Today's Topics

Primes & Greatest Common Divisors

- Prime representations
- Important theorems about primality
- Greatest Common Divisors
- Least Common Multiples

Once and for all, what are prime numbers?

Definition: A prime number is a positive integer p that is divisible by only 1 and itself. If a number is not prime, it is called a composite number.

Mathematically: p is prime $\leftrightarrow \forall x \in \mathbf{Z}^+ [(x \neq 1 \land x \neq p) \rightarrow x \nmid p]$

Examples: Are the following numbers prime or composite?

- 23
- 42
- 17
- 3
- 9

Any positive integer can be represented as a unique product of prime numbers!

Theorem (The 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 nondecreasing size.

Examples:

- $100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$
- $641 = 641$
- $999 = 3 \times 3 \times 3 \times 37 = 3^3 \times 37$
- $1024 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^{10}$

Note: Proving the fundamental theorem of arithmetic requires some mathematical tools that we have not yet learned.

This leads to a related theorem…

Theorem: If n is a composite integer, 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 $ab > \sqrt{n}\sqrt{n} = n$, which is a contradiction. So either $a \le \sqrt{n}$ or $b \le \sqrt{n}$.
- Thus, n has a divisor less than $\sqrt{n}$.
- 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 $\sqrt{n}$. ❑

Applying contraposition leads to a naive primality test

Corollary: If n is a positive integer that does not have a prime divisor less than √n, then n prime.

Example: Is 101 prime?

- The primes less than √101 are 2, 3, 5, and 7
- Since 101 is not divisible by 2, 3, 5, or 7, it must be prime

Example: Is 1147 prime?

- The primes less than √1147 are 2, 3, 5, 7, 11, 13, 17, 23, 29, and 31
- 1147 = 31 × 37, so 1147 must be composite

This approach can be generalized

The Sieve of Eratosthenes is a brute-force algorithm for finding all prime numbers less than some value *n*

Step 1: List the numbers less than *n*

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

Step 2: If the next available number is less than √n, cross out all of its multiples

Step 3: Repeat until the next available number is > √n

Step 4: All remaining numbers are prime

How many primes are there?

Theorem: There are infinitely many prime numbers.

Proof: By contradiction

- Assume that there are only a finite number of primes $p_1, \ldots, p_n$
- Let $Q = p_1 \times p_2 \times \ldots \times p_n + 1$ be a number
- By the fundamental theorem of arithmetic, Q can be written as the product of two or more primes.
- Note that no p_j divides Q
- Therefore, there must be some prime number not in our list. This prime number is either Q (if Q is prime) or a prime factor of Q (if Q is composite).
- This is a contradiction since we assumed that all primes were listed. Therefore, there are infinitely many primes. ❑

This is a non-constructive existence proof!

Group work!

Problem : Is 91 prime?

Greatest common divisors

Definition: 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 of a and b, denoted by gcd(a, b).

Note: We can (naively) find GCDs by comparing the common divisors of two numbers.

Example: What is the GCD of 24 and 36?

- Factors of 24: 1, 2, 3, 4, 6, 12
- Factors of 36: 1, 2, 3, 4, 6, 9, 12, 18
- ∴ gcd(24, 36) = 12

Sometimes, the GCD of two numbers is 1

Example: What is gcd(17, 22)?

- Factors of 17: 1, 17
- Factors of 22: 1, 2, 11, 22
- ∴ gcd(17, 22) = 1

Definition: 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 gcd(a_i, a_j) = 1 $\forall i,j$.

Example: Are 10, 17, and 21 pairwise coprime?

- Factors of 10: 1, 2, 5, 10
- Factors of 17: 1, 17
- Factors of 21: 1, 3, 7, 21

Yes!

We can leverage the fundamental theorem of arithmetic to develop a better algorithm

Let: $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$

Then:

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

Greatest multiple of p_1 in both a and b

Greatest multiple of p_2 in both a and b

Example: Compute gcd(120, 500)

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

Least common multiples

Definition: The least common multiple of the integers *a* and *b* is the smallest positive integer that is divisible by both *a* and *b*. The least common multiple of *a* and *b* is denoted lcm(*a*, *b*).

Example: What is lcm(3,12)?

- Multiples of 3: 3, 6, 9, 12, 15, …
- Multiples of 12: 12, 24, 36, …
- So lcm(3,12) = 12

Note: lcm(*a*, *b*) is guaranteed to exist, since a common multiple exists (i.e., *ab*).

We can leverage the fundamental theorem of arithmetic to develop a better algorithm

Let: $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$

Then:

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

Greatest multiple of p_1 in either a or b

Greatest multiple of p_2 in either a or b

Example: Compute lcm(120, 500)

- $120 = 2^3 \times 3 \times 5$
- $500 = 2^2 \times 5^3$
- So lcm(120, 500) = $2^3 \times 3 \times 5^3$ = 3000 << 120 × 500 = 60,000

LCMs are closely tied to GCDs

Note: $ab = \text{lcm}(a, b) \times \text{gcd}(a, b)$

Example: $a = 120 = 2^3 \times 3 \times 5$, $b = 500 = 2^2 \times 5^3$

- $120 = 2^3 \times 3 \times 5$
- $900 = 2^2 \times 5^3$
- lcm(120, 500) = $2^3 \times 3 \times 5^3$ = 3000
- gcd(120, 500) = $2^2 \times 3^0 \times 5$ = 20
- lcm(120, 500) × gcd(120, 500)
  = :

✓

Final Thoughts

- Prime numbers play an important role in number theory
- There are an infinite number of prime numbers
- Any number can be represented as a product of prime numbers; this has implications when computing GCDs and LCMs