Number Theory

Chapter 4

Edited by: Dr. Meshal Alfarhood

Primes and Greatest Common Divisors

Section 4.3

Section Summary

Prime Numbers and their Properties

Greatest Common Divisors and Least Common Multiples

The Euclidean Algorithm

gcds as Linear Combinations

Primes

Definition: An integer $p > 1$ is called *prime* if the only divisors of p are 1 and p.

- A positive integer that is > 1 and is not prime is called *composite*.
- **Examples**:
  - **7** is prime because its only positive divisors are 1 and 7.
  - **9** is composite because it is divisible by 3.

The Fundamental Theorem of Arithmetic

Theorem: Every positive integer > 1 can be written uniquely as a prime or as the product of primes.

Examples:

- **6** $= 2 \cdot 3$
- **100** $= 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
- **641** $= 641$
- **999** $= 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
- **1024** $= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Trial Division

Theorem: If n is a composite integer, then it has a prime divisor $\leq \sqrt{n}$.

- From Theorem, it follows that an integer is prime <u>if it is not divisible by any prime less than or equal to its square root</u>.
- **<u>Proof of Theorem:</u>**
  - Assume n is composite, then $n = ab \quad \ni 1 < a \leq b < n$
  - At any time, either $a \leq \sqrt{n}$ <u>or</u> b $\leq \sqrt{n}$
    - It cannot have both a $> \sqrt{n}$ and b $> \sqrt{n}$ → otherwise, $ab > \sqrt{n}\sqrt{n}$ = $ab > n$ → <u>contradiction</u>!
  - Consequently, we see that n has a positive divisor (a or b) not exceeding $\sqrt{n}$
  - This divisor is either prime or, by the fundamental theorem of arithmetic, has a prime divisor less than itself.

Trial Division [2]

How to decide if a number is prime?

Trial Division: divide n by all primes not exceeding $\sqrt{n}$ and conclude that n is prime if it is not divisible by any of these primes.

Examples:

1. Show that 101 is prime?

- The only primes not exceeding $\lfloor\sqrt{101}\rfloor$=10 → are 2, 3, 5, and 7.
- Because 101 is not divisible by 2, 3, 5, or 7 → 101 is prime.

2. Find the prime factorization of 7007?

- Perform divisions by successive primes: $2\nmid 7007$, $3\nmid 7007$, $5\nmid 7007$
- $7|7007$ → $\frac{7007}{7} = 1001$
- $7|1001$ → $\frac{1001}{7} = 143$
- $7\nmid 143$
- $11|143$ → $\frac{143}{11} = 13$ → 7007 = $7 \cdot 7 \cdot 11 \cdot 13$

Infinitude of Primes

Euclid

Theorem: There are infinitely many primes.

Proof: Assume finitely many primes: $[p_1, p_2, \ldots, p_n]$ $(\neg p)$

- Let $q = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$
- q is either:
  1. Prime → **contradiction!** (Not in the finite prime list)
  2. Composite → by the fundamental theorem of arithmetic, it can be written as a product of primes.
     - But none of the primes in the finite list $[p_1, p_2, \ldots\ldots, p_n]$ divides q; since the remainder will be always 1.
     - Hence, there is a prime not on the list divides q. → **contradiction!**
- Consequently, there are infinitely many primes.

Greatest Common Divisor

Definition: Let a and b be integers, not both zero. The largest integer d such that $d|a$ and also $d|b$ is called the greatest common divisor of a and b.

- The greatest common divisor of a and b is denoted by gcd(a,b).
- **Examples**:
  1. What is the greatest common divisor of 24 and 36?
     - **Solution**: gcd(24, 36) = 12
  2. What is the greatest common divisor of 17 and 22?
     - **Solution**: gcd(17,22) = 1

Greatest Common Divisor 2

Definition 1: The integers *a* and *b* are ***relatively prime*** if their greatest common divisor is **1**.

- **Example**: 17 and 22 are relatively prime; because gcd(17,22)=1

Definition 2: The integers $a_1, a_2, \ldots, a_n$ are ***pairwise relatively prime*** if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

- **Example 1**: Determine whether the integers **10, 17 and 21** are pairwise relatively prime.
  - **Solution**: Because gcd(10,17) = 1, gcd(10,21) = 1, and gcd(17,21) = 1, 10, 17, and 21 are pairwise relatively prime.
- **Example 2**: Determine whether the integers **10, 19, and 24** are pairwise relatively prime.
  - **Solution**: Because gcd(10,24) = 2; 10, 19, and 24 are not pairwise relatively prime.

Dividing Congruences by an Integer

- Dividing both sides of a valid congruence by an integer <u>does not always</u> produce a valid congruence.
- But dividing by an integer <u>relatively prime to the modulus</u> does produce a valid congruence:

Theorem: Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c,m) = 1$, then $a \equiv b \pmod{m}$.

- **<u>Proof</u>**:
  - $ac \equiv bc \pmod{m} \rightarrow m \mid ac - bc \rightarrow m \mid c(a - b)$
  - Since $\gcd(c,m) = 1 \rightarrow m \nmid c$
  - Therefore, $m \mid (a-b)$ → Hence, $a \equiv b \pmod{m}$

Finding gcd Using Prime Factorizations

Suppose the prime factorizations of *a* and *b* are:

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}, \qquad b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n},$$

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

Example: **Find gcd(120,500).**

- **120** = $2^3 \cdot 3 \cdot 5$
- **500** = $2^2 \cdot 5^3$
- **gcd(120,500)** $= 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)}$

  $= 2^2 \cdot 3^0 \cdot 5^1$

  $= 20$

Least Common Multiple

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

- It is denoted by lcm(*a*,*b*).
- The least common multiple can also be computed from the prime factorizations.

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

- **Example: Find lcm(120,500).**

$$\operatorname{lcm}(120,500) = \operatorname{lcm}(2^3 \cdot 3 \cdot 5,\ 2^2 \cdot 5^3)$$

$$= 2^{\max(3,2)} \cdot 3^{\max(1,0)} \cdot 5^{\max(1,3)}$$

$$= 2^3 \cdot 3 \cdot 5^3 = 3000$$

Theorem: Let a and b be positive integers. Then:

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

Euclidean Algorithm

- The Euclidean algorithm is an efficient method for computing the greatest common divisor of two integers.
- **Example**: Find gcd(91, 287).
  - $287 = 3 \cdot 91 + 14$ — Divide 287 by 91
  - $91 = 6 \cdot 14 + 7$ — Divide 91 by 14
  - $14 = 2 \cdot 7 + 0$ — Divide 14 by 7

Stopping condition

$$\boxed{\mathbf{gcd(287, 91) = gcd(91, 14) = gcd(14, 7) = 7}}$$

The gcd is the **last nonzero remainder** in the sequence of divisions.

Euclidean Algorithm 2

The Euclidean algorithm expressed in pseudocode is:

```
procedure gcd(a, b)
x := a
y := b
while  y ≠ 0
    r := x mod y
    x := y
    y := r
return x
```

```
procedure rec_gcd(a, b)
If (b==0):
    return a
Else:
    return rec_gcd(b, a%b)
```

Euclidean Algorithm 3

Lemma: Let $a = bq + r$, where a, b, q, and r are integers. Then **gcd(*a*,*b*) = gcd(*b*,*r*)**.

Proof:

- Suppose that $d|a$ and $d|b$ → $d|(xa \pm yb)$
- Let $x=1$ and $y=q$ → $d|(a - bq)$ → $d|r$
- Thus, if $d|a$ and $d|b$ then $d|r$. In other words, the common divisor of a,b,r is the same.

gcds as Linear Combinations

Theorem: If a and b are positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb$.

- **Example 1:** $\gcd(6,14) = (-2) \cdot 6 + 1 \cdot 14 = 2$.
- **Example 2:** Express gcd(252,198) as linear combinations.
  - First, use the Euclidean algorithm to find gcd(252,198):
    - $252 = 1 \cdot 198 + 54$
    - $198 = 3 \cdot 54 + 36$
    - $54 = 1 \cdot 36 + \mathbf{18}$
    - $36 = 2 \cdot 18 + 0$
  - Second, working backwards:
    - $18 = 54 - 1 \cdot 36$
    - $18 = 54 - 1 \cdot (198 - 3 \cdot 54)$
    - $18 = 4 \cdot 54 - 1 \cdot 198$
    - $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot \underline{252} - 5 \cdot \underline{198}$

$\boxed{\gcd(252,198) = 4 \cdot 252 - 5 \cdot 198 = \mathbf{18}}$

gcds as Linear Combinations 2

Lemma: If a, b, and c are positive integers such that gcd(a,b) = 1 and $a|bc$, then $a|c$.

Proof: Assume gcd(a, b) = 1 and a|bc

- Since gcd(a, b) = 1, there are integers s and t such that $sa + tb = 1$.
- Multiplying both sides of the equation by c, yields $sac + tbc = c$.
- a|sac and a|tbc → a|sac+tbc → a|c