A little bit about primes

John McCleary

Vassar College LLI

October 18 2024

Numbers

What is the biggest number known?

What do we mean by *known*?

How about if we know every single digit in the number, and the number is not some trivial thing?

Numbers

The answer at the moment[1] is

$$2^{82\,589\,933} - 1.$$

This number has 24 862 048 decimal digits. It was discovered December 7, 2018 and verified by December 21, 2018..

Here are the first few: (see `mersenne.org` for more).

[1] There may be an announcement of a larger such number any day now. Verification is under way.

1488944457420413255478064584723979166030262739927953241852712894252
1323936106447531030997113218033717475283440142358756005197751832658
5649184293195970822950634334345109731369920534231064114059526476787
6746819332211781849375477107986211226534792788629942124472358169794
6442467372269911156615468898349878577880899273633363565129754335286
2574521790554111356785480302953825923182904046191880806667200792222
4457105930988153887394047699962279207194319396507712065726965912877
8891780444893214525405268925811066972135872605813039683144951084398
1458542118442001484377016106429038958170829770594188899487932701608
1279727414348185908077459964865519006267229417152151375452828119103
0824461144012351159456852196747038826579037625519936415833523853151
5428184558688259535895472102988098477808837016863514197252401327722
3153442722574718130614762581537465586626911838102926072292274274159
1677805540986193572204715936611931996160718058420541094365289984777
5316826224519087060254159129057555150340191957520869909228059505868
2348342343339022215780517544789315206811414437205217972195325090923
5527812846017542915009972903387013545695298798195320350480795142078
. . . 7902591

Mersenne prime

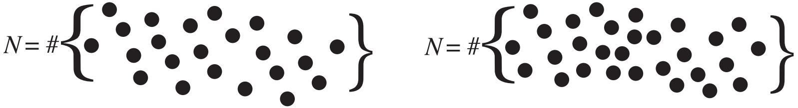
A number P is a *Mersenne prime* if it is a prime number of the form

$$P = 2^q - 1.$$

Lots of words here need defining. Marin Mersenne (1588–1648) was an ordained Catholic priest. He worked in Paris and was interested in many things. He became a center of communication between folks working on scientific studies, sometimes making new connections between them. Mersenne primes were the subject of some correspondence.

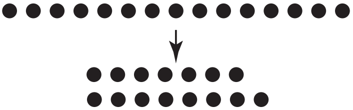
What are prime numbers?

What is a prime number?



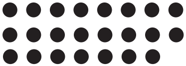
Step 1: Put your stones in rows of two.

If you get a rectangular array, jot down 2, and take one of the rows and repeat. If you get a leftover stone, proceed to step 2.

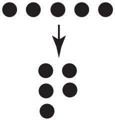


What is a prime number?

Step 2: Put your (remaining) objects in rows of three.



If you get a rectangular array, jot down 3, and take one row and repeat. If you get any leftover objects, proceed to step 3.



What is a prime number?

Step 3: Put your (remaining) objects in rows of 5. (Notice we don't have to do rows of 4, because they were done in Step 1.)

If you get a rectangular array, jot down 5, and take one row and repeat. If that row has only one object in it, then STOP.

If you get leftover stones, proceed to step 4. *Unless* your array is square or longer down than across, at which point you can STOP. If you never get a rectangle, then your N is **prime**. If you jotted down some numbers, then got to 1, your number is **composite** and N is equal to the product of the numbers you jotted down.

What is a prime number?

Definition. A *prime number* is a whole number greater than 1 that is divisible by only two numbers—itself and 1. If a whole number has a divisor that is greater than 1 and less than the number, the number is called *composite*.

$$2, 3, 5, 7, 11, 13, 17, 19, \dots, 7919, \dots, 2^{82{,}589{,}933} - 1, \dots$$

The number $2^{82{,}589{,}933} - 1$ is the 51st Mersenne prime.

Fundamental facts

The Fundamental Theorem of Arithmetic. Every natural number $n > 1$ is either prime or a product of prime numbers, in fact, in a unique way.

An informal argument for this is what you did with the m&m's to obtain the prime factorization of your N.

How many prime numbers are there?

Euclid: Book IX, Proposition 20. *There are infinitely many primes.*

Fundamental facts

A proof from *the Book*: Suppose M is a big number. We will prove that there is a prime number bigger than M.

Suppose $2, 3, \ldots, p_{n-1}, p_n$ are all the primes that are less than or equal to M. Make the following numbers:

$$\mathcal{B} = (2 \cdot 3 \cdot \cdots \cdot p_{n-1} \cdot p_n) \text{ and } \mathcal{C} = \mathcal{B} + 1.$$

Notice that $\mathcal{C}$ is odd, so 2 does not divide $\mathcal{C}$. Also 3 divides $\mathcal{B}$, so 3 cannot divide $\mathcal{C}$ because there is a 1 added on. In fact, every prime 2, 3, $\ldots$, p_{n-1}, p_n divides $\mathcal{B}$, and so none of them divides $\mathcal{C}$.

But SOME prime divides $\mathcal{C}$, so it must be bigger than M.

How do we find primes?

Sieve of Eratosthenes 2nd century B.C.E.

	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

Sieve of Eratosthenes

	2	3		5		7		9
11		13		15		17		19
21		23		25		27		29
31		33		35		37		39
41		43		45		47		49
51		53		55		57		59
61		63		65		67		69
71		73		75		77		79
81		83		85		87		89
91		93		95		97		99

Sieve of Eratosthenes

	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			

Sieve of Eratosthenes

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

Sieve of Eratosthenes

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

Every number between 1 and 100 has a divisor among 2, 3, 5, or 7 ($100 = 10^2$), or is prime. So all remaining numbers are prime. There are 25 primes between 1 and 100.

Back to the Mersenne primes

The first thing to know is that, if $P = 2^q - 1$ is a Mersenne prime, then q is a prime number. Here are the first few Mersenne primes: $3 = 2^2 - 1, 7 = 2^3 - 1$, $31 = 2^5 - 1$, $127 = 2^7 - 1, \dots$

But $2^{11} - 1 = 2047 = 23 \times 89$.

Carrying on, the following are Mersenne primes,

$$2^{13} - 1,\ 2^{17} - 1,\ 2^{19} - 1,\ 2^{31} - 1,\ 2^{61} - 1,\ 2^{89} - 1.$$

Mersenne, in his letters, claimed that for $q = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257, that $2^q - 1$ is prime. It is NOT true for $q = 67$, and $q = 257$, which give composite numbers. Also he missed three, namely, $q = 61, 89$, and 107.

To date, there are 51 Mersenne primes known.

Some excellent patterns

- For every natural number n, 2 divides $n^2 - n$.

This is easy to know: If n is even, then n^2 is even and $n^2 - n$ is a difference of even numbers and so it is even.

If n is odd, then n^2 is odd and so $n^2 - n$ is a difference of odd numbers, and so it is even.

Notice that we obtained an infinite number of facts—one for each n. And we know for sure that the fact is true.

Does anything else like this happen?

Some excellent patterns

When we were making patters of rectangles with remainders we were demonstrating

The Division Algorithm. Given a number n and a divisor $d > 0$, there are numbers q and r for which

$$n = (q \times d) + r,$$

and $0 \leq r < d$.

This fact is the basis for long division. When we try to make a rectangle, the number left over satisfies $0 \leq r < d$, because, if it were larger, we would make another row.

Let's focus on the remainders.

Some excellent patterns

divisor	n	r	n	r	n	r	n	r	n	r	n	r
3	2^3-2	0	3^3-3	0	4^3-4	0	5^3-5	0	6^3-6	0	7^3-7	0
4	2^4-2	2	3^4-3	2	4^4-4	0	5^4-5	0	6^4-6	2	7^4-7	2
5	2^5-2	0	3^5-3	0	4^5-4	0	5^5-5	0	6^5-6	0	7^5-7	0
6	2^6-2	2	3^6-3	0	4^6-4	0	5^6-5	0	6^6-6	0	7^6-7	0
7	2^7-2	0	3^7-3	0	4^7-4	0	5^7-5	0	6^7-6	0	7^7-7	0

Notice for the prime divisor rows, the remainders are all equal to zero—that is, the divisor goes into the number evenly.

Some excellent patterns

Theorem of Fermat (1601–1665): *If p is a prime number, then p divides $a^p - a$ for any natural number a.*

Recall the binomial formulas:

$$(a+b)^2 = a^2 + 2ab + b^2$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3.$$

Let's prove the case of $p = 3$ by induction. We know that 3 divides $1^3 - 1 = 0$. If you like, 3 also divides $2^3 - 2 = 6$. Suppose 3 divides $N^3 - N$. Consider:

$$(N+1)^3 - (N+1) = N^3 + 3N^2 + 3N + 1 - (N+1) = (N^3 - N) + 3N^2 + 3N.$$

Since 3 divides $N^3 - N$ and 3 divides $3N^2 + 3N$, then 3 divides $(N+1)^3 - (N+1)$. By induction, we get to any number, so 3 divides $M^3 - M$ for any natural number M.

Some excellent patterns

The same ladder argument holds true for any prime number p because of the properties of binomial coefficients.

In fact, this pattern can be used to determine if a number is prime:

Theorem. *If n is a natural number and n divides $a^n - a$ for all natural numbers a, then n is a prime.*

Some excellent patterns

Recall our primes found with the sieve:

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	
		53			59
61				67	
71		73			79
		83			89
				97	

Notice the pairs: 3 and 5, 5 and 7, 11 and 13, 17 and 19, 29 and 31, 41 and 43, 59 and 61, 71 and 73. The next pair is 101 and 103.

These pairs are called *twin primes*.

Some excellent patterns

Are there infinitely many pairs of twin primes?

This is an open question. It is known that there are $808,675,888,577,436$ many twin prime pairs less than 10^{18}.

In 2013, Yitang Zhang announced a proof that for some even number $2K$ less than 70 million, there are infinitely many pairs of primes of the form p and $p + 2K$. Further work has shown that $2K$ can be less than 246.

Some excellent patterns

In a letter dated 7 June, 1742, Christian Goldbach (1690–1764) suggested to Leonhard Euler (1707–1783) that every even integer greater than 2 is the sum of two primes.

Euler replied to Goldbach: That every even number is a sum of two primes, I consider an entirely certain theorem in spite of that I am not able to demonstrate it.

$$
\begin{array}{rcl@{\qquad}rcl}
8 & = & 3+5 & 24 & = & 5+19 \\
10 & = & 3+7 & 26 & = & 7+19 \\
12 & = & 5+7 & 28 & = & 5+23 \\
14 & = & 3+11 & 30 & = & 7+23 \\
16 & = & 5+11 & 32 & = & 3+29 \\
18 & = & 7+11 & 34 & = & 5+29 \\
20 & = & 7+13 & 36 & = & 7+29 \\
22 & = & 5+17 & 38 & = & 7+31
\end{array}
$$