date: 2025-11-10

1 primes, gcd's, and lcm's

a **prime number** is a positive integer p greater than 1 that is divisible by only 1 and itself. if a number is *not* prime, then it is a **composite number**. mathematically, we can write this as:

$$p \text{ is prime} \Leftrightarrow p > 1 \land \forall x \in \mathbb{Z}^+[(x \neq 1 \land x \neq p) \rightarrow x \nmid p]$$

prime numbers are pretty special; in fact, any positive integer can be presented as a unique product of prime numbers.

theorem (fundamental theorem of arithmetic): every positive integer greater than 1 can be written uniquely as a prime or the product of two or more primes where the prime factors are written in order of non-decreasing size.

1.1 is a number prime?

the fundamental theorem of arithmetic leads to a related theorem:

theorem: if n is a composite integer (not a prime number), then n has a prime divisor less than or equal to $\sqrt{n}$.

proof: if n is composite, then it has a positive integer factor a with $1 < a < n$ by definition. this means that $n = ab$, where b is an integer greater than 1.

assume $a > \sqrt{n}$ and $b > \sqrt{n}$. then $ab > \sqrt{n} \cdot \sqrt{n} = n$, which is a contradiction. so either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. therefore, n has a divisor less than or equal to $\sqrt{n}$. by the fundamental theorem of arithmetic, this divisor is either prime, or is a product of primes. in either case, n has a prime divisor less than or equal to $\sqrt{n}$. ■

corollary: if n is a positive integer that does not have a prime divisor less than or equal to $\sqrt{n}$, then n is prime.

we can use that corollary to determine whether if a number is prime (rather) trivially:

- is 101 prime?
  - primes that are $\leq \sqrt{101} (\sim 10.05)$ are 2, 3, 5, and 7.
  - since 101 is not divisible by 2, 3, 5, or 7, it must be prime.
- is 1147 prime?
  - primes that are $\leq \sqrt{1147} (\sim 33.87)$ are 2, 3, 5, 7, 11, 13, 17, 23, 29, and 31.

- $1147 = 31 \times 37$, so 1147 must be composite.

1.1.1 finding prime numbers

the **sieve of eratosthenes** is a brute-force algorithm for finding all prime numbers less than some value n.

here is the general process (the pseudocode follows):
1. list the numbers less than n
2. if the next available prime numbers is less than $\sqrt{n}$, cross out all of its multiples
3. repeat until the next available number is greater than $\sqrt{n}$
4. all remaining numbers are prime.

algorithm: sieve of eratothenes

```
1 procedure sieve(n: ℕ)
2 |  create a boolean array A[2..n], filled with true
3 |  for i from 2 to ⌊√n⌋
4 |  |  if A[i] is true
5 |  |  |  for j from i², i² + i, i² + 2i, i² + 3i ..., to n
6 |  |  |  |  A[j] := false
7 |  return all i such that A[i] is true
```

1.1.2 aside: how many primes are there?

theorem: there are infinitely many prime numbers.

proof: assume that there are only a finite number of primes $p_1, p_2, ..., p_n$. therefore, there exists a number Q such that $Q = (p_1 \times p_2 \times ... \times p_n) + 1$; and by the fundamental theorem of arithmetic, Q can be written as the product of two or more primes. however, Q is not divisible by any of the primes $p_1, p_2, ..., p_n$ because dividing Q by any of these primes would leave a remainder of 1. since none of our primes can divide Q, that means Q must be divisible by *another* prime that wasn't included in our collection. that means, the prime number that is either Q, or a prime factor of Q (if Q is a composite number). this contradicts our assumption that we have listed all possible primes, and there are infinitely many prime numbers. ■

1.2 greatest common divisors

let a and b be integers, not both zero. the largest integer d such that $d \mid a$ and $d \mid b$ is called the **greatest common divisor (gcd)** of a and b, denoted by $\gcd(a, b)$.

sometimes, the gcd of two numbers is 1; for example, 17 and 22. if $\gcd(a, b) = 1$, we say that a and b are **relatively prime**, or **coprime**. we say that $a_1, a_2, ..., a_n$ are **pairwise relatively prime** if $\forall i, j \gcd(a_i, a_j) = 1$.

1.2.1 finding gcd by prime factorization

usually, the most trivial way to find the gcd between two numbers is by enumerating all the possible factors of both numbers, and then finding the common factor. however, we can leverage the fundamental theorem of arithmetic to develop a better algorithm.

let the prime factorization of a and b be:

$$a = p_i^{a_1} \times p_2^{a_2} \times ... \times p_n^{a_n}$$

$$b = p_i^{b_1} \times p_2^{b_2} \times ... \times p_n^{b_n}$$

then, we take the *minimum* of the exponents:

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} \times p_2^{\min(a_2, b_2)} \times ... \times p_n^{\min(a_n, b_n)}$$

for example, we want to find $\gcd(120, 500)$.

- $120 = 2^3 \times 3 \times 5$
- $500 = 2^3 \times 5^3$

therefore, $\gcd(120, 500) = 2^3 \times 3^0 \times 5 = 20$.

1.2.2 euclid's algorithm

another way to find the gcd of two numbers is by using euclid's algorithm. based on the observation that $\gcd(a, b) = \gcd(b, a \bmod b)$, we can iteratively reduce the problem size until we reach a remainder of 0. the algorithm can be described in the pseudocode below:

algorithm: euclid's algorithm

```
1 procedure euclid(a: ℤ⁺, b: ℤ⁺)
2     while b ≠ 0
3         r := a mod b
4         a := b
5         b := r
6     return a
```

the value returned in a is the last non-zero remainder, which corresponds to the greatest common divisor.

1.2.2.1 example

we want to find $\gcd(414, 662)$. we first divide the larger num(b) by the smaller num(a), and keep the remainder(r). then, we shift left; the small number(a) become the big number(b), and we divide it by the remainder(r). we repeat this process until the remainder is 0, and the last non-zero remainder is the gcd.

$$
\begin{aligned}
662 &= 414 \times 1 + 248 \\
414 &= 248 \times 1 + 166 \\
248 &= 166 \times 1 + 82 \\
166 &= 82 \times 2 + \boxed{2} \\
82 &= 2 \times 41 + 0
\end{aligned}
$$

1.3 least common multiples

the **least common multiple** of the integers a and b, where neither is 0, is the smallest positive integer that is divisible by both a and b. the least common multiple of a and b is denoted by $\operatorname{lcm}(a, b)$.

we can find the least common multiple of an integer by enumerating the multiples of each number, and finding the first common multiple.

1.3.1 finding the lcm by prime factorization

similarly, we can also use the fundamental theorem of arithmetic to find it more efficiently:

let the prime factorizations of a and b be:

$$a = p_i^{a_1} \times p_2^{a_2} \times ... \times p_n^{a_n}$$
$$b = p_i^{b_1} \times p_2^{b_2} \times ... \times p_n^{b_n}$$

then, we take the *maximum* of the exponents:

$$\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} \times p_2^{\max(a_2, b_2)} \times ... \times p_n^{\max(a_n, b_n)}$$

for example, we want to find $\operatorname{lcm}(120, 500)$.

- $120 = 2^3 \times 3 \times 5$
- $500 = 2^2 \times 5^3$

therefore, $\operatorname{lcm}(120, 500) = 2^3 \times 3 \times 5^3 = 3000 \ll 120 \times 500 = 60000$.

1.3.2 aside: relationship between lcm and gcd

$$ab = \operatorname{lcm}(a, b) \times \gcd(a, b)$$