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:

$9 \equiv 17 \pmod{4}$ is true, so we also have $9 \bmod 4 = 1$ 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 $\pm 1, \pm 2, \pm 3, \text{ and } \pm 6$.
The common divisors of 25 and 50 are $\pm 1, \pm 5, \pm 10, \text{ and } \pm 25$.

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...

4 Practice problems

week 1

Section 4.1 (Divisibility and Modular Arithmetic)

Questions: 3, 5, 13, 21, 31

3.prove that if $a \mid b$ then $a \mid bc$ for all integers c:

by the definition of Divisibility, we know that if $a \mid b$, then $b = ak$ for some integer k. if we multiply both sides by c, we get $bc = akc$. since $akc = a(kc)$, and kc is an integer, we can say that $a \mid bc$.

5.Show that if $a \mid b$ and $b \mid a$ where $a, b \in \mathbb{Z}$, then $a = b$ or $a = -b$:

by the definition of Divisibility, we know that if $a \mid b$, then $b = ak$ for some integer k. similarly, if $b \mid a$, then $a = bm$ for some integer m.
substituting the first equation into the second, we get $a = (ak)m$, or $a = akm$.
dividing both sides by a (which is nonzero), we get $1 = km$. since k and m are integers, the only way for their product to be 1 is if both are 1 or both are -1. thus, if $k = 1$, then $b = a$, and if $k = -1$, then $b = -a$.

13.What are the quotient and remainder when:

(a) 19 is divided by 7

$$19 = 2 \cdot 7 + 5 \quad \Rightarrow \quad 19 \div 7 = 2, \quad 19 \bmod 7 = 5$$

(b) -111 is divided by 11

$$-111 = -11 \cdot 11 + 10 \quad \Rightarrow \quad -111 \div 11 = -11, \quad -111 \bmod 11 = 10$$

(c) 789 is divided by 23

$$789 = 34 \cdot 23 + 7 \quad \Rightarrow \quad 789 \div 23 = 34, \quad 789 \bmod 23 = 7$$

(d) 1001 is divided by 13

$$1001 = 77 \cdot 13 + 0 \quad \Rightarrow \quad 1001 \div 13 = 77, \quad 1001 \bmod 13 = 0$$

(e) 0 is divided by 19

$$0 = 0 \cdot 19 + 0 \quad \Rightarrow \quad 0 \div 19 = 0, \quad 0 \bmod 19 = 0$$

(f) 3 is divided by 5

$$3 = 0 \cdot 5 + 3 \quad \Rightarrow \quad 3 \div 5 = 0, \quad 3 \bmod 5 = 3$$

(g) -1 is divided by 3

$$-1 = -1 \cdot 3 + 2 \quad \Rightarrow \quad -1 \div 3 = -1, \quad -1 \bmod 3 = 2$$

(h) 4 is divided by 1

$$4 = 4 \cdot 1 + 0 \quad \Rightarrow \quad 4 \div 1 = 4, \quad 4 \bmod 1 = 0$$

21.Let m be a positive integer. Show that $a \equiv b \pmod{m}$ if $a \bmod m = b \bmod m$:

by the definition of congruence modulo m, we know that if $a \equiv b \pmod{m}$, then $m \mid (a - b)$. this means that $a - b = mk$ for some integer k. adding b to both sides, we get $a = mk + b$. taking both sides modulo m, we get $a \bmod m = (mk + b) \bmod m$. since $mk \bmod m = 0$, we have $a \bmod m = b \bmod m$.

31.Find the integer a such that:

(a) $a \equiv -15 \pmod{27}$ and $-26 \leq a \leq 0$

$a = -15$ (already in the interval, so the solution is $a = -15$).

(b) $a \equiv 24 \pmod{31}$ and $-15 \leq a \leq 15$

$a = 24 - 31 = -7$ (in the interval, so the solution is $a = -7$).

(c) $a \equiv 99 \pmod{41}$ and $100 \leq a \leq 140$

$a = 99 + 41 = 140$ (in the interval, so the solution is $a = 140$).

Section 4.3 (Primes and Greatest Common Divisors)

Questions: 3, 13, 17, 19, 25, 30, 31, 33, 39, 41, 43, 45

3.Find the prime factorization of each of the following integers:

(a) 88

$$88 = 2 \cdot 2 \cdot 2 \cdot 11 = 2^3 \cdot 11$$

(b) 126

$$126 = 2 \cdot 3 \cdot 3 \cdot 7 = 2^1 \cdot 3^2 \cdot 7$$

(c) 729

$$729 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 3^6$$

(d) 1001

$$1001 = 7 \cdot 11 \cdot 13 = 7^1 \cdot 11^1 \cdot 13^1$$

(e) 1111

$$1111 = 11 \cdot 101 = 11^1 \cdot 101^1$$

(f) 909090

$$909090 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 37 = 2^1 \cdot 3^3 \cdot 5^1 \cdot 7^1 \cdot 13^1 \cdot 37^1$$

13. prove or disprove that there are three consecutive odd positive integers that are primes, that is odd primes of the form p, p+2, and p+4:

Let p be an odd prime. then consider $p, p+2, p+4$ in $\pmod 3$.

- If $p \equiv 0 \pmod 3$, then $p = 3$ (since p is prime). Then $p + 2 = 5$ (prime), but $p + 4 = 7$ (also prime). So this case works.
- If $p \equiv 1 \pmod 3$, then $p + 2 \equiv 0 \pmod 3$. Since $p + 2 > 3$, it is divisible by 3 and not prime.
- If $p \equiv 2 \pmod 3$, then $p + 4 \equiv 0 \pmod 3$. Since $p + 4 > 3$, it is divisible by 3 and not prime.

Therefore the only set of three consecutive odd positive integers that are primes is 3, 5, and 7.

17. Determine whether the integers in each of these sets are pairwise relatively prime:

(a) $11, 15, 19$

$$\gcd(11, 15) = 1, \quad \gcd(11, 19) = 1, \quad \gcd(15, 19) = 1$$

they are relatively prime.

(b) $14, 15, 21$

$$\gcd(14, 15) = 1, \quad \gcd(14, 21) = 7, \quad \gcd(15, 21) = 3$$

they are not relatively prime.

(c) $12, 17, 31, 37$

$$\gcd(12, 17) = 1, \quad \gcd(12, 31) = 1, \quad \gcd(12, 37) = 1,$$

$$\gcd(17, 31) = 1, \quad \gcd(17, 37) = 1, \quad \gcd(31, 37) = 1$$

they are relatively prime.

(d) $7, 8, 9, 11$

$$\gcd(7, 8) = 1, \quad \gcd(7, 9) = 1, \quad \gcd(7, 11) = 1,$$

$$\gcd(8, 9) = 1, \quad \gcd(8, 11) = 1, \quad \gcd(9, 11) = 1$$

they are relatively prime.

19. Show that if $2^n - 1$ is prime, then n is prime:

By contrapositive, if n is not prime, then $2^n - 1$ is not prime. Let $n = ab$, where $a, b > 1$. Then $2^n - 1 = 2^{ab} - 1$. This can be factored as: $(2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + ... + 2^a + 1)$. Since both factors are greater than 1, $2^n - 1$ is not prime.

25. What are the greatest common divisors of these pairs of integers:

(a) $3^7 \cdot 5^3 \cdot 7^3$ and $2^{11} \cdot 3^5 \cdot 5^9$

$$\gcd(3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9) = 3^{\min(7,5)} \cdot 5^{\min(3,9)} \cdot 7^{\min(3,0)} = 3^5 \cdot 5^3 \cdot 7^0 = 3^5 \cdot 5^3$$

(b) $11 \cdot 13 \cdot 17$ and $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

(c) 23^{31} and 23^{17}

(d) $41 \cdot 43 \cdot 53$ and $41 \cdot 43 \cdot 53$

(e) $3^{13} \cdot 5^{17}$ and $2^{12} \cdot 7^{21}$

(f) 1111 and 0