Definition 28. Let $a, b \in \mathbb{Z}$ (both not zero). The **least common multiple** $\operatorname{lcm}(a,b)$ of a and b is the smallest positive integer m such that $a|m$ and $b|m$.

Example 29. $\operatorname{lcm}(12,42) = \operatorname{lcm}(2^2 \cdot 3, 2 \cdot 3 \cdot 7) = 2^2 \cdot 3 \cdot 7 = 84 = \frac{12 \cdot 42}{6}$

Lemma 30. For $a, b \in \mathbb{N}$, $\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$.

Proof. Write $d = \gcd(a,b)$ and $m = \frac{ab}{d}$. Note that $a|m$ because $\frac{m}{a} = \frac{b}{d}$ is an integer. Likewise, $b|m$. In other words, m is a common multiple of a and b. We still need to show that it is the smallest.

Let n be a positive integer such that $a|n$ and $b|n$. (We need to show that $m \leqslant n$. We do that by showing $m|n$.)

Recall that $d = ax + by$ for some integers x, y. Using that, we find that

$$\frac{n}{m} = \frac{nd}{ab} = \frac{n(ax+by)}{ab} = \frac{n}{b}x + \frac{n}{a}y$$

is an integer. That is, $m|n$. □

3 More on primes

Example 31. The **sieve of Eratosthenes** is an efficient way to find all primes up to some n.

Write down all numbers $2, 3, 4, \ldots, n$. We begin with 2 as our first prime. We proceed by crossing out all multiples of 2, because these are not primes. The smallest number we didn't cross out is 3, our next prime. We again proceed by crossing out all multiples of 3, because these are not primes. The smallest number we didn't cross out is 5 (note that it has to be prime because, by construction, it is not divisible by any prime less than itself).

Problem. If $n = 10^6$, at which point can we stop crossing out numbers?

We can stop when our "new prime" exceeds $\sqrt{n} = 1000$. All remaining numbers have to be primes. Why?!

Example 32. (Euclid) There are infinitely many primes.

Proof. Assume (for contradiction) there is only finitely many primes: $p_1, p_2, \ldots, p_n$.
Consider the number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.
Each prime p_i divides $N - 1$ and so p_i does not divide N.
Thus any prime dividing N is not on our list. Contradiction. □

Historical note. This is not necessarily a proof by contradiction, and Euclid (300BC) himself didn't state it as such. Instead, one can think of it as a constructive machinery of producing more primes, starting from any finite collection of primes.

A variation. Can we replace $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ in the proof with $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n - 1$? Yes! (If $n \geqslant 2$.)

Playing with numbers.

$2 + 1 = 3$ is prime. $2 \cdot 3 + 1 = 7$ is prime. $2 \cdot 3 \cdot 5 + 1 = 31$ is prime. $2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ is prime. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ is prime. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$ is not prime.

Let $P_n = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ where p_i is the ith prime. If P_n is prime, it is called a primorial prime. We have just checked that P_1, P_2, P_3, P_4, P_5 are primes but that P_6 is not a prime.

The next primorial primes are $P_{11}, P_{75}, P_{171}, P_{172}$. It is not known whether there are infinitely P_n which are prime.

More shamefully, it is not known whether there are infinitely many P_n which are not prime.

See, for instance: http://mathworld.wolfram.com/PrimorialPrime.html

Example 33. In 12/2018, a new largest (proven) prime was found: $2^{82,589,933}-1$.

https://www.mersenne.org/primes/?press=M82589933

This is a **Mersenne prime** (like the last 17 record primes). It has a bit over 24.8 million (decimal) digits (versus 23.2 for the previous record). The prime was found as part of GIMPS (Great Internet Mersenne Prime Search), which offers a $3,000 award for each new Mersenne prime discovered.

The EFF (Electronic Frontier Foundation) is offering $150,000 (donated anonymously for that specific purpose) for the discovery of the first prime with at least 100 million decimal digits.

https://www.eff.org/awards/coop

[Prizes of $50,000 and $100,000 for primes with 1 and 10 million digits have been claimed in 2000 and 2009.]

Example 34. $(p, p+2)$ is a twin prime pair if both p and $p+2$ are primes.

Just making sure. $(2,3)$ is the only pair $(p, p+1)$ with p and $p+1$ both prime. (Why?!)

Some twin prime pairs. $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$, $(71,73)$, $(101,103)$, ...

Largest known one: $2996863034895 \cdot 2^{1290000} \pm 1$ ($388,342$ decimal digits; found 2016)

Twin prime conjecture. Euclid already conjectured in 300 BCE that there are infinitely many twin primes. Despite much effort, noone has been able to prove that in more than 20 centuries.

Recent progress. It is now known that there are infinitely many pairs of primes (p_1, p_2) such that the gap between p_1 and p_2 is at most 246 (the break-through in 2013 due to Yitang Zhang had $7 \cdot 10^7$ instead of 246).

Example 35. (Bertrand's postulate) For any $n > 1$, the interval $(n, 2n)$ contains at least one prime.

Advanced comment. Let $\pi(x)$ be the number of primes $\leqslant x$. It follows from Betrand's postulate that $\pi(2^n) \geqslant n$.

To prove that, note that 2 is a prime and that each of the (disjoint!) intervals $(2,4)$, $(4,8)$, $(8,16)$, ..., $(2^{n-1}, 2^n)$ contains at least one prime.

This is a very poor bound. For instance, we find $\pi(2^{20}) \geqslant 20$ where 2^{20} is a little bigger than 10^6. Compare that to the actual numbers in the prime number theorem below.

Historical comment. This was conjectured by Bertrand in 1845 (he checked up to $n = 3 \cdot 10^6$), and proved by Chebyshev in 1852.

The following famous and deep result quantifies the infinitude of primes.

Theorem 36. (prime number theorem) Let $\pi(x)$ be the number of primes $\leqslant x$. Then

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

In other words: Up to x, there are roughly $x/\ln(x)$ many primes.

Examples.

proportion of primes up to 10^6: $\frac{78,498}{10^6} = 7.85\%$ vs the estimate $\frac{1}{\ln(10^6)} = \frac{1}{6\ln(10)} = 7.24\%$

proportion of primes up to 10^{12}: $\frac{37,607,912,018}{10^{12}} = 3.76\%$ vs the estimate $\frac{1}{\ln(10^{12})} = \frac{1}{12\ln(10)} = 3.62\%$

An example of huge relevance for crypto. Many cryptographic schemes require us to be able to generate large random primes, where large typically means numbers with about 2048 binary digits.

By the PNT, the proportion of primes up to 2^{2048} is about $\frac{1}{\ln(2^{2048})} = 0.0704\%$.

That means, roughly, 1 in 1500 numbers of this magnitude are prime. That means we (i.e. our computer) can efficiently generate large random primes by just repeatedly generating large random numbers and discarding those that are not prime (we will discuss primality testing in cryptography).

Comment. Here, $\ln(x)$ is the logarithm with base e. Isn't it wonderful how Euler's number $e \approx 2.71828$ is sneaking up on the primes?

Historical comment. Despite progress by Chebyshev (who succeeded in 1852 in showing that the quotient in the above limit is bounded, for large x, by constants close to 1), the PNT was not proved until 1896 by Hadamard and, independently, de la Vallée Poussin, who both used new ideas due to Riemann.