The Pythagoreans and Perfection

The Proof in Euclid

The Pythagoreans were interested in perfect numbers, that is, numbers, such as 6 and 28, that equal the sum of their proper divisors. If \( s(n) \) denotes the sum of all the divisors of a positive integer \( n \), including \( n \) itself, then \( n \) is perfect if and only if \( s(n) = 2n \).

The culmination of Book IX of Euclid’s Elements (300 B.C.), is a proof that any positive integer of the form

\[ n = 2^{m-1}(2^m - 1) \]

is perfect, provided \( 2^m - 1 \) is prime. The proof is probably due to the Pythagorean Archytas (428–347 B.C.). It goes as follows.

If \( p = 2^m - 1 \) is prime, then the divisors of \( n = 2^{m-1}p \) are

\[ 1, \ 2, \ 2^2, \ \ldots, \ 2^{m-1}, \ p, \ 2p, \ \ldots, \ 2^{m-1}p \]

Thanks to unique factorisation, we know this list is complete. The sum of these divisors is

\[ (1 + 2 + 2^2 + \cdots + 2^{m-1})(1 + p) = (2^m - 1)(1 + p) = p2^m = 2n \]

It should be noted that, although Archytas attempted to give a fully rigorous proof of unique factorisation for numbers of the form \( 2^{m-1}(2^m - 1) \), he failed to do so. The first fully rigorous demonstration of unique factorisation was given only in 1801, by Carl Friedrich Gauss (1777–1855).

W. S. Anglin, *Mathematics: A Concise History and Philosophy*

© Springer-Verlag New York, Inc. 1994
Mersenne Primes

An integer of the form \(2^m - 1\) is prime only if \(m\) is prime. For if \(m = ab\), with \(a, b > 1\), we have the following factorisation:

\[
2^{ab} - 1 = (2^a - 1)(2^{ab-1} + 2^{ab-2} + \cdots + 2^a + 1)
\]

The converse is not true. Although 11 is prime, \(2^{11} - 1\) is the product of 23 and 89.

Primes of the form \(2^m - 1\) give rise, as we have seen, to perfect numbers. Such primes are called Mersenne primes, after Father Marin Mersenne (1588–1648). In the preface of his *Cogitata Physico-Mathematica* (1644), Mersenne correctly stated that the first 8 perfect numbers are given by

\[
m = 2, \ 3, \ 5, \ 7, \ 13, \ 17, \ 19, \ 31
\]

He also claimed that \(2^{67} - 1\) is prime. Here he erred. In 1903, Frank Nelson Cole gave a lecture that consisted of two calculations. First Cole calculated \(2^{67} - 1\). Then he worked out the product

\[
193,707,721 \times 761,838,257,287
\]

He did not say a single word as he wrote down the numbers. The two calculations agreed, and Cole received a standing ovation. He had factored \(2^{67} - 1\), proving Mersenne wrong.

Lucas’s Test

A French artillery officer and schoolteacher, Edouard Lucas (1842–1891), found an efficient way of testing whether \(2^m - 1\) is prime. His ideas were refined by Derrick H. Lehmer (1905–), leading to the following algorithm.

Let

\[
\begin{align*}
    u_1 &= 4 \\
    u_{n+1} &= u_n^2 - 2
\end{align*}
\]

Thus \(u_2 = 14\), and \(u_3 = 194\). If \(m > 2\) then \(2^m - 1\) is prime just in case \(2^m - 1\) is a factor of \(u_{m-1}\). For example, since \(2^5 - 1\) is a factor of \(u_4 = 37,634\), it follows that \(2^5 - 1\) is prime, and hence

\[
2^4(2^5 - 1) = 496
\]

is perfect.

Thanks to Lucas’s test — and the computer — we know that \(2^m - 1\) is prime when \(m\) has the 32 values given in the table. The ancient Greeks knew just the first 4 Mersenne primes. Mersenne himself knew the first 8.