CISC203 notes
Discrete Structures II

Andrew Aquino

Introduction

To whom this may concern, these are some notes for CISC203, a course I took in the fall of 2025. I am writing these notes for my own benefit, and I make no claims about their accuracy or completeness. Use at your own risk.

Check me out at https://github.com/andrewSmellz

Contents

1 Group Theory

1.1 Division

Definition 1: $(a \mid b)$
Let $a, b \in \mathbb{Z}$, with $a \neq 0$. If $b = ak$ for some $k \in \mathbb{Z}$, then we say that a divides b, or that a is a divisor of b.

$$\text{This is denoted as: } a \mid b$$

Theorem 2: (Division Algorithm)
Let $a, b \in \mathbb{Z}$, with $b > 0$. There exists a unique pair of integers q and r such that:

$$a = qb + r \quad \text{where} \quad 0 \leq r < b$$

This expresses a as a multiple of b plus a remainder r. Additionally, we call d the divisor, a the dividend, q the quotient, and r the remainder.

Definition 3: (Division and Modulus)
Let $a, b \in \mathbb{Z}$, with $b > 0$. Then we define the division and modulus operations as follows:

$$q = a \div b, \quad r = a \bmod b$$

where q and r are the unique pair of numbers (by Theorem 2) where $a = qb + r$ and $0 \leq r < b$.

Definition 4: (Congruence Modulo n)
Let $x, y, n \in \mathbb{Z}$, with $n > 0$. If $n \mid (x - y)$, we can say that x and y are congruent modulo n. This is denoted as: $x \equiv y \pmod{n}$. The set of all integers congruent to an integer a modulo n is called the congruence class of a modulo n.

Example 5:
$53 \equiv 23 \pmod{10}$ means that $53 - 23 = 30$ is a multiple of 10.
However, $53 \bmod 10 = 3$ and $23 \bmod 10 = 3$, meaning that the remainder of $53 \div 10$ is 3.

Theorem 6:
Let $a, b, n \in \mathbb{Z}$, with $n > 0$. Then

$$a \equiv b \pmod{n} \iff a \bmod n = b \bmod n$$

Example 7:

$$9 \equiv 17 \pmod{4} \text{ is true, so we also have } 9 \bmod 4 = 1 \text{ and } 17 \bmod 4 = 1$$

1.2 Greatest Common Divisor

Definition 8: (Common Divisor)
Let $a, b \in \mathbb{Z}$. If an integer d divides both a and b, we say that d is a **common divisor** of a and b.

Example 9:
The common divisors of 12 and 18 are $\pm 1, \pm 2, \pm 3,$ and ± 6.
The common divisors of 25 and 50 are $\pm 1, \pm 5, \pm 10,$ and ± 25.

Definition 10: (Greatest Common Divisor)
Let $a, b \in \mathbb{Z}$. We say that an integer d is the greatest common divisor of a and b, provided that:

1. d is a common divisor of a and b
2. If $e \mid a$ and $e \mid b$, then $e \leq d$

The greatest common divisor of a and b is denoted as $\gcd(a, b)$. By definition it is always positive.

Example 11:
The greatest common divisor of 18 and 12 is 6. Using the naive method:

1. Find all divisors of a
2. Find all divisors of b

3. Choose the largest number that is a divisor of both a and b

Theorem 12: (Fundamental Theorem of Arithmetic)
Every integer greater than 1 can be written uniquely as a prime or as the product of primes, written in nondecreasing order.

Example 13:
the prime factorizations of 20,23,288, and 621 are:

$$r_0 = 20 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5,$$

$$r_1 = 23 = 23,$$

$$r_2 = 288 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^5 \cdot 3^2,$$

$$r_3 = 621 = 3 \cdot 3 \cdot 3 \cdot 23 = 3^3 \cdot 23$$

We can find the greatest common divisor of two numbers by taking the product of all common prime factors. That is,

$$\gcd(r_0, r_2) = 2^2 = 4 \quad \text{and} \quad \gcd(r_2, r_3) = 3^2 = 9.$$

Since r_0 does not have any common prime factors with r_3, we have

$$\gcd(r_0, r_3) = 1.$$

We can also find the least common multiple of two numbers using this method.

However, the above method is inefficient. In fact, for large numbers that are often used in public-key cryptography, factoring is not even computationally feasible. We will see a much more efficient method, called the *Euclidean Algorithm*.

Definition 14: (Relatively Prime)
Let $a, b \in \mathbb{Z}$. We say a and b are relatively prime if $\gcd(a, b) = 1$.

Example 15:
From Example 13, 20 and 621 are relatively prime.

1.3 Euclidean Algorithm

Lemma 16:
Let $a = bq + r$, where $a, b, q, r \in \mathbb{Z}$. Then $\gcd(a, b) = \gcd(b, r)$. This forms the basis for the Euclidean Algorithm:

1. Let $c = a \bmod b$.
2. If $c = 0$, then $\gcd(a, b) = b$. Stop.
3. Otherwise, the answer is $\gcd(b, c)$.

Example 17:

$$\begin{aligned}360 \bmod 84 &= 24\\ 84 \bmod 24 &= 12\\ 24 \bmod 12 &= 0\end{aligned}$$

so, $\gcd(360, 84) = 12$.

Example 18:
to find $\gcd(720, 26)$ using the Euclidean Algorithm:

$$\begin{aligned}720 \bmod 26 &= 16\\ 26 \bmod 16 &= 10\\ 16 \bmod 10 &= 6\\ 10 \bmod 6 &= 4\\ 6 \bmod 4 &= 2\\ 4 \bmod 2 &= 0\end{aligned}$$

so, $\gcd(720, 26) = 2$.
Theorem 19:
Let $a, b \in \mathbb{Z}$, at least one nonzero. The gcd d of a and b can be written as:

$$d = ax + by$$

for some integers x and y.
We can use the Euclidean Algorithm to find x and y.
Recall from Theorem 2 that for any integers a and b with $b > 0$, if we divide

a by b we obtain $r = a \bmod b$ such that: (the remainder) and $q = a \div b$ (the quotient), and we can write $a = bq + r$.
Note that in the first step of the Euclidean Algorithm, we only kept track of the remainder ($a \bmod b$) but now we will also keep track of the quotient ($a \div b$), and will write each line in the form $a = bq + r$.

2 Recurrence Relations

Coming soon...

3 Graphs and Trees

Coming soon...