

## 14.1 Divisibility & Modular Arithmetic

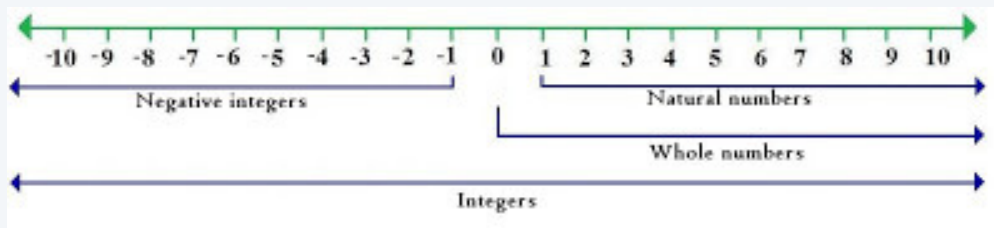
[@2021 A.D. Gunawardena](#)

## 14.1 Divisibility & Modular Arithmetic

- introduction
- divisibility
- congruences
- Equivalence relations

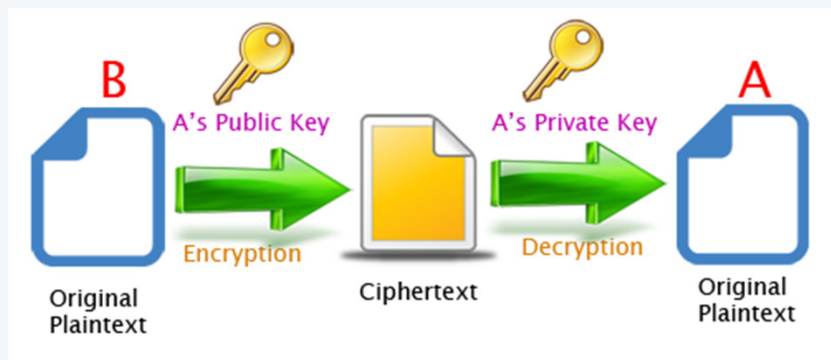
## Number theory

**Number theory** - is the mathematics devoted to the study of the set of integers and their properties



[This Photo](#) by Unknown Author is licensed under [CC BY-ND](#)

Number theory plays a crucial part in a very important branch of computer security called cryptography.



[This Photo](#) by Unknown Author is licensed under [CC BY](#)

DO NOT DISTRIBUTE

## Public-private key encryption

Public-private key encryption allows most of our online transactions to be secure. This concept is based on number theory and difficulty of factoring large numbers.

### RSA Encryptor/Decryptor/Key Generator/Cracker

Directions are at the bottom.

Public  
Modulus  
(hexadecimal): e75d78949dd6e6b180d23626817ddf32a9717287ac06cebf92f77903e20d7880989c6aded37d8519037b54c0bde7e67422e730afc73a881861333a543d0f90706eb8c9e58cade8586c3618f89c538b0ecf8ae81ae21e5ba4e35f3f78c334e57b8d564f042ad2bb8383c8e6604f3b5edab48fc0914ac888c023c7e5f488d4953

This Photo by Unknown Author is licensed under CC BY-SA

Public  
Exponent  
(hexadecimal):

10001

Private  
Exponent  
(hexadecimal): 923fe89ff1224e13783de912f019f403df4e223a96c87ada68795c9ad2c2f7203ad7ed4a4fa0ab71eb7afb7445b07030af8a1318a7ba28932f8065ce1b0f36ca414ea7fecfc4ee2589ff001579cb16357b5b26f3c83ee108982ef9672d28d1a119a46c3e91a893c8ced68aa54c58528e22da79f08af1f318babe923297d61499



## 14.1 Mathematics of Finite Sets ...

- introduction
- divisibility
- congruences
- Equivalence relations

## Divisibility of integers

---

If  $a$  and  $b$  are integers with  $a \neq 0$ ,  
define “ $a$  divides  $b$ ” as there exists an integer  $c$ , such that  $b = a c$

**Notation.** We write  $a \mid b$  when “ $a$  divides  $b$ ”

Examples.  $3 \mid 12$

### Lemmas.

If  $a \mid b$  and  $a \mid c$ , then  $a \mid (b + c)$

If  $a \mid b$ , then  $a \mid b c$  for all integers  $c$

If  $a \mid b$  and  $b \mid c$  then  $a \mid c$

## Division of linear combinations

---

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

Proof.

## The division algorithm

---

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

### Examples.

Given  $a = 21$ ,  $d = 5$ , find  $q$  and  $r$

Given  $a = -21$ ,  $d = 5$ , find  $q$  and  $r$



## Relative Primality

---

Integers that have no prime factor in common are called relatively prime.

If  $a$  and  $b$  have no common factors, then  $\gcd(a, b) = 1$

### **Greatest Common Divisor.**

The greatest common divisor of two integers  $a$  and  $b$  is the largest integer that divides both  $a$  and  $b$

The set  $Z_m$

---

Let  $m$  be a positive integer

Let  $Z_m$  be the set of all non-negative integers less than  $m$

That is,  $Z_m = \{0, 1, 2, \dots, m-1\}$

Example.  $Z_5 = \{0, 1, 2, 3, 4\}$

## Modular Arithmetic

---

Let  $a \equiv b \pmod{m}$

**Additive identity.** For any  $a$ , there exists a  $b$  such that  $a + b \equiv 0 \pmod{m}$

In this case, the  $b$  is called the additive identity of  $a$  and vice versa

**Multiplicative identity.**

For any  $a$ , there exists a  $b$  such that  $a \cdot b \equiv 1 \pmod{m}$

## Lemma

---

Let  $n$  be a positive integer. If  $k$  is relatively prime to  $n$ , then there exists an integer  $k^{-1}$  such that:

$$k \cdot k^{-1} = 1 \pmod{n}$$



## 14.1 Mathematics of Finite Sets ...

- divisibility
- congruences
- Equivalence relations

## Mathematics of Finite Sets

---

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.**  $5 \sim 3 \pmod{2}$

**Congruent Class.** The congruent class of an integer  $a$ , denoted  $[a]$  is defined as

$$[a] = \{ b \in \mathbb{Z} \mid a \text{ is congruent to } b \}$$

## Workshop

---

Find the congruent classes of the following ( $m = 5$ )

$$[1] =$$

$$[4] =$$



## 14.1 Mathematics of Finite Sets ...

- divisibility
- congruences
- Equivalence relations



# Reachability

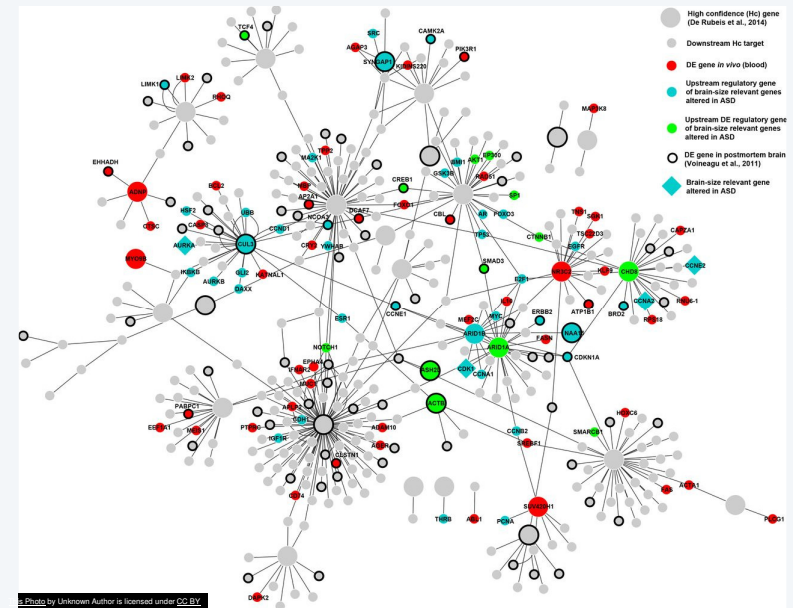
## Reachability

Is there a connection between any two given nodes?

## Possible relation.

A node x is related to node y  
if x can be reached by y  
and vice versa

**Connectivity.** Let R be a relation on a set A, the connectivity relation  $R^*$  consists of pairs (a,b) such that there is a path of length at least 1 from a to b in R



## An equivalence relation

---

A relation  $R$  on a set  $A$  is called an ***equivalence relation*** if it is reflexive, symmetric, and transitive

**Reflexive.**  $a R a$

**Symmetric.**  $a R b$  implies  $b R a$

**Transitive.**  $a R b$  and  $b R c$  implies  $a R c$

Example.

Let  $R = \{(a, b) \mid \text{there exists a path from } a \text{ to } b\}$

Show that  $R$  is an equivalence relation

## Equivalence Classes

---

An equivalence class of  $a$ , denoted by  $[a] = \{b \mid a = b \bmod M\}$

What is the equivalence class of 12, given  $m = 5$ ?

**Exercise.** Find  $12^8 \bmod 5$  using equivalence classes

Hint. 12 is in  $[2]$

## Proofs involving equivalence relations

---

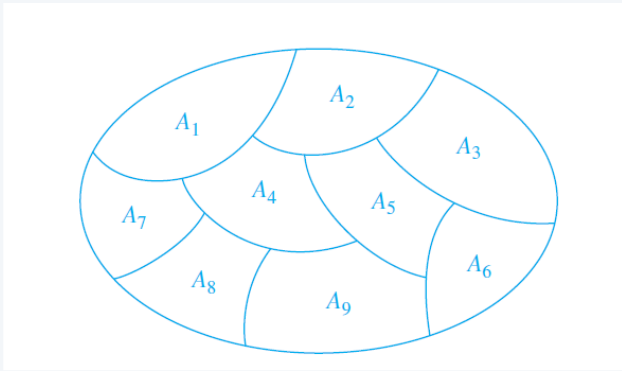
Let  $R$  be an equivalence relation on  $S$ . Let  $x, y$  in  $S$ . Then  $x$  in  $[y]$  implies  $[x] = [y]$

Proof.

## Partitioning a set

---

A set can be partitioned into its equivalence classes with respect to an equivalent relation  $R$



**Example.** Set of integers  $\mathbb{Z}$ , can be partitioned into 5 equivalent classes subject to relation  $a \equiv b \pmod{5}$

# INTRODUCTION TO DISCRETE STRUCTURES

## 14.1 Mathematics of Finite Sets ...

- divisibility
- congruences
- Equivalence relations

# INTRODUCTION TO DISCRETE STRUCTURES



## 14.1 Mathematics of Finite Sets

1.1-1.2

[@2021 A.D. Gunawardena](#)

DO NOT DISTRIBUTE