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. Additionally, as of 9/17/2025 2:49AM, some of this was edited by copilot so I cannot guarantee the accuracy as well as relevance to the course Use at your own risk.
I will continue to edit these notes as the course goes on as well as verify the accuracy of the content.

ps on 09/16/2025, I was intoxicated while writing these notes :3
Check me out at `https://github.com/andrewSmellz`
If you find any issues, please report them in the Issues section of the repository.

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.

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 b 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 integers (by Theorem 2) for which $a = qb + r$ 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 $\pm 1, \pm 2, \pm 3, \text{ and } \pm 6$.
The common divisors of 25 and 50 are $\pm 1, \pm 5, \pm 25$.

Definition 10: (Greatest Common Divisor)
Let $a, b \in \mathbb{Z}$. An integer $d \geq 0$ is the greatest common divisor of a and b if:

1. d divides a and d divides b (so d is a common divisor), and
2. for every common divisor e of a and b we have $e \mid d$.

We denote the greatest common divisor of a and b by $\gcd(a, b)$.

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 positive 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 (up to ordering of equal primes) as a product of primes.

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 with the minimum exponents. 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 the maximum exponents in their prime factorizations.

However, the above method is inefficient for very large numbers. 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:

$$\begin{aligned} 720 \bmod 26 &= 18 \quad (26 \cdot 27 = 702,\ 720 - 702 = 18), \\ 26 \bmod 18 &= 8, \\ 18 \bmod 8 &= 2, \\ 8 \bmod 2 &= 0. \end{aligned}$$

so, $\gcd(720, 26) = 2$.

Theorem 19:
Let $a, b \in \mathbb{Z}$, not both zero. 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 $r = a \bmod b$ (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 $a = bq + r$.

Example 20: Using the Euclidean algorithm, we can find the integers x and y such that $360x + 84y = \gcd 360, 84$ as follows:

$$360 = 84 \cdot 4 + 24$$

$$84 = 24 \cdot 3 + 12$$
$$24 = 12 \cdot 2 + 0$$

Thus, $\gcd(360, 84) = 12$.
Now let us rearrange each of the lines above (except for the last one which we dont need) so that the remainders are on the left hand side of the equals sign, and everything else is on the right hand side, with the quotients enclosed in the round parentheses:

$$24 = 360 + 84 \cdot (-4)$$

$$12 = 84 + 24 \cdot (-3)$$

Notice that the first equation above contains 360 and the second equations contains 84, and we want an equation in the form $360x + 84y$. working backwards, replace 24 in the second equation with the first equation as follows:

$$12 = 84 + (360 + 84 \cdot (-4)) \cdot (-3)$$

$$= 84 + 360 \cdot (-3) + 84 \cdot 12$$
$$= 360 \cdot (-3) + 84 \cdot 13$$

Thus, $x = -3$ and $y = 13$ and we have $360 \cdot (-3) + 84 \cdot 13 = \gcd 360, 84 = 12$.

Example 21: bruh its just another one like example 20 just do it yourself if you want to know the numbers are $1205x + 37y = \gcd(1205, 37)$.

1.4 Extended Euclidean Algorithm

In the previous examples we expressed $\gcd(a, b)$ in the form $ax + by$ by first executing the Euclidean algorithm and then working backwards to perform substituions to obtain the integers x and y. The extended Euclidean algorithm can obtain x and y with a single forward pass of the algorithm.
observe from Example 20 that each step j of the algorithm (starting from $j = 0$) performs the computation $r_j = r_{j+1} \cdot q_{j+1} + r_{j+2}$. thus we can represent the steps of the algorithm in a tabular form as follows:

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	360	84	4	24
1	84	24	3	12
2	24	12	2	0

The extended euclidean algorithm keeps track of two additional values

$$s_j = s_{j-2} - q_{j-1} \cdot s_{j-1}$$

and

$$t_j = t_{j-2} - q_{j-1} \cdot t_{j-1}$$

with the initial values fixed to $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$. After reaching the final step of j of the Euclidean Algorithm, we must compute one final iteration of s_{j+1} and t_{j+1}. The result is as follows:

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	360	84	4	24	1	0
1	84	24	3	12	0	1
2	24	12	2	0	$1 - (4)(0) = 1$	$0 - (4)(1) = -4$
3	12				$0 - (3)(1) = -3$	$1 - (3)(-4) = 13$

Now, we take $x = s_3$ and $y = t_3$, which yields $\gcd 360, 84 = 12 = (-3) \cdot 360 + (13) \cdot 84$.

1.5 Modular Arithmetic

We are accustomed to performing arithmetic on infinite sets of numbers like $\mathbb{Z}$ and $\mathbb{R}$. But sometimes we need to perform arithmetic on a finite set, and we need it to make sense and be consistent with normal arithmetic.
we will focus on the sets defined by $\mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}$ for some integer $n \geq 2$.
$\mathbb{Z}_n$ is the set of remainders we can get when we divided integers by n. we call this number system the integers $\bmod n$.
one of the important features we want to build into our mathematical operations for finite sets is closure: the property that when we apply an operation to two elements of the set, the result is also an element of the set.

Definition 22: (Modular Addition and Multiplication)
we will use the symbols $\oplus, \odot, \ominus,$ and $\oslash$ to denote addition mod n, multiplication mod n, subtraction mod n, and division mod n, respectively.

let $\boldsymbol{n}$ be a positive integer and let $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}_{\boldsymbol{n}}$. then we define:

$$\boldsymbol{a \oplus b = (a + b) \bmod n}$$

$$\boldsymbol{a \odot b = (a \cdot b) \bmod n}$$

$$\boldsymbol{a \ominus b = (a - b) \bmod n}$$

$$\boldsymbol{a \oslash b = (a \cdot b^{-1}) \bmod n}$$

where $\boldsymbol{b^{-1}}$ is the multiplicative inverse of $\boldsymbol{b}$ modulo $\boldsymbol{n}$, if it exists.
NOTE: because we end each calculation with the **mod*n*** operation, the results of these operations are always in $\mathbb{Z}_{\boldsymbol{n}}$. so we will have closure.

Example 23:
let $\boldsymbol{n = 7}$. we have the following:

$$\boldsymbol{3 \oplus 6 = (3 + 6) \bmod 7 = 2}$$

$$\boldsymbol{3 \odot 6 = (3 \cdot 6) \bmod 7} = 4$$

let $\boldsymbol{n = 8}$. we have the following:

$$\boldsymbol{3 \oplus 6 = (3 + 6) \bmod 8 = 1}$$

$$\boldsymbol{3 \odot 6 = (3 \cdot 6) \bmod 8 = 2}$$

NOTE: that the symbols $\oplus$ and $\odot$ depend on the context. if we are working in $\mathbb{Z}_{\boldsymbol{10}}$, then $\boldsymbol{5 \oplus 5 = 0}$, but if we are working in $\mathbb{Z}_{\boldsymbol{9}}$, then $\boldsymbol{5 \oplus 5 = 1}$.

Proposition 24:(properties of modular addition and modular multiplication)
let $\boldsymbol{n}$ be an integer with $\boldsymbol{n \geq 2}$. the operations $\oplus$ and $\odot$ on $\mathbb{Z}_{\boldsymbol{n}}$ have the following properties:

(a) **Associativity:** For all $\boldsymbol{a, b, c} \in \mathbb{Z}_{\boldsymbol{n}}$:

$$\boldsymbol{(a \oplus b) \oplus c = a \oplus (b \oplus c)}$$

$$\boldsymbol{(a \odot b) \odot c = a \odot (b \odot c)}$$

(b) **Commutativity:** For all $\boldsymbol{a, b} \in \mathbb{Z}_{\boldsymbol{n}}$:

$$\boldsymbol{a \oplus b = b \oplus a}$$

$$\boldsymbol{a \odot b = b \odot a}$$

(c) **Distributivity:** For all $\boldsymbol{a, b, c} \in \mathbb{Z}_{\boldsymbol{n}}$:

$$\boldsymbol{a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)}$$

(d) **identity element 0 for addition:** For all $\boldsymbol{a} \in \mathbb{Z}_{\boldsymbol{n}}$:

$$\boldsymbol{a} \oplus \mathbf{0} = \boldsymbol{a}$$

(e) **identity element 1 for multiplication:** For all $\boldsymbol{a} \in \mathbb{Z}_{\boldsymbol{n}}$:

$$\boldsymbol{a} \odot \mathbf{1} = \boldsymbol{a}$$

Let us prove the commutative property for addition:

$$\begin{aligned} \boldsymbol{a} \oplus \boldsymbol{b} &= (\boldsymbol{a} + \boldsymbol{b}) \textbf{ mod } \boldsymbol{n} \\ &= (\boldsymbol{b} + \boldsymbol{a}) \textbf{ mod } \boldsymbol{n} \\ &= \boldsymbol{b} \oplus \boldsymbol{a} \end{aligned}$$

1.6 Modular substraction

In ordinary arithmetic, when we write $\boldsymbol{a} - \boldsymbol{b} = \boldsymbol{x}$, we understand that this is equivalent to writing $\boldsymbol{a} = \boldsymbol{b} + \boldsymbol{x}$.
similarly, to find the value of x in the equation $\boldsymbol{a} \ominus \boldsymbol{b} = \boldsymbol{x}$, we can say that $\boldsymbol{x}$ is an element of $\mathbb{Z}_{\boldsymbol{n}}$ such that $\boldsymbol{a} = \boldsymbol{b} \oplus \boldsymbol{x}$.
this definition relies on the fact that there is exactly one $\boldsymbol{x} \in \mathbb{Z}_{\boldsymbol{n}}$ such that $\boldsymbol{a} = \boldsymbol{b} \oplus \boldsymbol{x}$.

Definition 25: (modular subtraction)
let $\boldsymbol{n}$ be a positive integer and $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}_{\boldsymbol{n}}$. then we define: $\boldsymbol{a} \ominus \boldsymbol{b}$ to be the unique element $\boldsymbol{x} \in \mathbb{Z}_{\boldsymbol{n}}$ such that $\boldsymbol{a} = \boldsymbol{b} \oplus \boldsymbol{x}$.
Altnernatively, we could have defined $\boldsymbol{a} \ominus \boldsymbol{b}$ to be $(\boldsymbol{a} - \boldsymbol{b}) \textbf{ mod } \boldsymbol{n}$.

Proposition 26: (modular subtraction)
let $\boldsymbol{n}$ be a positive integer and $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}_{\boldsymbol{n}}$. then:

$$\boldsymbol{a} \ominus \boldsymbol{b} = (\boldsymbol{a} - \boldsymbol{b}) \textbf{ mod } \boldsymbol{n}$$

proof:
First we need to show that $(\boldsymbol{a} - \boldsymbol{b}) \textbf{ mod } \boldsymbol{n} \in \mathbb{Z}_{\boldsymbol{n}}$. This is obvious from the defintiion of mod.
next, we show that if $\boldsymbol{x} = (\boldsymbol{a} - \boldsymbol{b}) \textbf{ mod } \boldsymbol{n}$, then $\boldsymbol{a} = \boldsymbol{b} \oplus \boldsymbol{x}$. so we take $\boldsymbol{b} \oplus \boldsymbol{x}$ and substitute $\boldsymbol{x} = (\boldsymbol{a} - \boldsymbol{b}) \textbf{ mod } \boldsymbol{n} = \boldsymbol{a} - \boldsymbol{b} + \boldsymbol{kn}$. then:

$$\begin{aligned} \boldsymbol{b} \oplus \boldsymbol{x} &= (\boldsymbol{b} + \boldsymbol{x}) \textbf{ mod } \boldsymbol{n} \\ &= (\boldsymbol{b} + (\boldsymbol{a} - \boldsymbol{b}) \textbf{ mod } \boldsymbol{n}) \textbf{ mod } \boldsymbol{n} \\ &= (\boldsymbol{b} + \boldsymbol{a} - \boldsymbol{b} + \boldsymbol{kn}) \textbf{ mod } \boldsymbol{n} \\ &= (\boldsymbol{a} + \boldsymbol{kn}) \textbf{ mod } \boldsymbol{n} \\ &= \boldsymbol{a} \textbf{ mod } \boldsymbol{n} \\ &= \boldsymbol{a} \end{aligned}$$

Example 27:
we will compute $\mathbf{2 \ominus 3}$ in two ways: using definition 25 and using proposition 26. first lets look at the addition table below, which shows all the values of $\boldsymbol{a \oplus b}$ for $\boldsymbol{a, b} \in \mathbb{Z}_\mathbf{5}$.

		$\boldsymbol{b}$				
	$\oplus$	**0**	**1**	**2**	**3**	**4**
	0	**0**	**1**	**2**	**3**	**4**
	1	**1**	**2**	**3**	**4**	**0**
a	**2**	**2**	**3**	**4**	**0**	**1**
	3	**3**	**4**	**0**	**1**	**2**
	4	**4**	**0**	**1**	**2**	**3**

by defintion 25, to find $\boldsymbol{x} = \mathbf{2 \ominus 3}$, we must find the value $\boldsymbol{x}$ that satisfies $\mathbf{2} = \mathbf{3} \oplus \boldsymbol{x}$. So in the table above, we look at the row for $\boldsymbol{a} = \mathbf{3}$ and step through each value until we find the column where thevalue is 2. we see that this happens when $\boldsymbol{x} = \mathbf{4}$.

by propsition 26, we can compute $\mathbf{2 \ominus 3}$ as follows:

$$\begin{aligned} \mathbf{2 \ominus 3} &= \mathbf{(2 - 3) \bmod 5} \\ &= \mathbf{(-1) \bmod 5} \\ &= \mathbf{4} \end{aligned}$$

1.7 Modular Division

Modular division is significantly different from the other three modular operations.
when working with the rational numbers $\boldsymbol{mathbbQ}$, when we write $\boldsymbol{x} = \boldsymbol{a/b}$, we understand that $\boldsymbol{x} = \boldsymbol{a \cdot b^{-1}}$, where $\boldsymbol{b^{-1}}$ is $\mathbf{1}/\boldsymbol{b}$ and is referred to as the reciprocal or inverse of $\boldsymbol{b}$. note that $\boldsymbol{b} = \mathbf{0}$ has no reciprocal, and for all other $\boldsymbol{b} \in \mathbb{Q}$, we have that $\boldsymbol{b \cdot b^{-1}} = \mathbf{1}$.

Similarly, it seems reasonable that for modular division in $\boldsymbol{mathbbZ_n}$, we should define $\boldsymbol{b^{-1}}$ as the element that satisfies $\boldsymbol{b} \odot \boldsymbol{b^{-1}} = \mathbf{1}$. however, not every element of $\mathbb{Z}_{\boldsymbol{n}}$ has a multiplicative inverse.

for example, consider the multiplcation table below, which shows all the values of $\boldsymbol{a} \odot \boldsymbol{b}$ for $\mathbb{Z}_\mathbf{10}$.

						$\boldsymbol{b}$					
	$\otimes$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
	0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	1	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
	2	**0**	**2**	**4**	**6**	**8**	**0**	**2**	**4**	**6**	**8**
	3	**0**	**3**	**6**	**9**	**2**	**5**	**8**	**1**	**4**	**7**
	4	**0**	**4**	**8**	**2**	**6**	**0**	**4**	**8**	**2**	**6**
a	**5**	**0**	**5**	**0**	**5**	**0**	**5**	**0**	**5**	**0**	**5**
	6	**0**	**6**	**2**	**8**	**4**	**0**	**6**	**2**	**8**	**4**
	7	**0**	**7**	**4**	**1**	**8**	**5**	**2**	**9**	**6**	**3**
	8	**0**	**8**	**6**	**4**	**2**	**0**	**8**	**6**	**4**	**2**
	9	**0**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**

in the table above, to find the reciprocal of an element $\boldsymbol{a}$ in $\mathbb{Z}_{\mathbf{10}}$, locate the element $\boldsymbol{b}$ for which $\boldsymbol{a} \odot \boldsymbol{b} = \mathbf{1}$.
all such occurrences in the table are highlighted in yellow.
note that:

- 0 has no reciprocal
- 1 has a reciprocal of 1
- 3 has a reciprocal of 7
- 7 has a reciprocal of 3
- 9 has a reciprocal of 9
- the other elements (2,4,5,6,8) have no reciprocal

Definition 28:(Modular recpiprocal)
let $\boldsymbol{n}$ be a positive integer and let $\boldsymbol{a} \in \mathbb{Z}_{\boldsymbol{n}}$. A reciprocal of $\boldsymbol{a}$ is an element $\boldsymbol{b} \in \mathbb{Z}_{\boldsymbol{n}}$ such that $\boldsymbol{a} \odot \boldsymbol{b} = \mathbf{1}$. an element of $\mathbb{Z}_{\boldsymbol{n}}$ that has a reciprocal is called invertible.
Note: $\boldsymbol{a}$ is only invertible if $\mathbf{gcd}(\boldsymbol{a}, \boldsymbol{n}) = \mathbf{1}$.

Theorem 29:(Invertible elements of $\mathbb{Z}_{\boldsymbol{n}}$)
let $\boldsymbol{n}$ be a positive integer and let $\boldsymbol{a} \in \mathbb{Z}_{\boldsymbol{n}}$. Then $\boldsymbol{a}$ is invertible if and only if $\mathbf{gcd}(\boldsymbol{a}, \boldsymbol{n}) = \mathbf{1}$.

proposition 30:
every element in $\mathbb{Z}_{\boldsymbol{n}}$ except $\mathbf{0}$ has is invertible if and only if $\boldsymbol{n}$ is prime.
proof:
if $\boldsymbol{n}$ is prime and $\boldsymbol{a} \in \mathbf{1}, \mathbf{2}, \ldots, \boldsymbol{n} - \mathbf{1}$, then the greatest common divisor of $\boldsymbol{n}$ and $\boldsymbol{a}$ is 1. so by theorem 29, $\boldsymbol{a}^{-\mathbf{1}}$ exists for all $\boldsymbol{a} \in \mathbf{1}, \mathbf{2}, \ldots, \boldsymbol{n} - \mathbf{1}$.

Definition 31:(Modular Division)
let $\boldsymbol{n}$ be a positive integer and let $\boldsymbol{b}$ be an invertible element of $\mathbb{Z}_{\boldsymbol{n}}$. let $\boldsymbol{a} \in \mathbb{Z}_{\boldsymbol{n}}$ be arbitrary. Then $\boldsymbol{a} \oslash \boldsymbol{b}$ is defined to be $\boldsymbol{a} \odot \boldsymbol{b}^{-\mathbf{1}}$.

Example 32:
in $\mathbb{Z}_{\mathbf{10}}$, calculcate $\mathbf{8} \oslash \mathbf{3}$. Note that $\mathbf{3}^{-\mathbf{1}} = \mathbf{7}$.

$$\begin{aligned} \mathbf{8} \oslash \mathbf{3} &= \mathbf{8} \odot \mathbf{3}^{-\mathbf{1}} \\ &= \mathbf{8} \odot \mathbf{7} \\ &= \mathbf{56 \bmod 10} \\ &= \mathbf{6.} \end{aligned}$$

Example 33:
in $\mathbb{Z}_{\mathbf{10}}$, calculcate $\mathbf{8} \oslash \mathbf{2}$. Note that $\mathbf{2}$ is not invertible so $\mathbf{8} \oslash \mathbf{2}$ is not defined.

Example 34:
in $\mathbb{Z}_{\mathbf{1205}}$, find $\mathbf{37^{-1}}$.
first we verify that 1205 and 37 are relatively prime by using the Euclidean Algorithm:

$$\begin{aligned} \mathbf{1205 \bmod 37 = 18} &\quad \mathbf{(37 \cdot 32 = 1184,\ 1205 - 1184 = 21),} \\ \mathbf{37 \bmod 18 = 1,} & \\ \mathbf{18 \bmod 1 = 0.} & \end{aligned}$$

so, $\mathbf{gcd(1205, 37) = 1 = 37(228) + 1205(-7)}$ and 37 is invertible in $\mathbb{Z}_{\mathbf{1205}}$.
now we wewrite the above equation by applying mod1205 on both sides:

$$\begin{aligned} \mathbf{37(228) + 1205(-7)} &\equiv \mathbf{1 \pmod{1205}} \\ \mathbf{37(228)} &\equiv \mathbf{1 \pmod{1205}} \end{aligned}$$

thus, $\mathbf{37^{-1} \equiv 228 \pmod{1205}}$.

there is 2 more examples but sorry its 4am if you are reading this though send me a message which is just a photo of a frog

1.8 Chinese remainder Theorem

suppose we have a box of bananas, we know that:

- if we distribute the bananas among 5 monkeys, we would have 1 left over
- if we distribute the bananas among 7 monkeys, we would have 2 left over
- there are less than 35 bananas in the box

How can we determine the number of bananas that are in the box? to do so we can write the following equations, where $\boldsymbol{x}$ denotes the number of bananas in the box:

$$\boldsymbol{x = 5k + 1} \quad \text{for some integer } \boldsymbol{k}$$

$$\boldsymbol{x = 7l + 2} \quad \text{for some integer } \boldsymbol{l}$$

in other words we have:

$$\boldsymbol{x \equiv 1 \pmod 5}$$

$$\boldsymbol{x \equiv 2 \pmod 7}$$

we need to find $\boldsymbol{x}$. So, let us substitute the firste equation into the second as follows:

$$\begin{aligned} \boldsymbol{1 + 5k} &\equiv \mathbf{2 \pmod 7} \\ \boldsymbol{5k} &\equiv \mathbf{1 \pmod 7} \\ \boldsymbol{k} &\equiv \mathbf{5^{-1} \pmod 7} \\ \boldsymbol{k} &\equiv \mathbf{3 \pmod 7} \quad (\text{since } \mathbf{5 \cdot 3 \equiv 1 \pmod 7}) \end{aligned}$$

this means that $\boldsymbol{k = 3 + 7t}$ for some non negative integer $\boldsymbol{t}$. Now we substite our equation for $\boldsymbol{K}$ into the first equation $\boldsymbol{x = 1 + 5k}$:

$$\begin{aligned} x &= 1 + 5(3 + 7t) \\ &= 16 + 35t \end{aligned}$$

notice for all $\boldsymbol{t > 0}$ we have $\boldsymbol{x > 35}$. But we know that we have less than 35 bananas in the box. so we know that $\boldsymbol{t = 0}$ and thus $\boldsymbol{x = 16}$, meaning that we have 16 bananas in the box.

Theorem 37:(Chinese Remainder Theorem)
let $\boldsymbol{a, b, m, n}$ be integers with $\boldsymbol{m > 0}$ and $\boldsymbol{n > 0}$. if $\boldsymbol{\gcd(m, n) = 1}$. there is a unique integer $\boldsymbol{x_0}$ with $\boldsymbol{0 \leq x_0 < mn}$ such that:

$$x_0 \equiv a \pmod{m}$$

$$x_0 \equiv b \pmod{n}$$

furthermore, every solution to these equations differs from $\boldsymbol{x_0}$ by a multiple of $\boldsymbol{mn}$.

Theorem 38:(Generalized Chinese Remainder Theorem)
let $\boldsymbol{n_1, n_2, \ldots, n_m}$ be positive and pairwise relatively prime integers.
let $\boldsymbol{a_1, a_2, \ldots, a_m}$ be arbitrary integers.
there is an integer $\boldsymbol{x_0}$ that satisfies the system of congruences:

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

$$\vdots$$

$$x \equiv a_m \pmod{n_m}$$

furthermore, every solution to this system of congruences differs from $\boldsymbol{x_0}$ by a multiple of $\boldsymbol{N = n_1 n_2 \cdots n_m}$

Example 39:
solve the system of congruences:

$$\boldsymbol{x \equiv 1 \pmod 5}$$

$$\boldsymbol{x \equiv 2 \pmod 7}$$

$$\boldsymbol{x \equiv 3 \pmod 6}$$

note that from the start of this sedction, we found that $\boldsymbol{x = 16 + 35t}$ when solving for the first two congurences, now we substitute that result into the third congurence as follows:

$$\boldsymbol{16 + 35t \equiv 3 \pmod 6}$$

from which we obtain:

$$\boldsymbol{35t \equiv -13 \equiv 5 \pmod 6}$$

since $\boldsymbol{35 \equiv 5 \pmod 6}$, we have:

$$\boldsymbol{5t \equiv 5 \pmod 6}$$

so:

$$\boldsymbol{t \equiv 5 \cdot 5^{-1} \pmod 6}$$

$$\boldsymbol{t = equiv 1 \pmod 6}$$

so we have $\boldsymbol{t = 1 + 6s}$ for some non negative integer $\boldsymbol{s}$. Now we substitute $\boldsymbol{t = 1 + 6s}$ into $\boldsymbol{x = 16 + 35t}$ to obtain:

$$\begin{aligned} \boldsymbol{x} &= \boldsymbol{16 + 35(1 + 6s)} \\ &= \boldsymbol{51 + 210s} \end{aligned}$$

Note that $\boldsymbol{x}$ is a solution to the three congruences for any value of $\boldsymbol{s}$, so we have infinitely many solutions. Also note that the term $\boldsymbol{210s}$ tells us that we only have one solution less than 210, and that each solution to the euqaiton differs from the next by a multiple of 210, and $\boldsymbol{210 = 5 \cdot 7 \cdot 6}$ which is the product of the moduli.

1.9 Groups

Informally, you are already familiar with operations. For example, the addition operation + takes a pair of numbers as input, and produces their sum as output. Now, we give the formal definition of an operation.

Definition 1:(Operation)
let $\boldsymbol{A}$ be a set. An operation on $\boldsymbol{A}$ is a function that maps elements in $\boldsymbol{A \times A}$ to elements in $\boldsymbol{A}$.

Example 2:
Consider the operations $\oplus$**,** $\odot$**,** and $\ominus$, which are all functions from $\mathbb{Z}_{\boldsymbol{n}} \times \mathbb{Z}_{\boldsymbol{n}}$ to $\mathbb{Z}_{\boldsymbol{n}}$. Where

$\mathbb{Z}_{\boldsymbol{n}} = \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \boldsymbol{n} - \mathbf{1}\}$.
the operation $\oslash$ is a function from $\mathbb{Z}_{\boldsymbol{p}}^* \times \mathbb{Z}_{\boldsymbol{p}}^*$ to $\mathbb{Z}_{\boldsymbol{p}}^*$, where $\boldsymbol{p}$ is a prime number and $\mathbb{Z}_{\boldsymbol{p}}^* = \mathbb{Z}_{\boldsymbol{p}} \setminus \{\mathbf{0}\}$.
a common symbol used to generically represent an operation is $*$.

Definition 3:(properties of operations)
Let $*$ be an operation on a set $\boldsymbol{A}$. the following are some important properties that the operation may have.

1. **Commutative property:** $*$ is commutative on $\boldsymbol{A}$ provided that $\boldsymbol{a} * \boldsymbol{b} = \boldsymbol{b} * \boldsymbol{a}$ for all $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{A}$.
2. **Closure property:** $*$ is closed on $\boldsymbol{A}$ provided that $\boldsymbol{a} * \boldsymbol{b} \in \boldsymbol{A}$ for all $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{A}$.
3. **Associative property:** $*$ is associative on $\boldsymbol{A}$ provided that $(\boldsymbol{a} * \boldsymbol{b}) * \boldsymbol{c} = \boldsymbol{a} * (\boldsymbol{b} * \boldsymbol{c})$ for all $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \boldsymbol{A}$.
4. **Inverses:** Suppose that $\boldsymbol{e} \in \boldsymbol{A}$ is the identity element. We can call $\boldsymbol{b}$ an inverse of $\boldsymbol{a}$ provided that $\boldsymbol{a} * \boldsymbol{b} = \boldsymbol{b} * \boldsymbol{a} = \boldsymbol{e}$.

Example 4:
to be continued...

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, if $a \mid b$ then $b = ak$ for some integer k. Multiplying both sides by c gives $bc = akc$. Since $akc = a(kc)$ and kc is an integer, we have $a \mid bc$.

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, 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 gives $a = (ak)m$, or $a = akm$. If $a \neq 0$, dividing both sides by a yields $1 = km$. Since k and m are integers, the only integer solutions to $km = 1$ are $k = m = 1$ or $k = m = -1$. Thus, if $k = 1$, then $b = a$, and if $k = -1$, then $b = -a$. (If $a = 0$, then the divisibility statements imply $b = 0$, and the conclusion $a = b$ also holds.)

13. What are the quotient and remainder when:

(a) 19 is divided by 7

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

(b) -111 is divided by 11

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

(Note: this follows the convention that remainders are in $\mathbf{0, \ldots, 10}$.)

(c) 789 is divided by 23

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

(d) 1001 is divided by 13

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

(e) 0 is divided by 19

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

(f) 3 is divided by 5

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

(g) -1 is divided by 3

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

(h) 4 is divided by 1

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

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

Suppose $\boldsymbol{a \bmod m = b \bmod m}$. Then there exist integers $\boldsymbol{q_a, q_b}$ and a remainder $\boldsymbol{r}$ with $\boldsymbol{0 \leq r < m}$ such that

$$\boldsymbol{a = mq_a + r, \qquad b = mq_b + r.}$$

Subtracting gives $\boldsymbol{a - b = m(q_a - q_b)}$, so $\boldsymbol{m \mid (a - b)}$. Hence $\boldsymbol{a \equiv b \pmod{m}}$.

31. Find the integer $\boldsymbol{a}$ such that:

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

$$\boldsymbol{a = -15} \quad \text{(already in the interval, so the solution is } \boldsymbol{a = -15}\text{).}$$

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

$$\boldsymbol{a = 24 - 31 = -7} \quad \text{(in the interval, so the solution is } \boldsymbol{a = -7}\text{).}$$

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

$$\boldsymbol{a = 99 + 41 = 140} \quad \text{(in the interval, so the solution is } \boldsymbol{a = 140}\text{).}$$

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

$$\mathbf{88 = 2 \cdot 2 \cdot 2 \cdot 11 = 2^3 \cdot 11}$$

(b) 126

$$\mathbf{126 = 2 \cdot 3 \cdot 3 \cdot 7 = 2 \cdot 3^2 \cdot 7}$$

(c) 729

$$\mathbf{729 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 3^6}$$

(d) 1001

$$\mathbf{1001 = 7 \cdot 11 \cdot 13}$$

(e) 1111

$$\mathbf{1111 = 11 \cdot 101}$$

(f) 909090

$$\mathbf{909090 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 37 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 37}$$

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

Let $\boldsymbol{p}$ be an odd prime, and consider $\boldsymbol{p, p+2, p+4}$ modulo $\mathbf{3}$.

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

Therefore the only set of three consecutive odd positive integers that are all prime is $\mathbf{3, 5, 7}$.

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

(a) $\mathbf{11, 15, 19}$

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

they are pairwise relatively prime.

(b) $\mathbf{14, 15, 21}$

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

they are not pairwise relatively prime.

(c) $\mathbf{12, 17, 31, 37}$

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

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

they are pairwise relatively prime.

(d) $\mathbf{7, 8, 9, 11}$

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

they are pairwise relatively prime.

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

By contrapositive, if n is not prime (so $n = ab$ with $a, b > 1$), then

$$2^n - 1 = 2^{ab} - 1 = (2^a - 1)\left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1\right),$$

so $2^n - 1$ is composite. Therefore if $2^n - 1$ is prime then n must be prime.

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

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

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

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

$$\gcd(11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3) = 1$$

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

$$\gcd(23^{31}, 23^{17}) = 23^{17}$$

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

$$\gcd(41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53) = 41 \cdot 43 \cdot 53$$

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

$$\gcd(3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}) = 1$$

(f) 1111 and 0

$$\gcd(1111, 0) = 1111.$$

From this point on, I have begun sipping a cut water, moose on the line, money on the mind.

30.If the product of two integers is $2^7 \cdot 3^8 \cdot 5^2 \cdot 7^{11}$ and their greatest common divisor is $2^3 \cdot 3^4 \cdot 5$, what is their least common multiple?

By definition, for positive integers a and b,

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

Therefore

$$\operatorname{lcm}(a, b) = \frac{a \cdot b}{\gcd(a, b)} = \frac{2^7 \cdot 3^8 \cdot 5^2 \cdot 7^{11}}{2^3 \cdot 3^4 \cdot 5} = 2^4 \cdot 3^4 \cdot 5^1 \cdot 7^{11}.$$

31.Show that if a and b are positive integers, then $ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$:

By the prime factorization theorem, we can write a and b as:

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}$$

$$b = p_1^{f_1} \cdot p_2^{f_2} \cdot \cdots \cdot p_k^{f_k}$$

where $p_1, p_2, \ldots, p_k$ are the primes appearing in either factorization (exponent possibly zero for some primes). The gcd and lcm can be written as:

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} \cdot p_2^{\min(e_2, f_2)} \cdot \cdots \cdot p_k^{\min(e_k, f_k)}$$

$$\operatorname{lcm}(a, b) = p_1^{\max(e_1, f_1)} \cdot p_2^{\max(e_2, f_2)} \cdot \cdots \cdot p_k^{\max(e_k, f_k)}$$

Multiplying these together, we get:

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = p_1^{\min(e_1, f_1) + \max(e_1, f_1)} \cdot \cdots \cdot p_k^{\min(e_k, f_k) + \max(e_k, f_k)}.$$

Since $\min(x, y) + \max(x, y) = x + y$, we have:

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = p_1^{e_1 + f_1} \cdot \cdots \cdot p_k^{e_k + f_k} = a \cdot b.$$

33. Use the Euclidean algorithm to find:

(a) $\mathbf{gcd(12, 18)}$

$$\mathbf{18 \bmod 12 = 6, \quad 12 \bmod 6 = 0}$$

so, $\mathbf{gcd(12, 18) = 6}$.

(b) $\mathbf{gcd(111, 201)}$

$$\mathbf{201 \bmod 111 = 90, \quad 111 \bmod 90 = 21, \quad 90 \bmod 21 = 6, \quad 21 \bmod 6 = 3, \quad 6 \bmod 3 = 0}$$

so, $\mathbf{gcd(111, 201) = 3}$.

(c) $\mathbf{gcd(1001, 1331)}$

$$\mathbf{1331 \bmod 1001 = 330, \quad 1001 \bmod 330 = 11, \quad 330 \bmod 11 = 0}$$

so, $\mathbf{gcd(1001, 1331) = 11}$.

(d) $\mathbf{gcd(12345, 54321)}$

$$\mathbf{54321 \bmod 12345 = 4941, \quad 12345 \bmod 4941 = 2463, \quad 4941 \bmod 2463 = 15,}$$

$$\mathbf{2463 \bmod 15 = 3, \quad 15 \bmod 3 = 0}$$

so, $\mathbf{gcd(12345, 54321) = 3}$.

(e) $\mathbf{gcd(1000, 5040)}$

$$\mathbf{5040 \bmod 1000 = 40, \quad 1000 \bmod 40 = 0}$$

so, $\mathbf{gcd(1000, 5040) = 40}$.

(f) $\mathbf{gcd(9888, 6060)}$

$$\mathbf{9888 \bmod 6060 = 3828, \quad 6060 \bmod 3828 = 2232, \quad 3828 \bmod 2232 = 1596,}$$

$$\mathbf{2232 \bmod 1596 = 636, \quad 1596 \bmod 636 = 324, \quad 636 \bmod 324 = 312,}$$

$$\mathbf{324 \bmod 312 = 12, \quad 312 \bmod 12 = 0}$$

so, $\mathbf{gcd(9888, 6060) = 12}$.

39. Express the greatest common divisor of each of these pairs of integers as a linear combination of the integers:

(a) 10,11

$$\mathbf{11 = 1 \cdot 10 + 1,}$$
$$\mathbf{10 = 10 \cdot 1 + 0.}$$

Thus, $\mathbf{gcd(10, 11) = 1}$.

Back-substitute:

$$\mathbf{1 = 11 - 1 \cdot 10,}$$

so

$$\mathbf{1 = 10(-1) + 11(1).}$$

(b) 21,44

$$\mathbf{44 = 2 \cdot 21 + 2, \quad 21 = 10 \cdot 2 + 1, \quad 2 = 2 \cdot 1 + 0.}$$

Thus, $\mathbf{gcd(21, 44) = 1}$.

Back-substitution:

$$\mathbf{1 = 21 - 10 \cdot 2 = 21 - 10(44 - 2 \cdot 21) = 21 \cdot 21 - 44 \cdot 10,}$$

so

$$\mathbf{1 = 21(21) + 44(-10).}$$

(c) 36,48

$$\mathbf{48 = 1 \cdot 36 + 12, \quad 36 = 3 \cdot 12 + 0.}$$

Thus, $\mathbf{gcd(36, 48) = 12}$.

Back-substitution:

$$\mathbf{12 = 48 - 1 \cdot 36,}$$

so

$$\mathbf{12 = 36(-1) + 48(1).}$$

(d) 34,55

$$\mathbf{55 = 1 \cdot 34 + 21,}$$
$$\mathbf{34 = 1 \cdot 21 + 13,}$$
$$\mathbf{21 = 1 \cdot 13 + 8,}$$
$$\mathbf{13 = 1 \cdot 8 + 5,}$$
$$\mathbf{8 = 1 \cdot 5 + 3,}$$
$$\mathbf{5 = 1 \cdot 3 + 2,}$$
$$\mathbf{3 = 1 \cdot 2 + 1,}$$
$$\mathbf{2 = 2 \cdot 1 + 0.}$$

Back-substitution gives the linear combination

$$\mathbf{1 = 34(-21) + 55(13).}$$

(e) 117,213

$$\begin{aligned}
\mathbf{213} &= \mathbf{1 \cdot 117 + 96,} \\
\mathbf{117} &= \mathbf{1 \cdot 96 + 21,} \\
\mathbf{96} &= \mathbf{4 \cdot 21 + 12,} \\
\mathbf{21} &= \mathbf{1 \cdot 12 + 9,} \\
\mathbf{12} &= \mathbf{1 \cdot 9 + 3,} \\
\mathbf{9} &= \mathbf{3 \cdot 3 + 0.}
\end{aligned}$$

Back-substitution yields

$$\mathbf{3 = 117(-20) + 213(11).}$$

(f) 0,223

If one argument is 0, say $\mathbf{gcd(0, 223) = 223}$ and we can write

$$\mathbf{223 = 0 \cdot 0 + 223 \cdot 1,}$$

so $\mathbf{gcd(0, 223) = 223 = 0(0) + 223(1)}$.

(g) 123,2347

(See the extended Euclidean algorithm in Section 45 for a full worked example; result below.)

(h) 3454,4666

(Left as an exercise; use the Euclidean algorithm and back-substitute.)

(i) 9999,11111

(Left as an exercise; use the Euclidean algorithm and back-substitute.)

41. Use the extended Euclidean algorithm to express $\mathbf{gcd(26, 91)}$ as a linear combination of 26 and 91:

$$\mathbf{91 = 3 \cdot 26 + 13, \quad 26 = 2 \cdot 13 + 0.}$$

Thus, $\mathbf{gcd(26, 91) = 13}$.
Back-substitution:

$$\mathbf{13 = 91 - 3 \cdot 26,}$$

so

$$\mathbf{13 = 26(-3) + 91(1).}$$

43. Use the extended Euclidean algorithm to express $\mathbf{gcd(144, 89)}$ as a linear combination of 144 and 89:

$$\begin{aligned}
\mathbf{144} &= \mathbf{1 \cdot 89 + 55,} \\
\mathbf{89} &= \mathbf{1 \cdot 55 + 34,} \\
\mathbf{55} &= \mathbf{1 \cdot 34 + 21,} \\
\mathbf{34} &= \mathbf{1 \cdot 21 + 13,} \\
\mathbf{21} &= \mathbf{1 \cdot 13 + 8,} \\
\mathbf{13} &= \mathbf{1 \cdot 8 + 5,} \\
\mathbf{8} &= \mathbf{1 \cdot 5 + 3,} \\
\mathbf{5} &= \mathbf{1 \cdot 3 + 2,} \\
\mathbf{3} &= \mathbf{1 \cdot 2 + 1,} \\
\mathbf{2} &= \mathbf{2 \cdot 1 + 0.}
\end{aligned}$$

Thus, $\mathbf{gcd(144, 89) = 1}$. Back-substitution (working upward) yields the correct linear combination

$$\mathbf{1 = 34 \cdot 144 - 55 \cdot 89,}$$

so

$$\mathbf{gcd(144, 89) = 1 = 144(34) + 89(-55).}$$

45. Describe the extended Euclidean algorithm using pseudocode:

$$\boldsymbol{ax + by = \gcd(a, b).}$$

Pseudocode:

1. **Input:** Two integers $\boldsymbol{a, b}$.
2. **Output:** $\boldsymbol{\gcd(a, b)}$ and integers $\boldsymbol{x, y}$ such that $\boldsymbol{ax + by = \gcd(a, b)}$.
3. If $\boldsymbol{b = 0}$, then:
   (a) return $\boldsymbol{(a, 1, 0)}$.
4. Otherwise:
   (a) Recursively call the algorithm with $\boldsymbol{(b, a \bmod b)}$.
   (b) Suppose it returns $\boldsymbol{(d, x_1, y_1)}$ such that $\boldsymbol{bx_1 + (a \bmod b)y_1 = d}$.
   (c) Then set:
   $$\boldsymbol{x = y_1, \quad y = x_1 - \left\lfloor \frac{a}{b} \right\rfloor y_1.}$$
   (d) Return $\boldsymbol{(d, x, y)}$.

Example with $\boldsymbol{a = 123}$, $\boldsymbol{b = 2347}$:

1. Call EEA$\boldsymbol{(123, 2347)}$.
2. Since $\boldsymbol{b \neq 0}$, compute $\boldsymbol{123 \bmod 2347 = 123}$ and recurse on $\boldsymbol{(2347, 123)}$.
3. Call EEA$\boldsymbol{(2347, 123)}$. Compute:
   $$\boldsymbol{2347 = 123 \cdot 19 + 10, \quad 123 = 10 \cdot 12 + 3, \quad 10 = 3 \cdot 3 + 1, \quad 3 = 1 \cdot 3 + 0.}$$
4. Back-substitute and compute the coefficients. One correct identity is:
   $$\boldsymbol{123(-706) + 2347(37) = 1.}$$
5. Therefore $\boldsymbol{\gcd(123, 2347) = 1}$ and one solution is $\boldsymbol{x = -706}$, $\boldsymbol{y = 37}$.

week 2

Section 4.4 (Solving Congruences)

Questions: 5, 9, 11, 15, 21, 22, 23, 27

5. Find an inverse of $\boldsymbol{a}$ modulo $\boldsymbol{m}$ of each of these pairs:

(a) $\boldsymbol{a = 4, m = 9}$

$$\text{must find } \boldsymbol{x} \text{ such that } \boldsymbol{4x \equiv 1 \pmod{9}}.$$

Using the extended Euclidean algorithm:

$$\begin{aligned} 9 &= 2 \cdot 4 + 1, \\ 4 &= 4 \cdot 1 + 0. \end{aligned}$$

Back-substituting gives:

$$1 = 9 - 2 \cdot 4.$$

Rearranging to isolate the coefficient of 4 gives $\boldsymbol{1 = (-2) \cdot 4 + 1 \cdot 9}$, so one inverse is $\boldsymbol{x = -2 \equiv 7 \pmod{9}}$.

$$\therefore 4^{-1} \equiv 7 \pmod{9}.$$

(b) $\boldsymbol{a = 19, m = 141}$ Using the extended Euclidean algorithm (steps omitted for brevity but can be computed), one finds

$$1 = 19(52) + 141(-7),$$

so $\boldsymbol{19^{-1} \equiv 52 \pmod{141}}$.

(c) $\boldsymbol{a = 55, m = 89}$ Using the extended Euclidean algorithm one finds

$$1 = 55(34) + 89(-21),$$

therefore $\boldsymbol{55^{-1} \equiv 34 \pmod{89}}$.

(d) $\boldsymbol{a = 89, m = 232}$ Using the extended Euclidean algorithm one finds

$$1 = 89(73) + 232(-28),$$

therefore $\boldsymbol{89^{-1} \equiv 73 \pmod{232}}$.

9. Solve the congruence $\boldsymbol{4x \equiv 5 \pmod{9}}$:

From question 5(a), $\boldsymbol{4^{-1} \equiv 7 \pmod{9}}$. Multiplying both sides of the congruence by $\boldsymbol{4^{-1}}$ gives:

$$x \equiv 5 \cdot 7 \pmod{9}$$

$$x \equiv 35 \pmod{9}$$

Reducing $\boldsymbol{35}$ modulo $\boldsymbol{9}$ gives:

$$x \equiv 8 \pmod{9}$$

11. Solve each of these congruences:

(a) $\mathbf{19x \equiv 4 \pmod{141}}$
From question 5(b), $\mathbf{19^{-1} \equiv 52 \pmod{141}}$.

$$x \equiv 4 \cdot 52 \equiv 208 \equiv 67 \pmod{141}.$$

(b) $\mathbf{55x \equiv 34 \pmod{89}}$
From question 5(c), $\mathbf{55^{-1} \equiv 34 \pmod{89}}$.

$$x \equiv 34 \cdot 34 \equiv 1156 \equiv 88 \pmod{89}.$$

(c) $\mathbf{89x \equiv 2 \pmod{232}}$
From question 5(d), $\mathbf{89^{-1} \equiv 73 \pmod{232}}$.

$$x \equiv 2 \cdot 73 \equiv 146 \pmod{232}.$$

15. Show that if m is an integer greater than 1 and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{\frac{m}{\gcd(c,m)}}$:

Suppose $ac \equiv bc \pmod{m}$. Then $m \mid c(a-b)$. Let $d = \gcd(c,m)$ and write $c = dc_1$ and $m = dm_1$, so that $\gcd(c_1, m_1) = 1$. Since $m \mid c(a-b)$, we have $dm_1 \mid dc_1(a-b)$. Cancelling the common factor d gives $m_1 \mid c_1(a-b)$. Because $\gcd(c_1, m_1) = 1$, it follows that $m_1 \mid (a-b)$. Therefore $a \equiv b \pmod{m_1}$. Finally, since $m_1 = \frac{m}{d}$, we conclude that

$$a \equiv b \pmod{\tfrac{m}{\gcd(c,m)}}.$$

21.Use the construction in the proof of the Chinese Remainder Theorem to find all solutions to the system:

$$x \equiv 1 \pmod{2}, \quad x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 4 \pmod{11}.$$

Let $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, and $m_4 = 11$. Then $M = m_1m_2m_3m_4 = 330$. We compute:

$$M_1 = \frac{M}{m_1} = 165, \quad M_2 = \frac{M}{m_2} = 110, \quad M_3 = \frac{M}{m_3} = 66, \quad M_4 = \frac{M}{m_4} = 30.$$

Next, we find the inverses:

$$y_1 \text{ such that } 165y_1 \equiv 1 \pmod{2} \implies y_1 = 1,$$

$$y_2 \text{ such that } 110y_2 \equiv 1 \pmod{3} \implies y_2 = 2,$$

$$y_3 \text{ such that } 66y_3 \equiv 1 \pmod{5} \implies y_3 = 1,$$

$$\boldsymbol{y_4} \text{ such that } \mathbf{30}\boldsymbol{y_4} \equiv \mathbf{1} \pmod{\mathbf{11}} \implies \boldsymbol{y_4} = \mathbf{7}.$$

Now, we can construct the solution:

$$\boldsymbol{x \equiv a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4 \pmod{M}}.$$

Substituting the values we found:

$$\boldsymbol{x} \equiv \mathbf{1 \cdot 165 \cdot 1 + 2 \cdot 110 \cdot 2 + 3 \cdot 66 \cdot 1 + 4 \cdot 30 \cdot 7 \pmod{330}}.$$

Calculating each term:

$$\boldsymbol{x} \equiv \mathbf{165 + 440 + 198 + 840 \equiv 1643 \pmod{330}}.$$

Reducing **1643** modulo **330** gives:

$$\boldsymbol{x} \equiv \mathbf{323 \pmod{330}}.$$

Thus, the solution to the system is:

$$\boldsymbol{x} \equiv \mathbf{323 \pmod{330}}.$$

22.Solve the system of congruences $\boldsymbol{x \equiv 3 \pmod 6}$ and $\boldsymbol{x \equiv 4 \pmod 7}$ using back substitution:

From the first congruence, $\boldsymbol{x = 6k + 3}$. Substitute into the second:

$$\boldsymbol{6k + 3 \equiv 4 \pmod 7 \implies 6k \equiv 1 \pmod 7.}$$

Since $\boldsymbol{6^{-1} \equiv 6 \pmod 7}$, $\boldsymbol{k \equiv 6 \pmod 7}$. So $\boldsymbol{k = 7m + 6}$ and

$$\boldsymbol{x = 6(7m + 6) + 3 = 42m + 39.}$$

Therefore $\boldsymbol{x \equiv 39 \pmod{42}}$.

27. Find all solutions (if any) to the system:

$$\boldsymbol{x \equiv 7 \pmod 9, \quad x \equiv 4 \pmod{12}, \quad x \equiv 16 \pmod{21}.}$$

From the first congruence, $\boldsymbol{x = 9k + 7}$. Substitute into the second:

$$\boldsymbol{9k + 7 \equiv 4 \pmod{12} \implies 9k \equiv 9 \pmod{12}.}$$

Since $\boldsymbol{\gcd(9, 12) = 3}$, divide through by 3 to get $\boldsymbol{3k \equiv 3 \pmod 4}$, i.e. $\boldsymbol{k \equiv 1 \pmod 4}$. So $\boldsymbol{k = 1 + 4t}$ and

$$\boldsymbol{x = 9(1 + 4t) + 7 = 16 + 36t.}$$

Substitute into the third congruence:

$$\boldsymbol{16 + 36t \equiv 16 \pmod{21} \implies 36t \equiv 0 \pmod{21}.}$$

Since $\boldsymbol{\gcd(36, 21) = 3}$, divide by 3: $\boldsymbol{12t \equiv 0 \pmod 7}$. Because $\boldsymbol{12 \equiv 5 \pmod 7}$ and $\boldsymbol{\gcd(5, 7) = 1}$, we get $\boldsymbol{t \equiv 0 \pmod 7}$, so $\boldsymbol{t = 7s}$. Thus

$$\boldsymbol{x = 16 + 36 \cdot 7s = 16 + 252s, \quad s \in \mathbb{Z}.}$$

Therefore $\boldsymbol{x \equiv 16 \pmod{252}}$.

Week 3

Section 4.1 (Divisibility and Modular Arithmetic)

Questions: 48, 49, 50

48.Show that $\mathbb{Z}_m$ with addition modulo $\boldsymbol{m}$, where $\boldsymbol{m \geq 2}$ is an integer, satisfies closure, associativity, and commutativity; $\mathbf{0}$ is an additive identity; and for every $\boldsymbol{a} \in \mathbb{Z}_m$ the element $\boldsymbol{m - a}$ is an additive inverse of $\boldsymbol{a}$:

Closure: For any $\boldsymbol{a, b} \in \mathbb{Z}_m$, the sum $\boldsymbol{a + b}$ (taken modulo $\boldsymbol{m}$) is again an element of $\mathbb{Z}_m$. Thus $\mathbb{Z}_m$ is closed under addition modulo $\boldsymbol{m}$.

Associativity: Integer addition is associative, and reducing modulo $\boldsymbol{m}$ preserves associativity, so for any $\boldsymbol{a, b, c} \in \mathbb{Z}_m$,

$$\boldsymbol{(a + b) + c \equiv a + (b + c) \pmod{m}.}$$

Commutativity: Integer addition is commutative, hence so is addition modulo $\boldsymbol{m}$:

$$\boldsymbol{a + b \equiv b + a \pmod{m}.}$$

Additive identity: The class $\mathbf{0} \in \mathbb{Z}_m$ satisfies $\boldsymbol{a + 0 \equiv a \pmod{m}}$ for all $\boldsymbol{a} \in \mathbb{Z}_m$.

Additive inverses: For any $\boldsymbol{a} \in \mathbb{Z}_m$, the element $\boldsymbol{m - a}$ (interpreted modulo $\boldsymbol{m}$) satisfies $\boldsymbol{a + (m - a) \equiv 0 \pmod{m}}$.

Therefore $\mathbb{Z}_m$ is an abelian group under addition modulo $\boldsymbol{m}$.

49. Show that $\mathbb{Z}_m$ with multiplication modulo m, where $m \geq 2$ is an integer, satisfies closure, associativity, and commutativity, and 1 is a multiplicative identity. Is it a group?

Closure: For $a, b \in \mathbb{Z}_m$, the product $a \cdot b \pmod{m}$ lies in $\mathbb{Z}_m$.

Associativity: Integer multiplication is associative, and reduction modulo m preserves associativity.

Commutativity: Integer multiplication is commutative, so multiplication modulo m is commutative.

Multiplicative identity: $1 \in \mathbb{Z}_m$ satisfies $a \cdot 1 \equiv a \pmod{m}$ for all $a \in \mathbb{Z}_m$.

Is it a group? Not necessarily. Not every element of $\mathbb{Z}_m$ has a multiplicative inverse modulo m. For example, when $m = 4$, the element 2 has no inverse modulo 4. Thus $\mathbb{Z}_m$ under multiplication is a commutative monoid with identity 1, but it is a group only when every nonzero element is invertible — which happens exactly when m is prime. The subgroup of units

$$\mathbb{Z}_m^\times = \{[a]_m : \gcd(a, m) = 1\}$$

is an abelian group under multiplication modulo m.

50.Show that the distributive property of multiplication over addition holds for $\mathbb{Z}_{\boldsymbol{m}}$, where $\boldsymbol{m} \geq \mathbf{2}$ is an integer.

For any $\boldsymbol{a, b, c} \in \mathbb{Z}_{\boldsymbol{m}}$, integer arithmetic satisfies $\boldsymbol{a(b+c) = ab + ac}$. Reducing both sides modulo $\boldsymbol{m}$ preserves equality, so

$$\boldsymbol{a \cdot (b + c) \equiv a \cdot b + a \cdot c \pmod{m}.}$$

Thus, the distributive law holds in $\mathbb{Z}_{\boldsymbol{m}}$.