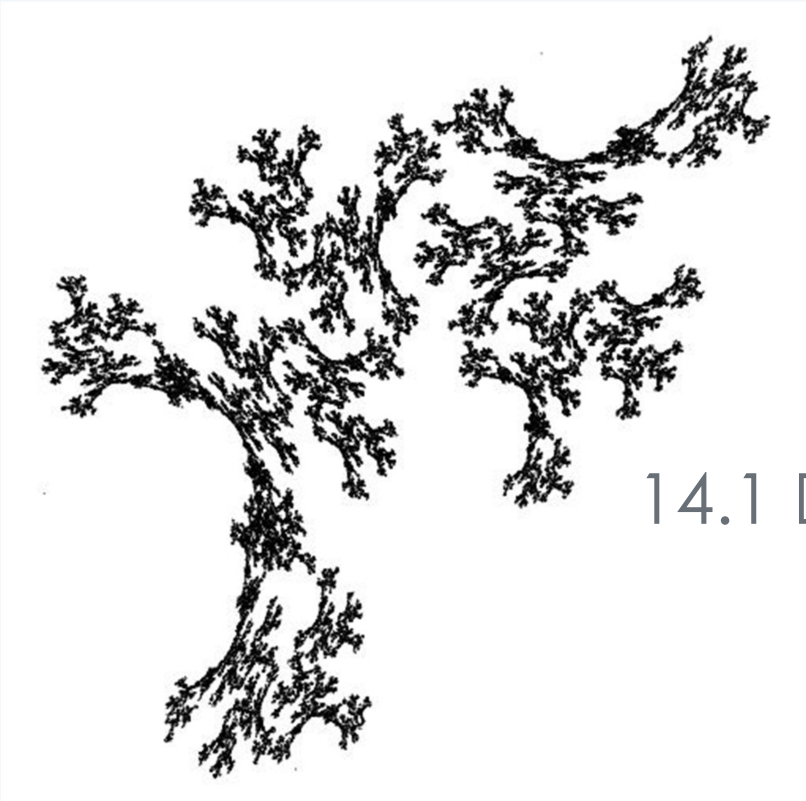
INTRODUCTION TO
DISCRETE STRUCTURES

14.1 Divisibility & Modular Arithmetic

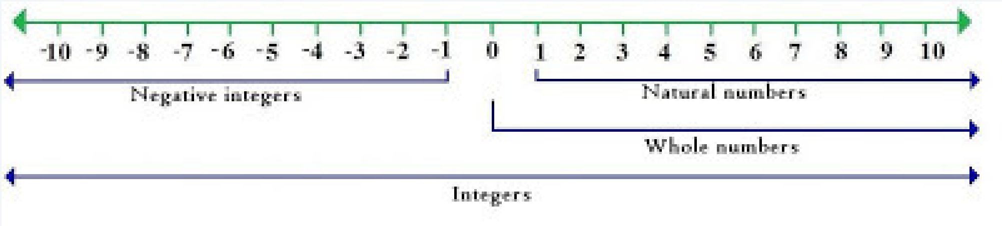


14.1 Divisibility & Modular Arithmetic

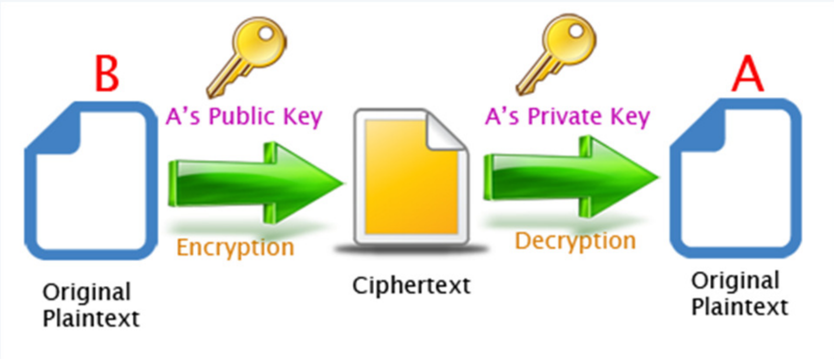
- introduction
- divisibility
- congruences
- Equivalence relations

Number theory

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



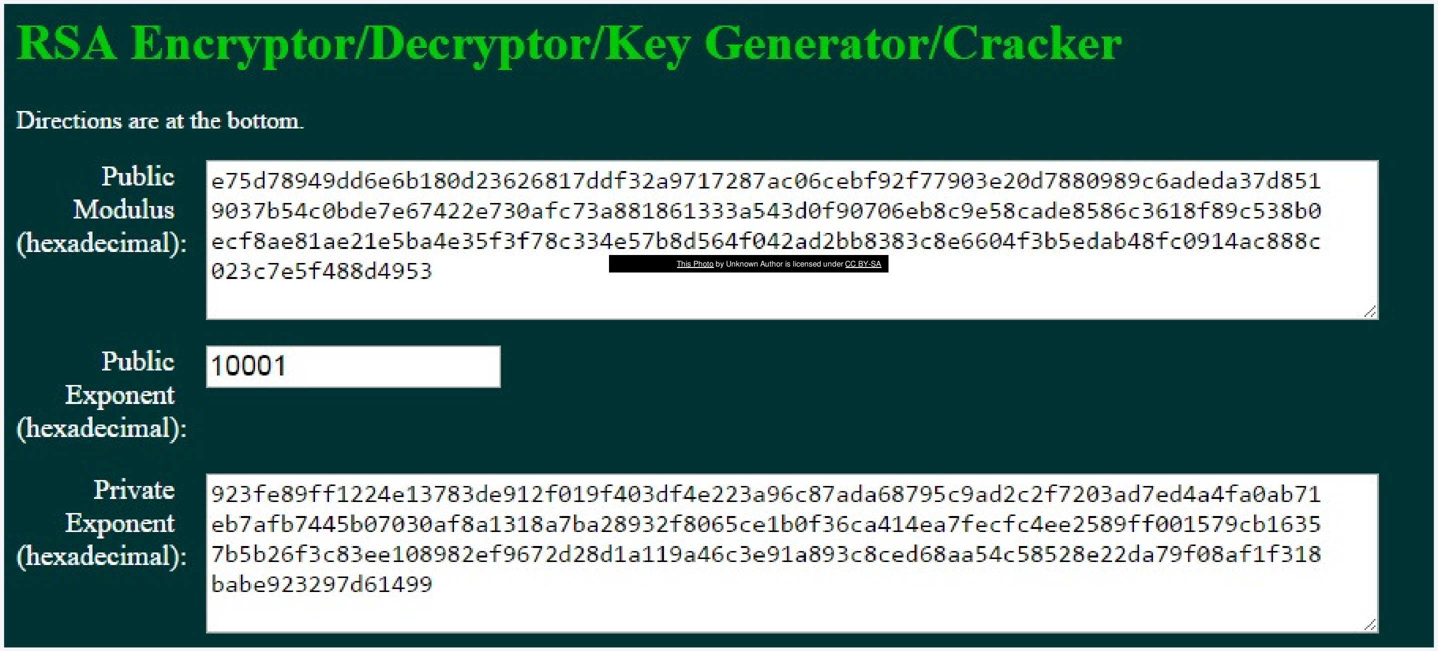
Number theory plays a crucial part in a very important branch of computer security called cryptography.

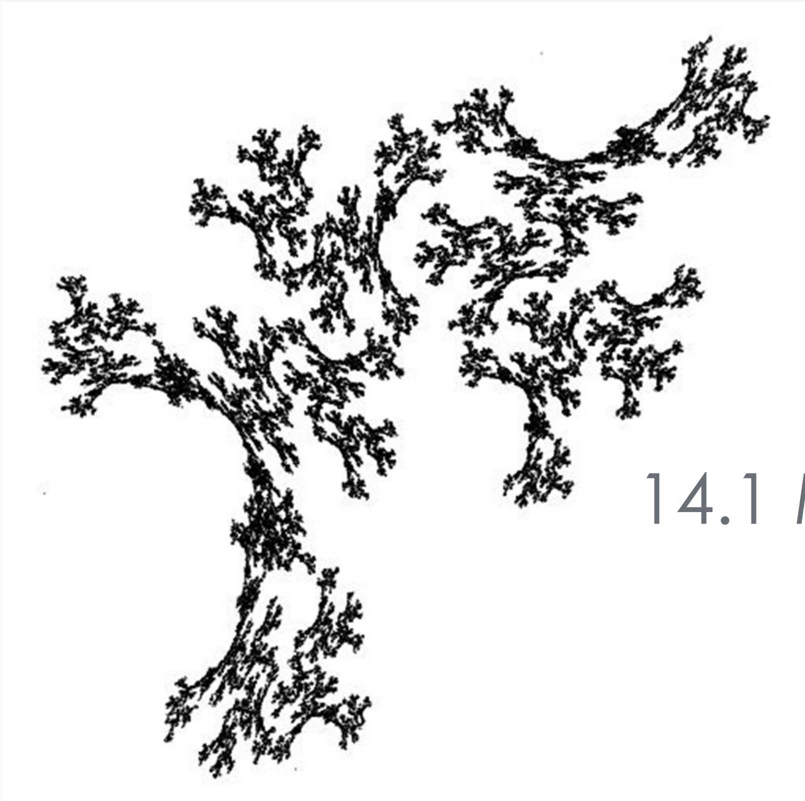


Public-private key encryption

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.





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

$0 \le r < d$ 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, $Z_m = \{0,1, 2, \ldots, m-1\}$

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

Modular Arithmetic

Let a = b mod (m)

Additive identity. For any a, there exists a b such that a + b = 0 (mod m)

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

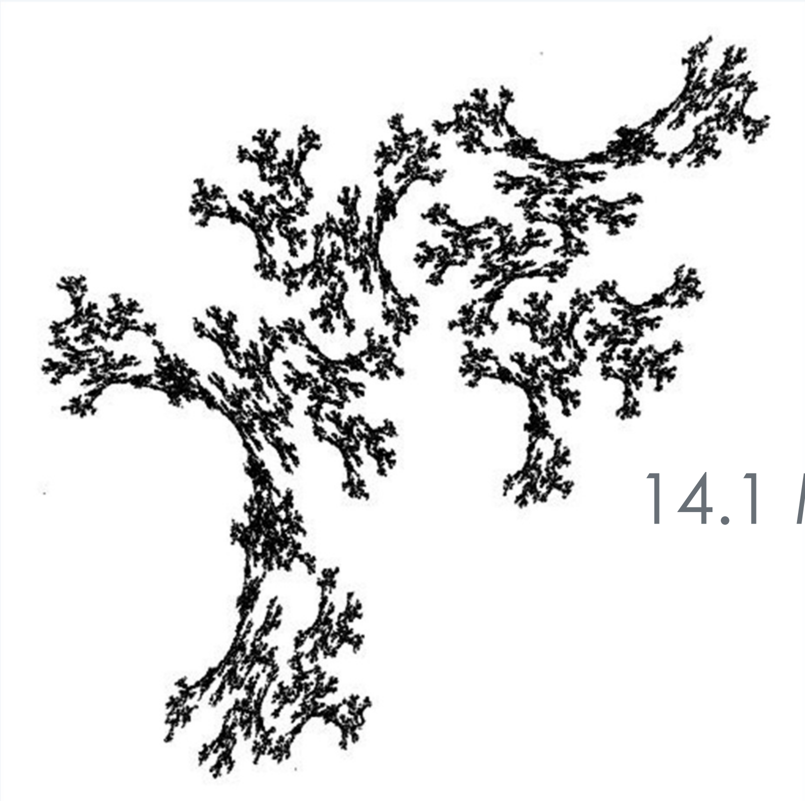
Multiplicative identity.

For any a, there exists a b such that a. b = 1 (mod m)

Lemma

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

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



14.1 Mathematics of Finite Sets …

- divisibility
- congruences
- Equivalence relations

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 ~ 3 (mod 2)

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

[a] = { b in Z | a is congruent to b}

Workshop

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

$[1] =$

$[4] =$

INTRODUCTION TO
DISCRETE STRUCTURES

14.1 Mathematics of Finite Sets …

- divisibility
- congruences
- Equivalence relations

Reachability

Reachability

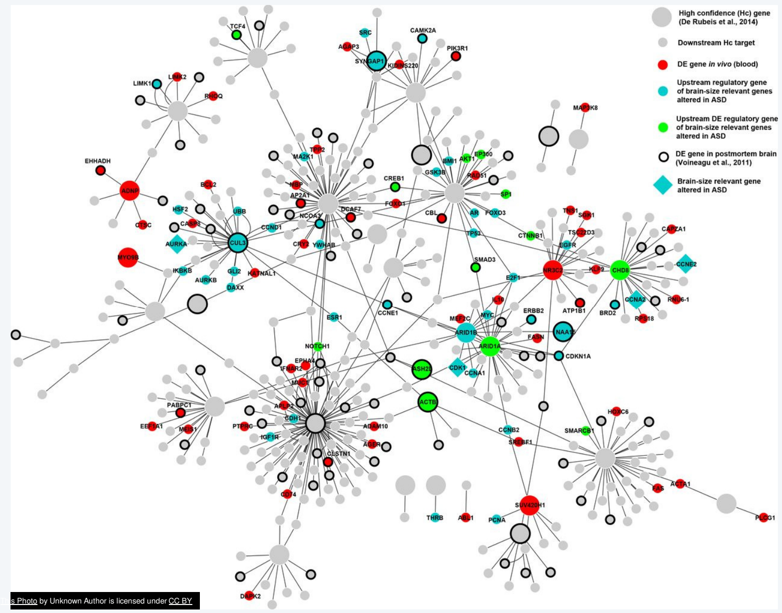
Is there a connection between any two given nodes?

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) | there exists a path from a to b }

Show that R is an equivalence relation

Equivalence Classes

An equivalence class of a, denoted by [a] = {b | a = b mod M}

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

Exercise. Find 12^8 mod 5 using equivalence classes

Hint. 12 is in [2]

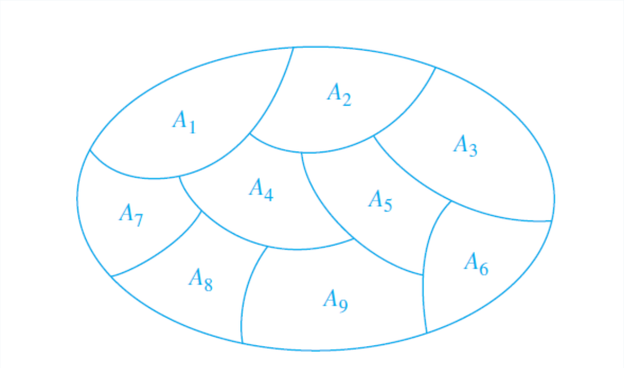
Proofs involving equivalence relations

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



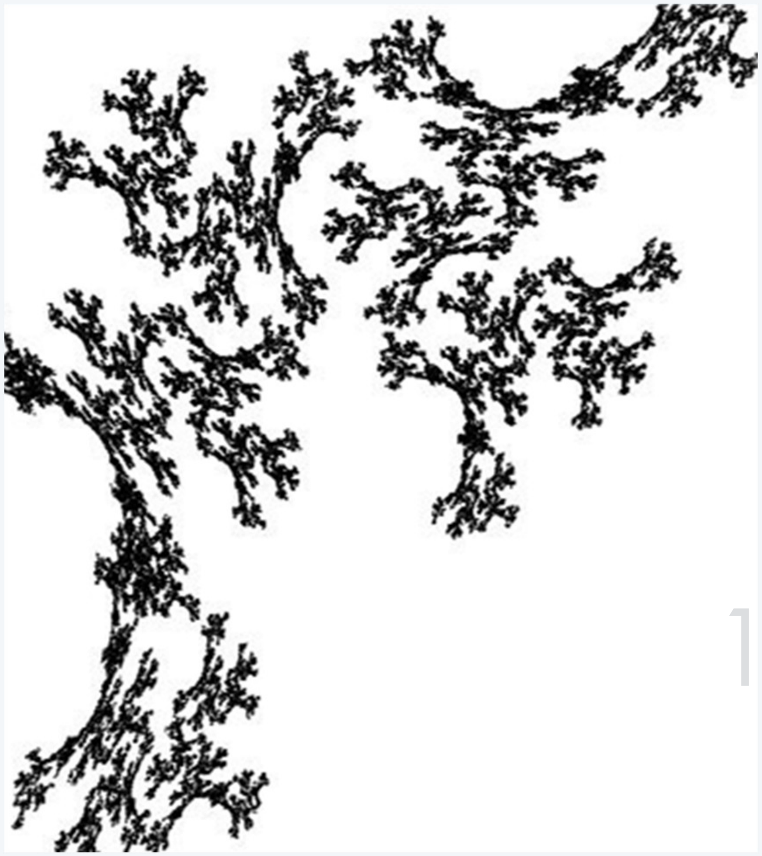
Example. Set of integers Z, can be partitioned into 5 equivalent classes subject to relation a = b mod 5

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