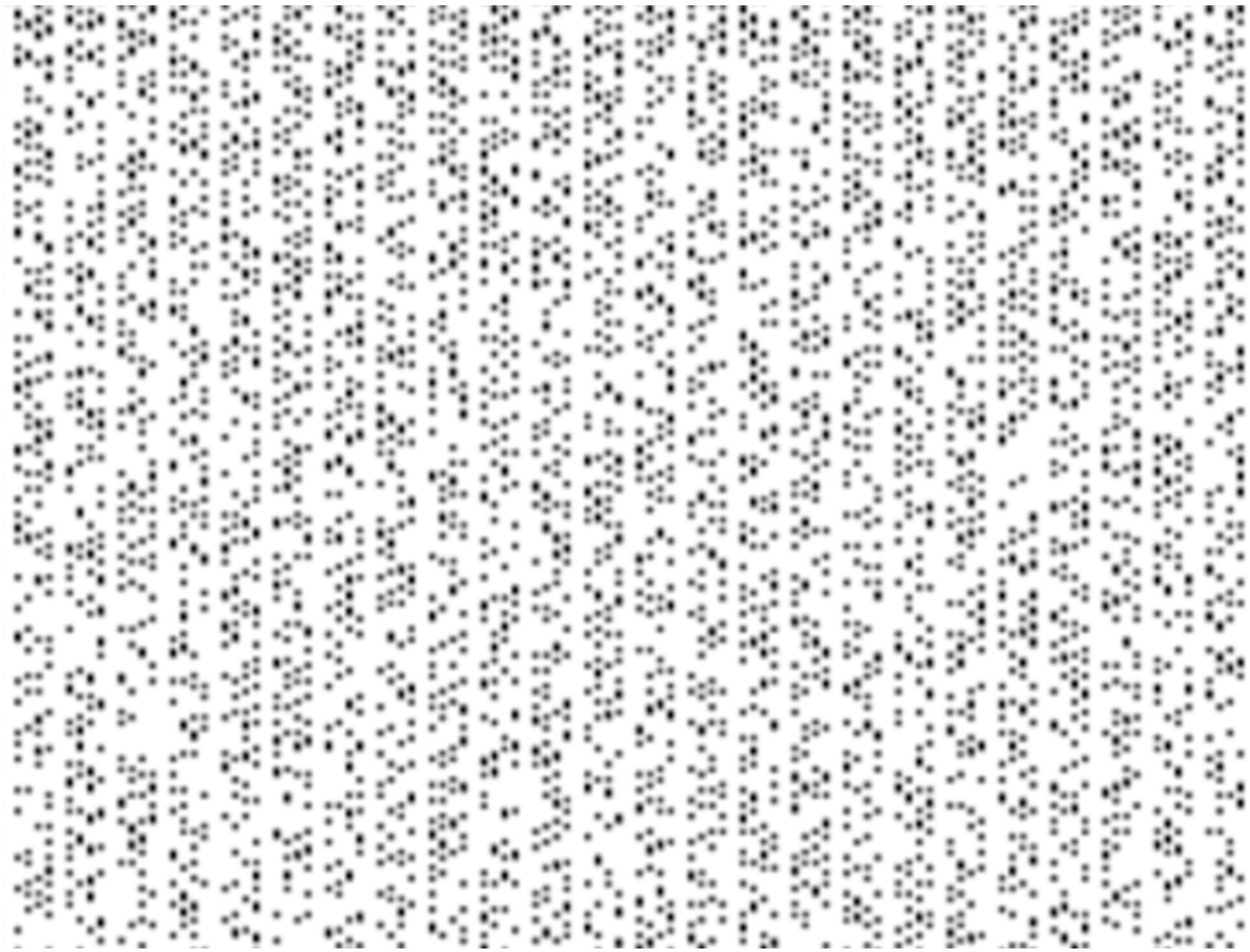
A newly discovered prime number makes its debut

Avner Bar-Hen, Cnam

Published on January 30, 2018 – Updated on February 14, 2019

It’s an excellent opportunity to take a small tour through the wonderful world of prime numbers to see how this result was achieved and why it is so interesting.



Prime numbers

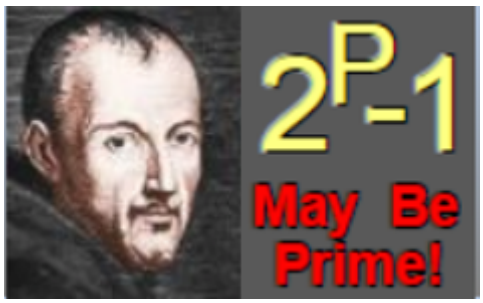
On December 26, 2017, J. Pace, G. Woltman, S. Kurowski, A. Blosser, and their co-authors announced the discovery of a new prime number): 2^{2321}-1.. A prime number is one that is divisible only by itself and the number 1, that is, essentially a number that has no divisor. Some speak of prime numbers as the atoms of the mathematical universe, others as precious stones.
It is to Euclid that we owe the first two definitions of a prime number:

> Any number is the unique product of prime factors.

> They are infinite in number. The demonstration of this result is regarded as the first proof by absurdity: Suppose there is only a finite number of prime numbers, so they are all smaller than an integer n. Any integer greater than n would therefore be divisible by a prime number less than n. However, the number (2 * 3 * … * n) + 1 is not divisible by any integer from 2 to n since the remainder of the division is always 1 – a contradiction of the preceding sentence.

Eratosthenes, who lived from -276 to -194, proposed a process that allows us to find all prime numbers less than a given natural number N. The process consists of eliminating from a table integers from 2 to N that are multiples of those numbers. By deleting all the multiples, there remain only integers that are not multiples of any integer, and so are prime numbers. The search for efficient algorithms is an active research topic – for example for the Lucas-Lehmer test.

After the Greek era, there was a long dark period that lasted until the end of the 16th century and the arrival of French theologian and mathematician Marin Mersenne (1588-1648). He was an advocate of Catholic orthodoxy, yet also believed that religion must welcome any updated truth. He was a Cartesian and translator of Galileo.



Marin Mersenne. http://primes.utm.edu/mersenne/LukeMirror/mersenne.htm, CC BY
Mersenne was looking for a formula that would generate all the prime numbers. In particular, he studied the numbers $M_p = 2^p-1$, where p is prime. These numbers are now called Mersenne numbers or Mersenne primes. In 1644 he wrote that Mp is prime for p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257, and compound – in other words, non-prime – for the other 44 lower p values at 257. These definition actually commits five errors: M61, M89 and M107 are prime, while M67 and M257 are not.

Stamp issued in 2004 in Liechtenstein featuring a large prime number, 213466917-1. pascalgavillet.blog.tdg.ch, CC BY
The new prime number discovered at the very end of 2017 corresponds to M77232917. It has 23,249,425 digits – almost a million digits more than the previous record-holding prime. If the number were contained by a document written in the font Times New Roman with a point size of 10 and standard page margins, it would fill 3,845 pages.

The official date of discovery of a prime number is the day that someone declares the result. This is in keeping with tradition: M4253 is reputed not to have one because in 1961 the American mathematician Alexander Hurwitz read a printer output from the end forward, and found M4423 a few seconds before seeing M4253. The previous Mersenne number also had a complicated history: the computer reported the result to the server on September 17, 2015, but a bug blocked the email. The prime number remained unnoticed until January 7, 2016.

Quantum cryptography

Intel. Author provided, CC BY

We often refer to the use of prime numbers in cryptography, but they're too big to be really useful. (There is hope that quantum cryptography will change things.) Historically, Mersenne's search for prime numbers has been used as a test for computer hardware. In 2016, the premium95 community discovered a flaw in Intel's Skylake CPU as well as many PCs. This prime number was found as part of the Great Internet Mersenne Prime Search Project (GIMPS).

2^{2321}-1 is the 50th Mersenne prime and if the challenge to discover the 51st tempts you, the verification program is available to all – and there's even a $3,000 prize.

Avner Bar-Hen, Professeur du Cnam, *Conservatoire national des arts et métiers (CNAM)*