Primes: the indivisible and the indispensable (1)

Philomathes • 21 Jan 2025

Sieve of Eratosthenes

There’s a common saying that one bottle of soju fills seven (technically 7.5) soju glasses. While the number seven is often considered lucky, it’s far from welcome at a drinking table. Split the bottle between two or three people, and you’re left with awkward fractions because seven can’t be evenly divided. Why is that? The reason lies in the fact that seven can only be divided by 1 and itself. Inevitably, after finishing a bottle, we find ourselves raising a hand and calling out, “Another bottle, please!”

Prime numbers, like the number seven, have likely captivated minds since the early days of civilization, when mathematics itself was just being born. This fascination—perhaps even obsession—with prime numbers stems from a simple question:

“Why are some numbers divisible only by 1 and themselves?”

For instance, the number 4 can be divided by 1, 2, and 4. (Such numbers are called the *factors* or the *divisors* of 4.) In contrast, the factors of 5 are only 1 and 5 itself. Similarly, 6 has factors such as 1, 2, 3, and 6, whereas 7, like 5, is divisible only by 1 and itself. Numbers like 5 and 7, which can only be divided by 1 and themselves, are called *prime numbers*. On the other hand, numbers like 4 and 6 that have additional factors are called *composite numbers*. There’s one unique number that is neither prime nor composite: the number 1. While it may seem that 1 deserves to be considered prime based on the definition, mathematicians have deliberately chosen not to classify it as such.

Before diving into the many stories surrounding prime numbers, let’s first explore a method to identify them. The *Sieve of Eratosthenes* is a straightforward algorithm that relies on basic arithmetic to find prime numbers. Let’s use this method to identify all prime numbers less than 50. Start by writing down the numbers from 1 to 50.

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

First, exclude the number 1, as it is not a prime number by definition.

Next, remove all multiples of 2 except for 2 itself. After this step, the table will look like this:

	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

Then, remove all multiples of 3 except for 3 itself.

	2	3	5	7	
11		13		17	19
		23	25		29
31			35	37	
41		43		47	49

Continue removing all multiples of 5 (excluding 5) and all multiples of 7 (excluding 7). Although you could repeat this process for 11, 13, and so on, by the time you remove the multiples of 7, no composite numbers remain in the table. The final table will look like this, where the "survivors" are all prime numbers.

	2	3	5	7	

11	13	17	19
	23		29
31		37	
41	43	47	

If you’ve diligently drawn your own sieve, you might have noticed that as the numbers get larger, prime numbers become increasingly sparse. For instance, to determine whether 11 is a prime number, you only need to check whether it can be evenly divided by numbers smaller than 11. However, verifying whether 101 is prime requires checking it against all numbers up to 101. In other words, the larger the number, the more divisors need to be checked, and the likelihood of being a prime decreases.[1]

This raises an intriguing question: Is there a point where prime numbers completely vanish? Could there exist a largest prime number?

---

1. Technically, the term "probability" here is misleading. The primality of a number is not a random event, like flipping a coin, but rather an established fact. Nonetheless, we can calculate the "probability" of a number being prime through statistical means, a methodology known as *Cramér’s model*.↩