MC4010 - Discrete Mathematics

Number Theory and Cryptography

Dr T. Mayooran

Department of Inter Disciplinary Studies, Faculty of Engineering, University of Jaffna

2023-12-13

"Mathematics is the queen of sciences and the theory of numbers is the queen of mathematics." (Karl Friedrich Gauss)

All contents of these slides are agglomerated from recommended reference textbook of this course.

Slides are prepared through RMarkdown Beamer presentation option and executed via RStudio.

Introduction

- The part of mathematics devoted to the study of the set of integers and their properties is known as number theory. In this section we will develop some of the important concepts of number theory including many of those used in computer science.
- Number theory plays an essentially role both in classical cryptography, first used thousands of years ago, and modern cryptography, which plays an essential role in electronic communication.

Outline

1. Divisibility and Modular Arithmetic
2. Primes and Greatest Common Divisors
3. Solving Congruences
4. Cryptography

Based on the current syllabus of MC4010 course, "Cryptography" will not be covered for the exams for this semester.

Divisibility

Divisibility When dividing an integer by a second non zero integer, the quotient may or may not be an integer. For example, $12/3 = 4$ while $9/4 = 2.25$. The issue of divisibility is addressed in the following definition.

Definition If a and b are integers with $a \neq 0$, then a divides b if there exists an integer c such that $b = ac$.

- When a divides b we write $a|b$.
- We say that a is a factor or divisor of b and b is a multiple of a.
- If $a|b$ then b/a is an integer (namely the c above).
- If a does not divide b, we write a $a \nmid b$.

Back to the above examples, we see that 3 divides 12, denoted as $3|12$, and 4 does not divide 9, denoted as $4 \nmid 9$.

Theorem 1

Let a, b, c be integers, where $a \neq 0$.

1. If $a|b$ and $a|c$, then $a|(b + c)$.
2. If $a|b$, then $a|bc$ for all integers c.
3. If $a|b$ and $b|c$, then $a|c$.

Proof:

Work out!

Practice problem:

If a, b, and c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|mb+nc$ whenever m and n are integers.

Division Algorithm

When an integer is divided by a positive integer, there is a quotient and a remainder. This is traditionally called the "Division Algorithm", but it is really a theorem.

Theorem 2

If a is an integer and d a positive integer, then there are unique integers q and r , with $0 \leq r < d$, such that $a = dq + r$

- a is called the dividend.
- d is called the divisor.
- q is called the quotient. $q = a$ div d
- r is called the remainder. $r = a \mod d$

Example

1. What are the quotient and remainder when 101 is divided by 11?

Solution:

We have

$$101 = 11.9 + 2.$$

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

2. 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 $1 = -11 \mod 3$.

Using successive subtractions to find q and r:

$a = 101$ and $d = 11$

101	
- 11	46
90	- 11
- 11	35
79	- 11
- 11	24
68	- 11
- 11	13
57	- 11
- 11	2
46	

$q = 9$ as we subtracted 11, 9 times $r = 2$ since this was the last value before getting negative.

Modular Arithmetic

- In some situations we care only about the remainder of an integer when it is divided by some specified positive integer.
- For instance, when we ask what time it will be (on a 24-hour clock) 50 hours from now, we care only about the remainder when 50 plus the current hour is divided by 24. Because we are often interested only in remainders, we have special notations for them.
- We have already introduced the notation $a \mod m$ to represent the remainder when an integer a is 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 $a \not\equiv b \pmod{m}$.

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 $17 \equiv 5 (mod 6)$. However, because $24 - 14 = 10$ is not divisible by 6, we see that $24 \not\equiv 14 \pmod{6}$.

Theorems

The following theorem says that two numbers being congruent modulo m is equivalent to their having the same remainders when dividing by 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 $a \mod m = b \mod m$.

Example: 10 and 26 are congruent modulo 8, since their difference is 16 or 16, which is divisible by 8.

When dividing 10 and 26 by 8 we get

$$10 = 1 \times 8 + 2$$

and $26 = 4 \times 8 + 2$.

So $10 \mod 8 = 2 = 16 \mod 8$.

Theorems and Corollary

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 $a = b + km$

Theorem 5

Let m be a positive integer. If $a \equiv b(\mod m)$ and $c \equiv d(\mod m)$, then $a + c \equiv b + d(\mod m)$ and $ac \equiv bd(\mod m)$.

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

$$(a + b) \mod m = ((a \mod m) + (b \mod m)) \mod m$$

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

Proofs??

Proof for Corollary:

By the definition of mod m and the definition of congruence modulo m, we know that $a \equiv (a \mod m)(\mod m)$, and $b \equiv (b \mod m)(\mod m)$. Applying Theorem 5, we get

$$(a+b) \mod m = ((a \mod m) + (b \mod m)) \mod m$$

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

Using Theorem 3, from the above congruences we get the equalities in the statement of the theorem.

Congruence Relation summary

If a and b are integers and m is a positive integer, then a is congruent to b modulo m iff $m|(a-b)$.

- The notation $a \equiv b(\mod m)$ says that a is congruent to b modulo m.
- We say that $a \equiv b(\mod m)$ is a congruence and that m is its modulus.
- Two integers are congruent $\mod m$ if and only if they have the same remainder when divided by m.
- If a is not congruent to b modulo m, we write $a \not\equiv b(\mod m)$.

Number Theory: Applications

Results from Number Theory have countless applications in mathematics as well as in practical applications including security, memory management, authentication, coding theory, etc. We will only examine (in breadth) a few here..

- Hash Functions
- Pseudorandom Numbers
- Fast Arithmetic Operations
- Linear congruences, C.R.T., Cryptography

Hashing Functions

A hashing table is a data structure that allows for direct access to data. If done carefully, and under certain assumptions, we can search for a record with a set of n records in expected time $O(1)$.

Each record is uniquely identified by a key (e.g. of keys are student number for a student record, account number for bank account records, call number for book records in a library, etc).

One of the most common hash functions uses modular arithmetic: $h(k) = k \mod m$; where m is the number of memory addresses.

Advantages: easy to compute, function is onto (all memory address can be used). Since two different integers k_1 and k_2 may be mapped to the same location if $k_1 \equiv k_2 (\mod m)$, collisions may arises. Methods for finding an alternate location for a key are employed (collision resolution techniques).

Hashing Functions

Some notation: $\mathbb{Z}_m = \{0, 1, 2, \cdots, m-2, m-1\}$. Define a hash function $h : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ as

$$h(k) = k \mod m$$

That is, h maps all integers into a subset of size m by computing the remainder of k/m.

In general, a hash function should have the following properties It must be easily computable.

It should distribute items as evenly as possible among all values addresses. To this end, m is usually chosen to be a prime number.

It is also common practice to define a hash function that is dependent on each bit of a key

It must be an onto function (surjective). Hashing is so useful that many languages have support for hashing (perl, Lisp, Python).

However, the function is clearly not one-to-one. When two elements, $x_1 \neq x_2$ hash to the same value, we call it a collision. There are many methods to resolve collisions, here are just a few.

- Open Hashing (aka separate chaining) – each hash address is the head of a linked list. When collisions occur, the new key is appended to the end of the list.
- Closed Hashing (aka open addressing) – when collisions occur, we attempt to hash the item into an adjacent hash address. This is known as linear probing.

Pseudorandom Numbers

Many applications, such as randomized algorithms, require that we have access to a random source of information (random numbers).

However, there is not truly random source in existence, only weak random sources: sources that appear random, but for which we do not know the probability distribution of events.

Pseudorandom numbers are numbers that are generated from weak random sources such that their distribution is “random enough”.

We need random numbers in several types of algorithms, such as:

- randomized algorithms: algorithms that need to flip a coin to behave unbiasedly),
- simulation algorithms: where probability models are used to explain behaviour (example: arrival rate of subway passengers).

A systematic method of generating a number cannot be truly random, so we call them pseudorandom number generators. The most common method for such generators is the linear congruential method.

Pseudorandom Numbers- linear congruential method

One method for generating pseudorandom numbers is the linear congruential method.

Choose four integers:

- m, the modulus,
- a, the multiplier,
- c the increment and
- x_0 the seed.

Such that the following hold:

- $2 \leq a < m$
- $0 \leq c < m$
- $0 \leq x_o < m$

Our goal will be to generate a sequence of pseudorandom numbers,

$$\{x_n\}_{n=1}^{\infty}$$

with $0 \leq x_n \leq m$ by using the congruence

$$x_{n+1} = (ax_n + c) \mod m$$

For certain choices of m, a, c, x_0, the sequence $\{x_n\}$ becomes periodic. That is, after a certain point, the sequence begins to repeat. Low periods lead to poor generators.

Furthermore, some choices are better than others; a generator that creates a sequence $0, 5, 0, 5, 0, 5, \cdots$ is obvious bad - its not uniformly distributed.

For these reasons, very large numbers are used in practice.

Example

Let $m = 17, a = 5, c = 2, x_0 = 3$. Then, find the sequence (write down at least the first five elements in the sequence) by using the linear congruential method.

Slide will be updated soon!

Don't hesitate to contact us if you have any questions about this course's teaching contents.

Also don't forget to check out the course page and Microsoft Team folder,

- course page https://mayooran1987.github.io/MC4010_E21/
- Microsoft Team folder