (2^m)^k$. We use the Geometric Series formula with $x = 2^m$ to obtain

$$2^n - 1 = (2^m)^k - 1 = (2^m - 1)\big((2^m)^{k-1} + (2^m)^{k-2} + \cdots + (2^m)^2 + (2^m) + 1\big).$$

This shows that if n is composite then $2^n - 1$ is composite. We have verified the following fact.

Proposition 1. *If $a^n - 1$ is prime for some numbers $a \geq 2$ and $n \geq 2$, then a must equal 2 and n must be a prime.*

This means that if we are interested in primes of the form $a^n - 1$ we only need to consider the case that $a = 2$ and n is prime. Primes of the form

$$2^p - 1$$

are called *Mersenne primes*. The first few Mersenne primes are

$$2^2 - 1 = 3, \quad 2^3 - 1 = 7, \quad 2^5 - 1 = 31, \quad 2^7 - 1 = 127, \quad 2^{13} - 1 = 8191.$$

Of course, not every number $2^p - 1$ is prime. For example,

$$2^{11} - 1 = 2047 = 23 \cdot 89 \quad \text{and} \quad 2^{29} - 1 = 536870911 = 233 \cdot 1103 \cdot 2089.$$

The Mersenne primes are named after Father Marin Mersenne (1588–1648), who asserted in 1644 that $2^p - 1$ is prime for

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

and that these are the only primes less than 258 for which $2^p - 1$ is prime. It is not known how Mersenne discovered these "facts," especially since it turns out that his list is not correct. The complete list of primes p less than 10000 for which $2^p - 1$ is prime is[1]

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279,$$
$$2203, 2281, 3217, 4253, 4423, 9689, 9941.$$

It is a nontrivial problem to check a large number for primality, and indeed it wasn't until 1876 that E. Lucas proved conclusively that $2^{127} - 1$ is prime. Lucas's 39-digit number remained the largest known prime until the 1950s, when the advent of electronic computing machines made it possible to check numbers with hundreds of digits for primality. Table 1 lists Mersenne primes that have been discovered in recent years using computers, together with the names of the people who made the discoveries. The largest known prime has more than 12 million digits!

The most recent Mersenne primes in Table 1 were unearthed using specialized software as part of Woltman's Great Internet Mersenne Prime Search. You, too, can take part in the search for world record primes[2] by downloading software from the GIMPS website

`www.mersenne.org/prime.htm`

Further historical and topical information about Mersenne primes is available at

`www.utm.edu/research/primes/mersenne.shtml`

Of course, although it is interesting to see a list like this of the world's largest known primes, there is no huge mathematical significance in finding a few more Mersenne primes. Far more interesting from a mathematical perspective is the following question. The answer is not known.

[1] Notice that Father Mersenne made five mistakes, three of omission (61, 89, 107) and two of commission (67, 257).

[2] Andy Warhol opined that in the future everyone will be famous for 15 minutes. One route to such fame is to find the largest known (Mersenne) prime. And the quest for bigger and better primes continues.

p	Discovered by	Date
521, 607 1279, 2203 2281	Robinson	1952
3217	Riesel	1957
4253 4423	Hurwitz	1961
9689 9941 11213	Gillies	1963
19937	Tuckerman	1971
21707	Noll Nickel	1978
23209	Noll	1979
44497	Noll Slowinski	1979
86243	Slowinski	1982
132049	Slowinski	1983
216091	Slowinski	1985
110503	Colquitt Welsch	1988

p	Discovered by	Date
756839	Slowinski Gage	1992
859433	Slowinski Gage	1994
1257787	Slowinski Gage	1996
1398269*	Armengaud	1996
2976221*	Spence	1997
3021377*	Clarkson	1998
6972593*	Hajratwala	1999
13466917*	Cameron	2001
20996011*	Shafer	2003
24036583*	Findley	2004
25964951*	Nowak	2005
30402457*	Boone, Cooper	2005
32582657*	Boone, Cooper	2006
37156667*	Elvenich	2008
42643801*	Strindmo	2009
43112609*	Smith	2008

Table 1: Primes $p \geq 500$ for Which $2^p - 1$ Is Known to be Prime
*Discovered with GIMPS (Woltman, Kurokowski,...)

Question 2. Are there infinitely many Mersenne primes, or does the list of Mersenne primes eventually stop?

Exercises

1. If $a^n + 1$ is prime for some numbers $a \geq 2$ and $n \geq 1$, show that n must be a power of 2.

2. Let $F_k = 2^{2^k} + 1$. For example, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$. Fermat thought that all the F_k's might be prime, but Euler showed in 1732 that F_5 factors as $641 \cdot 6700417$, and in 1880 Landry showed that F_6 is composite. Primes of the form F_k are called *Fermat primes*. Show that if $k \neq m$, then the numbers F_k and F_m have no common factors; that is, show that $\gcd(F_k, F_m) = 1$. [*Hint*. If $k > m$, show that F_m divides $F_k - 2$.]

3. The numbers $3^n - 1$ are never prime (if $n \geq 2$), since they are always even. However, it sometimes happens that $(3^n - 1)/2$ is prime. For example, $(3^3 - 1)/2 = 13$ is prime.
(a) Find another prime of the form $(3^n - 1)/2$.

(b) If n is even, show that $(3^n - 1)/2$ is always divisible by 4, so it can never be prime.

(c) Use a similar argument to show that if n is a multiple of 5 then $(3^n - 1)/2$ is never a prime.

(d) Do you think that there are infinitely many primes of the form $(3^n - 1)/2$?

Mersenne Primes and Perfect Numbers

The ancient Greeks observed that the number 6 has a surprising property. If you take the proper divisors of 6, that is, the divisors other than 6 itself, and add them up, you get back the number 6. Thus, the proper divisors of 6 are 1, 2, and 3, and when you add these divisors, you get

$$1 + 2 + 3 = 6.$$

This property is rather rare, as can be seen by looking at a few examples:

n	Sum of Proper Divisors of n	
6	$1 + 2 + 3 = 6$	Sum is just right (perfect!).
10	$1 + 2 + 5 = 8$	Sum is too small.
12	$1 + 2 + 3 + 4 + 6 = 16$	Sum is too large.
15	$1 + 3 + 5 = 9$	Sum is too small.
20	$1 + 2 + 4 + 5 + 10 = 22$	Sum is too large.
28	$1 + 2 + 4 + 7 + 14 = 28$	Sum is just right (perfect!).
45	$1 + 3 + 5 + 9 + 15 = 33$	Sum is too small.

The Greeks called these special numbers perfect. That is, a *perfect number* is a number that is equal to the sum of its proper divisors. So far, we have discovered two perfect numbers, 6 and 28. Are there others?

The Greeks knew a method for finding some perfect numbers and, interestingly enough, their method is closely related to the Mersenne primes. The following assertion occurs as Proposition 36 of Book IX of Euclid's *Elements*.

From Chapter 15 of *A Friendly Introduction to Number Theory*, Fourth Edition. Joseph H. Silverman.
Copyright © 2013 by Pearson Education, Inc. All rights reserved.

Theorem 1 (Euclid's Perfect Number Formula)**.** *If $2^p - 1$ is a prime number, then $2^{p-1}(2^p - 1)$ is a perfect number.*

The first two Mersenne primes are $3 = 2^2 - 1$ and $7 = 2^3 - 1$. Euclid's Perfect Number Formula applied to these two Mersenne primes gives the two perfect numbers we already know,

$$2^{2-1}(2^2 - 1) = 6 \qquad \text{and} \qquad 2^{3-1}(2^3 - 1) = 28.$$

The next Mersenne prime is $2^5 - 1 = 31$, and Euclid's formula gives us a new perfect number,

$$2^{5-1}(2^5 - 1) = 496.$$

To check that 496 is perfect, we need to sum its proper divisors. Factoring $496 = 2^4 \cdot 31$, we see that the proper divisors of 496 are

$$1, 2, 2^2, 2^3, 2^4 \quad \text{and} \quad 31, 2 \cdot 31, 2^2 \cdot 31, 2^3 \cdot 31.$$

We could just add these numbers, but to illustrate the general method we will sum them in two stages. First

$$1 + 2 + 2^2 + 2^3 + 2^4 = 31,$$

and second

$$31 + 2 \cdot 31 + 2^2 \cdot 31 + 2^3 \cdot 31 = 31(1 + 2 + 2^2 + 2^3) = 31 \cdot 15.$$

Now adding the two pieces gives $31 + 31 \cdot 15 = 31 \cdot 16 = 496$, so 496 is indeed perfect.

Using the same sort of idea, we can easily verify that Euclid's Perfect Number Formula is true in general. We let $q = 2^p - 1$, and we need to check that $2^{p-1}q$ is a perfect number. The proper divisors of $2^{p-1}q$ are

$$1, 2, 4, \ldots, 2^{p-1} \quad \text{and} \quad q, 2q, 4q, \ldots, 2^{p-2}q.$$

We add these numbers using the formula for the Geometric Series. The Geometric Series formula (slightly rearranged) says that

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

Putting $x = 2$ and $n = p$, we get

$$1 + 2 + 4 + \cdots + 2^{p-1} = \frac{2^p - 1}{2 - 1} = 2^p - 1 = q.$$

And we can use the formula with $x = 2$ and $n = p - 1$ to compute

$$\begin{aligned} q + 2q + 4q + \cdots + 2^{p-2}q &= q(1 + 2 + 4 + \cdots + 2^{p-2}) \\ &= q\left(\frac{2^{p-1} - 1}{2 - 1}\right) \\ &= q(2^{p-1} - 1). \end{aligned}$$

So if we add all the proper divisors of $2^{p-1}q$, we get

$$1 + 2 + 4 + \cdots + 2^{p-1} + q + 2q + 4q + \cdots + 2^{p-2}q = q + q(2^{p-1} - 1) = 2^{p-1}q.$$

This shows that $2^{p-1}q$ is a perfect number.

We can use Euclid's Perfect Number Formula to write down many more perfect numbers. In fact, we get one perfect number for each Mersenne prime that we can find. The first few perfect numbers obtained in this fashion are listed in the following table. As you will observe, the numbers get large rather quickly.

p	2	3	5	7	13	17
$2^{p-1}(2^p - 1)$	6	28	496	8128	33550336	8589869056

We can also list perfect numbers that are incredibly huge. For example,

$$2^{756838}(2^{756839} - 1) \qquad \text{and} \qquad 2^{859432}(2^{859433} - 1)$$

are perfect numbers. The latter has more than half a million digits!

A natural question to ask at this point is whether Euclid's Perfect Number Formula actually describes all perfect numbers. In other words, does every perfect number look like $2^{p-1}(2^p - 1)$ with $2^p - 1$ prime, or are there other perfect numbers? Approximately 2000 years after Euclid's death, Leonhard Euler showed that Euclid's formula at least gives all *even* perfect numbers.

Theorem 2 (Euler's Perfect Number Theorem)**.** *If n is an even perfect number, then n looks like*

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

where $2^p - 1$ is a Mersenne prime.

We will prove Euler's theorem at the end of this chapter, but first we need to discuss a function that will be needed for the proof. This function, which is denoted by the Greek letter σ (sigma), is equal to

$$\sigma(n) = \text{sum of all divisors of } n \text{ (including 1 and } n).$$

Here are a few examples:

$$\begin{aligned}\sigma(6) &= 1+2+3+6 &&= 12\\ \sigma(8) &= 1+2+4+8 &&= 15\\ \sigma(18) &= 1+2+3+6+9+18 &&= 39.\end{aligned}$$

We can also give some general formulas. For example, if p is a prime number, then its only divisors are 1 and p, so $\sigma(p) = p+1$. More generally, the divisors of a prime power p^k are the numbers $1, p, p^2, \ldots, p^k$, so

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

To study the sigma function further, we make a short table of its values.

$\sigma(1)=1$	$\sigma(2)=3$	$\sigma(3)=4$	$\sigma(4)=7$	$\sigma(5)=6$
$\sigma(6)=12$	$\sigma(7)=8$	$\sigma(8)=15$	$\sigma(9)=13$	$\sigma(10)=18$
$\sigma(11)=12$	$\sigma(12)=28$	$\sigma(13)=14$	$\sigma(14)=24$	$\sigma(15)=24$
$\sigma(16)=31$	$\sigma(17)=18$	$\sigma(18)=39$	$\sigma(19)=20$	$\sigma(20)=42$
$\sigma(21)=32$	$\sigma(22)=36$	$\sigma(23)=24$	$\sigma(24)=60$	$\sigma(25)=31$
$\sigma(26)=42$	$\sigma(27)=40$	$\sigma(28)=56$	$\sigma(29)=30$	$\sigma(30)=72$
$\sigma(31)=32$	$\sigma(32)=63$	$\sigma(33)=48$	$\sigma(34)=54$	$\sigma(35)=48$
$\sigma(36)=91$	$\sigma(37)=38$	$\sigma(38)=60$	$\sigma(39)=56$	$\sigma(40)=90$
$\sigma(41)=42$	$\sigma(42)=96$	$\sigma(43)=44$	$\sigma(44)=84$	$\sigma(45)=78$
$\sigma(46)=72$	$\sigma(47)=48$	$\sigma(48)=124$	$\sigma(49)=57$	$\sigma(50)=93$
$\sigma(51)=72$	$\sigma(52)=98$	$\sigma(53)=54$	$\sigma(54)=120$	$\sigma(55)=72$
$\sigma(56)=120$	$\sigma(57)=80$	$\sigma(58)=90$	$\sigma(59)=60$	$\sigma(60)=168$
$\sigma(61)=62$	$\sigma(62)=96$	$\sigma(63)=104$	$\sigma(64)=127$	$\sigma(65)=84$

An examination of this table reveals that $\sigma(mn)$ is frequently equal to the product $\sigma(m)\sigma(n)$ and, after a little further analysis, we notice that this seems to be true when m and n are relatively prime. Thus, the sigma function appears to obey the same sort of multiplication formula as the phi function. We record this rule, together with the formula for $\sigma(p^k)$.

Theorem 3 (Sigma Function Formulas)**. (a)** *If p is a prime and $k \geq 1$, then*

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

(b) *If* $\gcd(m,n) = 1$*, then*

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

Just as with the phi function, we can use the sigma function formulas to easily compute $\sigma(n)$ for large values of n. For example,

$$\begin{aligned}\sigma(16072) &= \sigma(2^3 \cdot 7^2 \cdot 41) \\ &= \sigma(2^3) \cdot \sigma(7^2) \cdot \sigma(41) \\ &= (1+2+2^2+2^3)(1+7+7^2)(1+41) \\ &= 15 \cdot 57 \cdot 42 = 35910,\end{aligned}$$

and

$$\begin{aligned}\sigma(800000) &= \sigma(2^8 \cdot 5^5) \\ &= \left(\frac{2^9-1}{2-1}\right)\left(\frac{5^6-1}{5-1}\right) \\ &= 511 \cdot \frac{15624}{4} = 1995966.\end{aligned}$$

At this point you probably expect that I will show you how to prove the multiplication formula for the sigma function. But I won't! You have now made enough progress in number theory that it is time for you to start acting as a mathematician yourself.[1] So I am going to ask you to prove the formula $\sigma(mn) = \sigma(m)\sigma(n)$ for relatively prime integers m and n. Don't be discouraged and give up if you don't succeed at first. One suggestion I can give you is to try to discover *why* the formula is true before you attempt to give a general proof. So, for example, first look at numbers like $21 = 3 \cdot 7$ and $65 = 5 \cdot 13$ that are products of two primes and list their divisors. This should enable you to prove that $\sigma(pq) = \sigma(p)\sigma(q)$ when p and q are distinct prime numbers. Then try some m's and n's that have two or three divisors each and try to see how the divisors of m and n fit together to give divisors of mn. If you can describe this precisely enough, you should be able to prove that $\sigma(mn) = \sigma(m)\sigma(n)$. Remember, though, that you'll need to use the fact that m and n are relatively prime.

How is the sigma function related to perfect numbers? A number n is perfect if the sum of its divisors, other than n itself, is equal to n. The sigma function $\sigma(n)$ is the sum of the divisors of n, including n, so it has an "extra" n. Therefore,

$$n \text{ is perfect exactly when } \sigma(n) = 2n.$$

We are now ready to prove Euler's formula for even perfect numbers, which we restate here for your convenience.

[1] Your mission, should you decide to accept it, is to prove the multiplication formula for the sigma function. Should you be captured or killed in this endeavor, we will be forced to deny all knowledge of your activities. Good luck!

Theorem 4 (Euler's Perfect Number Theorem)**.** *If n is an even perfect number, then n looks like*

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

where $2^p - 1$ is a Mersenne prime.

Proof. Suppose that n is an even perfect number. The fact that n is even means that we can factor it as

$$n = 2^k m \qquad \text{with } k \geq 1 \text{ and } m \text{ odd.}$$

Next we use the sigma function formulas to compute $\sigma(n)$,

$$\begin{aligned}
\sigma(n) &= \sigma(2^k m) && \text{since } n = 2^k m, \\
&= \sigma(2^k)\sigma(m) && \text{using the multiplication formula for } \sigma \\
& && \text{and the fact that } \gcd(2^k, m) = 1, \\
&= (2^{k+1} - 1)\sigma(m) && \text{using the formula for } \sigma(p^k) \text{ with } p = 2.
\end{aligned}$$

But n is supposed to be perfect, which means that $\sigma(n) = 2n = 2^{k+1}m$. So we have two different expressions for $\sigma(n)$, and they must be equal,

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

The number $2^{k+1} - 1$ is clearly odd, and $(2^{k+1} - 1)\sigma(m)$ is a multiple of 2^{k+1}, so 2^{k+1} must divide $\sigma(m)$. In other words, there is some number c such that $\sigma(m) = 2^{k+1}c$. We can substitute this into the above equation to get

$$2^{k+1}m = (2^{k+1} - 1)\sigma(m) = (2^{k+1} - 1)2^{k+1}c,$$

and then canceling 2^{k+1} from both sides gives $m = (2^{k+1} - 1)c$. To recapitulate, we have shown that there is an integer c such that

$$m = (2^{k+1} - 1)c \qquad \text{and} \qquad \sigma(m) = 2^{k+1}c.$$

We are going to show that $c = 1$ by assuming that $c > 1$ and deriving a false statement. (This is called a "proof by contradiction.") So suppose that $c > 1$. Then $m = (2^{k+1} - 1)c$ would be divisible by the distinct numbers

$$1, \quad c, \quad \text{and} \quad m.$$

(N.B. The fact that our original number n was even means that $k \geq 1$, so c and m are different.) Of course, m is probably divisible by many other numbers, but in any case we find that

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

However, we also know that $\sigma(m) = 2^{k+1}c$, so

$$2^{k+1}c \geq 1 + 2^{k+1}c.$$

Therefore, $0 \geq 1$, which is an absurdity. This contradiction shows that c must actually be equal to 1, which means that

$$m = (2^{k+1} - 1) \qquad \text{and} \qquad \sigma(m) = 2^{k+1} = m + 1.$$

Which numbers m have the property that $\sigma(m) = m + 1$? These are clearly the numbers whose only divisors are 1 and m, since otherwise the sum of their divisors would be larger. In other words, $\sigma(m) = m + 1$ exactly when m is prime. We have now proved that if n is an even perfect number then

$$n = 2^k(2^{k+1} - 1) \qquad \text{with } 2^{k+1} - 1 \text{ a prime number.}$$

We know that if $2^{k+1} - 1$ is prime then $k + 1$ must itself be prime, say $k + 1 = p$. So every even perfect number looks like $n = 2^{p-1}(2^p - 1)$ with $2^p - 1$ a Mersenne prime. This completes our proof of Euler's Perfect Number Theorem. □

Euler's Perfect Number Theorem gives an excellent description of all even perfect numbers, but it says nothing about odd perfect numbers.

Question 5 (Odd Perfect Number Quandary)**.** Are there any odd perfect numbers?

To this day, no one has been able to discover any odd perfect numbers, although this is not through lack of trying. Many mathematicians have written many research papers (more than 50 papers in the last 50 years) studying these elusive creatures, and it is currently known that there are no odd perfect numbers less than 10^{300}. However, no one has yet been able to prove conclusively that none exist, so for now, odd perfect numbers are like the little man in the poem:

Last night I met upon the stair,
A little man who wasn't there.
He wasn't there again today.
I wish to heck he'd go away.

Anonymous

If you do some experimentation with small numbers, you might suspect that $\sigma(n) < 2n$ for all odd numbers. If this were true, it would certainly prove that there are no odd perfect numbers, but unfortunately it is not true. The first odd

number for which it is false is $n = 945 = 3^3 \cdot 5 \cdot 7$, which has $\sigma(945) = 1920$. This example should serve as a warning against believing a fact to be true simply because it has been checked for lots of small numbers. It is perfectly all right to make conjectures based on numerical data, but mathematicians insist on rigorous proofs precisely because such data can be misleading.

Exercises

1. If m and n are integers with $\gcd(m, n) = 1$, prove that $\sigma(mn) = \sigma(m)\sigma(n)$.

2. Compute the following values of the sigma function.
(a) $\sigma(10)$ **(b)** $\sigma(20)$ **(c)** $\sigma(1728)$

3. **(a)** Show that a power of 3 can never be a perfect number.
(b) More generally, if p is an odd prime, show that a power p^k can never be a perfect number.
(c) Show that a number of the form $3^i \cdot 5^j$ can never be a perfect number.
(d) More generally, if p is an odd prime number greater than 3, show that the product $3^i p^j$ can never be a perfect number.
(e) Even more generally, show that if p and q are distinct odd primes, then a number of the form $q^i p^j$ can never be a perfect number.

4. Show that a number of the form $3^m \cdot 5^n \cdot 7^k$ can never be a perfect number.

5. Prove that a square number can never be a perfect number. [*Hint*. Compute the value of $\sigma(n^2)$ for the first few values of n. Are the values odd or even?]

6. A perfect number is equal to the sum of its divisors (other than itself). If we look at the product instead of the sum, we could say that a number is *product perfect* if the product of all its divisors (other than itself) is equal to the original number. For example,

m	Product of factors	
6	$1 \cdot 2 \cdot 3 = 6$	product perfect
9	$1 \cdot 3 = 3$	product is too small
12	$1 \cdot 2 \cdot 3 \cdot 4 \cdot 6 = 144$	product is too large
15	$1 \cdot 3 \cdot 5 = 15$	product perfect.

So 6 and 15 are product perfect, while 9 and 12 are not product perfect.
(a) List all product perfect numbers between 2 and 50.
(b) Describe all product perfect numbers. Your description should be precise enough to enable you easily to solve problems such as "Is 35710 product perfect?" and "Find a product perfect number larger than 10000."
(c) Prove that your description in (b) is correct.

7.  **(a)** Write a program to compute $\sigma(n)$, the sum of all the divisors of n (including 1 and n itself). You should compute $\sigma(n)$ by using a factorization of n into primes, not by actually finding all the divisors of n and adding them up.

(b) As you know, the Greeks called n *perfect* if $\sigma(n) = 2n$. They also called n *abundant* if $\sigma(n) > 2n$, and they called n *deficient* if $\sigma(n) < 2n$. Count how many n's between 2 and 100 are perfect, abundant, and deficient. Clearly, perfect numbers are very rare. Which do you think are more common, abundant numbers or deficient numbers? Extend your list for $100 < n \le 200$ and see if your guess still holds.

8. The Greeks called two numbers m and n an *amicable pair* if the sum of the proper divisors of m equals n and simultaneously the sum of the proper divisors of n equals m. (The proper divisors of a number n are all divisors of n excluding n itself.) The first amicable pair, and the only one (as far as we know) that was known in ancient Greece, is the pair $(220, 284)$. This pair is amicable since

$$\begin{aligned} 284 &= 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 \qquad \text{(divisors of 220)} \\ 220 &= 1 + 2 + 4 + 71 + 142 \qquad \text{(divisors of 284).} \end{aligned}$$

(a) Show that m and n form an amicable pair if and only if $\sigma(n)$ and $\sigma(m)$ both equal $n + m$.

(b) Verify that each of the following pairs is an amicable pair of numbers.

$$(220, 284),\ (1184, 1210),\ (2620, 2924),\ (5020, 5564),\ (6232, 6368),$$
$$(10744, 10856),\ (12285, 14595).$$

(c) There is a rule for generating amicable numbers, although it does not generate all of them. This rule was first discovered by Abu-l-Hasan Thabit ben Korrah around the ninth century and later rediscovered by many others, including Fermat and Descartes. The rule says to look at the three numbers

$$\begin{aligned} p &= 3 \cdot 2^{e-1} - 1, \\ q &= 2p + 1 = 3 \cdot 2^e - 1, \\ r &= (p + 1)(q + 1) - 1 = 9 \cdot 2^{2e-1} - 1. \end{aligned}$$

If all of p, q, and r happen to be odd primes, then $m = 2^e pq$ and $n = 2^e r$ are amicable. Prove that the method of Thabit ben Korrah gives amicable pairs.

(d) Taking $e = 2$ in Thabit ben Korrah's method gives the pair $(220, 284)$. Use his method to find a second pair. If you have access to a computer that will do factorizations for you, try to use Thabit ben Korrah's method to find additional amicable pairs.

9. 💻 Let

$$s(n) = \sigma(n) - n = \text{sum of proper divisors of } n;$$

that is, $s(n)$ is equal to the sum of all divisors of n other than n itself. So n is perfect if $s(n) = n$, and (m, n) are an amicable pair if $s(m) = n$ and $s(n) = m$. More generally, a collection of numbers $n_1, n_2, \ldots, n_t$ is called *sociable* (of order t) if

$$s(n_1) = n_2, \quad s(n_2) = n_3, \quad \ldots, \quad s(n_{t-1}) = n_t, \quad s(n_t) = n_1.$$

(An older name for a list of this sort is an *Aliquot cycle*.) For example, the numbers

$$14316,\ 19116,\ 31704,\ 47616,\ 83328,\ 177792,\ 295488,$$
$$629072,\ 589786,\ 294896,\ 358336,\ 418904,\ 366556,\ 274924,$$
$$275444,\ 243760,\ 376736,\ 381028,\ 285778,\ 152990,\ 122410,$$
$$97946,\ 48976,\ 45946,\ 22976,\ 22744,\ 19916,\ 17716$$

are a sociable collection of numbers of order 28.

(a) There is one other collection of sociable numbers that contains a number smaller than 16000. It has order 5. Find these five numbers.

(b) Up until 1970, the only known collections of sociable numbers of order at least 3 were these two examples of order 5 and 28. The next such collection has order 4, and its smallest member is larger than $1{,}000{,}000$. Find it.

(c) Find a sociable collection of order 9 whose smallest member is larger than

$$800{,}000{,}000.$$

This is the only known example of order 9.

(d) Find a sociable collection of order 6 whose smallest member is larger than

$$90{,}000{,}000{,}000.$$

There are two known examples of order 6; this is the smallest.