




# Perfect Numbers

In mathematics, a perfect number is defined as an integer which is the sum of its proper positive divisors, that is, the sum of the positive divisors not including the number. Equivalently, a perfect number is a number that is half the sum of all of its positive divisors, or  $\sigma(n) = 2n$ .

The first perfect number is 6, because 1, 2 and 3 are its proper positive divisors and  $1 + 2 + 3 = 6$ . The next perfect number is  $28 = 1 + 2 + 4 + 7 + 14$ . The next perfect numbers are 496 and 8128. These first four perfect numbers were the only ones known to the ancient Greeks.

Euclid discovered that the first four perfect numbers are generated by the formula  $2^{n-1}(2^n - 1)$ . Noticing that  $2^n - 1$  is a prime number in each instance, Euclid proved that the formula  $2^{n-1}(2^n - 1)$  gives an even perfect number whenever  $2^n - 1$  is prime (Euclid, Prop. IX.36).

Two millennia after Euclid, Euler proved that the formula  $2^{n-1}(2^n - 1)$  will yield all the even perfect numbers. Thus, every Mersenne prime will yield a distinct even perfect number—there is a concrete one-to-one association between even perfect numbers and Mersenne primes. This result is often referred to as the “Euclid-Euler Theorem”. As of December 2006 only 44 Mersenne primes are known, which means there are 44 perfect numbers known, the largest being  $232,582,656 \times (232,582,657 - 1)$  with 19,616,714 digits. It is still uncertain whether there are infinitely many Mersenne primes and perfect numbers.



# Graeco-Latin square

A Graeco-Latin square or Euler square of order  $n$  over two sets  $S$  and  $T$ , each consisting of  $n$  symbols, is an  $n \times n$  arrangement of cells, each cell containing an ordered pair  $(s,t)$ , where  $s$  is in  $S$  and a  $t$  is in  $T$ , such that

- \* every row and every column contains exactly one  $s$  in  $S$  and exactly one  $t$  in  $T$ , and
- \* no two cells contain the same ordered pair of symbols.


The two sets are commonly taken to be  $S = \{A, B, C, \dots\}$ , the first  $n$  upper-case letters from the Latin alphabet, and  $T = \{\alpha, \beta, \gamma, \dots\}$ , the first  $n$  lower-case letters from the Greek alphabet—hence the name Graeco-Latin square. Several examples are given below.

A $\alpha$	B $\gamma$	C $\beta$
B $\beta$	C $\alpha$	A $\gamma$
C $\gamma$	A $\beta$	B $\alpha$

A $\alpha$	B $\gamma$	C $\delta$	D $\beta$
B $\beta$	A $\delta$	D $\gamma$	C $\alpha$
C $\gamma$	D $\alpha$	A $\beta$	B $\delta$
D $\delta$	C $\beta$	B $\alpha$	A $\gamma$

A $\alpha$	B $\delta$	C $\beta$	D $\epsilon$	E $\gamma$
B $\beta$	C $\epsilon$	D $\gamma$	E $\alpha$	A $\delta$
C $\gamma$	D $\alpha$	E $\delta$	A $\beta$	B $\epsilon$
D $\delta$	E $\beta$	A $\epsilon$	B $\gamma$	C $\alpha$
E $\epsilon$	A $\gamma$	B $\alpha$	C $\delta$	D $\beta$

\* In the 1780s, Leonhard Euler demonstrated methods for constructing Graeco-Latin squares where  $n$  is odd or a multiple of 4. Observing that no order-2 square exists and unable to construct an order-6 square (see thirty-six officers problem), he conjectured that none exist when  $n$  congruent 2 (mod 4). Indeed, the non-existence of order-6 squares was definitely confirmed in 1901 by Gaston Tarry through exhaustive enumeration of all possible arrangements of symbols. In 1959, Bose and Shrikhande found some counterexamples to Euler's conjecture, then Parker found a counterexample of order 10. In 1960, Parker, Raj Chandra Bose and Shrikhande showed Euler's conjecture to be false for all  $n \geq 10$ . Thus, Graeco-Latin squares exist for all orders  $n \geq 3$  except  $n = 6$ .


$$x^3 + y^3 = z^3$$

For various special exponents  $n$ , the theorem had been proven over the years, but the general case remained elusive. The first case proved was the case  $n = 4$ , which was proved by Fermat himself using the method of infinite descent. Using a similar method, Euler proved the theorem for  $n = 3$ . While his original method contained a flaw, it has been the basis of a lot of research about the theorem.

$$a^p \equiv a \pmod{p}$$
$$a^{\varphi(n)} \equiv 1 \pmod{p}$$

Pierre de Fermat first stated the theorem in a letter dated October 18, 1640 to his friend and confidant Frénicle de Bessy as the following:  $p$  divides  $a^{p-1} - 1$ , whenever  $p$  is prime and  $a$  is coprime to  $p$ .


As usual, Fermat did not prove his assertion, only stating:

Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers; de quoi je vous enverrois la démonstration, si je n'apprehendois d'être trop long.

(And this proposition is generally true for all progressions and for all prime numbers; the proof of which I would send to you, if I were not afraid to be too long.)

Euler first published a proof in 1736 in a paper entitled “Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio”, but Leibniz left virtually the same proof in an unpublished manuscript from sometime before 1683.




$$2^{2^5} + 1 = 641 * 6700417$$

Fermat numbers and Fermat primes were first studied by Pierre de Fermat, who conjectured that all Fermat numbers are prime. Indeed, the first five Fermat numbers  $F_0, \dots, F_4$  are easily shown to be prime. However, this conjecture was refuted by Leonhard Euler in 1732 when he showed the factorization above. Euler proved that every factor of  $F_n$  must have the form  $k2^{n+1} + 1$ . For  $n = 5$ , this means that the only possible factors are of the form  $64k + 1$ . Euler found the factor  $641 = 10 \times 64 + 1$ .

It is widely believed that Fermat was aware of Euler's result, so it seems curious why he failed to follow through on the straightforward calculation to find the factor. One common explanation is that Fermat made a computational mistake and was so convinced of the correctness of his claim that he failed to double-check his work.

$$x^3 - y^2 = 2$$





# Euler's Theorem in Geometry

Euler's theorem states that the distance  $d$  between the circumcenter and incenter of a triangle can be expressed as

$$d^2 = R(R - 2r),$$

where  $R$  and  $r$  denote the circumradius and inradius respectively (the radii of the above two circles).

From the theorem follows the Euler inequality:

$$R \geq 2r$$





