BROWN

Classification of Perfect Numbers

Problems from the History of Mathematics

Lecture 8 — February 16, 2018

Brown University

Perfect Numbers

We define the sum-of-divisors function $\sigma(n)$ as the sum over the positive divisors of an integer n:

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

A perfect number is an integer which satisfies $\sigma(n) = 2n$.

Examples: $6,\ 28, 496, \ldots$

Perfect numbers were first introduced by the Pythagoreans, who, in their characteristically cultish ways, equated perfect numbers with marriage, health, and beauty on account of their harmony of proportions.

Perfect Numbers in Elements

In Proposition IX.36, Euclid proves the following result:

> *If as many numbers as we please beginning from a unit be set out continuously in double proportion, until the sum of all becomes prime, and if the sum multiplied into the last make some number, the product will be perfect.*

In other words,

Theorem (Euclid):

If $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is perfect.

Proof: Since $\sigma(mn) = \sigma(m)\sigma(n)$ when $(m, n) = 1$, we have

$$\sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1) \cdot 2^p. \qquad \square$$

The Greeks applied this formula to find the four perfect numbers 6, 28, 496, and 8128, which correspond to $p = 2, 3, 5, 7$.

Early Study and Conjectures

The Greeks were unable to produce larger perfect numbers with Euclid's formula because factoring $2^p - 1$ becomes difficult as p grows.[1]

This did not stop Nicomachus from making the following conjecture:

Conjecture (Nicomachus, c. 100 AD):

If n is perfect, then $n = 2^{p-1}(2^p - 1)$ with $2^p - 1$ prime.

This conjecture was made again in 1496 by Jacques Lefèvre.

[1] Note that $2^p - 1$ prime implies that p is prime, so these candidate numbers are already sparser than you might think.

Odd Perfect Numbers?

Ibn al-Haytham made a weaker version of Nicomachus' conjecture

Conjecture (al-Haytham, c. 1000 AD):

If n is perfect **and even**, then $n = 2^{p-1}(2^p - 1)$ with $2^p - 1$ prime.

His conjecture is particularly interesting in that the Greeks likely assumed that all perfect numbers were even. (More on this later.)

Contributions of Euler

The Euler–Euclid Theorem

Ibn al-Haytham's conjecture about even perfect numbers was settled in the affirmative by the Swiss mathematician Leonhard Euler.

The Euler–Euclid Theorem (1747):

n is perfect and even **if and only if** $n = 2^{p-1}(2^p - 1)$ with $2^p - 1$ prime.

Proof: Let $n = 2^k x$ be even, with x odd. Then $\sigma(n) = (2^{k+1} - 1)\sigma(x)$, and n perfect gives $(2^{k+1} - 1)\sigma(x) = 2^{k+1}x$. We have $2^{k+1} - 1 \mid x$, so $(2^{k+1} - 1)y = x$ for some y. Thus $\sigma(x) = 2^{k+1}y$.

The integer x has $x = (2^{k+1} - 1)y$ and y as divisors. But just these two divisors already sum to $\sigma(x)$, so x has exactly two divisors. We conclude that $x = 2^{k+1} - 1$ is prime. □

Mersenne Primes

By the Euler–Euclid theorem, even perfect numbers are in bijection with primes $M_p := 2^p - 1$. Primes of this form are known as Mersenne primes in honor of the French friar and polymath Marin Mersenne (1588–1648).

The Lucas–Lehmer test[2] gives a fast $O(p^2 \log p \log\log p)$ algorithm to test the primality of M_p. For this reason, most of the largest primes in the computer age have been Mersenne primes.[3]

The Lucas–Lehmer Test

Let p be prime. Define a sequence $\{s_i\}$ by setting $s_0 = 4$ and

$$s_i = s_{i-1}^2 - 2.$$

Then M_p is prime if and only if $s_{p-2} \equiv 0 \bmod M_p$.

[2] First proven by Lucas in 1856, with improvements from Lehmer in 1930.

[3] Specifically, the largest known prime has been Mersenne since 1952 except during 1989–1992, when it was $391581 \cdot 2^{216193} - 1$.

Odd Perfect Numbers

Odd Perfect Numbers

The Euler–Euclid theorem reduces the study of *even* perfect numbers to that of Mersenne primes. It does not say anything about the potential for odd perfect numbers.

If n is an odd perfect number, then

1. $n > 10^{1500}$ (Ochem–Pascal–Rao–Michaël 2012)
2. n has at least 101 prime factors and at least 10 distinct prime factors
3. the largest prime factor of n exceeds 10^8
4. the largest prime power dividing n exceeds 10^{62}.

Suffice to say that odd perfect numbers are not believed to exist.

Odd Perfect Numbers

The first serious work on odd perfect numbers comes from Euler.

Theorem (Euler):

Let n be an odd perfect number. Then $n = p^k m^2$, in which p is a prime power such that $p \equiv 1 \bmod 4$ and $k \equiv 1 \bmod 4$.

Proof: If q is prime and $q^k \| n$, then $\sigma(q^k) \mid \sigma(n)$. Since

$$\sigma(q^k) = 1 + \ldots + q^k \equiv \begin{cases} k+1 \mod 4, & q \equiv 1 \mod 4 \\ \frac{1}{2}(1+(-1)^k) \mod 4, & q \equiv 3 \mod 4, \end{cases}$$

each factor $\sigma(q^k)$ of $\sigma(n)$ has a factor of 2 unless k is even. But $2 \| \sigma(n)$, so n has at most one prime factor with odd multiplicity.

Call this factor p^k. If $p \equiv 3 \bmod 4$, then $4 \mid \sigma(p^k)$. Thus $p \equiv 1 \bmod 4$ and $k \equiv 1 \bmod 4$. $\square$

Questions?