Discrete mathematics

NUMBER THEORY

ATHASIT SURARERKS

Mathematics is the Queen of the sciences,
and number theory is the Queen of mathematics.
C.F.GAUSS (1777-1855)

NUMBER THEORY

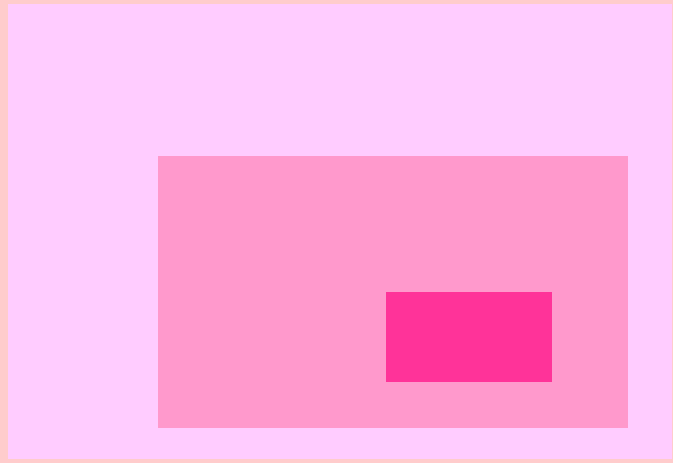
Contents

- Introduction
- Theory of Divisibility
- Diophantine Equations
- Theory of Congruence
- Prime number
- Computer Systems Design
- Cryptography & Information Security

BACKGROUND KNOWLEDGE

- Floor function
- Ceiling function
- Modularity
- Divisibility

Floor and ceiling functions



Floor & ceiling functions Definitions 1 & 2

- **Floor function** $\lfloor x \rfloor$

  the **greatest integer** that is less than or equal to x.

- **Ceiling function** $\lceil x \rceil$

  the **smallest integer** that is greater than or equal to x.

Floor & ceiling functions

Floor function

- $\lfloor x \rfloor$ is the **greatest integer** that is less than or equal to x.
- $\lfloor x \rfloor = n$ where n is an integer satisfying

$$x - 1 < n \leq x$$

Are two statements equivalent ?

Floor & ceiling functions

Ceiling function

- $\lceil x \rceil$ is the **smallest integer** that is greater than or equal to x.
- $\lceil x \rceil = n$ where n is an integer satisfying

$$x \le n < x + 1$$

Are two statements equivalent ?

F : continuous f^n

: mono increasing f^n

$x \in \mathbb{Z} \rightarrow F(x) \in \mathbb{Z}$

Show $\lfloor F(x) \rfloor = \lfloor F(\lfloor x \rfloor) \rfloor$ *

Proof : 1) $\lfloor x \rfloor \leq x$ by def^n

$F(\lfloor x \rfloor) \leq F(x)$ F : mono inc.

$\lfloor F(\lfloor x \rfloor) \rfloor \leq \lfloor F(x) \rfloor$

2) $y \leq \lfloor x \rfloor$

$\lfloor F(x) \rfloor = F(y) \leq F(\lfloor x \rfloor)$

$\lfloor \lfloor F(x) \rfloor \rfloor \leq \lfloor F(\lfloor x \rfloor) \rfloor$

$\lfloor F(x) \rfloor \leq \lfloor F(\lfloor x \rfloor) \rfloor$

Ex.

$F(x) = \sqrt{x}$

$\lfloor \sqrt{x} \rfloor = \lfloor \sqrt{\lfloor x \rfloor} \rfloor$

Note

$\lfloor x \rfloor \leq x$

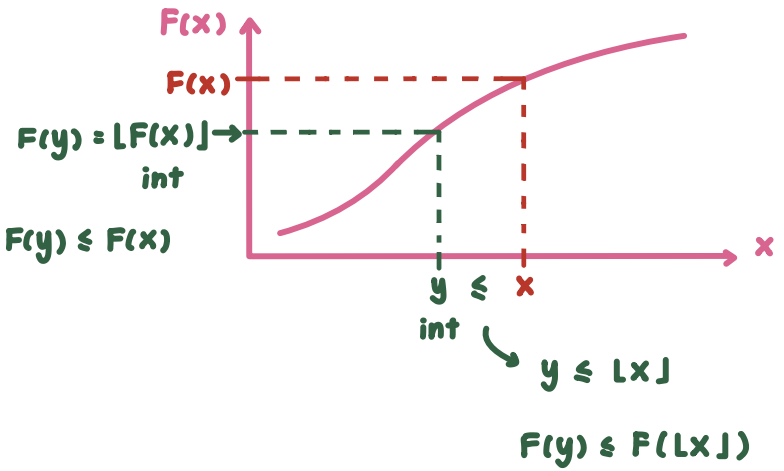
$\lfloor F(\lfloor x \rfloor) \rfloor \leq \lfloor F(x) \rfloor$

$\forall x, y \in \mathbb{R} \ (x \leq y \rightarrow \lfloor x \rfloor \leq y)$

$\lfloor F(x) \rfloor \leq \lfloor F(\lfloor x \rfloor) \rfloor$

$\geq$

Note



Interesting theorem

Let F be a continuous & monotonically increasing function.
If F satisfies the following condition:

F (x) is an integer only if x is an integer

then $\lfloor F(x) \rfloor = \lfloor F(\lfloor x \rfloor) \rfloor$ and $\lceil F(x) \rceil = \lceil F(\lceil x \rceil) \rceil$.

Proof:

Show that $\lfloor F(x) \rfloor = \lfloor F(\lfloor x \rfloor) \rfloor$.

Let f be a continuous & monotonically increasing function.

Since $\lfloor x \rfloor \le x$, we have $F(\lfloor x \rfloor) \le F(x)$ and $\lfloor F(\lfloor x \rfloor) \rfloor \le \lfloor F(x) \rfloor$.

Let $y < x$. That is $\lfloor F(y) \rfloor < \lfloor F(x) \rfloor$.

Since f is continuous, there exists z such that $F(z) = \lfloor F(x) \rfloor$ with $y < z \le x$. Then z is an integer (f satisfies the condition).

We also have that $z \le \lfloor x \rfloor$. That is $\lfloor F(x) \rfloor = F(z) \le F(\lfloor x \rfloor)$.

$\lfloor F(x) \rfloor = \lfloor \lfloor F(x) \rfloor \rfloor \le \lfloor F(\lfloor x \rfloor) \rfloor$.

Q.E.D.

Interesting theorem

Let F be a continuous & monotonically increasing function.
If F satisfies the following condition:

F (x) is an integer only if x is an integer

then $\lfloor F(x) \rfloor = \lfloor F(\lfloor x \rfloor) \rfloor$ and $\lceil F(x) \rceil = \lceil F(\lceil x \rceil) \rceil$.

Proof:

Show that $\lfloor F(x) \rfloor = \lfloor F(\lfloor x \rfloor) \rfloor$.

Let f be a continuous & monotonically increasing function.

Since $\lfloor x \rfloor \le x$, we have $F(\lfloor x \rfloor) \le F($ $F(\lfloor x \rfloor) \rfloor \le \lfloor F(x) \rfloor$.

$\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$

Let $y < x$. That is

Since f is continu exists z such that $F(z) = \lfloor F(x) \rfloor$ with $y < z \le x$. Then z is an integer (f satisfies the condition).

We also have that $z \le \lfloor x \rfloor$. That is $\lfloor F(x) \rfloor = F(z) \le F(\lfloor x \rfloor)$.

$\lfloor F(x) \rfloor = \lfloor \lfloor F(x) \rfloor \rfloor \le \lfloor F(\lfloor x \rfloor) \rfloor$. Q.E.D.

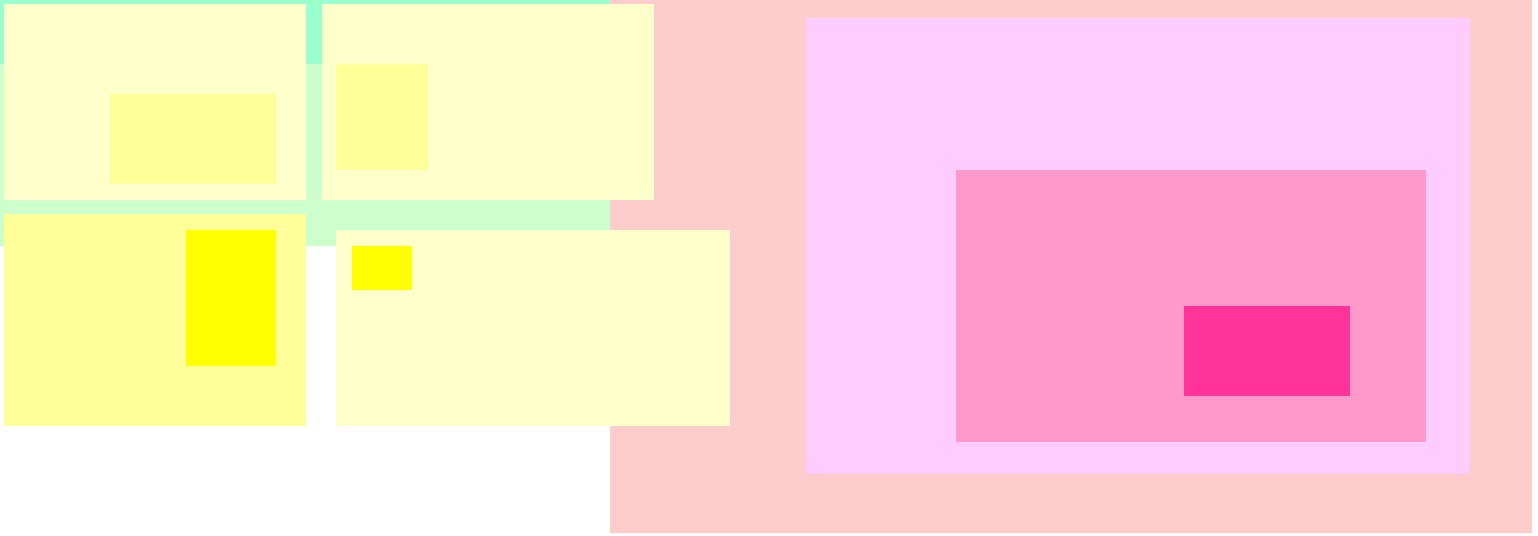
Definition 5 & 6

Floor function

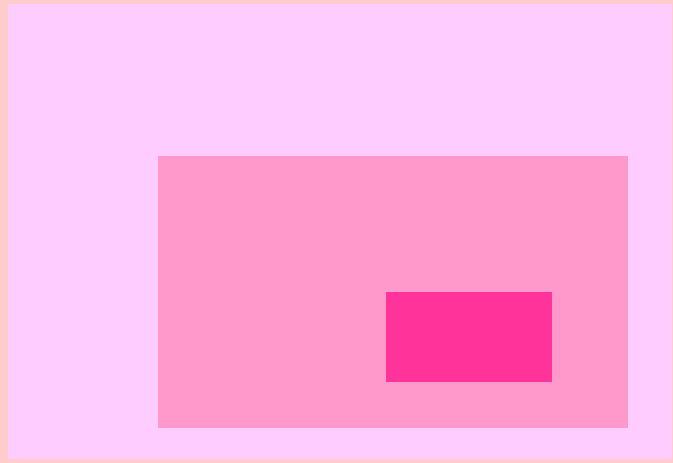
$\lfloor x \rfloor = n$ where n is an integer such that
$x = n + \varepsilon$ with $0 \leq \varepsilon < 1$.

Ceiling function

$\lceil x \rceil = m$ where m is an integer such that
$x = m - \delta$ with $0 \leq \delta < 1$.



Divisibility and modularity



Divisibility

Definition 7

For any integers m and n, where m is not zero,

m **divides** n, denoted by **m | n** (or n is divisible by m),

if there is an integer c such that

$$m \times c = n.$$

m is called a **factor** of n, and

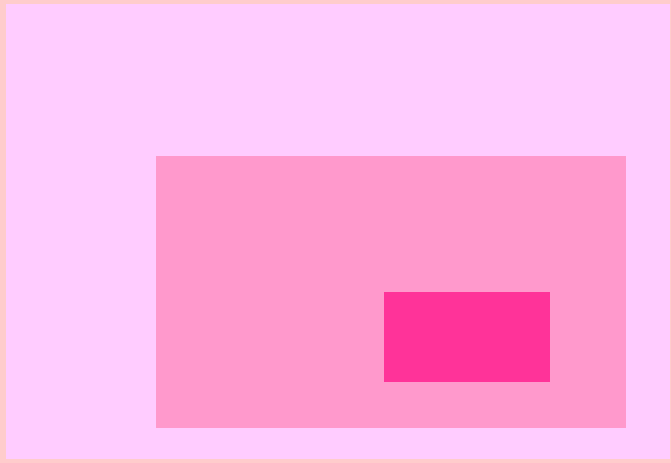
n is said to be a **multiple** of m.

Divisibility

Theorem 8

Let a, b, and c be three integers, then

1. if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$,
2. if $a \mid b$ then $a \mid bc$ for all integer c,
3. if $a \mid b$ and $b \mid c$ then $a \mid c$ (b is not zero).



Modularity Definition 9

A **modulo *n*** function, where *n* is an integer, is a function from an integer *m* to the remainder of *m* over *n*. This is usually denoted by ***m* mod *n***.

Examples

- **7 mod 4 = 3**
- **-5 mod 3 = 1**
- **2^{1234} mod 15 = 4**
- **2^{340} mod 341 = 1**
- **a mod b = c**

Modularity
Definition 9

A **modulo *n*** function, where *n* is an integer, is a function from an integer *m* to the remainder of *m* over *n*. This is usually denoted by ***m* mod *n***.

Express this by mathematical formula

For any integers *m*, *n*.

$$m \bmod n = m - \lfloor m / n \rfloor \times n.$$

***n* is called *modulus*.**

***m* mod n is an integer.**

Theorem 10

EXERCISE

Show that $0 \leq m \bmod n < n$

Modularity

Definition 9

A **modulo *n*** function, where *n* is an integer, is a function from an integer *m* to the remainder of *m* over *n*. This is usually denoted by ***m* mod *n***.

Show that $0 \le m \bmod n < n$

Theorem 10

$(m/n) - 1 < \lfloor (m/n) \rfloor \le (m/n)$

$m - n < \lfloor (m/n) \rfloor n \le m$ — divide by n

$-m \le -\lfloor (m/n) \rfloor n < -m + n$ — decrease by m

$0 \le m - \lfloor (m/n) \rfloor n < n$ — by Definition

$0 \le m \bmod n < n$

Modularity
Definition 9

A **modulo *n*** function, where *n* is an integer, is a function from an integer *m* to the remainder of *m* over *n*. This is usually denoted by ***m* mod *n***.

Show that $0 \leq m \bmod n < n$

Theorem 10

$(m/n)-1 < \lfloor (m/n) \rfloor \leq (m/n)$	by Definition 1
$m-n < \lfloor (m/n) \rfloor n \leq m$	multiply by n
$-m \leq -\lfloor (m/n) \rfloor n < -m+n$	multiply by -1
$0 \leq m - \lfloor (m/n) \rfloor n < n$	increasing by m
$0 \leq m \bmod n < n$	

Exercises

NUMBER THEORY

PROVE THESE STATEMENTS

Prove these statements

- QUESTION 4.1

  For integers m, n, and c where m is not zero,

  if $m \mid nc$ and $\gcd(m, n) = 1$ then $m \mid c$.

- QUESTION 4.2

  For integers m, n, c, and d,

  if $m \mid c$ and $n \mid d$ then $mn \mid cd$.

- QUESTION 4.3

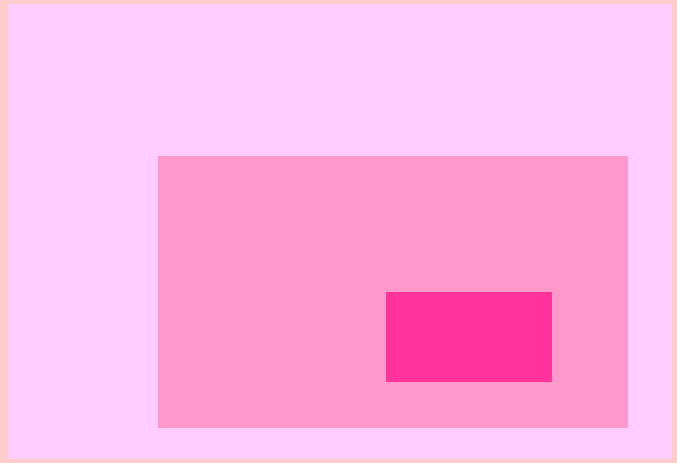
  For integers m, n and c, if $mc \mid nc$ then $m \mid n$.

Lesson 1

INTRODUCTION

Introduction

Brief review of the fundamental ideas of number theory and then present some mathematical preliminaries of elementary number theory.



Introduction

Number theory :
the theory of the properties of integers such as

Properties of numbers

- parity
- primality
- Multiplicativity
- additivity

Parity

Parity

Some well-known results, actually already known to Euclid, about the parity property of integers are as follows:

$even_1 \pm even_2 \pm even_3 \pm \ldots \pm even_k$ = even, if any positive k.

$odd_1 \pm odd_2 \pm odd_3 \pm \ldots \pm odd_k$ = even, if k is even.

$odd_1 \pm odd_2 \pm odd_3 \pm \ldots \pm odd_k$ = odd, if k is odd.

$odd_1 \times odd_2 \times odd_3 \times \ldots \times odd_k$ = odd, for any positive k.

$even \times odd_1 \times odd_2 \times \ldots \times odd_k$ = even, if there is at least 1 even.

Parity

Error detection and correction method (parity check)

One additional bit at the end of code is 1 if the number of 1's is odd, otherwise it is 0.

EXAMPLE

Let two codes be 1101001001 and 1001011011. Then the new codes will be

11010010011 and 10010110110.

For example, after transmission we know there is an error if transmitted code is

11010110011 and 10010110110.

ERROR IS DETECTED BUT CANNOT CORRECT

PARITY CHECK

Error detection and correction method (parity check)

1	0	0	1	0	1	1	0	0
1	0	1	1	1	0	1	1	0
1	1	0	0	0	0	0	1	1
0	1	1	0	0	1	0	0	1
0	0	0	1	1	0	0	0	0
1	0	1	0	1	0	1	0	1
0	1	0	0	0	0	0	0	1
1	0	0	1	1	0	1	0	0
1	1	0	0	0	0	0	0	0

PARITY CHECK

Error detection and correction method (parity check)

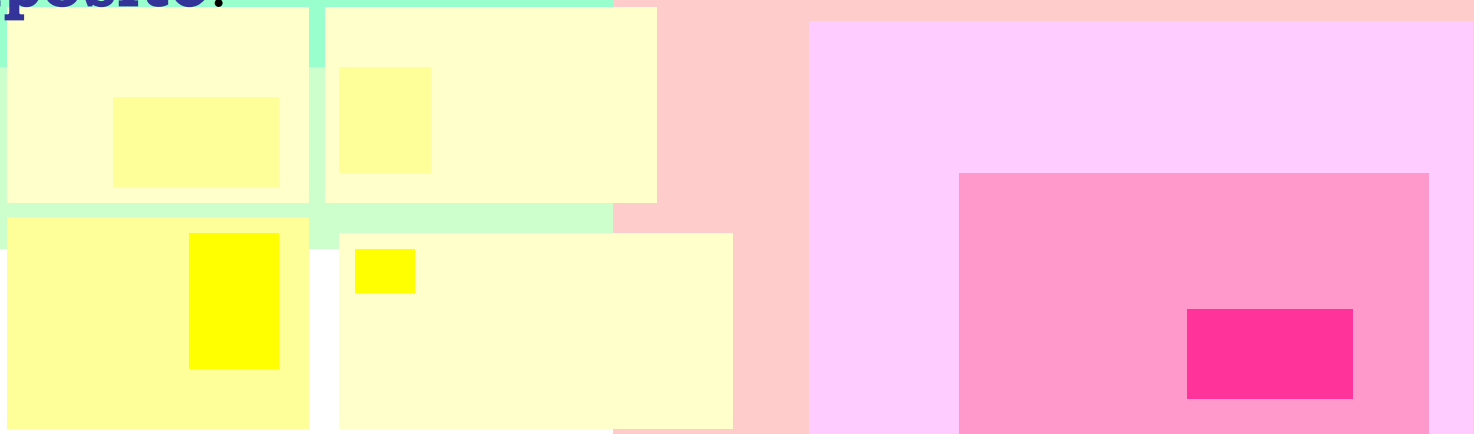
1	0	0	1	0	1	1	0	0
1	0	1	1	1	0	1	1	0
1	1	0	0	0	0	0	1	1
0	1	1	0	0	1	0	0	1
0	0	0	1	1	0	0	0	0
1	0	**0**	0	1	0	1	0	1
0	1	0	0	0	0	0	0	1
1	0	0	1	1	0	1	0	0
1	1	0	0	0	0	0	0	0

Primality

PRIMALITY

Definition 1.3.1

A positive integer $n > 1$ that has only two distinct factors, 1 and n itself is called **prime**; otherwise, it is called **composite**.



SOME INTERESTING RESULTS

- There are infinitely many primes. [Euclid]
- Only one even prime: 2
- Two largest twin primes (p and p+2),[1995]
  $570918348 \times 10^{5120} \pm 1$ and
  $242206083 \times 2^{38880} \pm 1$. [11713 digits]
- It is not known : infinitely many twin primes?
- infinitely many pairs (p, p+2) with
  p is prime and
  p+2 a product of most two primes.
  [J.R.Chen]
- Prime triples (p, p+2, p+6) : (347, 349, 353)
- Prime triples (p, p+4, p+6) : (307, 311, 313)
- Only one prime triples (p, p+2, p+4) : (3, 5, 7)

SOME INTERESTING RESULTS

Ancient Chinese mathematicians,

If p is a prime number, then $p \mid 2^p - 2$.

Example: 5 is a prime number, and $5 \mid 30$.

But, there are some composites that satisfy this condition.

Example: $341 = 11 \times 31$ is not prime, $341 \mid 2^{341} - 2$.

SOME INTERESTING RESULTS

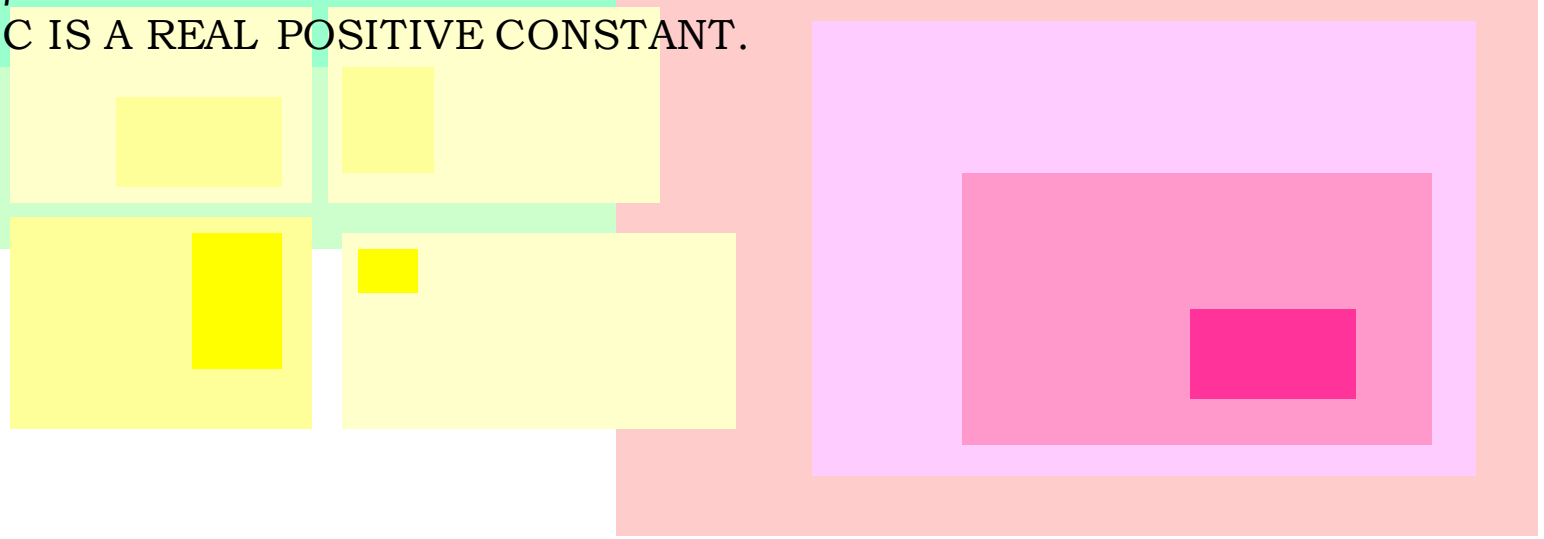
PROBLEM: IT IS NOT EASY TO TEST WHETHER OR NOT A LARGE NUMBER n IS PRIME.

NEEDS TO TEST UP TO $n^{1/2}$

THE CURRENT BEST ALGORITHM FOR PRIMALITY TESTING NEEDS AT MOST

$$\beta^{c \log \log \beta} \text{ (BIT OPERATIONS)}$$

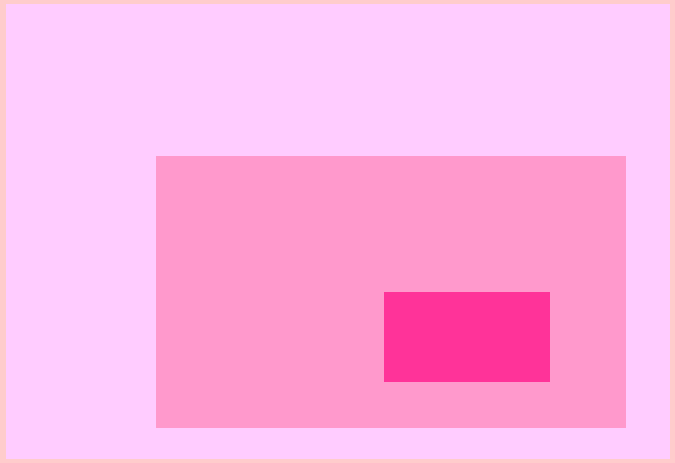
WHERE β IS A NUMBER OF BITS NEEDED FOR n
C IS A REAL POSITIVE CONSTANT.



The Sieve of Eratosthenes

Algorithm for finding all primes up to an integer n.

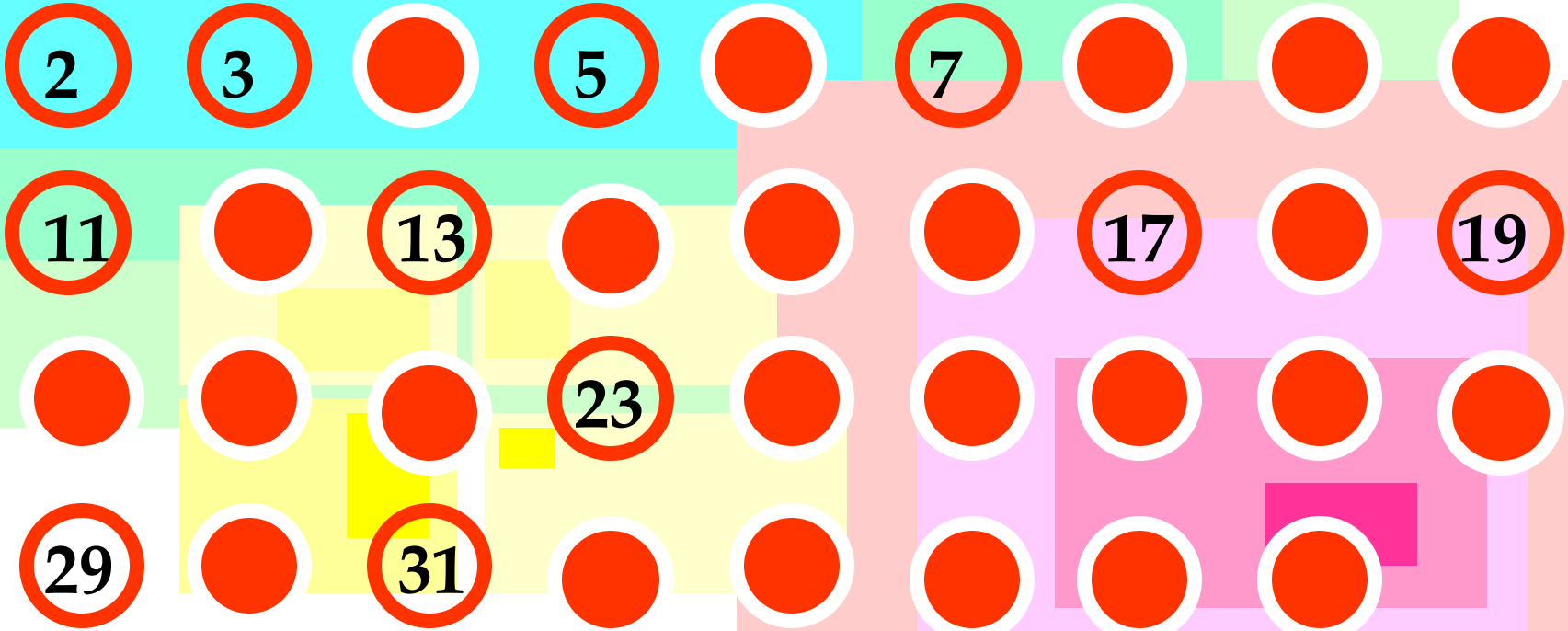
- Create a list of integers from 2 to n.
- For prime p, from 2 up to n, delete all multiples $p < pm \leq n$.
- Print the integers remaining in the list.



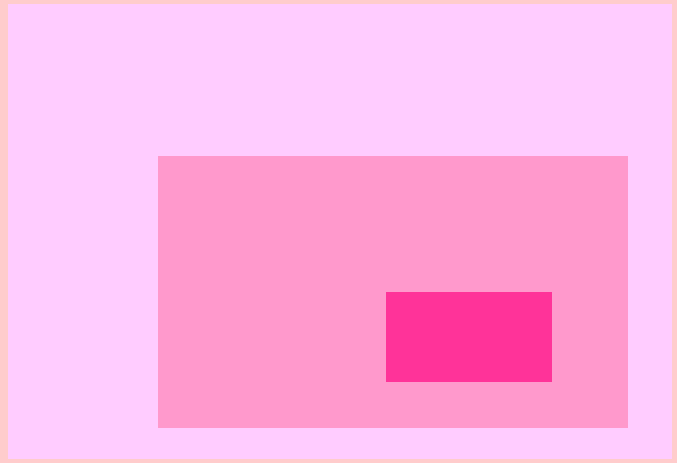
The Sieve of Eratosthenes

Algorithm for finding all primes up to an integer n.

QUESTION: Find all primes un to 36.



Multiplicativity



Fundamental Theorem of Arithmetic

[Proposed by Euclid]

Every positive integer $n > 1$ can be written **uniquely** as the product of **primes**.

?

!

PROOF

[Proved by Gauss, 1777-1855]

Fundamental Theorem of Arithmetic

[Proposed by Euclid]

Every positive integer n > 1 can be written **uniquely** as the **product of primes**.

PROOF:

The proof can be separated into two parts:

1. Show that every positive integer n > 1 can be written as the **product of primes**.
2. Show that there is a **unique** product of primes.

Proof : uniqueness

$\forall n \geq 1$, $\exists p_1, p_2, \dots, p_r \in \mathbb{P}rime \quad n = p_1 p_2 \cdots p_r$

By contradiction, $\exists q_1, q_2, \dots, q_s \in \mathbb{P}rime \quad n = q_1 q_2 \cdots q_s$ } diff

case 1 $\exists i,j \quad p_i = q_j$

Let $S = \{ n = 1 \mid n$ can be expressed more than one prime fac $\}$

$\therefore S \neq \emptyset$

Let a the smallest int in S

$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$

$\frac{a}{p_i} = p_1 \cdots p_{i-1} p_{i+1} \cdots p_r = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s = \frac{a}{q_j}$

$\frac{a}{p_i} \in \mathbb{Z}$ $\therefore \frac{a}{p_i} \in S$ but $\frac{a}{p_i} < a$

contradict a the smallest

case 2 $\forall i,j \quad p_i \neq q_j$

$p_1 > q_1$

consider $N = (p_1 - q_1) q_2 \cdots q_s$

$p_1 \nmid N$ $\qquad$ $p_1 \nmid q_k \quad (k \neq 1)$

$p_1 q_2 \cdots q_s - q_1 q_2 \cdots q_s$

$p_1 q_2 \cdots q_s - p_1 \cdots p_r$

$p_1 (q_2 \cdots q_s - p_2 \cdots p_r) = N$ $\quad p_1 \mid N$

contradict

Additivity

ADDITIVITY

THE LITTLE GOLDBACH CONJECTURE
TERNARY GOLDBACH CONJECTURE

Ch. Goldbach 1690-1764, proposed two conjectures

Every odd integer > 7 is the sum of 3 odd primes.
Every even integer > 4 is the sum of 2 odd primes.

EXAMPLES:

$6 = 3+3$
$8 = 3+5$
$9 = 3+3+3$
$10 = 3+7 = 5+5$
$11 = 3+3+5$
$12 = 5+7$
$13 = 3+3+7 = 3+5+5$
$14 = 3+11$
$15 = 3+5+7 = 5+5+5$
$16 = 3+13 = 5+11$

(The second conjecture implies the first.)

Lesson 2

THEORY OF DIVISIBILITY

Greatest common divisor
&
Least common multiple

$gcd(a,b)$; $a,b \in \mathbb{Z}$

$gcd(15,24)$

$15 = 3 \times 5$

$24 = 2 \times 2 \times 2 \times 3$

$gcd(15,24) = 3$ ✗

$lcm(15,24) = 3 \times 2 \times 2 \times 2 \times 5$

$24 \bmod 15 = 9$

$15 \bmod 9 = 6$

$9 \bmod 6 = 3$ → $gcd(15,24)$

$6 \bmod 3 = 0$

$0 \le a \bmod b < b$

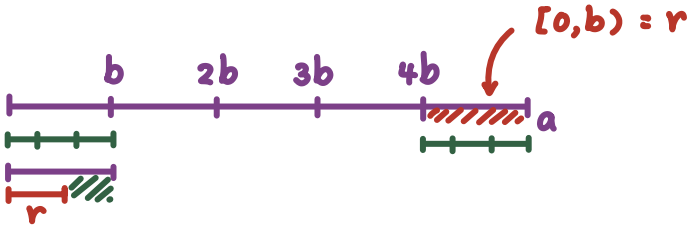
$gcd(a,b) = d$

$m \mid a \wedge m \mid b$

$\therefore m \le d$

$m \mid d$

$ab = lcm(a,b) \times gcd(a,b)$



$a \bmod b = c$

$b \bmod c = d$

$\vdots$

$d = gcd(a,b)$

$$gcd(a,b) = gcd(a \bmod b, b)$$

Proof Euclid

Greatest common divisor

Definition 2.2.1.

Let a,b be integers, not both zero. The largest divisor d such that d | a and d | b is called the **greatest common divisor** of a and b, denoted by gcd(a,b).

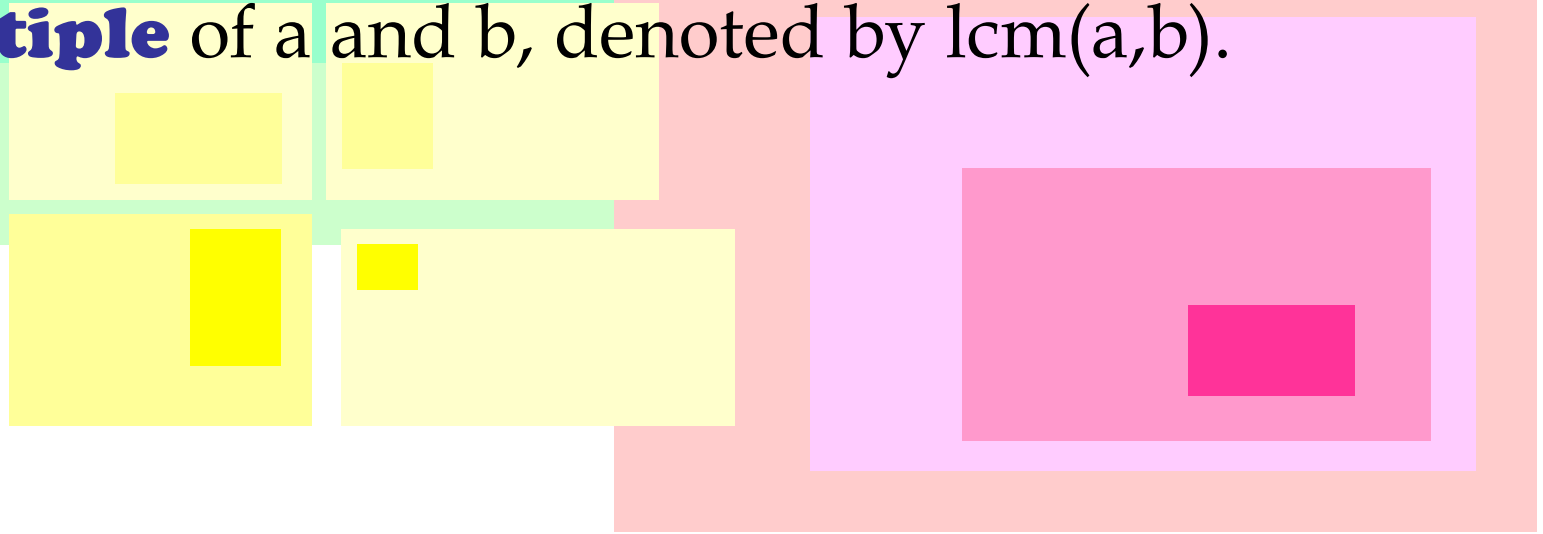
Integer a and b is called **relative prime** if gcd(a,b) is 1.

If gcd(a,b) = 1 and a | bc then a | c.

Least common multiple

Definition 2.2.2.

Let a,b be integers, not both zero. The smallest multiple d such that d is a multiple of a and d is a multiple of b is called the **least common multiple** of a and b, denoted by lcm(a,b).



Theoretical results

Theorem 2.2.3.

Let a, b be integers, not both zero and

let m = gcd(a, b).

Suppose that x is a common divisor of a, b.

Then x | m.

PROOF

Theoretical results

Theorem 2.2.4.

Let a, b be integers, not both zero and

let m = lcm(a, b).

Suppose that x is a common multiple of a, b.
Then m | x.

PROOF

Fundamental problem

How to find the greatest common divisor of two positive integers *a* and *b* ?

Easy !!!!

By factoring of *a* and *b*

Factoring is one of the **most difficult** solving problem.

The man who can answer the question

Euclid's division theorem

Given two integers a and b, where $b > 0$,

There exist **unique** integers q and r such that

$$a = bq + r \text{ where } 0 \le r < b.$$

b is called the divisor
a is called the dividend
q is called the quotient
r is called the remainder.

PROOF?

Brief, the proof can be separated into two parts:

1. Show that **there exist** two integers q and r satisfying $0 \le r < b$.
2. Show that q and r are **unique**.

Exercises 5

NUMBER THEORY

PROVE THESE STATEMENTS

Prove these statements

Given two integers a and b where $b > 0$. From Euclid's division theorem, there exist two integers q and r, $a = bq + r$

and $0 \leq r < b$.

- QUESTION 5.1

  Show that $r = a \bmod b$.

- QUESTION 5.2

  Show that $\gcd(a, b) = \gcd(b, r)$.

Division Algorithm

$\forall a,b \in \mathbb{Z}, b > 0$

$\exists q,r \in \mathbb{Z}$ $a = bq + r$ $(r = a \bmod b)$

where $0 \le r < b$

$(q, r$ unique$)$

Note $a = 24$, $b = 15$

$24 = 15 \times \underline{0} + \underline{24}$ (-1, 39)

$\underline{1} \quad \underline{9}$

2 -6

q r

$r = a - bq$

$q = \frac{a-r}{b}$

Proof: 1) Show $\exists q,r \in \mathbb{Z}$, $a = bq + r$ and $0 \le r < b$

Let $R = \{a - bq \mid q \in \mathbb{Z}\}$

We found that let $q = -|a|$ $q \in \mathbb{Z}$

$a - bq = a - -|a|b \ge 0$ $\therefore R \neq \emptyset$

By well-ordering principle,

let $\underline{s}$ be the smallest non-neg int in R

We have to show that $0 \le s < b$

By contradiction, assume $s \ge b$

consider $s - b \ge 0$ but $s - b < s$ $\therefore s - b \notin R$

since $s \in R$ $\exists q_1 \in \mathbb{Z}$ $a = bq_1 + s$

$= b(q_1 + 1) + (s - b)$

$\therefore (s-b) = a - b(q_1 + 1)$ $\therefore (s-b) \in R$

$\therefore 0 \le s < b$

contradict

2) Uniqueness Let $q_1, q_2, r_1, r_2 \in \mathbb{Z}$

$a = bq_1 + r_1$; $0 \le r_1 < b$

$a = bq_2 + r_2$; $0 \le r_2 < b$

and $q_1 \neq q_2 \wedge r_1 \neq r_2$

$bq_1 + r_1 = bq_2 + r_2$

$b(q_1 - q_2) = (r_2 - r_1)$

$|b(q_1 - q_2)| = |r_2 - r_1|$

$\underline{b}|q_1 - q_2| = |r_2 - r_1| \rightarrow 0 \le |r_2 - r_1| < b$

int = int < b

$bA = B < b$

$\therefore A = 0$

$\therefore q_1 = q_2$

contradict

$r = a \bmod b$

Given a, b

$a = bq_0 + r_1$ ($b \to r_0$) $\quad a \bmod b = r_1 \quad 0 \le r_1 < r_0$

$b = r_1 q_1 + r_2$ ($b \to r_0$) $\quad b \bmod r_1 = r_2 \quad 0 \le r_2 < r_1$

$r_1 = r_2 q_2 + r_3 \quad r_1 \bmod r_2 = r_3 \quad 0 \le r_3 < r_2$

$\vdots$

$r_{n-1} = r_n q_n \quad r_{n+1} = 0$

$\downarrow$

$\gcd(a,b) = r_n$

$\gcd(1128, 251)$

iterator	r_i	q_i
	1128	
0	251	4
1	124	2
2	3	41
$n = 3$	1	3
4	0	

Euclid's algorithm

An algorithm for computing the greatest common divisor of two integers a and b, $b > 0$, using the condition:

$$\gcd(a,b) = \gcd(a \bmod b,\ b) \text{ if } b < a.$$

Division algorithm

For any integer a and any positive integer b, there are unique q_0 and r_1 such that

$a = bq_0 + r_1, \quad 0 \le r_1 < b.$

$b = r_1q_1 + r_2, \quad 0 \le r_2 < r_1$

$r_1 = r_2q_2 + r_3, \quad 0 \le r_3 < r_2$

....

$r_{n-1} = r_nq_n + 0, \quad r_{n+1} = 0.$

$\gcd(a,b) = r_n.$

It is the oldest algorithm that has survived to the present day.
D.E.Knuth

Euclid's algorithm

Example: Find gcd(435, 246)

i	r_i	q_i
	435	
0	246	1
1	189	1
2	57	3
3	18	3
4	3	6
5	0	

$a = 435$

$b = 246 = r_0$

$a = r_0 \times q_0 + r_1$

$435 = 246 \times 1 + 189$

$r_0 = r_1 \times q_1 + r_2$

$246 = 189 \times 1 + 57$

$r_1 = r_2 \times q_2 + r_3$

$189 = 57 \times 3 + 18$

$r_2 = r_3 \times q_3 + r_4$

$57 = 18 \times 3 + 3$

$r_3 = r_4 \times q_4 + r_5$

$18 = 3 \times 6 + 0$

$\gcd(435,246) = 3 = r_4$

$n = 4$

Euclid's algorithm

Division algorithm

For any integer a and any positive integer b, there are unique q_0 and r_1 such that

$a = bq_0 + r_1, \quad 0 \le r_1 < b.$

$b = r_1q_1 + r_2, \quad 0 \le r_2 < r_1$

$r_1 = r_2q_2 + r_3, \quad 0 \le r_3 < r_2$

....

$r_{n-1} = r_nq_n + 0, \quad r_{n+1} = 0.$

$\gcd(a,b) = r_n.$

What is the relationship of all variables?

Exercises 6

NUMBER THEORY

FIND THE GREATEST COMMON DIVISOR

$r = a \bmod b$

Given a, b

$a = bq_0 + r_1$ ($b = r_0$) — $a \bmod b = r_1$ — $0 \le r_1 < r_0$

$b = r_1 q_1 + r_2$ ($b = r_0$) — $b \bmod r_1 = r_2$ — $0 \le r_2 < r_1$

$r_1 = r_2 q_2 + r_3$ — $r_1 \bmod r_2 = r_3$ — $0 \le r_3 < r_2$

$\vdots$

$r_{n-1} = r_n q_n$ — $r_{n+1} = 0$

$\downarrow$

$\gcd(a,b) = r_n$

$a = r_0 q_0 + r_1$ — $\frac{r_0}{r_1} = q_1 + \frac{r_1}{r_2}$

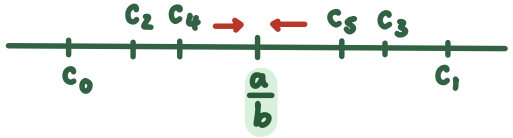
$\frac{a}{b} = q_0 + \frac{r_1}{r_0}$ — $\frac{r_1}{r_2} = q_2 + \frac{r_3}{r_2}$

$$\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{r_2}{r_1}}$$

$$\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{r_3}{r_2}}}$$

$$\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots\, q_n}}}$$

Simple Continued Fraction



c_k : k^{th} convergent term

$$c_i = q_0 + \frac{1}{q_1 + \frac{1}{\ddots\, q_i}}$$

$$x = q_0 + \frac{1}{q_1 + \frac{1}{q_2}} < 1 \qquad x_1$$

$\lfloor x \rfloor = q_0$

$\lfloor x_1 \rfloor = q_1$

$$\lfloor x \rfloor = q_0 + \frac{1}{q_1 + \frac{1}{q_2 \ddots}}$$

$$\lfloor x_1 \rfloor = q_1 + \frac{1}{q_2 \ddots}$$

$$\lfloor x_2 \rfloor = q_2 + \frac{1}{q_3 \ddots}$$

$a \in \mathbb{Z}, b > 0$

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots\, q_n}}}$$

$$a = bq_0 + r_1; \quad 0 \le r < b \qquad (r_0)$$

---

gcd(1128, 251)

iterator	r_i	q_i
	1128	
0	251	4
1	124	2
2	3	41
n = 3	1	3
4	0	

$$1128 = 4 + \cfrac{1}{2 + \cfrac{1}{41 + \cfrac{1}{3}}}$$

[4, 1, 41, 3]

Ex. $x = \sqrt{2}$

$$x_0 = \sqrt{2}, \quad x_0 = q_0 + \frac{1}{x_1}$$

$$q_0 = \lfloor \sqrt{2} \rfloor = 1$$

$$\sqrt{2} = 1 + \frac{1}{x_1}$$

$$x_1 = \frac{1}{\sqrt{2}-1} \times \frac{\sqrt{2}+1}{\sqrt{2}+1} = \sqrt{2}+1 \qquad x_1 = q_1 + \frac{1}{x_2}$$

$$q_1 = \lfloor \sqrt{2}+1 \rfloor = 2$$

$$\sqrt{2}+1 = 2 + \frac{1}{x_2}$$

$$x_2 = \frac{1}{\sqrt{2}-1} \times \frac{\sqrt{2}+1}{\sqrt{2}+1} = \sqrt{2}+1$$

$$\therefore q_2 = 2 = q_1$$

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}$$

$$[1, \overline{2}] = [1, 2, 2, 2 \ldots]$$

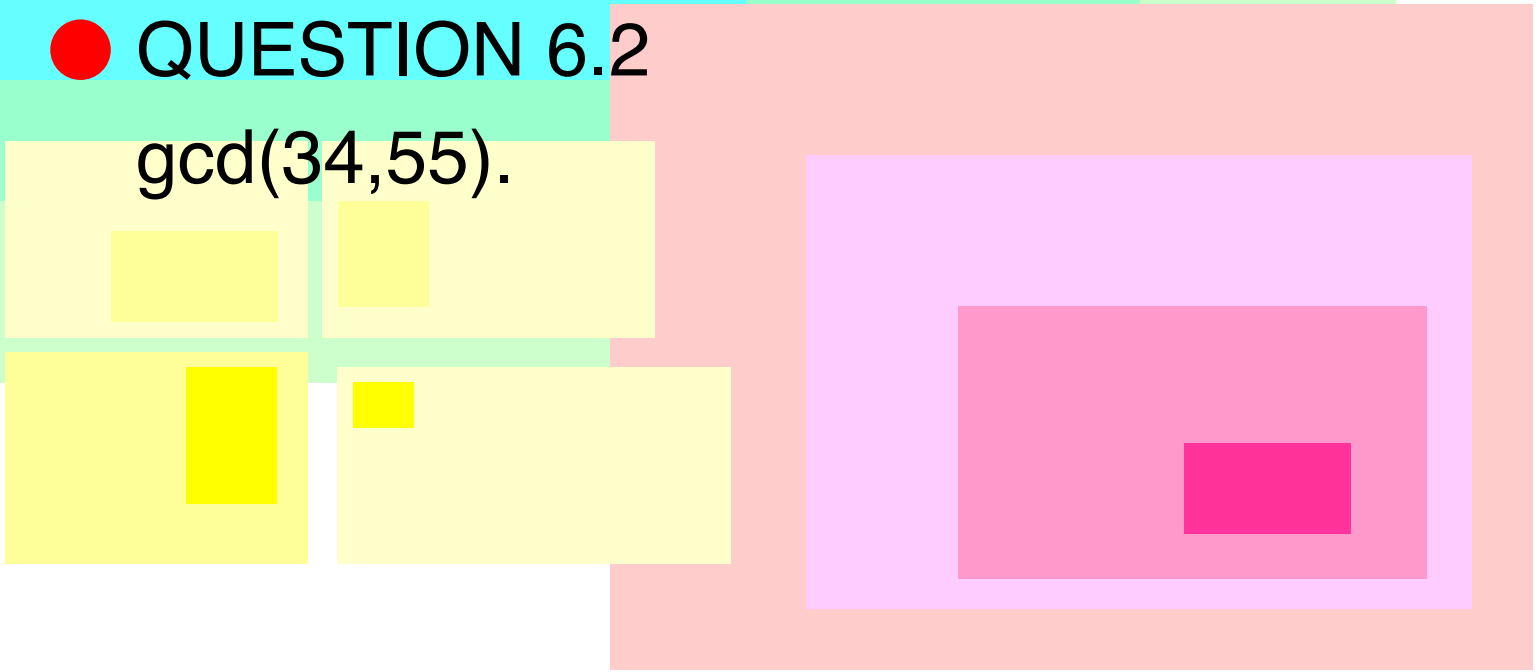
Euclid's division

Find the greatest common divisor using Euclid's division algorithm

- QUESTION 6.1

  gcd(340,250).
- QUESTION 6.2

  gcd(34,55).



Euclid's algorithm

Interesting fraction

$a = bq_0 + r_1, \quad (a/b) = q_0 + (r_1/b)$

$b = r_1 q_1 + r_2, \quad (b/r_1) = q_1 + (r_2/r_1)$

$(a/b) = q_0 + 1/(b/r_1) = q_0 + 1/(q_1 + (r_2/r_1))$

$r_1 = r_2 q_2 + r_3, \quad (r_1/r_2) = q_2 + (r_3/r_2)$

$(a/b) = q_0 + 1/(q_1 + 1/(q2 + (r_3/r_2)))$

....

$r_{n-1} = r_n q_n + 0,$

Euclid's algorithm

Interesting fraction

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

SIMPLE CONTINUED FRACTION
Denoted by $a/b = [q_0, q_1, q_2, \ldots, q_n]$

Euclid's algorithm

$$\frac{435}{246} = 1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{6}}}}$$

435 = 246 × 1 + 189
246 = 189 × 1 + 57
189 = 57 × 3 + 18
57 = 18 × 3 + 3
18 = 3 × 6 + 0

Simple continued fraction

Proposition

All rational number can be expressed by a **finite** simple continued fraction.

Proposition

All number that can be expressed by a simple continued fraction is an **algebraic** number.

Definition

A number *n* is said to be an algebraic number if it can be a root of an integral polynomial.

Simple continued fraction

Given a number x, how x can be expressed by a simple continued fraction.

A simple continued fraction of x is of the form

$$\boldsymbol{x = q_0 + 1 / (q_1 + 1 / (q_2 + 1 / (q_3 + 1 / (\ldots))))}$$

Since $q_1 \geq 1$ (by Euclid's algorithm), it is obtained that

$$1 / (q_1 + 1 / (q_2 + 1 / (q_3 + 1 / (\ldots)))) < 1.$$

This implies that $\mathbf{q_0 = \lfloor x \rfloor}$.

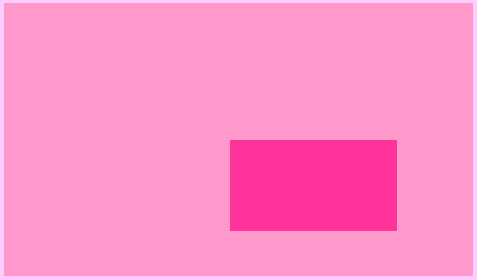
Let $x_1 = (q_1 + 1 / (q_2 + 1 / (q_3 + 1 / (\ldots))))$.

The relationship between x, q_0 and x_1 is then

$$\boldsymbol{x = q_0 + 1 / x_1}.$$

That is $x_1 = 1 / (x - q_0)$.

Repeat the process by considering $\mathbf{q_1 = \lfloor x_1 \rfloor}$.



Exercises 7

NUMBER THEORY

SIMPLE CONTINUED FRACTION

Bi-linear Diophantine Eq^{n}

$$ax + by = c$$

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \ddots} \qquad c_k = q_0 + \cfrac{1}{\ddots q_n} = \frac{P_k}{Q_k} \qquad P_k, Q_k \in \mathbb{Z}$$

$$c_n = \frac{P_n}{Q_n} = \frac{a}{b}$$

$$P_n \times \gcd(a,b) = a$$
$$Q_n \times \gcd(a,b) = b$$

$$c_0 = q_0 \quad P_0 = q_0 \quad Q_0 = 1$$

$$c_1 = q_0 + \frac{1}{q_1} = \frac{q_1 q_0 + 1}{q_1} \qquad P_1 = q_1 q_0 + 1 \qquad Q_1 = q_1$$

$$c_2 = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}} = q_0 + \frac{q_2}{q_2 q_1 + 1} = \frac{q_2 q_1 q_0 + q_0 + q_2}{q_2 q_1 + 1}$$

$$= \frac{q_2(q_1 q_0 + 1) + q_0}{q_2 q_1 + 1} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0}$$

$$\forall k \le n \quad P_k = q_k P_{k-1} + P_{k-2}$$
$$Q_k = q_k Q_{k-1} + Q_{k-2}$$

Lemma

$k \ge 2$

Consider $Q_1P_0 - P_1Q_0 = q_1q_0 - (q_1q_0+1)1$

$= -1$

$Q_2P_1 - P_2Q_1 = (q_2Q_1+Q_0)P_1 - (q_2P_1+P_0)Q_1$

$= P_1Q_0 - Q_1P_0$

$= 1$

$$\boxed{Q_kP_{k-1} - P_kQ_{k-1} = (-1)^k}$$

$\frac{a}{b} \to \frac{P_n}{Q_n}$ $\quad P_n \gcd(a,b) = a$

$\quad Q_n \gcd(a,b) = b$

solve $ax + by = c$

(integer)

$$\overset{b}{Q_n}P_{n-1} - \overset{a}{P_n}Q_{n-1} = (-1)^n$$

$$P_nQ_{n-1} - Q_nP_{n-1} = (-1)^{n-1}$$

$$P_n(-1)^{n-1}Q_{n-1} + Q_n(-1)^{n}P_{n-1} = 1$$

$ax + by = c$; c = multiple of $\gcd(a,b)$

$\therefore x = (-1)^{n-1}Q_{n-1} \times \gcd(a,b) \times c'$

$y = (-1)^n P_{n-1} \times \gcd(a,b) \times c'$

$c = \gcd(a,b) = c' \quad \exists c' \in \mathbb{Z}$

Ex. $1128x + 251y = 1$

$x = (-1)^{n-1} Q_{n-1}$

$y = (-1)^n P_{n-1}$

$n = 3$

$P_2 = 373$ $\quad \therefore x = (-1)^2 83 = 83$

$Q_2 = 83$ $\quad y = (-1)^3 373 = -373$

iterator	r_i	q_i	P_i	Q_i
	1128			
0	251	4	4	1
1	124	2	9	2
2	3	41	373	83
$n = 3$	1	3	1128	251
4	0			

$P_0 = q_0 \quad Q_0 = 1$

$P_1 = q_1 q_0 + 1 \quad Q_1 = q_1$

$$\forall k \le n \quad P_k = q_k P_{k-1} + P_{k-2}$$
$$Q_k = q_k Q_{k-1} + Q_{k-2} \qquad k \ge 2$$

Ex. $\overset{a}{24}x + \overset{b}{15}y = 30$

$\gcd(a,b) = 3$

$a = 3P_n$

$b = 3Q_n$

iterator	r_i	q_i	P_i	Q_i
	24			
0	15	1	1	1
1	9	1	2	1
2	6	1	3	2
$n = 3$	3	2	8	5
	0			

gcd

$$\overset{24}{d}P_n(-1)^{n-1}\overset{x}{Q}_{n-1} + \overset{15}{d}Q_n(-1)^n\overset{y}{P}_{n-1} = \overset{30}{d}$$

$$24 \times \underbrace{10 \times (-1)^{n-1} Q_{n-1}}_{x=20} + 15 \times \underbrace{10 \times (-1)^n P_{n-1}}_{y=-30} = 30$$

x/y มาจาก 3 ไม่ลง มาจาก 3 ไม่ลง

Ex. $24x + 15y = 22$

$24x + 15y = 3$ ← x, y ไม่ใช่ integer

$ax + by = c$ $\quad x_0, y_0$ = solution

$ax_0 + by_0 = c$

Assume others solution, x_1, y_1 $(x_1 = x_0 \wedge y_1 \neq y_0)$

$\therefore ax_1 + by_1 = c = ax_0 + by_0$

Assume $x_1 = x_0 + \delta x \; ; \; \delta x \in \mathbb{Z} \wedge \delta x \neq 0$

$y_1 = y_0 + \delta y \; ; \; \delta y \in \mathbb{Z} \wedge \delta y \neq 0$

$a(x_0 + \delta x) + b(y_0 + \delta y) = ax_0 + by_0$

$a\delta x + b\delta y = 0$

$a\delta x = -b\delta y$

$\delta x = -\frac{b}{a}\delta y \in \mathbb{Z}$

$\delta x = -\frac{\gcd(a,b)\,Q_n}{\gcd(a,b)\,P_n}\,\delta y$ $\qquad a = \gcd(a,b)\,P_n$ $\qquad b = \gcd(a,b)\,Q_n$

$\therefore \delta y = tP_n \quad \forall t \in \mathbb{Z}$

$\delta x = -\frac{Q_n \times tP_n}{P_n} = -tQ_n$ (same t)

$x = (-1)^{n-1} Q_{n-1} \gcd(a,b) \times c' - tQ_n$

$y = (-1)^{n} P_{n-1} \gcd(a,b) \times c' + tP_n$ $\qquad \forall t \in \mathbb{Z}$

$3x + 5y + 9z = 21 \qquad x, y, z \in \mathbb{Z}$

$3x + 5y = 21 - 9z$

↳ solve $3x + 5y = 1 \times (21 - 9z)$

$x = x_0 - tQ_n \qquad y = y_0 + tP_n$

$x = (x_0 - tQ_n)(21 - 9z) \qquad \forall t \in \mathbb{Z}$

$y = (y_0 + tQ_n)(21 - 9z)$

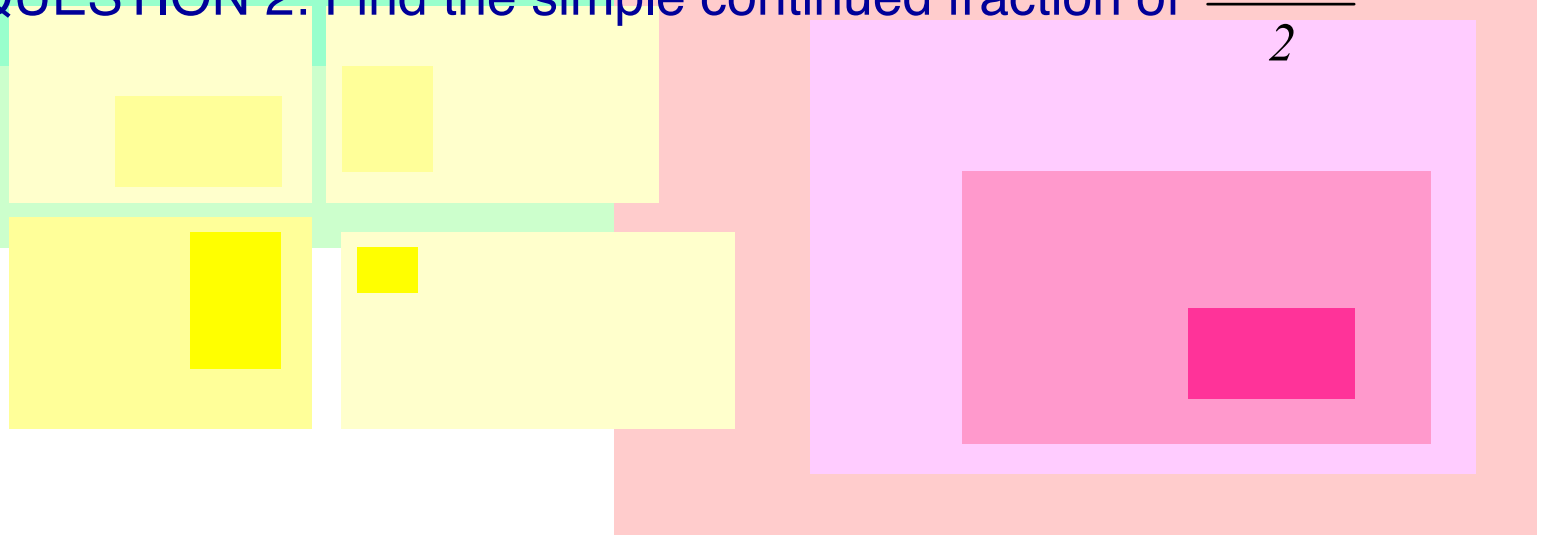
$\forall z \in \mathbb{Z}$

Simple continued fraction

QUESTION 1: Find the simple continued fraction of 34/55

QUESTION 2: Find the simple continued fraction of $\sqrt{7}$

QUESTION 2: Find the simple continued fraction of $\frac{1+\sqrt{5}}{2}$



The k^{th} convergent term

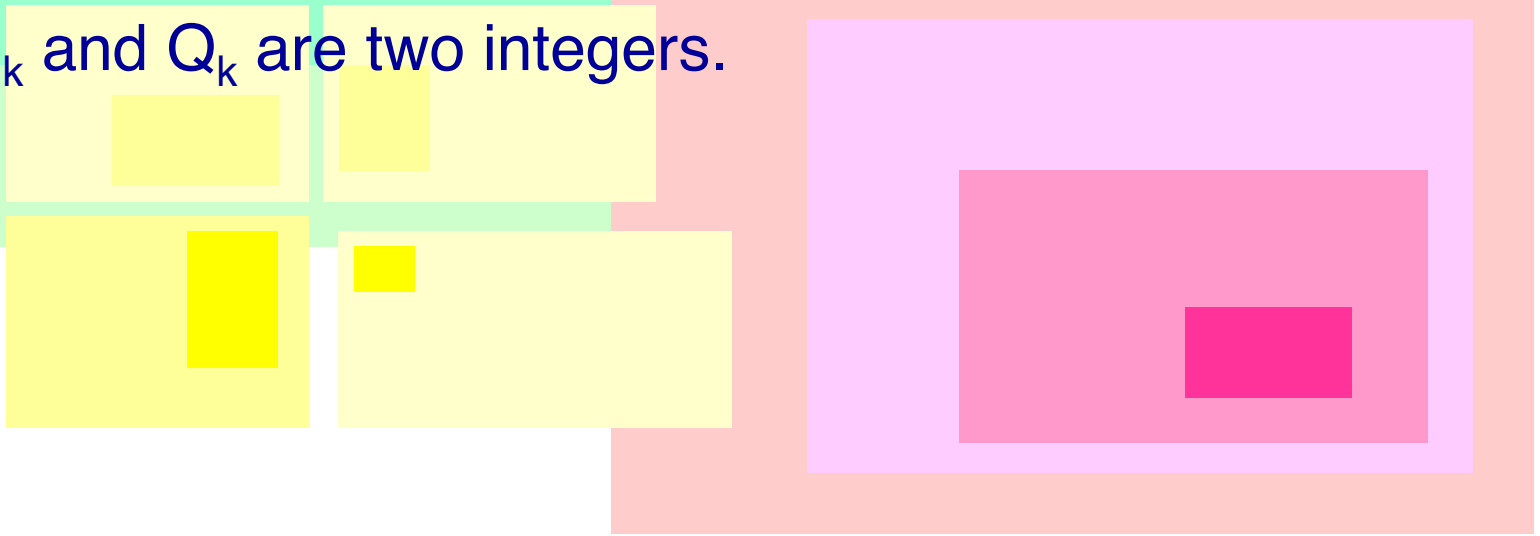
The k^{th} convergent term C_k of the expansion is

$$C_k = q_0 + 1 / (q_1 + 1 / (\ldots + 1 / q_k) \ldots)$$

Since C_k is a rational number, we have that

$$C_k = P_k / Q_k,$$

where P_k and Q_k are two integers.



The k^{th} convergent term

The recurrence relations for P_k and Q_k are expressed by the followings:

$$P_0 = q_0$$
$$Q_0 = 1$$
$$P_1 = q_1 q_0 - 1$$
$$Q_1 = q_1$$

For $k > 1$,

$$P_k = q_k P_{k-1} + P_{k-2}$$
$$Q_k = q_k Q_{k-1} + Q_{k-2}$$

Proposition

Given integers a and b, where $b > 0$, let $C_n = P_n/Q_n$ be the simple continued fraction of a/b. It is obtained that

$$\gcd(P_n, Q_n) = 1.$$

Example $\dfrac{435}{246} = 1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{6}}}}$

From the fraction, $C_4 = 145 / 82$ where $\gcd(145,82) = 1$.

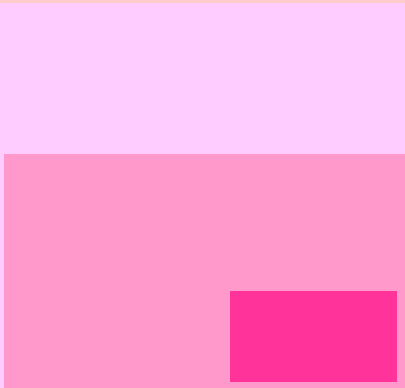
Proposition

Given integers a and b, where b > 0, let $C_n = P_n/Q_n$ be the simple continued fraction of a/b. It is obtained that

$$\gcd(P_n, Q_n) = 1.$$

This implies that

$$a = P_n \times \gcd(a,b)$$
$$b = Q_n \times \gcd(a,b).$$



Proposition

Given integers a and b, where $b > 0$, let $C_n = P_n/Q_n$ be the simple continued fraction of a/b. The relationship of P_k and Q_k is

$$Q_{k-1}P_k - P_{k-1}Q_k = (-1)^{k-1},$$

for $0 \le k \le n$.

Conclusion

$(-1)^{n-1}Q_{n-1} \times P_n - (-1)^{n-1}P_{n-1} \times Q_n = 1.$

$(-1)^{n-1}Q_{n-1} \times P_n \times d + (-1)^{n}P_{n-1} \times Q_n \times d = d.$

$(-1)^{n-1}Q_{N-1} \times P_n \times \gcd(a,b) + (-1)^{n}P_{n-1} \times Q_n \times \gcd(a,b) = \gcd(a,b).$

$(-1)^{n-1}Q_{n-1} \times a + (-1)^{n}P_{n-1} \times b = \gcd(a,b).$

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

Solving bilinear Diophantine equation

Given an equation $ax + by = c$.

- **$c = \gcd(a,b)$**

  $x = (-1)^{n-1}Q_{n-1}$ and $y = (-1)^{n}P_{n-1}$

- **$\gcd(a,b) \mid c$**

  There exists an integer e that $e \times \gcd(a,b) = c$.

  $x = (-1)^{n-1}Q_{n-1} \times e$ and $y = (-1)^{n}P_{n-1} \times e$

- **$\gcd(a,b) \nmid c$**

  There is not any integral solution.

Solving bilinear Diophantine equation

Given an equation 435x + 246y = 3.

i	r_i	q_i	P_i	Q_i
	435			
0	246	1	1	1
1	189	1	2	1
2	57	3	7	4
3	18	3	23	13
4	3	6	145	82
5	0			

$x = (-1)^{n-1}Q_{n-1}$

$x = (-1)^3\ 13$

$x = -13$

$y = (-1)^nP_{n-1}$

$y = (-1)^4\ 23$

$y = 23$

Verification : 435×(-13) + 246×23 = -5655 + 5658 = 3

Solving bilinear Diophantine equation

Other solutions ?

Let x_0 and y_0 be the solution of $ax + by = c$, and
let x_1 and y_1 be another solution.
Suppose that $x = x_0 + d_x$ and $y = y_0 + d_y$, d_x and d_y are integers.
Conclusion: $ax_0 + by_0 = c$

$ax + by = c$ or $ax_0 + ad_x + by_0 + bd_y = c$

$ad_x + bd_Y = 0$

Let $e = \gcd(a,b)$, we have $e \times P_n = a$ and $e \times Q_n = b$.
Then $\gcd(P_n,Q_n) = 1$.
From $ad_x = -bd_y$, we have that $(P_n \times e)d_x = -(Q_n \times e)d_y$

$P_n \times d_x = Q_n \times d_y$

This implies that $P_n \mid (Q_n \times d_y)$ but $\gcd(P_n,Q_n) = 1$, then $P_n \mid d_y$
d_y must be a multiple of P_n, or $\mathbf{d_y = P_n \times t}$ **for all** $\mathbf{t \in Z}$.

Then $\mathbf{d_x = -(Q_n/P_n) \times (P_n \times t) = -Q_n \times t}$.

All solution, $x = x_0 - Q_n t$ and $y = y_0 + P_n t$ for all $t \in Z$.

Solving bilinear Diophantine equation

Given an equation 435x + 246y = 3.

i	r_i	q_i	P_i	Q_i
	435			
0	246	1	1	1
1	189	1	2	1
2	57	3	7	4
3	18	3	23	13
4	3	6	145	82
5	0			

$x = (-1)^{n-1} Q_{n-1}$

$x = (-1)^3\ 13$

$x = -13$

$y = (-1)^n P_{n-1}$

$y = (-1)^4\ 23$

$y = 23$

Verification : 435×(-13) + 246×23 = -5655 + 5658 = 3

All solution

$x = -13 - 82t$

$y = 23 + 145t$

For all $t \in Z$

Exercises 5

NUMBER THEORY

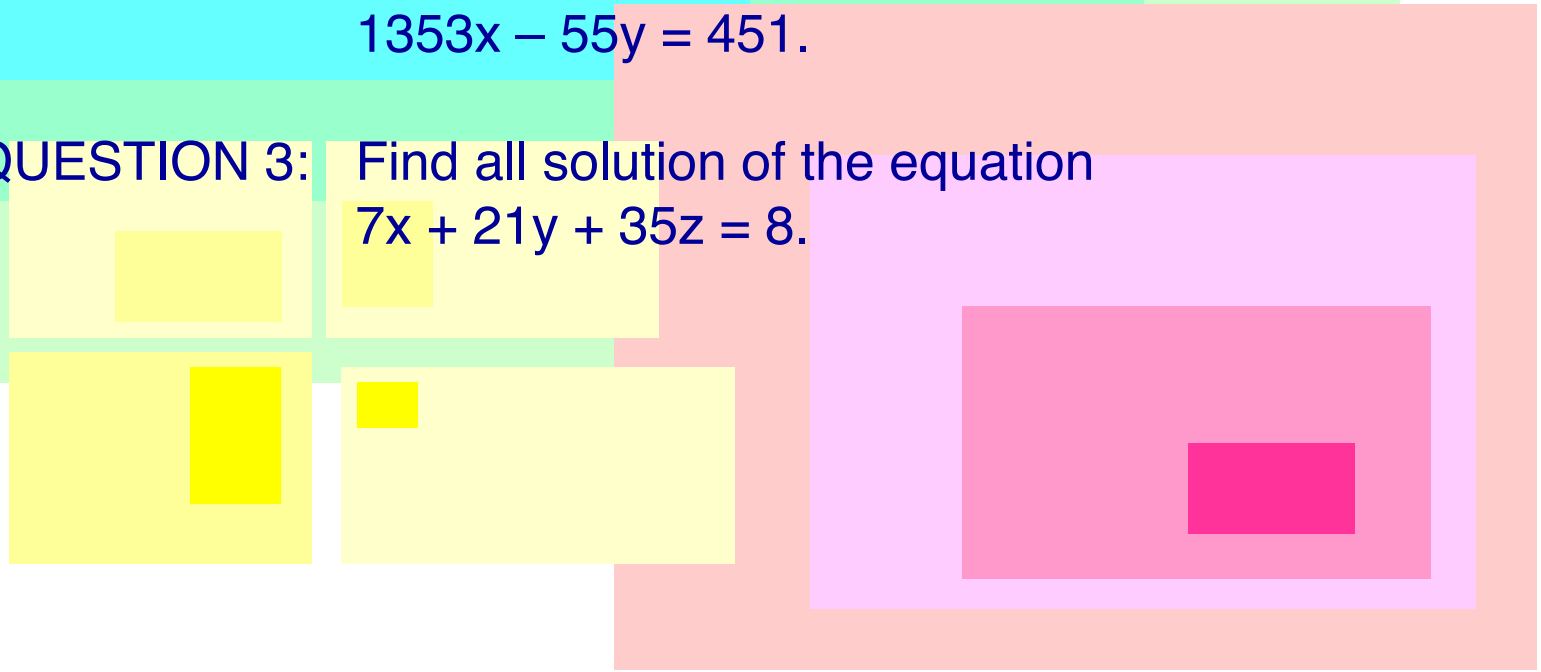
BILINEAR DIOPHANTINE EQUATION

Bilinear Diophantine equation

QUESTION 1: Find all solution of the equation
$146r + 41s + 32n = 4$.

QUESTION 2: Find all solution of the equation
$1353x - 55y = 451$.

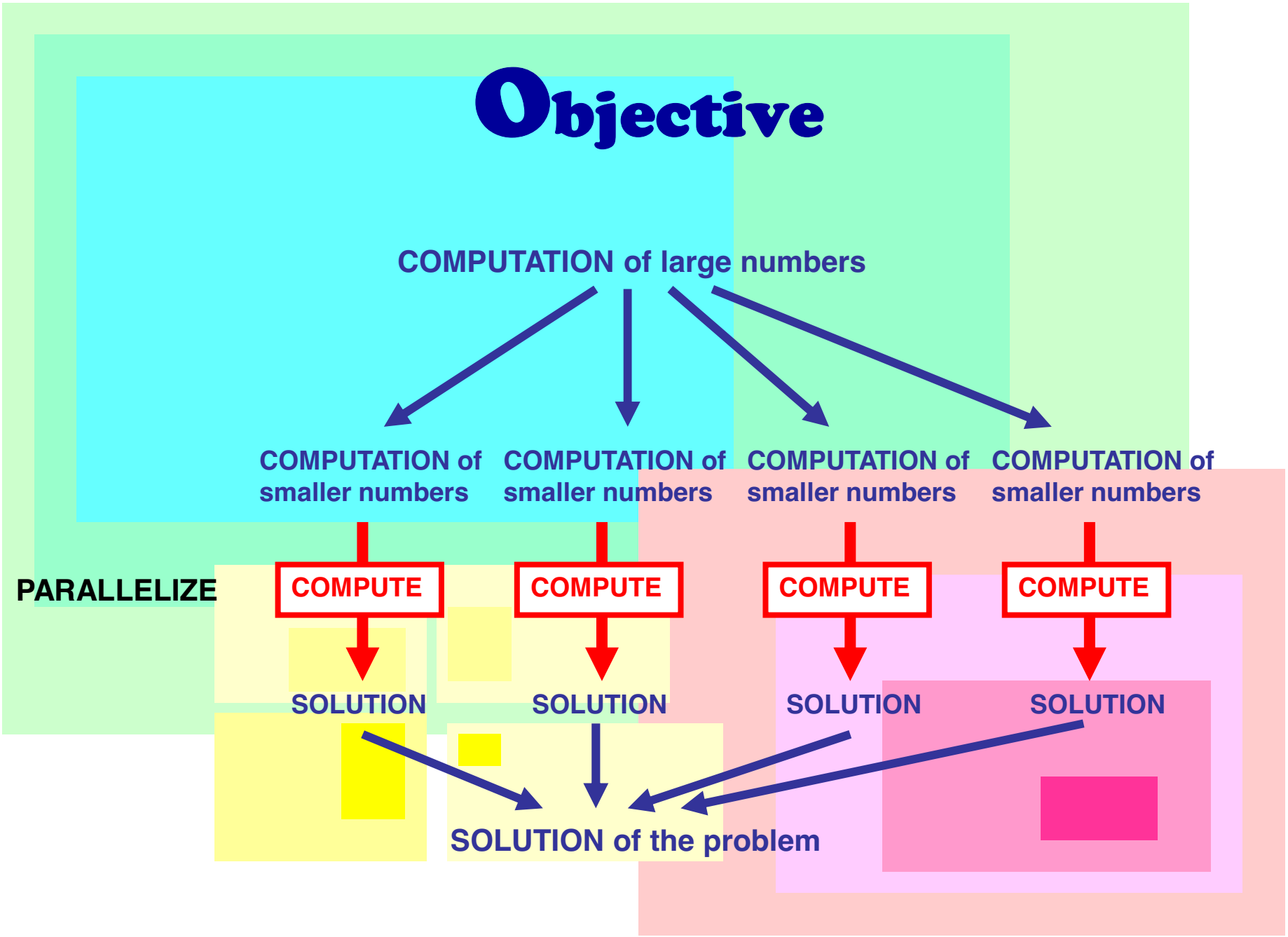
QUESTION 3: Find all solution of the equation
$7x + 21y + 35z = 8$.



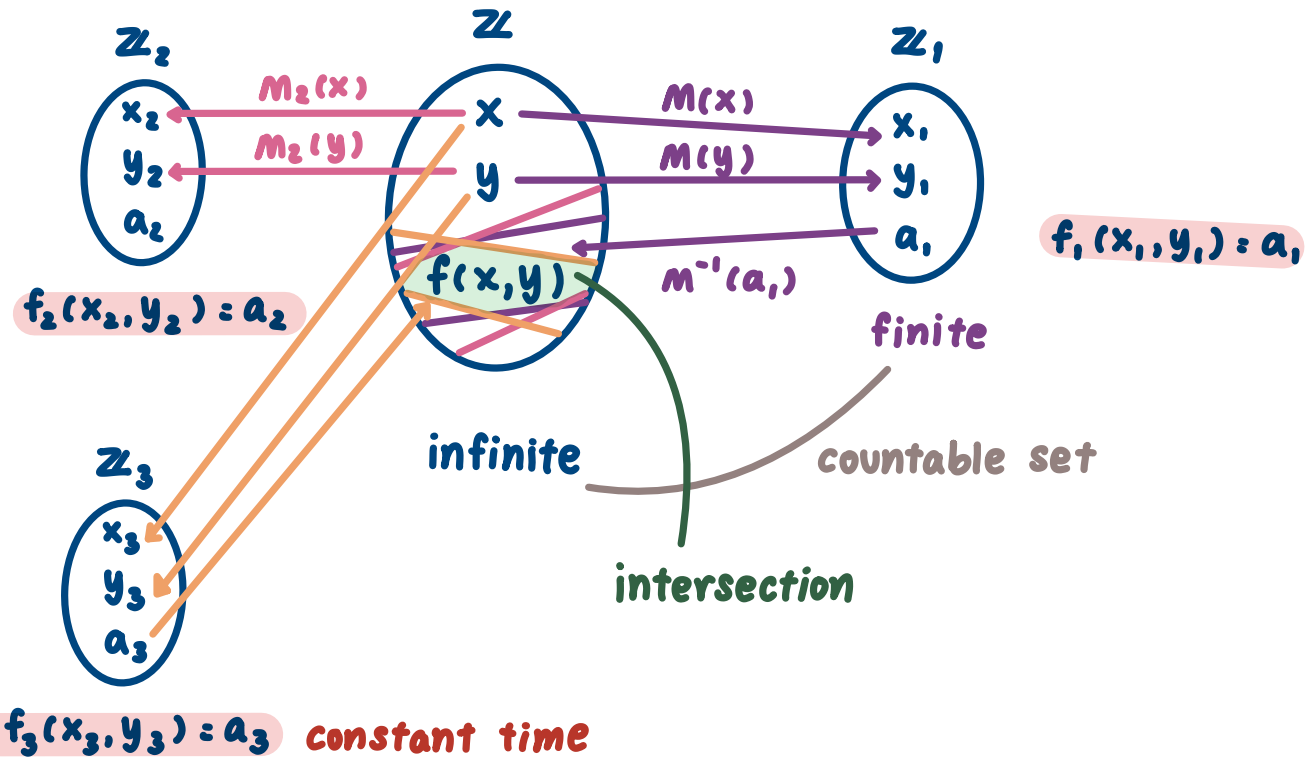
Contents

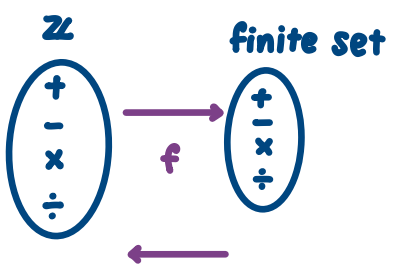
- Introduction
- Theory of Divisibility
- Diophantine Equations
- Theory of Congruence
- Prime number
- Computer Systems Design
- Cryptography & Information Security

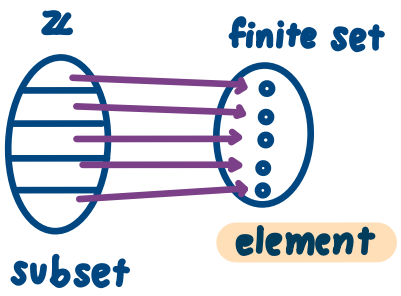
Objective

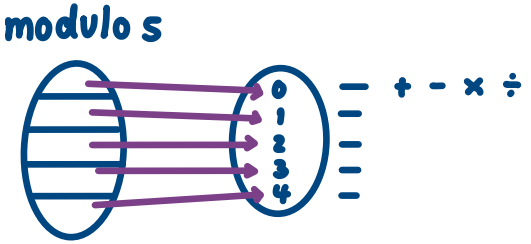

COMPUTATION of large numbers
COMPUTATION of smaller numbers
COMPUTATION of smaller numbers
COMPUTATION of smaller numbers
COMPUTATION of smaller numbers
PARALLELIZE
COMPUTE
COMPUTE
COMPUTE
COMPUTE
SOLUTION
SOLUTION
SOLUTION
SOLUTION
SOLUTION of the problem

$x, y \in \mathbb{Z}$ $f(x,y)$









Congruence modulo n

$\forall a,b \in \mathbb{Z}$, $a \equiv b \pmod{n}$

iff $a \bmod n = b \bmod n$

$(a-b) \bmod n = 0$

$n \mid (a-b) \Rightarrow \exists x \in \mathbb{Z}$ $nx = a-b$

Residue class $\{[0]_n, [1]_n, \ldots, [n-1]_n\}$

$[x]_n = \{y \in \mathbb{Z} \mid x = y \pmod{n}\}$

$a \rightarrow [a]_n$

$b \rightarrow [b]_n$

$a+b$ $\quad [a]_n +_n [b]_n = [c]_n$

a/b $\quad [a]_n \div_n [b]_n = [d]_n$

Class = $\{[0]_5, [1]_5, \ldots [5]_5\}$

$7 + 19 = 26$

$[2]_5 +_5 [4]_5 = [1]_5 = [2+4]_5 = [6]_5 = [1]_5$ (same set)

$$[a]_5 +_5 [b]_5 = [a+b]_5$$

$x \in [a]_5 \rightarrow x \equiv a \pmod 5$

$5 \mid (x-a) \quad \exists m \in \mathbb{Z} \quad 5m = x-a$

$y \in [b]_5 \rightarrow y \equiv b \pmod 5$

$5 \mid (y-b) \quad \exists p \in \mathbb{Z} \quad 5p = y-b$

$x+y \quad 5m+5p = (x+y)-(a+b)$

$5(m+p)$

$\therefore 5 \mid (x+y)-(a+b)$

$(x+y) \equiv (a+b) \pmod 5$

$\forall n \in \mathbb{Z}^+ \quad [a]_n +_n [b]_n = [a+b]_n$

$[a]_n -_n [b]_n = [a-b]_n$

$[a]_n \times_n [b]_n = [ab]_n$

n = prime $[a]_n \div_n [b]_n = [a]_n \times_n [c]_n$

$x \in a \quad n \mid (x-a)$

$y \in b \quad n \mid (y-b)$

$xy \quad nm_1 = x-a$

$nm_2 = y-b$

$x = nm_1 + a$

$y = nm_2 + b$

$xy = n(\ldots\ldots) + ab$

$n \mid (xy-ab)$

$[a]_n \div_n [b]_n = [a]_n \times_n [c]_n$

$[b]_n \times_n [c]_n = [1]_n$

$[bc]_n = [1]_n \Rightarrow n \mid (bc-1)$

$bc \equiv 1 \pmod n$

$[a]_n \times_n [1]_n = [a]_n$

$[a]_n +_n [0]_n = [a]_n$

Ex. $n=6 \quad 24 \div 8 \rightarrow 3$

$[0]_6 \div 6 \; [2]_6 = [\;]_6$

n = prime

~~$[2]_6 \times [c]_6 = [1]_6$~~

~~$6m = 2c-1$~~

~~$2c-6m = 1$ find c~~

$\gcd(2,6) = 1$ ×

Ex. $n=5 \quad [a]_5 \div_5 [2]_5 = [a]_5 \times [3]_5 = [3a]_5$

$[a]_5 \times_5 [2]_5^{-1}$

$[2]_5^{-1} = [c]_5 \times [2]_5 = [1]_5 \quad \therefore 5 \mid 1-2c$

$[2]_5 \times [3]_5 = [1]_5$ ✓

$5m = 1-2c$

$2c+5m = 1$

$c = 3$

$24 \rightarrow [4]_5 \div [3]_5$

$8 \quad [4]_5 \times [2]_5 = [3]_5$

$[a_1]_{n_1}, [a_2]_{n_2}, \ldots, [a_k]_{n_k}$ find x

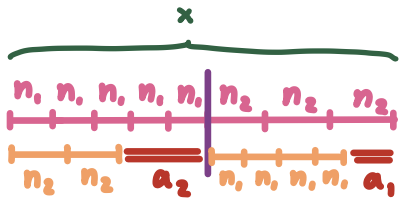
$x \equiv a_1 \pmod{n_1}$

$\equiv a_2 \pmod{n_2}$

$\vdots$

$\equiv a_k \pmod{n_k}$

Note



$b_1 n_1 = d_1 n_2 + a_2 \quad b_2 n_2 = d_2 n_2 + a_1$

$x = b_1 n_1 + b_2 n_2$ (known)

$x \equiv a_i \pmod{n_i} \quad (1 \le i \le k)$

Let $m_i = \prod_{\substack{j=1 \\ j \neq i}}^{k} n_j$

$m_1 = n_2 n_3 \ldots n_k$

$m_2 = n_1 n_3 \ldots n_k$

$\vdots$

$m_k = n_1 \ldots n_{k-1}$

$\gcd(n_i, n_j) = 1 \; ; \; \gcd(n_i, m_i) = 1 \; ; \; \gcd(n_i, m_j) = n_i \quad (i \neq j)$

$n_i \mid (x - a_i) \quad \exists r_i \in \mathbb{Z} \quad r_i n_i = x - a_i$

$\gcd(n_i, m_i) = 1 \quad \exists u_i, v_i \in \mathbb{Z} \quad u_i n_i + v_i m_i = 1$

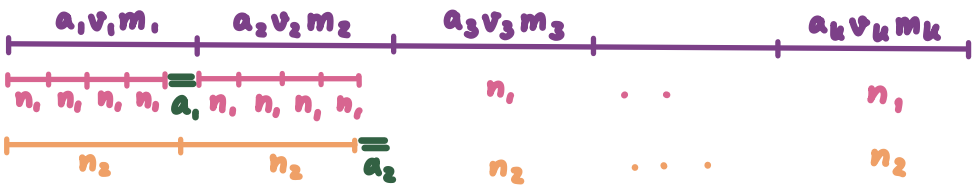
$v_i m_i - 1 = -u_i n_i$

$v_i m_i \equiv 1 \pmod{n_i}$

$a_i v_i m_i \equiv a_i \pmod{n_i}$

consider $a_i v_i m_i \bmod n_j = 0 \quad (j \neq i)$

$x = \sum_{i=1}^{k} a_i v_i m_i$



$x \equiv 2 \pmod 3$ | $n_1 = 3 \quad a_1 = 2$

$\equiv 4 \pmod 5$ | $n_2 = 5 \quad a_2 = 4$

$\equiv 1 \pmod 7$ | $n_3 = 7 \quad a_3 = 1$

find x

$m_1 = n_2 \times n_3 = 35$

$m_2 = n_1 \times n_3 = 21$

$m_3 = n_1 \times n_2 = 15$

Residue Number System (RNS)

$u_1 3 + v_1 35 = 1$ find $v_1 = 2$, $u_1 = -23$

$u_1 5 + v_1 21 = 1$ $v_2 = 1$, $u_2 = -4$

$u_1 7 + v_3 15 = 1$ $v_3 = 1$, $u_3 = -2$

$x = 2 \times 2 \times 35 + 4 \times 1 \times 21 + 1 \times 1 \times 15 = 239$

(CRT) Chinese Remainder Theorem

$x \equiv a_i \pmod{m_i} \quad \forall i = 1, \dots, k$

x_1, x_2 solution $\quad x_1 \equiv a_i \pmod{m_i}$

$x_2 \equiv a_i \pmod{m_i}$

$x_1 \equiv x_2 \pmod{m_i}$

$m_1 \mid (x_1 - x_2)$

$\exists z_1 \in \mathbb{Z},\ m_1 z_1 = x_1 - x_2$

$m_2 \mid (x_1 - x_2)$

$\exists z_2 \in \mathbb{Z},\ m_2 z_2 = x_1 - x_2$

$m_1 z_1 = m_2 z_2$

$\gcd(m_1, m_2) = 1$

$m_2 \mid m_1 z_1 \wedge \gcd(m_1, m_2) = 1 \quad \therefore m_2 \mid z_1$

$\exists c_2 \in \mathbb{Z} \quad m_2 c_2 = z_1$

$x_1 - x_2 = m_1 z_1 = m_1 m_2 c_2$

$m_3 \mid (x_1 - x_2) \quad x_1 - x_2 = m_1 m_2 m_3 c_3$

$M = \prod_{i=1}^{k} m_i \quad \therefore x_1 - x_2 = M c_k \ ; \ c_k \in \mathbb{Z}$

$M \mid (x_1 - x_2)$

$x_1 \equiv x_2 \pmod{M}$

$$\left.\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\equiv a_2 \pmod{m_2} \\ &\vdots \\ &\equiv a_k \pmod{m_k} \end{aligned}\right\} \text{find } x \in \mathbb{Z}$$

$$\begin{array}{r} 17 \\ +\ 38 \\ \hline x = 55 \end{array}$$

	mod 3	5	7
17 →	2	2	3
38 →	2	3	3
	$[2]_3 + [2]_3$		
	$[1]_3$	$[0]_5$	$[6]_7$

$x \equiv 1 \pmod 3$ $\quad a_1 = 1,\ n_1 = 3 \quad m_1 = n_2 \times n_3 = 35$

$\equiv 0 \pmod 5$ $\quad a_2 = 0,\ n_2 = 5 \quad m_2 = n_1 \times n_3 = 21$

$\equiv 6 \pmod 7$ $\quad a_3 = 6,\ n_3 = 7 \quad m_3 = n_1 \times n_2 = 15$

$u_1 3 + v_1 35 = 1$ $\quad$ find $v_1 = 2$

$u_2 5 + v_2 21 = 1$ $\quad v_2 = 1$

$u_3 7 + v_3 15 = 1$ $\quad v_3 = 1$

$$x = \sum_{i=1}^{k} a_i v_i m_i = 1 \times 2 \times 35 + 0 \times 1 \times 21 + 6 \times 1 \times 15$$

$$= 70 + 90 = 160$$

$n_1 \times n_2 \times n_3 = 3 \times 5 \times 7 = 105$

$x_1 = 55$) 105

$x_2 = 160$)

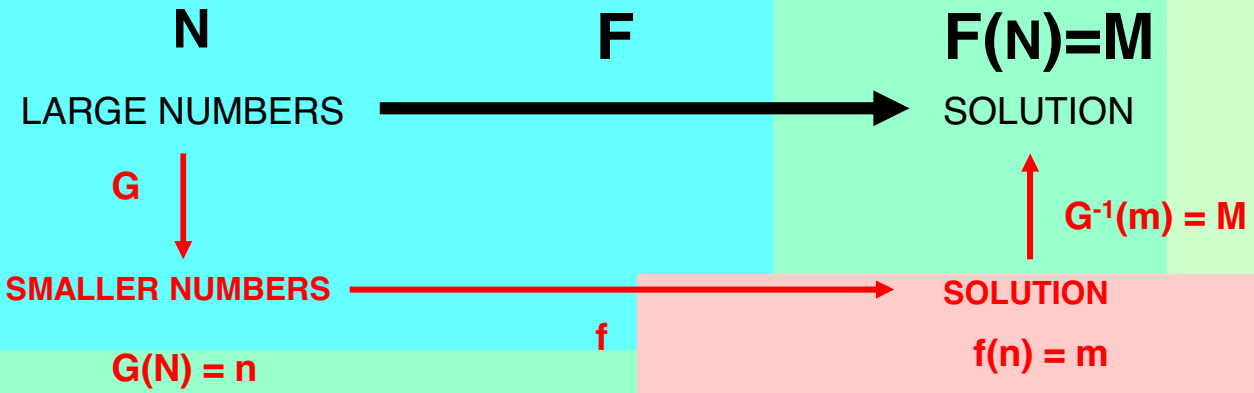
$x_3 = 265$

$\vdots$

$x \bmod M = \text{solution}$ → $0 \ldots M-1$

Theory of congruence

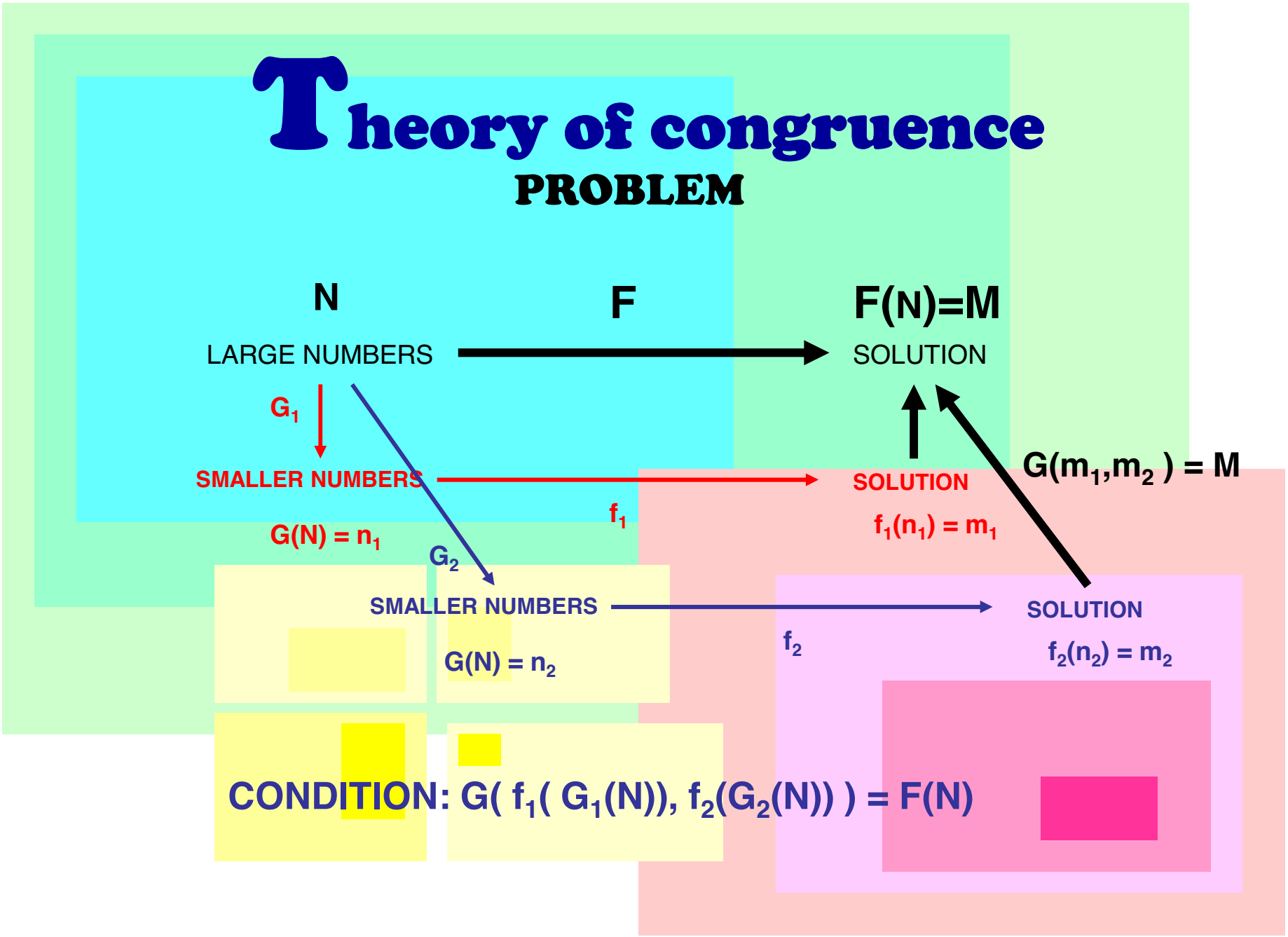
PROBLEM



CONDITION: $G^{-1}(f(G(N))) = F(N)$

Theory of congruence

PROBLEM



Theory of congruence

Definition

Let a be an integer.

Let n be a positive integer.

"**a mod n**" to be the remainder r, when a is divided by n.

That is $r = a \bmod n = a - \lfloor a/n \rfloor n$.

The **relation** from **a** to **b** is defined,

"**a congruent to b modulo n**" , denoted by **$a \equiv b \pmod n$**,

if n is a divisor of a-b, or equivalently,

if n | (a-b).

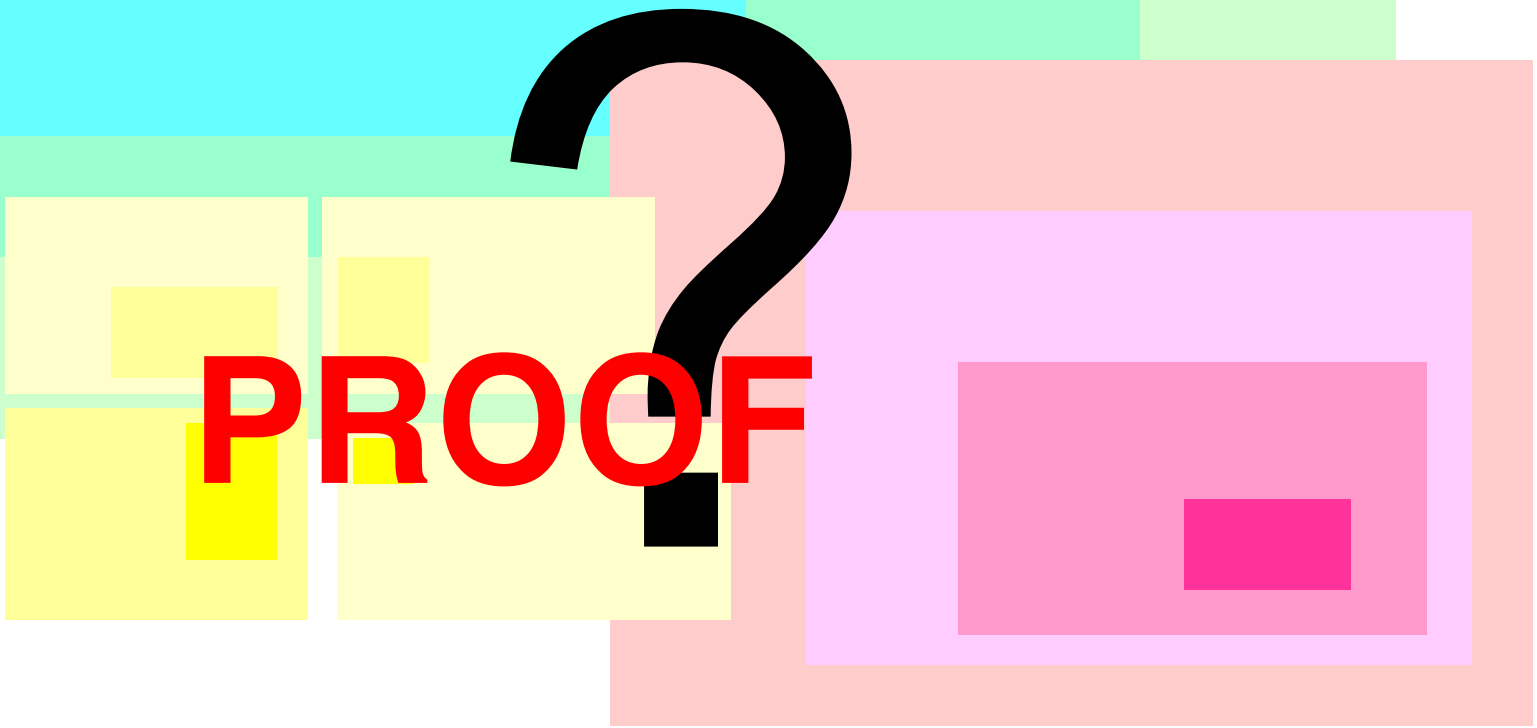
aRb iff $a \equiv b \pmod n$

Theory of congruence

Theorem

Let n be a positive integer.

The congruence modulo n is **reflexive**, **symmetric**, and **transitive**.



Theory of congruence

Definition

If $x \equiv a \pmod{n}$, then **a** is called a **residue of x modulo n**.

The residue class of a mod n,
denoted by $[a]_n$ is the set of all those integers
that are congruent to **a modulo n**.

That is

$$[a]_n = \{ x \mid x \in \mathbb{Z} \text{ and } x \equiv a \pmod{n} \}$$

$$= \{ a + kn \mid k \in \mathbb{Z} \}$$

Theory of congruence

Definition

If $x \equiv a \pmod{n}$ and $0 \le a \le n-1$, then
a is called **the least (nonnegative) residue** of x modulo n.

The set of all residue classes modulo n,
often denoted by $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$, is

$$\mathbb{Z}/n\mathbb{Z} = \{ [a]_n \mid 0 \le a \le n-1 \}.$$

EXAMPLE

$-a < 0$ is in $[n-a]_n$, provided $n \ge a$, since $-a \equiv n-a \pmod{n}$.

Theory of congruence

Define a function G from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ as follow: $G(a) = [a]_n$.

The computational problem in $\mathbb{Z}$ must be transferred into $\mathbb{Z}/n\mathbb{Z}$.

Define arithmetic operators in $\mathbb{Z}/n\mathbb{Z}$.

For any $[a]_n$ and $[b]_n$ in $\mathbb{Z}/n\mathbb{Z}$,

$$[a]_n +_n [b]_n = [a+b]_n$$

Example:

Compute x + y

Suppose that $G(x) = [a]_n$: $x \equiv a \pmod n$

and suppose that $G(y) = [b]_n$: $y \equiv b \pmod n$

Addition of G(x) and G(y) can be computed by $[a]_n +_n [b]_n = [a+b]_n$ which is equal to G(x+y).

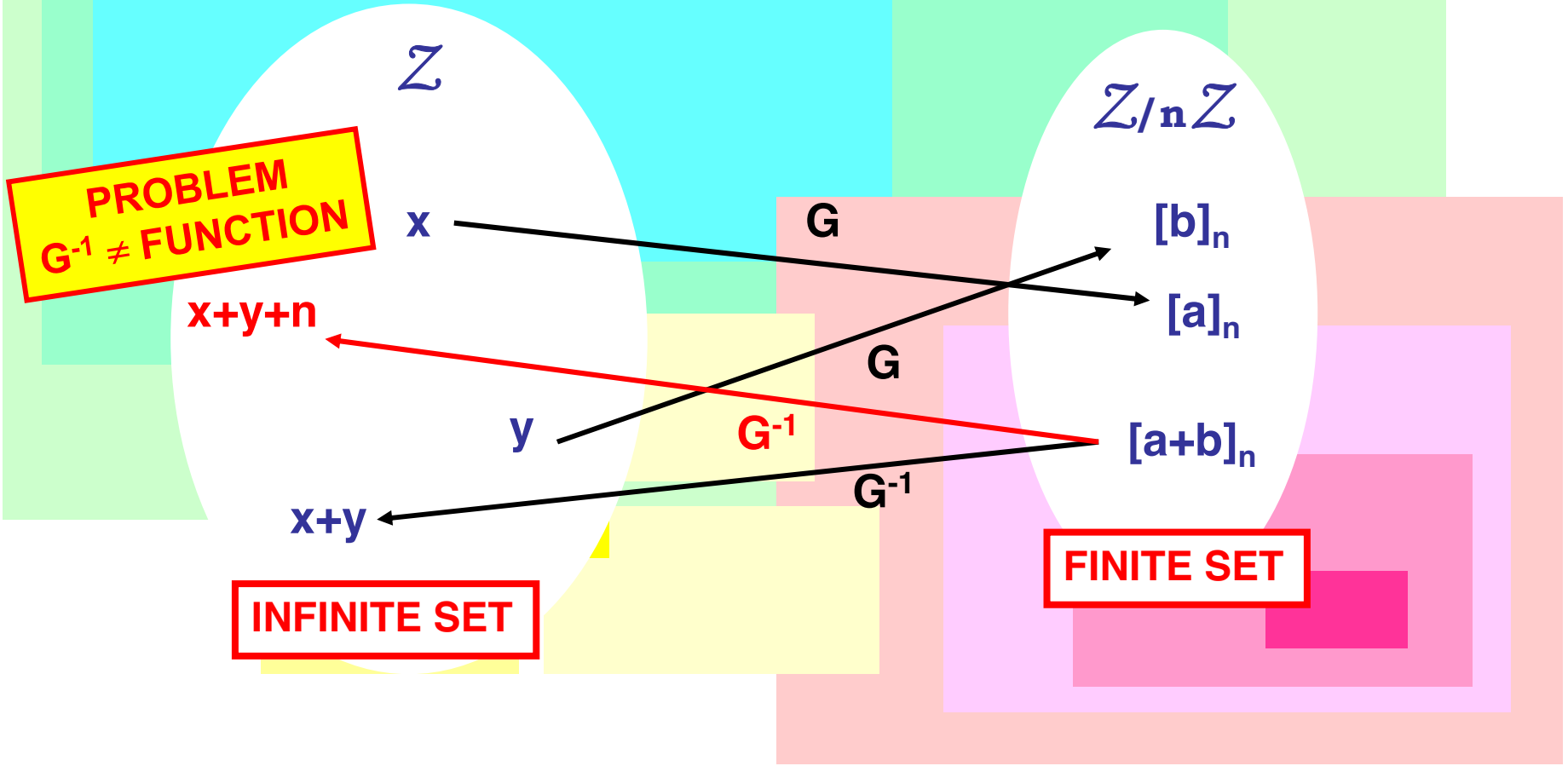
Since $(x + y) \equiv (a + b) \pmod n$.

Theory of congruence

EXAMPLE

OBJECTIVE: TO COMPUTE x + y

COMPUTE $[a]_n +_n [b]_n$



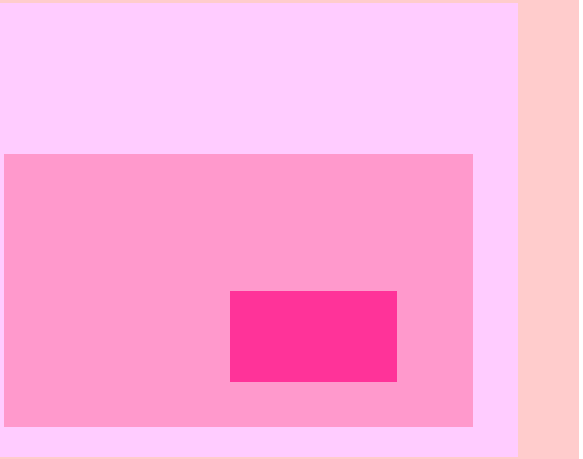
Theory of congruence

For any $[a]_n$ and $[b]_n$ in $\mathcal{Z}/n\mathcal{Z}$,

$$[a]_n +_n [b]_n = [a+b]_n$$
$$[a]_n -_n [b]_n = [a-b]_n$$
$$[a]_n \times_n [b]_n = [a \times b]_n$$

Problem,

$[a]_n \div_n [b]_n$ = ?



Theory of congruence

How to define the division operator?

In fact, the division is the inverse function of the multiplication.

In order to compute $[a]_n \div_n [b]_n$, we have to answer the question $[a]_n \times_n [b]_n^{-1}$, where $[b]_n^{-1}$ means the multiplicative inverse of $[b]_n$.

Definition

The **multiplicative inverse of $[b]_n$**, denoted by **$[b]_n^{-1}$**, is defined as $[b]_n \times_n [b]_n^{-1} = [1]_n$, where $[1]_n$ is the multiplicative identification.

The **multiplicative identification** : $[a]_n \times_n [1]_n = [a]_n$.

Theory of congruence

EXAMPLE

Consider the system $\mathbb{Z}/5\mathbb{Z} = \{ [0]_5, [1]_5, [2]_5, [3]_5, [4]_5 \}$.
Find the multiplicative inverse of $[3]_5$.

Solution:
Let $[x]_5$ be the multiplicative inverse of $[3]_5$.
By the definition, $[3]_5 \times [x]_5 = [1]_5$.
But $[3]_5 \times [x]_5 = [3x]_5$, it is obtained that $[3x]_5 = [1]_5$.
That is

$3x \equiv 1 \pmod 5$ **CONGRUENT EQUATION**
$5 \mid (3x - 1)$

Then $\exists y \in \mathbb{Z}$, such that $5y = 3x - 1$, find the value of x.
The problem becomes

$3x - 5y = 1$ [**BILINEAR DIOPHANTINE**]

Theory of congruence

EXAMPLE

Consider the system $\mathbb{Z}/5\mathbb{Z} = \{ [0]_5, [1]_5, [2]_5, [3]_5, [4]_5 \}$.
Find the multiplicative inverse of $[3]_5$.

Solution:
The problem becomes

$$3x - 5y = 1$$ [BILINEAR DIOPHANTINE]

The solution is $x = 2$.

VERIFICATION: $[3]_5 \times [2]_5 = [6]_5 = [1]_5$.

Theory of congruence

EXAMPLE

Consider the system $\mathbb{Z}/6\mathbb{Z} = \{ [0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6 \}$.
Find the multiplicative inverse of $[2]_6$.

Solution:
The problem becomes

$$2x - 6y = 1$$ [BILINEAR DIOPHANTINE]

NO INTEGRAL SOLUTION !!!!

EXAMINE: The equation **ax – ny = 1** has the solution only if **gcd(a,n) is 1**.
n is the base of the system,
a can be 1, 2, 3, …, n-1 (the residue).

Then **n** must be **prime**.

Note that $a \neq 0$ because the multiplicative inverse of 0 is not defined.

Theory of congruence

EXAMPLE

Consider the system $\mathbb{Z}/5\mathbb{Z} = \{ [0]_5, [1]_5, [2]_5, [3]_5, [4]_5 \}$.

The multiplicative inverse of $[1]_5$ is $\mathbf{[1]_5}$.

The multiplicative inverse of $[2]_5$ is $\mathbf{[3]_5}$.

The multiplicative inverse of $[3]_5$ is $\mathbf{[2]_5}$.

The multiplicative inverse of $[4]_5$ is $\mathbf{[4]_5}$.

EXAMPLE: $[2]_5 \div_5 [3]_5 = [2]_5 \times_5 [3]_5^{-1}$

$= [2]_5 \times_5 [2]_5$

$= [4]_5$.

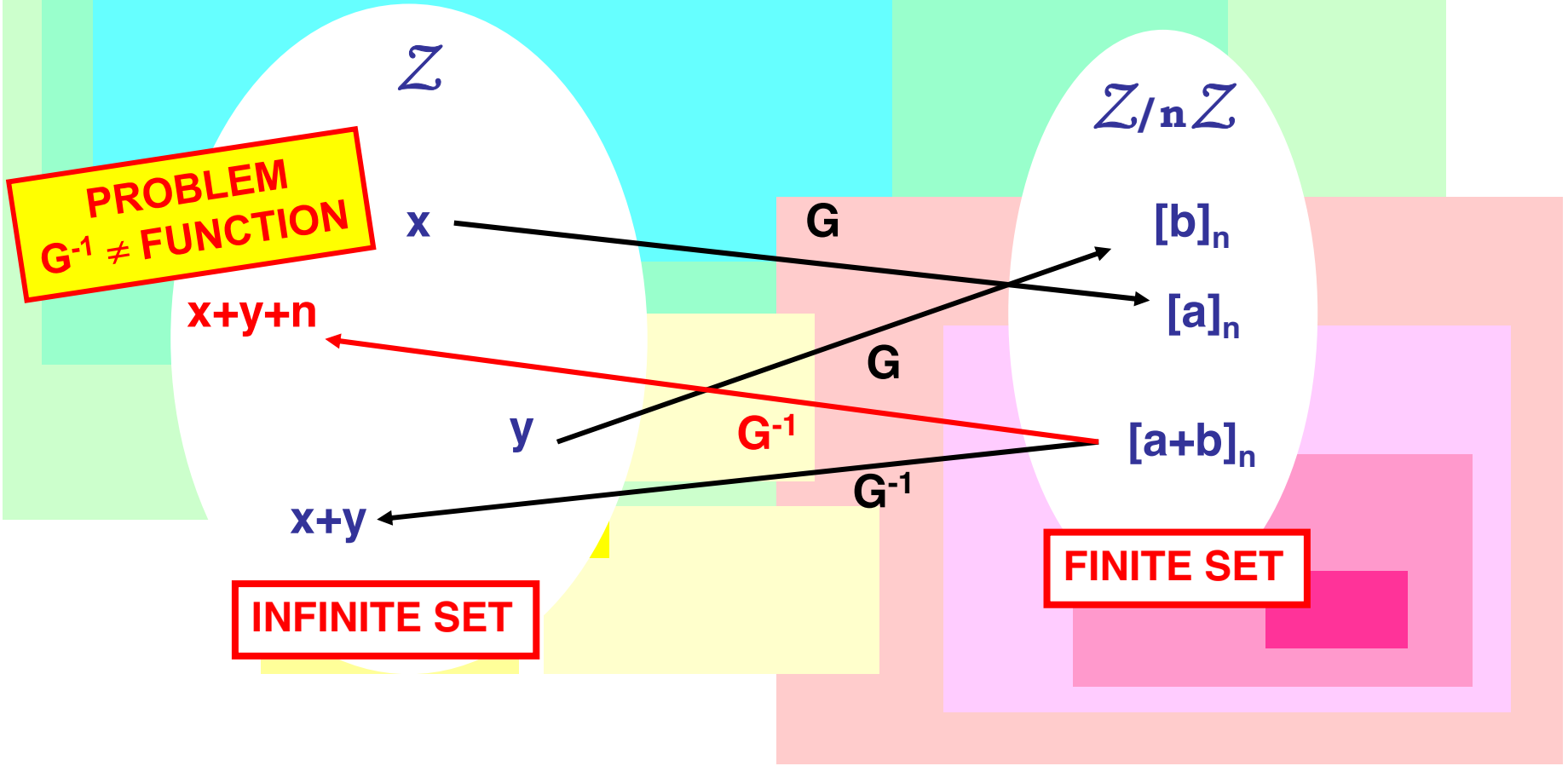
For instance, 42 ÷ 3 = 14.

Theory of congruence

EXAMPLE

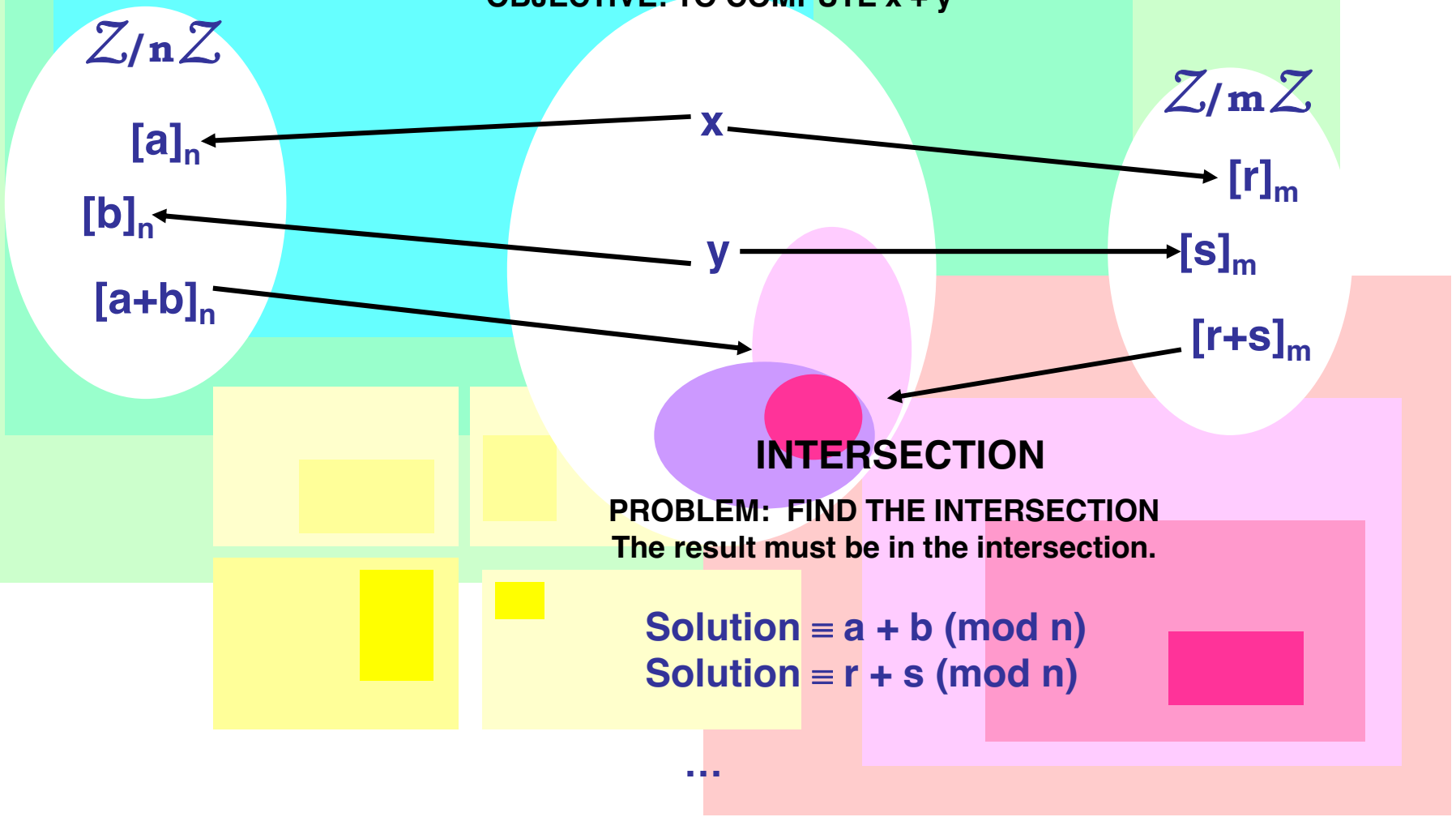
OBJECTIVE: TO COMPUTE x + y

COMPUTE $[a]_n +_n [b]_n$



Theory of congruence

OBJECTIVE: TO COMPUTE x + y



INTERSECTION

PROBLEM: FIND THE INTERSECTION
The result must be in the intersection.

Solution ≡ a + b (mod n)
Solution ≡ r + s (mod n)

…

Theory of congruence

CHINESE REMAINDER THEOREM

If $m_1, m_2, \ldots, m_k$ are pairwise relatively prime and greater than 1,
$a_1, a_2, \ldots, a_k$ are any integers,

then there is an integral solution x to the following simultaneous congruence:

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\ldots$$
$$x \equiv a_k \pmod{m_k}.$$

?

PROOF

If x and x' are two solutions, $x \equiv x' \pmod{M}$ where $M = m_1 m_2 \ldots m_k$.

Theory of congruence

CHINESE REMAINDER THEOREM

EXAMPLE

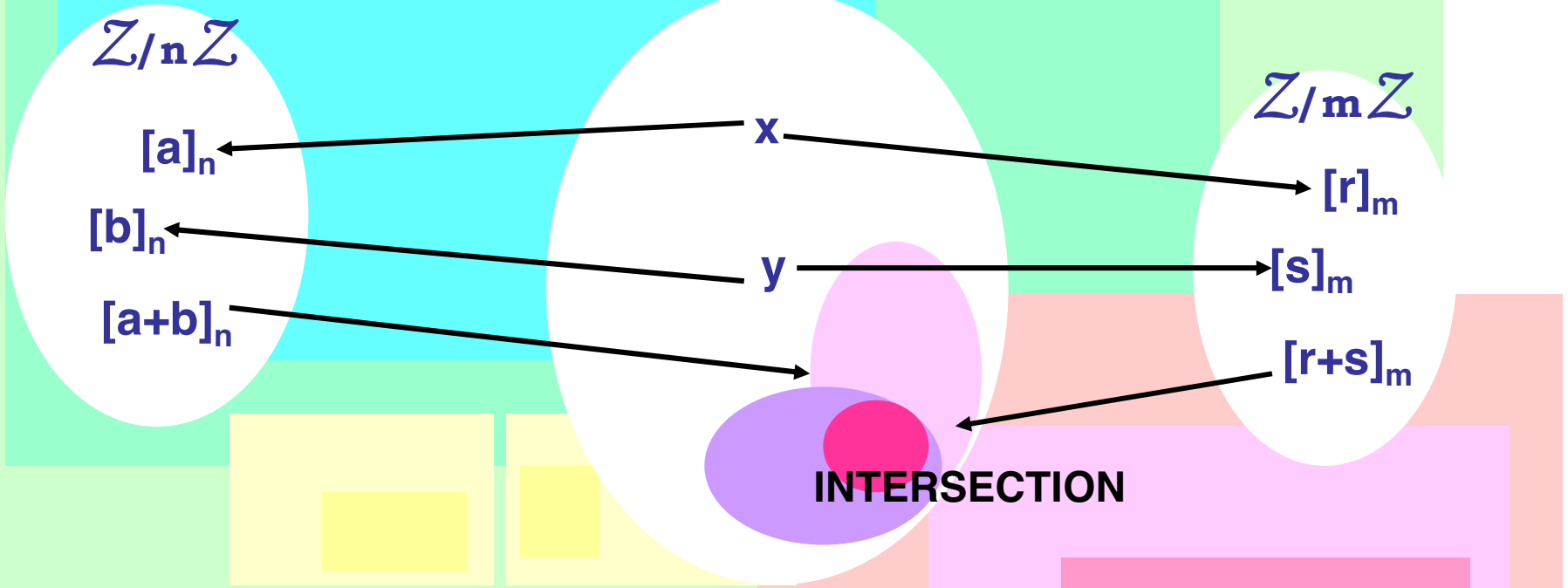
Consider the problem,

$x \equiv 2 \pmod 3$,
$x \equiv 3 \pmod 5$,
$x \equiv 2 \pmod 7$.

We have $M = m_1 m_2 m_3 = 3 \times 5 \times 7 = 105$,
$M_1 = m_2 m_3 = 35$,
$M'_1 = M_1^{-1} \pmod{m_1} = 35^{-1} \pmod 3 = 2$,
$M_2 = m_1 m_3 = 21$,
$M'_2 = M_2^{-1} \pmod{m_2} = 21^{-1} \pmod 5 = 1$,
$M_3 = m_1 m_2 = 15$,
$M'_3 = M_3^{-1} \pmod{m_3} = 15^{-1} \pmod 7 = 1$.

$x = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \pmod{105} = \mathbf{23}$.

Theory of congruence



RESIDUE NUMBER SYSTEM: RNS

Contents

- Introduction
- Theory of Divisibility
- Diophantine Equations
- Theory of Congruence
- Prime number
- Computer Systems Design
- Cryptography & Information Security

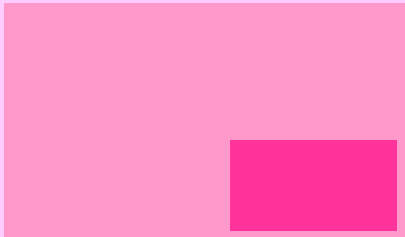
Prime

Fermat's Little Theorem

Let a be a positive integer.
Let p be a prime number.
if gcd(a,p) = 1, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

PROOF



The converse of the theorem

Let n be an odd positive integer.
If gcd(a,n) = 1 and $a^{n-1} \not\equiv 1 \pmod{n}$.
Then n is composite.

Prime

Euler's Theorem

Let a and n be positive integers with gcd(a,n) = 1.

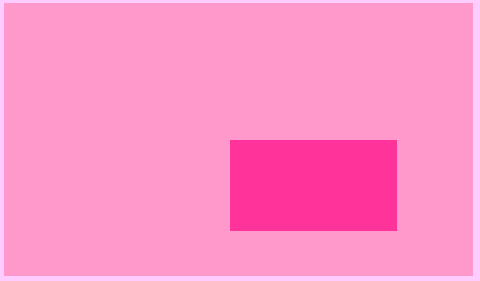
Then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Definition

Let n be a positive integer.
Euler's function, denoted by ϕ-function,
$\phi(n)$ is defined to be the number of positive integers $k < n$
which are relatively prime to n:

$$\phi(n) = \sum_{(1 \le k < n,\ \gcd(k,n) = 1)} 1.$$



Prime

Carmichael's Theorem

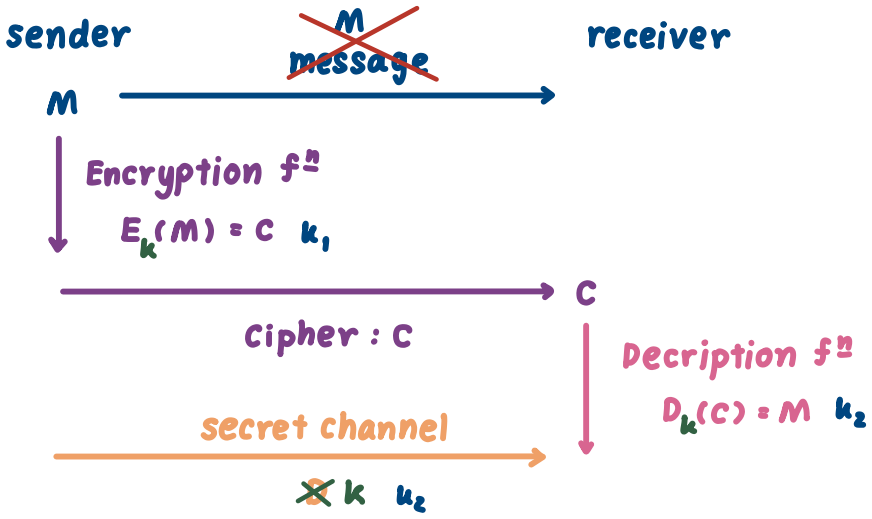
Let a and n be positive integers with gcd(a,n) = 1.
Then

$$a^{\lambda(n)} \equiv 1 \pmod{n}.$$

Definition

Let n be a positive integer.
Carmichael's λ-function, λ(n) is defined as follows

$\lambda(n) = \phi(n)$ if n is a prime.
$\lambda(p^u) = \phi(p^u)$ for $p = 2$ and $u \leq 2$
and for $p \geq 3$.
$\lambda(2^u) = \phi(2^u)/2$ for $u \geq 3$
$\lambda(n) = \text{lcm}(\lambda(p_1^{u1}), \lambda(p_2^{u2}), \ldots, \lambda(p_k^{uk}))$,
with $n = p_1^{u1}p_2^{u2}\ldots p_k^{uk}$ (prime factorization form).



M : message ⟶ C : Cipher

one-way f^n

"prime"

Merserme : $2^p - 1 = M_p$ (p = prime) ✗

Fermat : $2^{2^n} + 1 = F_n$ $(n = 0, 1, 2, \ldots)$

✗ $2^{2^{31}} + 1$

Fermat's little Theorem

$\forall a \in \mathbb{Z}^+$, p = prime, $\gcd(a,p) = 1$

$$a^{p-1} \equiv 1 \pmod{p}$$

Euler's Theorem

$n \in \mathbb{Z}^+$

$\gcd(a,n) = 1$

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

$$\phi(n) = \sum_{i=1}^{n-1} 1 \quad \gcd(n,i) = 1$$

$$\phi(p^n) = p^n \cdot p^{n-1}$$

$$\phi(n)\phi(m) = \phi(nm) \quad \gcd(n,m) = 1$$

Carmichael's Theorem

$$a^{\lambda(n)} \equiv 1 \pmod{n}$$

$\lambda(n) = \phi(n)$; n = prime

$\lambda(p^u) = \phi(p^u)$; $p = 2, u \leq 2 \;/\; p \geq 3$

$\lambda(2^u) = \phi(2^u)/2$; $u \geq 3$

$\lambda(n) = \mathrm{lcm}(\lambda(p_1^{u_1}), \lambda(p_2^{u_2}), \ldots, \lambda(p_u^{u_u}))$

$n = p_1^{u_1} p_2^{u_2} \ldots p_u^{u_u}$

$a^{\lambda(n)} \equiv 1 \pmod{n}$

$a^{\lambda(n)+1} \equiv a \pmod{n}$

$xy \bmod n = ((x \bmod n)\, y) \bmod n$

a^{uv}

$M^u \bmod n = C$ "RSA"

$C^v \bmod n = M$

Sender — Public-key u, C — Receiver (กำหนด key)

M → key 1 → $M^u \bmod n$ ⟶ M → key 2 → $C^v \bmod n = M$

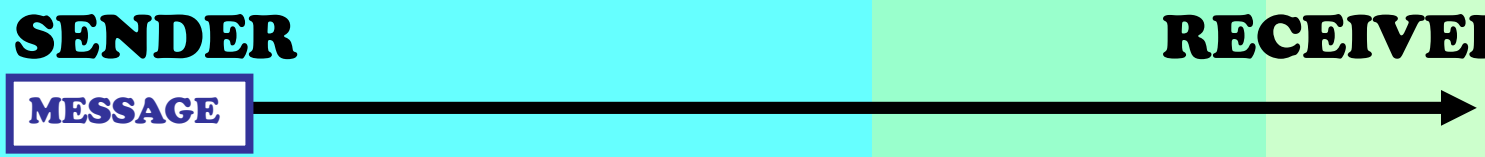
$uv = \lambda(n) + 1$

$a^{\lambda(n)} \equiv 1 \pmod{n}$

$a^{s\lambda(n)} \equiv 1 \pmod{n}$

"ISBN"

Cryptography



M = Message
C = Cipher texts
$C = E_k(M)$
k = Key
E_k = Encrypt function

Cryptography

M = Message
C = Cipher texts
$C = E_k(M)$
k = Key
E_k = Encrypt function

M = Message
C = Cipher texts
$C = E_k(M)$
k = Key
E_k = Encrypt function

CRYPTOGRAPHY FUNCTION

Encryption function: $C = E_k(M)$ and
Decryption function: $M = E_k(C)$

This implies that $M = E_k(E_k(M))$ = identity function.

Cryptography

SENDER **RECEIVER**

CIPHER

M = Message
C = Cipher texts
$C = E_k(M)$
k = Key
E_k = Encrypt function

M = Message
C = Cipher texts
$C = E_k(M)$
k = Key
E_k = Encrypt function

Stream (bit) ciphers

Let k = Random string
M = Message
C = Ciphertexts

- Encryption algorithm = $M \oplus k \rightarrow C$
- Decryption algorithm = $C \oplus k \rightarrow M$.

Cryptography

SENDER **RECEIVER**

CIPHER

M = Message
C = Cipher texts
$C = E_k(M)$
k = Key
E_k = Encrypt function

M = Message
C = Cipher texts
$C = E_k(M)$
k = Key
E_k = Encrypt function

Monographic (character) ciphers

Encryption algorithm: $C \equiv M + k \pmod{26}$, where $0 \leq M < 26$
Decryption algorithm: $M \equiv C - k \pmod{26}$, where $0 \leq C < 26$

Cryptography

SENDER **RECEIVER**

CIPHER

M = Message
C = Cipher texts
$C = E_k(M)$
k = Key
E_k = Encrypt function

M = Message
C = Cipher texts
$C = E_k(M)$
k = Key
E_k = Encrypt function

GENERATE KEY

KEY

SECRET KEY CRYPTOGRAPHY

NEED SECRET CHANNEL

Cryptography

PUBLIC KEY CRYPTOGRAPHY

RSA

SENDER → **RECEIVER**

M = Message
C = Cipher texts
$C = E_k(M)$
k = Key
E_k = Encrypt function

M = Message
C = Cipher texts
$C = E_k(M)$
k = Key
E_k = Encrypt function

CRYPTOGRAPHY FUNCTION

$M = E_k(E_k(M))$ = identity function

Asymmetric keys: α and β

$M = E_\alpha(E_\beta(M))$

Candidate function: $M = M^x \bmod N$

Cryptography

PUBLIC KEY CRYPTOGRAPHY

RSA

SENDER → **RECEIVER**

M = Message
C = Cipher texts
$C = E_k(M)$
k = Key
E_k = Encrypt function

M = Message
C = Cipher texts
$C = E_k(M)$
k = Key
E_k = Encrypt function

Candidate function: $M = M^x \bmod N$

$$a^{\lambda(n)} \equiv 1 \pmod{n}$$

$$a^{\lambda(n)+1} \equiv a \pmod{n}$$

$a^x \bmod n = a$ where $x = \lambda(n)+1$ and $a < n$ and **n is not prime**

$a = a^x \bmod n = (a^\alpha \bmod n)^\beta \bmod n$ where $x = \alpha\beta$

Encrypt:$E_{\alpha,n} = M^\alpha \bmod n$ and Decrypt:$E_{\beta,n}(C) = C^\beta \bmod n$

Cryptography

PUBLIC KEY CRYPTOGRAPHY

RSA

SENDER → **RECEIVER**

M = Message
C = Cipher texts
$C = E_{\alpha,n}(M)$
$E_{\alpha,n}$ = Encrypt function

M = Message
C = Cipher texts
$C = E_{\beta,n}(M)$
$E_{\beta,n}$ = Encrypt function

Candidate function: $M = M^x \bmod N$

Encrypt:$E_\alpha = M^\alpha \bmod n$ and Decrypt:$E_\beta(C) = C^\beta \bmod n$

$\lambda(n)+1 = x = \alpha\beta$

Public-keys: n and α, Secrete-key: β

Introduce an unknown variable K: $(\lambda(n) \times K)+1 = \alpha\beta$

Because $a^{\lambda(n)K} \equiv 1 \pmod n$.

Cryptography

PUBLIC KEY CRYPTOGRAPHY

RSA

GENERATE KEY

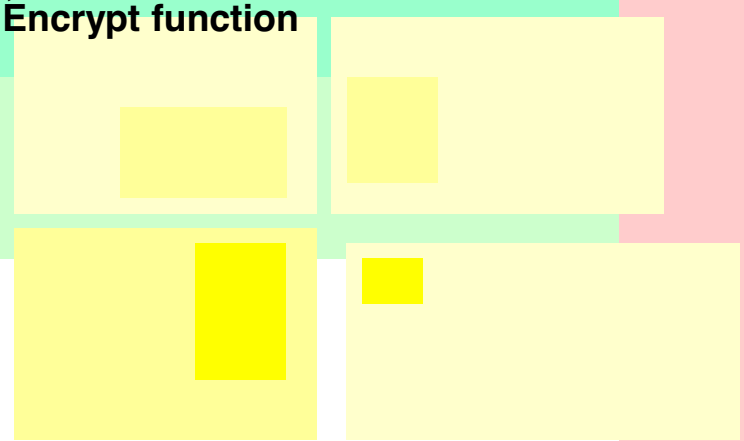
SENDER

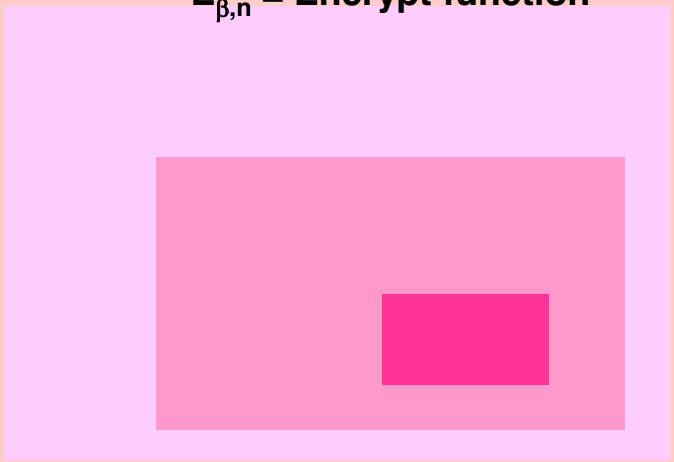
RECEIVER

KEY: n and α

M = Message
C = Cipher texts
$C = E_{\alpha,n}(M)$
$E_{\alpha,n}$ = Encrypt function

M = Message
C = Cipher texts
$C = E_{\beta,n}(M)$
$E_{\beta,n}$ = Encrypt function





Cryptography

PUBLIC KEY CRYPTOGRAPHY

RSA

GENERATE KEY

SENDER

RECEIVER

MESSAGE

M = Message
C = Cipher texts
$C = E_{\alpha,n}(M)$
$E_{\alpha,n}$ = Encrypt function

M = Message
C = Cipher texts
$C = E_{\beta,n}(M)$
$E_{\beta,n}$ = Encrypt function

Cryptography

PUBLIC KEY CRYPTOGRAPHY

RSA

GENERATE KEY

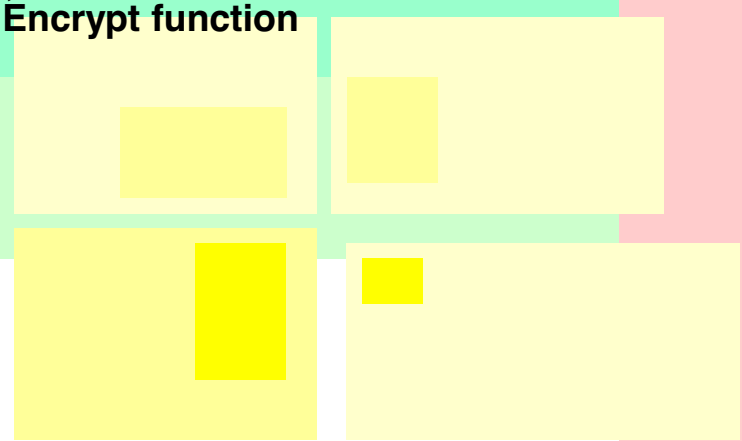
SENDER

RECEIVER

CIPHER

M = Message
C = Cipher texts
$C = E_{\alpha,n}(M)$
$E_{\alpha,n}$ = Encrypt function

M = Message
C = Cipher texts
$C = E_{\beta,n}(M)$
$E_{\beta,n}$ = Encrypt function



Cryptography

PUBLIC KEY CRYPTOGRAPHY

RSA

GENERATE KEY

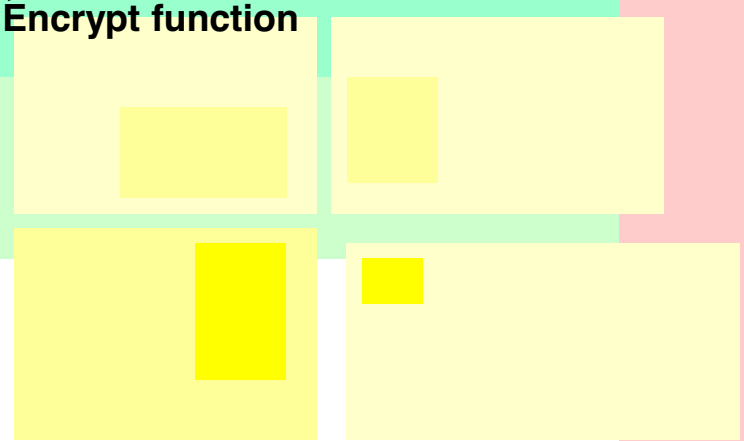
SENDER

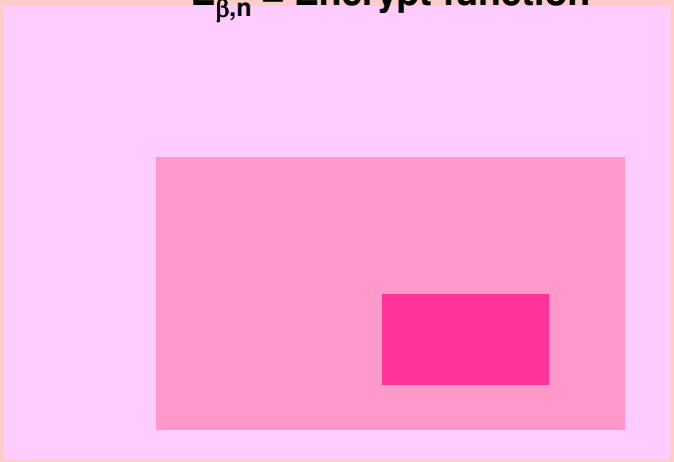
RECEIVER

MESSAGE

M = Message
C = Cipher texts
$C = E_{\alpha,n}(M)$
$E_{\alpha,n}$ = Encrypt function

M = Message
C = Cipher texts
$C = E_{\beta,n}(M)$
$E_{\beta,n}$ = Encrypt function





Cryptography

PUBLIC KEY CRYPTOGRAPHY

RSA

Example

The first step is to select two prime numbers.

$p = 47$ and $q = 71$ are two primes.

The second step is to compute: $n = 47 \times 71 = 3337$.

$\lambda(3337) = \text{lcm}(46,70) = 3220$.

The third step is to determine the public-key and private key:

We try to factorize $K\lambda(3220)+1$ for $K = 1, 2, 3, \ldots$ until we find a "good" factorization that can be used to obtain suitable *k* and *k'*.

for $K = 25$, $25\lambda(3220)+1 = 80501 = 79 \times 1019$

and $1019 = (79)^{-1} \bmod 3220$.

Then $\alpha = 79$ and $\beta = 1019$.

Note: **The public key is n = 3337**

The public-key is $\alpha = 79$

The private-key is $\beta = 1019$

The end