



M. F. Gilmullin, "Prime Numbers: A History Across the Centuries," *Mathematics with Mansur*, Dec. 1, 2024. [Online]. Available: <https://history-math.org/publications/hm-tt-1c23e0d766d2-en/>.

ESSAY

## Prime Numbers: A History Across the Centuries

"Prime numbers were made to be multiplied": their story stretches from ancient Greece to modern records and public-key cryptography.

Mansur Gilmullin · 01.12.2024 · EN

[Read this article on the journal website](#)



Perhaps this is how Eratosthenes invented the sieve of Eratosthenes: an algorithm for successively finding all primes from 1 to  $n$ . · [Source](#)

*"Prime numbers were made to be multiplied."*

*L. D. Landau*

The story of prime numbers is one of the histories of mathematics that continues across centuries and millennia. Beginning with Pythagoras and Euclid, it is still being written today, and may never end: there are infinitely many primes, and the need to find ever larger ones remains.

On 12 October 2024, Luke Durant of San Jose, California, discovered a new largest known prime:  $2^{136279841} - 1$ .

It was found through GIMPS, the Great Internet Mersenne Prime Search. The number has 41 024 320 decimal digits. In hexadecimal, it is the digit 1 followed by 34 069 960 F digits.

It belongs to the class of Mersenne primes and is the 52nd such number. These primes are extremely rare: only 52 are known. To find the new number, Durant used distributed-computing software linking thousands of servers around the world. His computing system spanned 24 data-centre regions in 17 countries.

The number has 16 million more digits than the previous record holder. Since 2018, the largest known prime had been  $2^{82589933} - 1$ , discovered by the American IT specialist Patrick Laroche. Its decimal representation contains 24 862 048 digits. It is the 51st Mersenne prime.

A few words about primes themselves. In Russia, almost every school pupil knows about them. Problems applying them even appear in the OGE and EGE school examinations. Numerous studies and books are devoted to them.

They have many beautiful properties, such as the factorisation of positive integers into primes — the fundamental theorem of arithmetic. Yet their properties are not all understood. Many questions concerning primes remain open.

A prime is a positive integer with exactly two distinct positive divisors. The mathematicians of ancient Greece already knew about them. Pythagoras studied prime, or “linear”, numbers. Eratosthenes invented the sieve of Eratosthenes, an algorithm for successively finding all primes from 1 to  $n$ . Euclid proved that there are infinitely many primes.

| 0  |    |    |    |    |    |    |    |    |     |
|----|----|----|----|----|----|----|----|----|-----|
| 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10  |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20  |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30  |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40  |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50  |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60  |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70  |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80  |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90  |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

The primes from 0 to 100, marked in red, can easily be found by hand using the sieve of Eratosthenes. · [Source](#)

Pierre de Fermat conjectured that every number of the form  $F_n = 2^{2^n} + 1$  is prime. For  $n = 0, 1, 2, 3, 4$ , the Fermat numbers are prime and equal to 3, 5, 17, 257, 65537.

No further Fermat primes have yet been found. It is unknown whether any are prime for  $n > 4$  or whether all remaining Fermat numbers are composite.



Pierre de Fermat (1607–1665). · [Source](#)

The French mathematician Marin Mersenne conjectured that numbers  $M_n = 2^n - 1$ , where  $n$  is prime, are also prime: the Mersenne numbers. Checking the conjecture was far beyond the capabilities of the time. Only in the twentieth century was it found to be false.



Marin Mersenne (1588–1648). · [Source](#)

Nevertheless, Mersenne numbers have long held the record as the largest known primes.

For a long time, primes were thought to have little use outside pure theoretical mathematics. This changed in the 1970s with the emergence of public-key cryptographic systems, in which primes formed the basis of early encryption algorithms such as RSA, named after Rivest, Shamir and Adleman.