Algebra of Numbers - Introduction

Topics:

Divisibility and modular arithmetic, Integer representations, Primes and the greatest common divisor, Congruence.

- **T**he part of mathematics devoted to the study of the set of integers and their properties is known as number theory.
- In this module we will develop some of the important concepts of number theory including many of those used in computer science. As we develop number theory, we will use the proof methods developed in **Module1** to prove many theorems.
- We will first introduce the notion of divisibility of integers, which we use to introduce modular, or clock, arithmetic.
- Modular arithmetic operates with the remainders of integers when they are divided by a fixed positive integer, called the modulus.

- Integers can be represented with any positive integer b greater than 1 as a base.
- In this module we discuss base b representations of integers and give an algorithm for finding them. In particular, we will discuss binary, octal, and hexadecimal (base 2, 8, and 16) representations.
- We will discuss prime numbers, *the positive integers that have only 1 and themselves as positive divisors.*
- We will prove that there are infinitely many primes; the proof we give is considered to be one of the most beautiful proofs in mathematics.
- We will discuss the distribution of primes and many famous open questions concerning primes.
- We will introduce the concept of greatest common divisors and study the Euclidean algorithm for computing them.
- We will introduce the fundamental theorem of arithmetic, a key result which tells us that every positive integer has a unique factorization into primes.

- At the end we will explain how to solve linear congruences, as well as systems of linear congruences, which we solve using the famous *Chinese remainder theorem.*
- We will also introduce the notion of pseudoprimes, which are composite integers masquerading as primes, and show how this notion can help us rapidly generate prime numbers.

Divisibility and Modular Arithmetic

- When an integer is divided by a second nonzero integer, the quotient may or may not be an integer.
- For example, $\frac{12}{3} = 4$ is an integer, whereas $\frac{11}{4} = 2.75$ is not.
- This leads to the following Definition.

DEFINITION: If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer.

When a divides b we say that a is a *factor* or *divisor* of b, and that b is a *multiple* of a.

The notation $a \mid b$ denotes that a divides b.

We write $a \nmid b$ when a does not divide b.

Remark: We can express $a \mid b$ using quantifiers as $\exists c\,(ac = b)$, where the universe of discourse is the set of integers

EXAMPLE: Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Solution: We see that $3 \nmid 7$, because $\frac{7}{3}$ is not an integer.

On the other hand, $3 \mid 12$ because $\frac{12}{3} = 4$.

EXAMPLE: Let n and d be positive integers. How many positive integers not exceeding n are divisible by d?

Solution: The positive integers divisible by d are all the integers of the form dk, where k is a positive integer.

Hence, the number of positive integers divisible by d that do not exceed n equals the number of integers k with $0 < dk \leq n$, or with $0 < k \leq n/d$. Therefore, there are $\lfloor n/d \rfloor$ positive integers not exceeding n that are divisible by d.

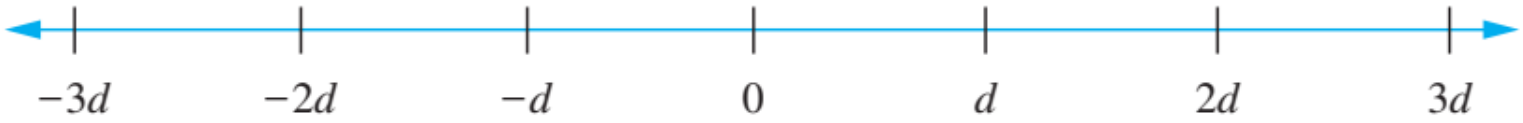

FIGURE 1 **Integers Divisible by the Positive Integer *d*.**

THEOREM 1

Theorem Let a, b, and c be integers, where $a \neq 0$. Then
(*i*) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
(*ii*) if $a \mid b$, then $a \mid bc$ for all integers c;
(*iii*) if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof:

We will give a direct proof of (*i*).

Suppose that $a \mid b$ and $a \mid c$. Then, from the definition of divisibility, it follows that there are integers s and t with $b = as$ and $c = at$.

Hence, $b + c = as + at = a(s + t)$.

Therefore, a divides $b + c$.

This establishes part (*i*) of the theorem.

The proofs of parts (*ii*) and (*iii*) are left as Exercises.
We now have a useful consequence followed by Theorem 1.

COROLLARY 1 If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ whenever m and n are integers.

Proof:

We will give a direct proof.

By part (ii) of Theorem 1 we see that $a \mid mb$ and $a \mid nc$ whenever m and n are integers.

By part (i) of Theorem 1 it follows that $a \mid (mb + nc)$.

The Division Algorithm

THEOREM 2 THE DIVISION ALGORITHM

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = d\,q + r$.

Proof:

Let S be the set of nonnegative integers of the form $a - dq$, where q is an integer that is $S = \{z \in N \mid z = a - dq\}$

This set is nonempty (one can prove it – small exercise) because $-dq$ can be made as large as desired (taking q to be a negative integer with large absolute value). By the well-ordering property, S has a least element

$r = a - dq_0$ for some q . (Cont….)

Note: The **well-ordering principle** states that every non-empty set of positive integers contains a least element

The integer r is nonnegative. It is also the case that $r < d$.

If it were not, then there would be a smaller nonnegative element in S, namely, $a - d(q_0 + 1)$.

To see this, suppose that $r \geq d$.
Because $a = d\,q_0 + r$,

it follows that $a - d(q_0 + 1) = (a - d\,q_0) - d = r - d \geq 0$.

Consequently, there are integers q and r with $0 \leq r < d$.

The proof that q and r are unique is left as Exercise (37).

Remark: Theorem 2 is not really an algorithm. (Why not?)
Nevertheless, we use its traditional name.

DEFINITION
In the equality given in the division algorithm, d is called the *divisor*, a is called the *dividend*, q is called the *quotient*, and r is called the *remainder*.

This notation is used to express the quotient and remainder:
$q = a \textbf{ div } d, \qquad r = a \textbf{ mod } d.$

Remark: Note that both $a \textbf{ div } d$ and $a \textbf{ mod } d$ for a fixed d are functions on the set of integers. Furthermore, when a is an integer and d is a positive integer, we have $a \textbf{ div } d = a/d$ and $a \textbf{ mod } d = a - d$.

Example: What are the quotient and remainder when 101 is divided by 11 ?

Solution: $101 = 11 * 9 + 2$.

Hence, the quotient when 101 is divided by 11 is $9 = 101 \textbf{ div } 11$, and the remainder is $2 = 101 \textbf{ mod } 11$.

- **Example:** What are the quotient and remainder when -11 is divided by 3 ?
  Solution: We have $-11 = 3(-4) + 1$.
  Hence, the quotient when -11 is divided by 3 is $-4 = -11$ **div** 3, and the remainder is $1 = -11$ **mod** 3.
  Note that the remainder cannot be negative.
- Consequently, the remainder is *not* -2, even though $-11 = 3(-3) - 2$, because $r = -2$ does not satisfy $0 \leq r < 3$.
- Note that the integer a is divisible by the integer d if and only if the remainder is zero when a is divided by d.

- **Remark:**

A programming language may have one, or possibly two, operators for modular arithmetic, denoted by mod (in BASIC, Maple, Mathematica, EXCEL, and SQL), % (in C, C++, Java, and Python), rem (in Ada and Lisp), or something else.

Be careful when using them, because for $a < 0$, some of these operators return $a - m\lceil a/m \rceil$ instead of $a \bmod m = a - m\lfloor a/m \rfloor$ (as shown in Exercise 18).

Also, unlike $a \bmod m$, some of these operators are defined when $m < 0$, and even when $m = 0$.

Modular Arithmetic

- We have already introduced the notation a **mod** m to represent the remainder when an integer a is divided by the positive integer m.
- We now introduce a different (but related) notation that indicates that two integers have the same remainder when they are divided by the positive integer m.
- *Definition:*

If a and b are integers and m is a positive integer, then a is *congruent to b modulo m* if m divides $a - b$.

We use the notation $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m.

- We say that $a \equiv b \pmod{m}$ is a **congruence** and that m is its **modulus** (plural **moduli**).
- If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

- **THEOREM 3**

Let a and b be integers, and let m be a positive integer.

Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$

Example: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6

Solution: Because 6 divides $17 - 5 = 12$, we see that $17 \equiv 5 \pmod{6}$. However, $24 - 14 = 10$ is not divisible by 6, hence, $24 \not\equiv 14 \pmod{6}$.

Note: The great German mathematician Karl Friedrich Gauss developed the concept of congruences at the end of the eighteenth century. The notion of congruences has played an important role in the development of number theory.

- Theorem 4 : Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof: If $a \equiv b \pmod{m}$, by the definition of congruence, we know that $m \mid (a - b)$.

That is, there is an integer k such that $a - b = km$, so that $a = b + km$.

Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, m divides $a - b$, so that $a \equiv b \pmod{m}$.

Note: The set of all integers congruent to an integer a modulo m is called the **congruence class** of a modulo m.

- **Theorem 5:**

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Proof: We use a direct proof.

Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by Theorem 4 there are integers s and t with $b = a + sm$ and $d = c + tm$.

Hence, $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$.

Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

- **Example:**

If $7 \equiv 2 \pmod 5$ and $11 \equiv 1 \pmod 5$,

By Theorem 5 it follows that
$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod 5$ and that
$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod 5$.

• **COROLLARY 2:**

Let m be a positive integer and let a and b be integers.

Then $(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$ and

$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

Proof: By the definitions of **mod** m and of congruence modulo m, we know that $a \equiv (a \bmod m) \pmod m$ and $b \equiv (b \bmod m) \pmod m$.

Hence, Theorem 5 tells us that

$a + b \equiv ((a \bmod m) + (b \bmod m)) \pmod m$

and

$ab \equiv ((a \bmod m)(b \bmod m)) \pmod m$.

Arithmetic Modulo m

- We define arithmetic operations on $\boldsymbol{Z}_m$, the set of nonnegative integers less than m, that is, the set

$\{0, 1, \ldots, m - 1\}$

- We define addition of these integers, denoted by $+_m$ by
  $a +_m b = (a + b) \textbf{ mod } m$,
  where the addition on the right-hand side of this equation is the ordinary addition of integers.
- We define multiplication of these integers, denoted by $\cdot_m$ by
  $a \cdot_m b = (a \cdot b) \textbf{ mod } m$,
  where the multiplication on the right-hand side of this equation is the ordinary multiplication of integers.
- The operations $+_m$ and $\cdot_m$ are called addition and multiplication modulo m and when we use these operations, we are said to be doing **arithmetic modulo** m.

- **Example:** Use the definition of addition and multiplication in $\boldsymbol{Z}_m$ to find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution:

Using the definition of addition modulo 11, we find that
$7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5,$

and

$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8.$

Hence $7 +_{11} 9 = 5$ and $7 \cdot_{11} 9 = 8$.

- The operations $+_m$ and $\cdot_m$ satisfy many of the same properties of ordinary addition and multiplication of integers. In particular, they satisfy these properties:

Closure If a and b belong to $\boldsymbol{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\boldsymbol{Z}_m$.

Associativity If a, b, and c belong to $\boldsymbol{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot m (b \cdot_m c)$.

Commutativity If a and b belong to $\boldsymbol{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.

Identity elements The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively. That is, if a belongs to $\boldsymbol{Z}_m$, then $a +_m 0 = 0 +_m a = a$ and $a \cdot_m 1 = 1 \cdot_m a = a$.

Additive inverses If $a = 0$ belongs to $\boldsymbol{Z}_m$, then $m - a$ is an additive inverse of a modulo m and 0 is its own additive inverse. That is $a +_m (m - a) = 0$ and $0 +_m 0 = 0$.

Distributivity If a, b, and c belong to $\boldsymbol{Z}_m$, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

- **Remark:** $\boldsymbol{Z}_m$ with the operations of addition modulo m $(+_m)$ and multiplication modulo m $(\cdot_m)$ satisfies the properties listed above. If $\boldsymbol{Z}_m$ satisfies properties with modular addition is said to be a **commutative group.**
- If $\boldsymbol{Z}_m$ satisfies the properties listed above with both of these operations($+_m$ and $\cdot_m$) is said to be a **commutative ring**.