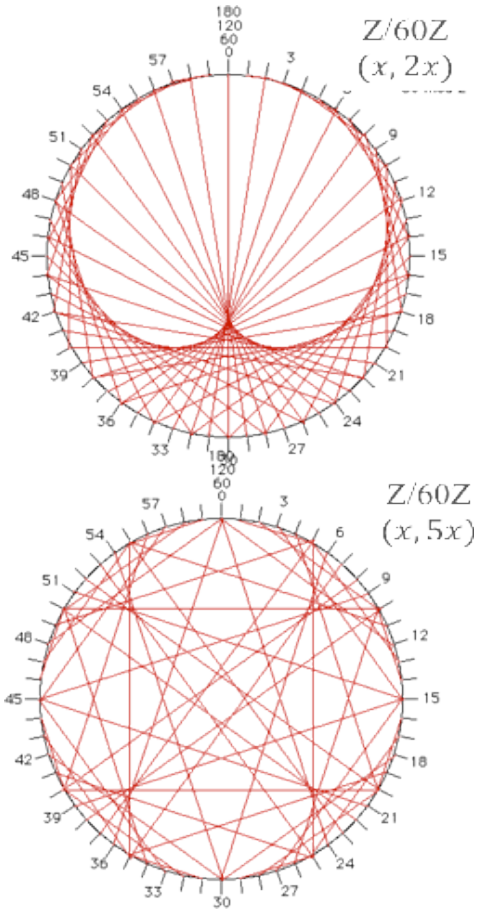
Week 7: Modular Arithmetic (Textbook Chapter 8)



Prof. Michael Gastpar

Slides by Prof. M. Gastpar and Prof. em. B. Rimoldi

EPFL

Spring Semester 2025

Outline

Introduction and Organization

Entropy and Data Compression

Cryptography

One-Time Pad, Perfect Secrecy, Public-Key (Diffie-Hellman)

Rudiments of Number Theory

Modular Arithmetic

Commutative Groups

Public-Key Cryptography

Summary of Chapter 2

Channel Coding

LAST WEEK

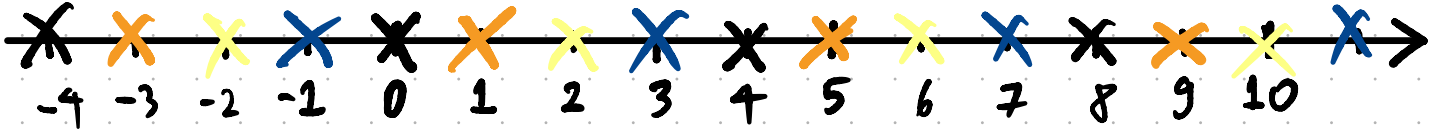
- MODULO RULES

$$(a + b) \bmod m = \left((a \bmod m) + (b \bmod m)\right) \bmod m$$

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

CONGRUENCE BY COLOR

Let $m = 4$ for example.



$-4 \equiv 0 \equiv 4 \equiv 8 \ldots \pmod 4$

$-3 \equiv 1 \equiv 5 \equiv 9 \ldots \pmod 4$

$-2 \equiv 2 \equiv 6 \equiv 10 \ldots \pmod 4$

$-1 \equiv 3 \equiv 7 \equiv 11 \ldots \pmod 4$

THIS WEEK

HOW TO FIND THE MULTIPLICATIVE INVERSE?

$$5x \mod 13 = 1$$

$$5x \equiv 1 \pmod{13}$$

Why Modular Arithmetic

Modular arithmetic is a foundation of number theory.

We need number theory for cryptography and for channel coding.

Instead of considering integers and congruences $\pmod m$, and write "equations" like

$$a + b \equiv c \pmod m$$
$$a \cdot b \equiv d \pmod m,$$

we would like to write the "usual" kind of equations like

$$a + b = c$$
$$a \cdot b = d,$$

even when the operations are $\bmod m$.

This can be done, if we give new meaning to a, b, c and d, namely we make them the congruence classes $[a]_m$, $[b]_m$, $[c]_m$ and $[d]_m$.

Instead of considering integers and congruences $\pmod m$, and write "equations" like

$$a + b \equiv c \pmod m$$
$$a \cdot b \equiv d \pmod m,$$

we would like to write the "usual" kind of equations like

$$a + b = c$$
$$a \cdot b = d,$$

even when the operations are $\bmod m$.

This can be done, if we give new meaning to a, b, c and d, namely we make them the congruence classes $[a]_m$, $[b]_m$, $[c]_m$ and $[d]_m$.

Definition (Congruence Classes)

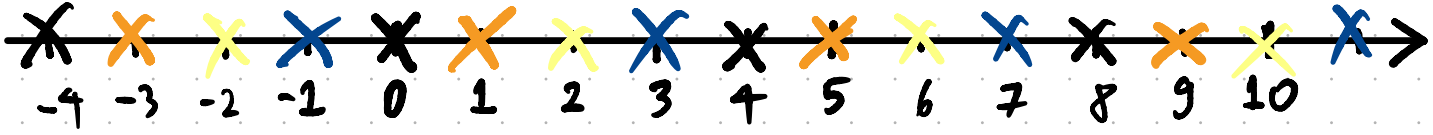
Let $m > 1$ be an integer, called the modulus.

The set of all integers congruent to $a \pmod{m}$ is called the **congruence class of** a **modulo** m.

It is denoted by $[a]_m$.

CONGRUENCE BY COLOR

Let $m = 4$ for example.



$-4 \equiv 0 \equiv 4 \equiv 8 \ldots \pmod 4$ $[0]_4$

$-3 \equiv 1 \equiv 5 \equiv 9 \ldots \pmod 4$ $[1]_4$

$-2 \equiv 2 \equiv 6 \equiv 10 \ldots \pmod 4$ $[2]_4$

$-1 \equiv 3 \equiv 7 \equiv 11 \ldots \pmod 4$ $[3]_4$

Example

- $[24]_2$ is the set of even integers. Same as $[0]_2$, $[2]_2$, etc.
- $[23]_2$ is the set of odd integers. Same as $[1]_2$, $[3]_2$, etc.
- $[a]_m = [b]_m$ iff $a \equiv b \pmod{m}$.

Definition ($\mathbb{Z}/m\mathbb{Z}$)

The set of all congruence classes modulo m is denoted by $\mathbb{Z}/m\mathbb{Z}$ (which is read "$\mathbb{Z}$ mod m") .

Note: Some authors use the notation $\mathbb{Z}_m$.

Example

- $\mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\}$.
- $\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$.
- etc.

NB: An element of $\mathbb{Z}/m\mathbb{Z}$ can be written in many ways

$$[a]_m = [a+m]_m = [a+2m]_m = \cdots$$

In particular:

- if $a = mq + r$, with $0 \leq r \leq m-1$, then

  $$[a]_m = [r]_m.$$

  We say that $[r]_m$ is in reduced form.

- every element of $\mathbb{Z}/m\mathbb{Z}$ has a unique representation in reduced form;

- $[b]_m$ is in reduced form iff $0 \leq b \leq m-1$.

Example

Which statements are correct?

1. $[-13]_9 = [5]_9$
2. $[13]_9 = [-5]_9$
3. $[13]_9 = [5]_9$
4. $[-13]_9 = [-5]_9$

Solution

1. $[-13]_9 = [5]_9$ is correct: $9 \mid -18$
2. $[13]_9 = [-5]_9$ is correct: $9 \mid 18$
3. $[13]_9 = [5]_9$ is incorrect: 9 does not divide 8
4. $[-13]_9 = [-5]_9$ is incorrect: 9 does not divide -8

In $\mathbb{Z}/m\mathbb{Z}$ we define the sum and the product as follows:

- $[a]_m + [b]_m = [a+b]_m$
- $[a]_m[b]_m = [ab]_m$

The sum set

$\{x : x = x_1 + x_2,$ where $x_1 \in [a]_m,$ $x_2 \in [b]_m\}$

The result is the same regardless the choice of representatives. In fact:

- If we choose $[a+km]_m$ instead of $[a]_m$
- and $[b+lm]$ instead of $[b]_m$
- then we obtain $[a+km]_m + [b+lm]_m = [a+km+b+lm]_m$ which is the same as $[a+b]_m$.

Idem for multiplication.

In $\mathbb{Z}/m\mathbb{Z}$ we define the sum and the product as follows:

- $[a]_m + [b]_m = [a+b]_m$
- $[a]_m[b]_m = [ab]_m$

The result is the same regardless the choice of representatives. In fact:

- If we choose $[a+km]_m$ instead of $[a]_m$
- and $[b+lm]$ instead of $[b]_m$
- then we obtain $[a+km]_m + [b+lm]_m = [a+km+b+lm]_m$ which is the same as $[a+b]_m$.

Idem for multiplication.

In $\mathbb{Z}/m\mathbb{Z}$ we define the sum and the product as follows:

- $[a]_m + [b]_m = [a+b]_m$
- $[a]_m[b]_m = [ab]_m$

The result is the same regardless the choice of representatives. In fact:

- If we choose $[a+km]_m$ instead of $[a]_m$
- and $[b+lm]$ instead of $[b]_m$
- then we obtain $[a+km]_m + [b+lm]_m = [a+km+b+lm]_m$ which is the same as $[a+b]_m$.

Idem for multiplication.

Example (addition and multiplication in $\mathbb{Z}/3\mathbb{Z}$)

If the value of m is implicit, e.g. $m = 3$, then we may write a instead of $[a]_3$.

The addition and multiplication tables are:

$\mathbb{Z}/3\mathbb{Z}$	$+$	$[0]_3$	$[1]_3$	$[2]_3$
	$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
	$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
	$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

$\mathbb{Z}/3\mathbb{Z}$	$\times$	$[0]_3$	$[1]_3$	$[2]_3$
	$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
	$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
	$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

Example (addition and multiplication in $\mathbb{Z}/4\mathbb{Z}$)

$\mathbb{Z}/4\mathbb{Z}$	$+$	0	1	2	3
	0	0	1	2	3
	1	1	2	3	0
	2	2	3	0	1
	3	3	0	1	2

$\mathbb{Z}/4\mathbb{Z}$	$\times$	0	1	2	3
	0	0	0	0	0
	1	0	1	2	3
	2	0	2	0	2
	3	0	3	2	1

Properties of $+$ in $\mathbb{Z}/m\mathbb{Z}$

The sum has the following properties:

- associativity:

$$[a]_m + ([b]_m + [c]_m) = ([a]_m + [b]_m) + [c]_m;$$

- there exists an additive identity, namely $[0]_m$:

$$[a]_m + [0]_m = [0]_m + [a]_m = [a]_m;$$

- there exists an inverse with respect to addition: every $[a]_m$ has an inverse, denoted $(-[a]_m)$, such that

$$[a]_m + (-[a]_m) = (-[a]_m) + [a]_m = [0]_m;$$

  the inverse of $[a]_m$ is $[-a]_m$;
- commutativity:

$$[a]_m + [b]_m = [b]_m + [a]_m;$$

Properties of $+$ in $\mathbb{Z}/m\mathbb{Z}$

The sum has the following properties:

- associativity:

$$[a]_m + ([b]_m + [c]_m) = ([a]_m + [b]_m) + [c]_m;$$

- there exists an additive identity, namely $[0]_m$:

$$[a]_m + [0]_m = [0]_m + [a]_m = [a]_m;$$

- there exists an inverse with respect to addition: every $[a]_m$ has an inverse, denoted $(-[a]_m)$, such that

$$[a]_m + (-[a]_m) = (-[a]_m) + [a]_m = [0]_m;$$

  the inverse of $[a]_m$ is $[-a]_m$;
- commutativity:

$$[a]_m + [b]_m = [b]_m + [a]_m;$$

Properties of $+$ in $\mathbb{Z}/m\mathbb{Z}$

The sum has the following properties:

- associativity:

$$[a]_m + ([b]_m + [c]_m) = ([a]_m + [b]_m) + [c]_m;$$

- there exists an additive identity, namely $[0]_m$:

$$[a]_m + [0]_m = [0]_m + [a]_m = [a]_m;$$

- there exists an inverse with respect to addition: every $[a]_m$ has an inverse, denoted $(-[a]_m)$, such that

$$[a]_m + (-[a]_m) = (-[a]_m) + [a]_m = [0]_m;$$

  the inverse of $[a]_m$ is $[-a]_m$;
- commutativity:

$$[a]_m + [b]_m = [b]_m + [a]_m;$$

Properties of $+$ in $\mathbb{Z}/m\mathbb{Z}$

The sum has the following properties:

- associativity:

$$[a]_m + ([b]_m + [c]_m) = ([a]_m + [b]_m) + [c]_m;$$

- there exists an additive identity, namely $[0]_m$:

$$[a]_m + [0]_m = [0]_m + [a]_m = [a]_m;$$

- there exists an inverse with respect to addition: every $[a]_m$ has an inverse, denoted $(-[a]_m)$, such that

$$[a]_m + (-[a]_m) = (-[a]_m) + [a]_m = [0]_m;$$

  the inverse of $[a]_m$ is $[-a]_m$;

- commutativity:

$$[a]_m + [b]_m = [b]_m + [a]_m;$$

Properties of $+$ in $\mathbb{Z}/m\mathbb{Z}$

The sum has the following properties:

- associativity:

$$[a]_m + ([b]_m + [c]_m) = ([a]_m + [b]_m) + [c]_m;$$

- there exists an additive identity, namely $[0]_m$:

$$[a]_m + [0]_m = [0]_m + [a]_m = [a]_m;$$

- there exists an inverse with respect to addition: every $[a]_m$ has an inverse, denoted $(-[a]_m)$, such that

$$[a]_m + (-[a]_m) = (-[a]_m) + [a]_m = [0]_m;$$

  the inverse of $[a]_m$ is $[-a]_m$;

- commutativity:

$$[a]_m + [b]_m = [b]_m + [a]_m;$$

Properties of $+$ in $\mathbb{Z}/m\mathbb{Z}$

The sum has the following properties:

- associativity:

$$[a]_m + ([b]_m + [c]_m) = ([a]_m + [b]_m) + [c]_m;$$

- there exists an additive identity, namely $[0]_m$:

$$[a]_m + [0]_m = [0]_m + [a]_m = [a]_m;$$

- there exists an inverse with respect to addition: every $[a]_m$ has an inverse, denoted $(-[a]_m)$, such that

$$[a]_m + (-[a]_m) = (-[a]_m) + [a]_m = [0]_m;$$

  the inverse of $[a]_m$ is $[-a]_m$;
- commutativity:

$$[a]_m + [b]_m = [b]_m + [a]_m;$$

Properties of $\times$ in $\mathbb{Z}/m\mathbb{Z}$

The multiplication has the following properties:

- associativity:
$$[a]_m([b]_m[c]_m) = ([a]_m[b]_m)[c]_m;$$
- multiplicative identity, namely $[1]_m$:
$$[a]_m[1]_m = [1]_m[a]_m = [a]_m;$$
- commutativity:
$$[a]_m[b]_m = [b]_m[a]_m;$$

Properties of $\times$ in $\mathbb{Z}/m\mathbb{Z}$

The multiplication has the following properties:

- associativity:
$$[a]_m([b]_m[c]_m) = ([a]_m[b]_m)[c]_m;$$
- multiplicative identity, namely $[1]_m$:
$$[a]_m[1]_m = [1]_m[a]_m = [a]_m;$$
- commutativity:
$$[a]_m[b]_m = [b]_m[a]_m;$$

Properties of $\times$ in $\mathbb{Z}/m\mathbb{Z}$

The multiplication has the following properties:

- associativity:

$$[a]_m([b]_m[c]_m) = ([a]_m[b]_m)[c]_m;$$

- multiplicative identity, namely $[1]_m$:

$$[a]_m[1]_m = [1]_m[a]_m = [a]_m;$$

- commutativity:

$$[a]_m[b]_m = [b]_m[a]_m;$$

Properties of $\times$ in $\mathbb{Z}/m\mathbb{Z}$

The multiplication has the following properties:

- associativity:
$$[a]_m([b]_m[c]_m) = ([a]_m[b]_m)[c]_m;$$
- multiplicative identity, namely $[1]_m$:
$$[a]_m[1]_m = [1]_m[a]_m = [a]_m;$$
- commutativity:
$$[a]_m[b]_m = [b]_m[a]_m;$$

Properties of $\times$ in $\mathbb{Z}/m\mathbb{Z}$

The multiplication has the following properties:

- associativity:
$$[a]_m([b]_m[c]_m) = ([a]_m[b]_m)[c]_m;$$
- multiplicative identity, namely $[1]_m$:
$$[a]_m[1]_m = [1]_m[a]_m = [a]_m;$$
- commutativity:
$$[a]_m[b]_m = [b]_m[a]_m;$$

The two operations have the following property:

- distributivity:

$$[a]_m([b]_m + [c]_m) = [a]_m[b]_m + [a]_m[c]_m;$$

THE NOTATION $k[a]_m$ IN $\mathbb{Z}/m\mathbb{Z}$

For an arbitrary positive integer k, $k[a]_m$ is a short hand for

$$\underbrace{[a]_m + [a]_m + \cdots + [a]_m}_{k \text{ times}}.$$

We can easily verify that

$$k[a]_m = [ka]_m = [k]_m[a]_m.$$

Some elements of $\mathbb{Z}/m\mathbb{Z}$ have the **multiplicative inverse**.

The multiplicative inverse of $[a]_m$, if it exists, is an element $[b]_m$ such that

$$[a]_m[b]_m = [b]_m[a]_m = [1]_m.$$

The multiplicative inverse, if it exists it is unique, and it is denoted by $([a]_m)^{-1}$.

Furthermore $\left(([a]_m)^{-1}\right)^{-1} = [a]_m$.

Proof that the inverse, if it exists, is unique:

- Suppose $ab = 1$ and $ac = 1$.
- Then $ab = ac$. Multiplying both sides by b yields
- $bab = bac$. But $ba = ab = 1$. Hence $b = c$. □

Proof that if b is the inverse of a, then the inverse of b is a.

If b is the inverse of a, then $ab = ba = 1$, which implies that a is the inverse of b. □

Exercise ($\mathbb{Z}/4\mathbb{Z}$)

Which elements of $\mathbb{Z}/4\mathbb{Z}$ have the multiplicative inverse? What is it?

$\mathbb{Z}/4\mathbb{Z}$	$\times$	0	1	2	3
	0	0	0	0	0
	1	0	1	2	3
	2	0	2	0	2
	3	0	3	2	1

Exercise ($\mathbb{Z}/4\mathbb{Z}$)

Which elements of $\mathbb{Z}/4\mathbb{Z}$ have the multiplicative inverse? What is it?

$\mathbb{Z}/4\mathbb{Z}$	$\times$	0	1	2	3
	0	0	0	0	0
	1	0	1	2	3
	2	0	2	0	2
	3	0	3	2	1

Solution

We see that

- $[1]_4$ and $[3]_4$ have the inverse ($[1]_4$ and $[3]_4$, respectively).
- $[2]_4$ has no inverse.
- $[0]_m$ has no inverse, regardless of m.

For any positive integer k,

- $([a]_m)^k$ is a short hand for $\underbrace{[a]_m[a]_m \cdots [a]_m}_{k \text{ times}}$;
- $([a]_m)^0 = [1]_m$ (empty product).
- Note that we do not consider negative exponents $([a]_m)^{-k}$ because it is problematic in general, with the exception of $([a]_m)^{-1}$, if course, which is simply the multiplicative inverse of $[a]_m$ whenever it exists.

Example

$$([3]_7)^{12} = \left(([3]_7)^2\right)^6 = ([2]_7)^6 = \left(([2]_7)^3\right)^2 = ([1]_7)^2 = [1]_7.$$

EXERCISE:

Suppose $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ has multiplicative inverse.

Question: Does there exist k such that

$$(*) \qquad \left([a]_m\right)^k = [0]_m \quad ?$$

Let b be the multiplicative inverse of a.

$$b^k a^k = b^k 0 = 0$$

$$b^{k-1} \underbrace{b a}_{=1} a^{k-1} = 0 \Rightarrow 1 = 0$$

$\times$

EXERCISE:

Suppose $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ has multiplicative inverse.

Question: Does there exist k such that

(*) $\left([a]_m\right)^k = [0]_m$ (?)

ANSWER: NO

DENOTE $[b]_m \stackrel{\text{def}}{=} \left([a]_m\right)^{-1}$.

(*) IMPLIES:

$$\underbrace{\left([b]_m\right)^k}_{\text{=}} \left([a]_m\right)^k = [0]_m$$

BUT $([b]_m)^{k-1}\underbrace{[b]_m}_{k-1}[a]_m([a]_m)^{k-1}$

$= ([bm])^{k-1}([a]_m)^{k-1}$

$= \ldots = [1]_m \neq [0]_m$

HENCE (*) MUST BE WRONG.

An equation of the form

$$[a]_m x = [b]_m$$

has a **unique** solution iff $[a]_m$ has the inverse. In this case,

$$x = ([a]_m)^{-1}[b]_m.$$

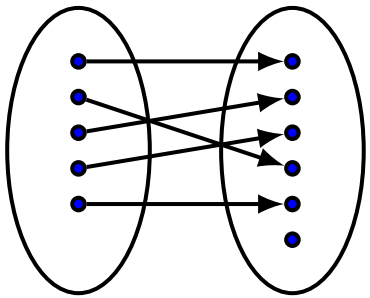
We prove a more general statement.

First a brief terminology review.

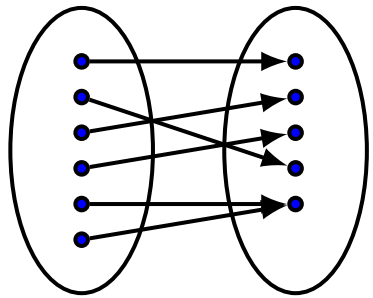
Recall that for a function $f : \mathcal{E} \to \mathcal{F}$

- $\mathcal{E}$ is the domain
- $\mathcal{F}$ is the codomain
- $f(\mathcal{E})$ is the image
- (the word *range* is sometimes used for the codomain, and sometimes for the image)

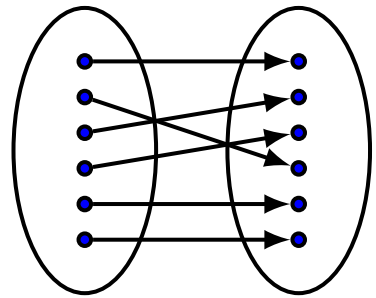
PIGEONHOLE PRINCIPLE



injective
(one-to-one)



surjective
(onto)



bijective
(one-to-one and onto)

Let $f : \mathcal{E} \to \mathcal{F}$, where $\mathcal{E}$ and $\mathcal{F}$ are finite sets.

- f injective $\Rightarrow |\mathcal{E}| \leq |\mathcal{F}|$
- f surjective $\Rightarrow |\mathcal{E}| \geq |\mathcal{F}|$
- f bijective $\Rightarrow |\mathcal{E}| = |\mathcal{F}|$

THEOREM

In $\mathbb{Z}/m\mathbb{Z}$, the following statements are equivalent: for a certain $[a]_m$:

(1) $[a]_m$ has the inverse;

(2) For all $[b]_m$, $[a]_m x = [b]_m$ has a unique solution;

(3) There exists a $[b]_m$, such that $[a]_m x = [b]_m$ has a unique solution.

Proof:

(1) $\Rightarrow$ (2): We multiply both sides of $[a]_m x = [b]_m$ by $[a]_m^{-1}$ and obtain the equivalent equation $x = [a]_m^{-1}[b]_m$, showing that there is a solution and the solution is unique.

(2) $\Rightarrow$ (1): For $[b]_m = [1]_m$ we obtain $[a]_m x = [1]_m$, which has a solution by assumption. The solution is the inverse of a.

(2) $\Rightarrow$ (3): True since (3) is a weaker statement than (2).

PROOF OF (3) $\Rightarrow$ (2).

CLAIM: $\exists\, b$ s.t. unique sol. $\Rightarrow \forall b$ unique sol.

PROOF OF (3) $\Rightarrow$ (2).

CLAIM: $\exists$ b s.t. unique sol. $\Rightarrow \forall b$ unique sol.

CLAIM': $\exists$ b s.t. either no sol or multiple sol

$\Rightarrow \nexists$ b s.t. unique sol.

PROOF OF (3) $\Rightarrow$ (2).

CLAIM: $\exists\, b$ s.t. unique sol. $\Rightarrow \forall b$ unique sol.

CLAIM': $\exists\, b$ s.t. either no sol or multiple sol

$\Rightarrow \nexists\, b$ s.t. unique sol.

CLAIM', FIRST HALF: $\exists\, b$ s.t. multiple sol

$\Rightarrow \nexists\, b$ s.t. unique sol.

PROOF OF (3) $\Rightarrow$ (2).

CLAIM: $\exists$ b s.t. unique sol. $\Rightarrow \forall b$ unique sol.

CLAIM': $\exists$ b s.t. either no sol or multiple sol

$\Rightarrow \nexists$ b s.t. unique sol.

CLAIM', FIRST HALF: $\exists$ b s.t. multiple sol

$\Rightarrow \nexists$ b s.t. unique sol.

PROOF: Let $[a]_m[x_1]_m = [b^*]_m$

$[a]_m[x_2]_m = [b^*]_m$ $([x_1]_m \neq [x_2]_m)$

Now define $[x_3]_m = [x_1]_n - [x_2]_m$

With this: $[a]_m [x_3]_m = [0]_m$ $\neq [0]_m$

Now select any $[\bar{b}]_m$.

Suppose $[a)_n [x_4]_m = [\bar{b}]_m$

But then

$$[a]_m \left([x_4]_n + [x_3]_m \right) = [\bar{b}]_m$$

So we have multiple solutions.

PROOF OF (3) $\Rightarrow$ (2).

CLAIM: $\exists$ b s.t. unique sol. $\Rightarrow$ $\forall b$ unique sol.

CLAIM': $\exists$ b s.t. either no sol or multiple sol

$\Rightarrow \nexists$ b s.t. unique sol.

CLAIM', FIRST HALF: $\exists$ b s.t. multiple sol

$\Rightarrow \nexists$ b s.t. unique sol.

CLAIM', SECOND HALF: $\exists$ b s.t. no sol

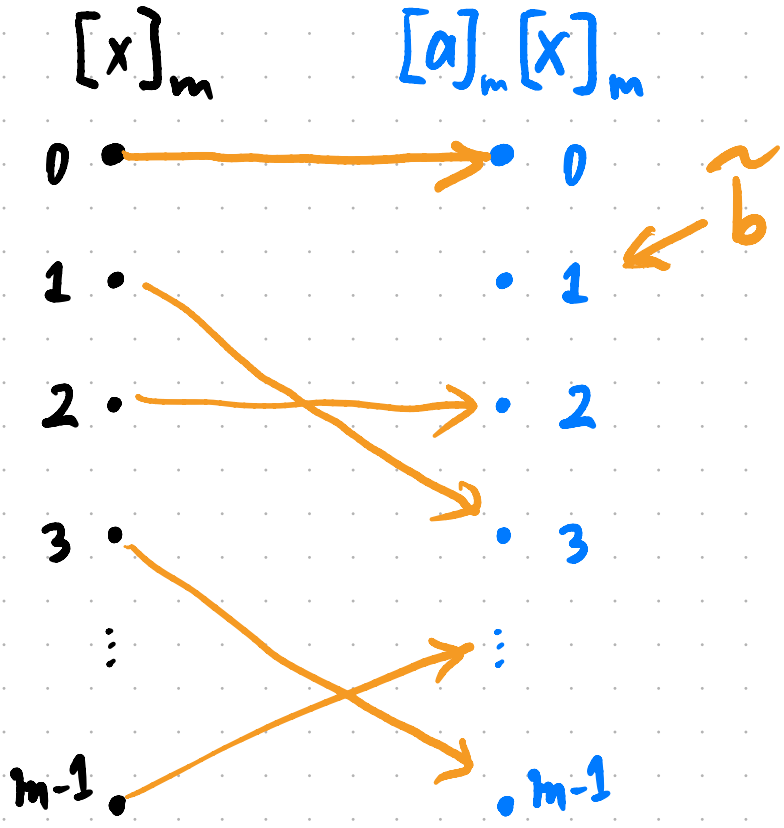
$\Rightarrow \nexists$ b s.t. unique sol.

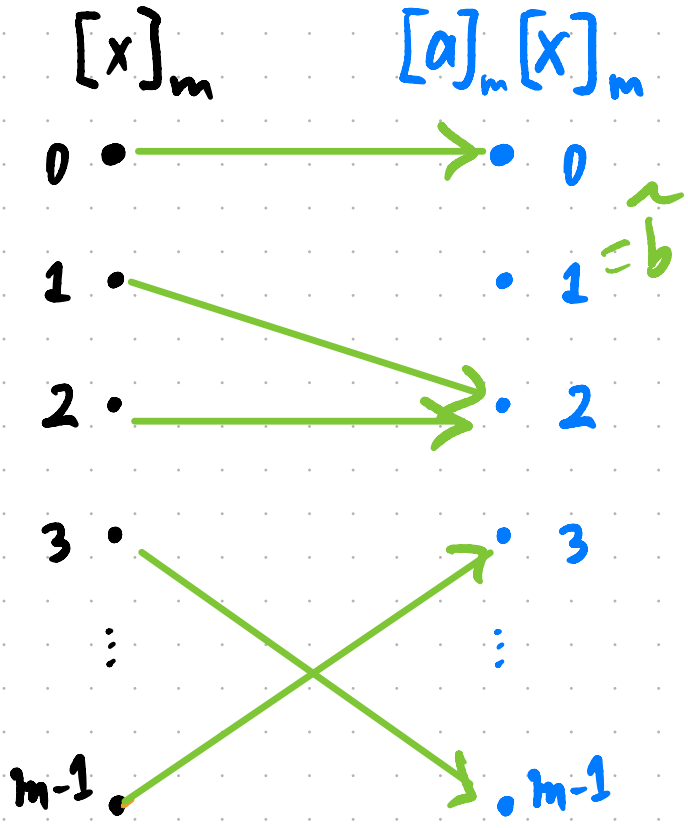
PROOF:

LET $[\tilde{b}]_m$ BE S.T. $[a]_m[x]_m \neq [\tilde{b}]_m$

FOR ALL

$[x]_m \in \mathbb{Z}/m\mathbb{Z}$


$[x]_m$
$[a]_m[x]_m$
0
1
2
3
m-1
0
1
2
3
m-1
$\tilde{b}$



Then, by pigeon hole, there must exist b^* s.t.

$$ax = b^*$$

has multiple solutions.

HENCE:

BY CLAIM', FIRST HALF

WE CAN COMPLETE THE PROOF.

□

(3) $\Rightarrow$ (2): We prove the contrapositive, i.e., we assume that there is a $[\tilde{b}]_m$ such that $[a]_m x = [\tilde{b}]_m$ has either no solution or multiple solutions, and we prove that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution.

- So suppose that $[a]_m x = [\tilde{b}]_m$ has no solution or multiple solutions.
- By the pigeonhole principle, the map $x \to ax$ is neither injective nor surjective.
- We can find a $[b^*]_m$ such that $[a]_m x = [b^*]_m$ has multiple solutions, say x_1 and x_2. Define $x_3 = x_1 - x_2 \neq [0]_m$.
- Hence, $[a]_m x_3 = [a]_m x_1 - [a]_m x_2 = [b^*]_m - [b^*]_m = [0]_m$.
- So the equation $[a]_m x = [0]_m$ has at least two solutions, x_3 and $[0]_m$.
- If $[a]_m x = [b]_m$ has a solution, say x_4, then $x_4 + x_3$ is also a solution.
- We conclude that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution. $\square$

(3) $\Rightarrow$ (2): We prove the contrapositive, i.e., we assume that there is a $[\tilde{b}]_m$ such that $[a]_m x = [\tilde{b}]_m$ has either no solution or multiple solutions, and we prove that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution.

- So suppose that $[a]_m x = [\tilde{b}]_m$ has no solution or multiple solutions.
- By the pigeonhole principle, the map $x \to ax$ is neither injective nor surjective.
- We can find a $[b^*]_m$ such that $[a]_m x = [b^*]_m$ has multiple solutions, say x_1 and x_2. Define $x_3 = x_1 - x_2 \neq [0]_m$.
- Hence, $[a]_m x_3 = [a]_m x_1 - [a]_m x_2 = [b^*]_m - [b^*]_m = [0]_m$.
- So the equation $[a]_m x = [0]_m$ has at least two solutions, x_3 and $[0]_m$.
- If $[a]_m x = [b]_m$ has a solution, say x_4, then $x_4 + x_3$ is also a solution.
- We conclude that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution. $\square$

(3) $\Rightarrow$ (2): We prove the contrapositive, i.e., we assume that there is a $[\tilde{b}]_m$ such that $[a]_m x = [\tilde{b}]_m$ has either no solution or multiple solutions, and we prove that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution.

- So suppose that $[a]_m x = [\tilde{b}]_m$ has no solution or multiple solutions.
- By the pigeonhole principle, the map $x \to ax$ is neither injective nor surjective.
- We can find a $[b^*]_m$ such that $[a]_m x = [b^*]_m$ has multiple solutions, say x_1 and x_2. Define $x_3 = x_1 - x_2 \neq [0]_m$.
- Hence, $[a]_m x_3 = [a]_m x_1 - [a]_m x_2 = [b^*]_m - [b^*]_m = [0]_m$.
- So the equation $[a]_m x = [0]_m$ has at least two solutions, x_3 and $[0]_m$.
- If $[a]_m x = [b]_m$ has a solution, say x_4, then $x_4 + x_3$ is also a solution.
- We conclude that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution. $\square$

(3) $\Rightarrow$ (2): We prove the contrapositive, i.e., we assume that there is a $[\tilde{b}]_m$ such that $[a]_m x = [\tilde{b}]_m$ has either no solution or multiple solutions, and we prove that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution.

- So suppose that $[a]_m x = [\tilde{b}]_m$ has no solution or multiple solutions.
- By the pigeonhole principle, the map $x \to ax$ is neither injective nor surjective.
- We can find a $[b^*]_m$ such that $[a]_m x = [b^*]_m$ has multiple solutions, say x_1 and x_2. Define $x_3 = x_1 - x_2 \neq [0]_m$.
- Hence, $[a]_m x_3 = [a]_m x_1 - [a]_m x_2 = [b^*]_m - [b^*]_m = [0]_m$.
- So the equation $[a]_m x = [0]_m$ has at least two solutions, x_3 and $[0]_m$.
- If $[a]_m x = [b]_m$ has a solution, say x_4, then $x_4 + x_3$ is also a solution.
- We conclude that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution. $\square$

(3) $\Rightarrow$ (2): We prove the contrapositive, i.e., we assume that there is a $[\tilde{b}]_m$ such that $[a]_m x = [\tilde{b}]_m$ has either no solution or multiple solutions, and we prove that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution.

- So suppose that $[a]_m x = [\tilde{b}]_m$ has no solution or multiple solutions.
- By the pigeonhole principle, the map $x \to ax$ is neither injective nor surjective.
- We can find a $[b^*]_m$ such that $[a]_m x = [b^*]_m$ has multiple solutions, say x_1 and x_2. Define $x_3 = x_1 - x_2 \neq [0]_m$.
- Hence, $[a]_m x_3 = [a]_m x_1 - [a]_m x_2 = [b^*]_m - [b^*]_m = [0]_m$.
- So the equation $[a]_m x = [0]_m$ has at least two solutions, x_3 and $[0]_m$.
- If $[a]_m x = [b]_m$ has a solution, say x_4, then $x_4 + x_3$ is also a solution.
- We conclude that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution. $\square$

(3) $\Rightarrow$ (2): We prove the contrapositive, i.e., we assume that there is a $[\tilde{b}]_m$ such that $[a]_m x = [\tilde{b}]_m$ has either no solution or multiple solutions, and we prove that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution.

- So suppose that $[a]_m x = [\tilde{b}]_m$ has no solution or multiple solutions.
- By the pigeonhole principle, the map $x \to ax$ is neither injective nor surjective.
- We can find a $[b^*]_m$ such that $[a]_m x = [b^*]_m$ has multiple solutions, say x_1 and x_2. Define $x_3 = x_1 - x_2 \neq [0]_m$.
- Hence, $[a]_m x_3 = [a]_m x_1 - [a]_m x_2 = [b^*]_m - [b^*]_m = [0]_m$.
- So the equation $[a]_m x = [0]_m$ has at least two solutions, x_3 and $[0]_m$.
- If $[a]_m x = [b]_m$ has a solution, say x_4, then $x_4 + x_3$ is also a solution.
- We conclude that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution. $\square$

(3) $\Rightarrow$ (2): We prove the contrapositive, i.e., we assume that there is a $[\tilde{b}]_m$ such that $[a]_m x = [\tilde{b}]_m$ has either no solution or multiple solutions, and we prove that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution.

- So suppose that $[a]_m x = [\tilde{b}]_m$ has no solution or multiple solutions.
- By the pigeonhole principle, the map $x \to ax$ is neither injective nor surjective.
- We can find a $[b^*]_m$ such that $[a]_m x = [b^*]_m$ has multiple solutions, say x_1 and x_2. Define $x_3 = x_1 - x_2 \neq [0]_m$.
- Hence, $[a]_m x_3 = [a]_m x_1 - [a]_m x_2 = [b^*]_m - [b^*]_m = [0]_m$.
- So the equation $[a]_m x = [0]_m$ has at least two solutions, x_3 and $[0]_m$.
- If $[a]_m x = [b]_m$ has a solution, say x_4, then $x_4 + x_3$ is also a solution.
- We conclude that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution. $\square$

(3) $\Rightarrow$ (2): We prove the contrapositive, i.e., we assume that there is a $[\tilde{b}]_m$ such that $[a]_m x = [\tilde{b}]_m$ has either no solution or multiple solutions, and we prove that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution.

- So suppose that $[a]_m x = [\tilde{b}]_m$ has no solution or multiple solutions.
- By the pigeonhole principle, the map $x \to ax$ is neither injective nor surjective.
- We can find a $[b^*]_m$ such that $[a]_m x = [b^*]_m$ has multiple solutions, say x_1 and x_2. Define $x_3 = x_1 - x_2 \neq [0]_m$.
- Hence, $[a]_m x_3 = [a]_m x_1 - [a]_m x_2 = [b^*]_m - [b^*]_m = [0]_m$.
- So the equation $[a]_m x = [0]_m$ has at least two solutions, x_3 and $[0]_m$.
- If $[a]_m x = [b]_m$ has a solution, say x_4, then $x_4 + x_3$ is also a solution.
- We conclude that for no $[b]_m$, $[a]_m x = [b]_m$ has a unique solution. $\square$

Exercise ($\mathbb{Z}/9\mathbb{Z}$)

If it exists, find the solution of $[4]_9 x = [3]_9$

Exercise ($\mathbb{Z}/9\mathbb{Z}$)

If it exists, find the solution of $[4]_9 x = [3]_9$

Solution

x	0	1	2	3	4	5	6	7	8
$[4]_9 x$	0	4	8	3	7	2	6	1	5

Pedestrian solution: From the above table we see that the solution is $[3]_9$. This approach requires having the above $[4]_9 x$ table.

Preferable solution (when possible): If it exists, we find the inverse of $[4]_9$. For now, we use the table to find $([4]_9)^{-1} = [7]_9$. Hence

$$x = [7]_9[3]_9 = [3]_9.$$

We will see how to find the inverse without constructing the table.

Example

If it exists, find the solution of $[2]_7 x + [3]_7 = [1]_7$

1. $\Leftrightarrow [2]_7 x = [1]_7 + (-[3]_7)$ (adding on both sides the negative of $[3]_7$ — always exists)
2. $\Leftrightarrow [2]_7 x = [-2]_7$
3. $\Leftrightarrow x = ([2]_7)^{-1}[5]_7$ (multiplying both sides by the inverse of $[2]_7$, which exists)
4. $\Leftrightarrow x = [4]_7[5]_7$ $(([2]_7)^{-1} = [4]_7)$
5. $\Leftrightarrow x = [20]_7$
6. $\Leftrightarrow x = [6]_7$

Example

If it exists, find the solution of $[2]_7 x + [3]_7 = [1]_7$

1. $\Leftrightarrow [2]_7 x = [1]_7 + (-[3]_7)$ (adding on both sides the negative of $[3]_7$ — always exists)
2. $\Leftrightarrow [2]_7 x = [-2]_7$
3. $\Leftrightarrow x = ([2]_7)^{-1}[5]_7$ (multiplying both sides by the inverse of $[2]_7$, which exists)
4. $\Leftrightarrow x = [4]_7[5]_7$ $(([2]_7)^{-1} = [4]_7)$
5. $\Leftrightarrow x = [20]_7$
6. $\Leftrightarrow x = [6]_7$

Example

If it exists, find the solution of $[2]_7 x + [3]_7 = [1]_7$

1. $\Leftrightarrow [2]_7 x = [1]_7 + (-[3]_7)$ (adding on both sides the negative of $[3]_7$ — always exists)
2. $\Leftrightarrow [2]_7 x = [-2]_7$
3. $\Leftrightarrow x = ([2]_7)^{-1}[5]_7$ (multiplying both sides by the inverse of $[2]_7$, which exists)
4. $\Leftrightarrow x = [4]_7[5]_7$ $(([2]_7)^{-1} = [4]_7)$
5. $\Leftrightarrow x = [20]_7$
6. $\Leftrightarrow x = [6]_7$

Example

If it exists, find the solution of $[2]_7 x + [3]_7 = [1]_7$

1. $\Leftrightarrow [2]_7 x = [1]_7 + (-[3]_7)$ (adding on both sides the negative of $[3]_7$ — always exists)
2. $\Leftrightarrow [2]_7 x = [-2]_7$
3. $\Leftrightarrow x = ([2]_7)^{-1}[5]_7$ (multiplying both sides by the inverse of $[2]_7$, which exists)
4. $\Leftrightarrow x = [4]_7[5]_7$ $(([2]_7)^{-1} = [4]_7)$
5. $\Leftrightarrow x = [20]_7$
6. $\Leftrightarrow x = [6]_7$

Example

If it exists, find the solution of $[2]_7 x + [3]_7 = [1]_7$

1. $\Leftrightarrow [2]_7 x = [1]_7 + (-[3]_7)$ (adding on both sides the negative of $[3]_7$ — always exists)
2. $\Leftrightarrow [2]_7 x = [-2]_7$
3. $\Leftrightarrow x = ([2]_7)^{-1}[5]_7$ (multiplying both sides by the inverse of $[2]_7$, which exists)
4. $\Leftrightarrow x = [4]_7[5]_7$ $(([2]_7)^{-1} = [4]_7)$
5. $\Leftrightarrow x = [20]_7$
6. $\Leftrightarrow x = [6]_7$

Example

If it exists, find the solution of $[2]_7 x + [3]_7 = [1]_7$

1. $\Leftrightarrow [2]_7 x = [1]_7 + (-[3]_7)$ (adding on both sides the negative of $[3]_7$ — always exists)
2. $\Leftrightarrow [2]_7 x = [-2]_7$
3. $\Leftrightarrow x = ([2]_7)^{-1}[5]_7$ (multiplying both sides by the inverse of $[2]_7$, which exists)
4. $\Leftrightarrow x = [4]_7[5]_7$ $(([2]_7)^{-1} = [4]_7)$
5. $\Leftrightarrow x = [20]_7$
6. $\Leftrightarrow x = [6]_7$

Example

If it exists, find the solution of $[2]_7 x + [3]_7 = [1]_7$

1. $\Leftrightarrow [2]_7 x = [1]_7 + (-[3]_7)$ (adding on both sides the negative of $[3]_7$ — always exists)
2. $\Leftrightarrow [2]_7 x = [-2]_7$
3. $\Leftrightarrow x = ([2]_7)^{-1}[5]_7$ (multiplying both sides by the inverse of $[2]_7$, which exists)
4. $\Leftrightarrow x = [4]_7[5]_7$ $(([2]_7)^{-1} = [4]_7)$
5. $\Leftrightarrow x = [20]_7$
6. $\Leftrightarrow x = [6]_7$

Example

If it exists, find the solution of $[3]_9 x + [2]_9 = [5]_9$

1. $\Leftrightarrow [3]_9 x = [5]_9 + [-2]_9$
2. $\Leftrightarrow [3]_9 x = [3]_9$

$([3]_9)^{-1}$ does not exist (see table below).

x	0	1	2	3	4	5	6	7	8
$[3]_9 x$	0	3	6	0	3	6	0	3	6

Yet, from the above table, we see that there are three solutions, namely

$$x = [1]_9,\ x = [4]_9,\ x = [7]_9.$$

THEOREM

Let $m > 1$ be integer.

The element $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ has a multiplicative inverse iff $\gcd(a, m) = 1$.

The proof is postponed (see Bézout's identity).

Example (Multiplicative inverses in $\mathbb{Z}/4\mathbb{Z}$)

$\mathbb{Z}/4\mathbb{Z}$	$\times$	0	1	2	3
	0	0	0	0	0
	1	0	1	2	3
	2	0	2	0	2
	3	0	3	2	1

$\gcd(a, 4) = 1$ for $a = 1, 3$.

Theorem ($\mathbb{Z}/p\mathbb{Z}$ with p prime)

If p is prime, all elements of $\mathbb{Z}/p\mathbb{Z}$ except $[0]_p$ have a multiplicative inverse.

Proof:

$$\gcd(a, p) = 1 \text{ for } a = 1, 2, \ldots, p-1$$

$$\gcd(0, p) = p.$$

□

Recall the Mod 97 – 10 procedure

1. Append 00 (i.e., multiply the number by 100)
2. Let r be the remainder after division by 97
3. The check digits are $c = 98 - r$ (written as a 2-digit number)
4. Replace 00 with c
5. Check: the resulting number mod 97 equals 1

Recall the example

1. $n = 212351234$
2. $n \longmapsto 21235123400 + 98 - 91 = 21235123407$
3. Check: $21235123407 \mod 97 = 1$. Check passed
4. If we transpose: 21253123407
5. Check: $21253123407 \mod 97 = 2$. Check **not** passed

WHY IT DETECTS TRANSPOSITIONS

Let us use the new notation to remind ourselves why an unmodified number passes the check:

Recall that $n \to 100n + 98 - (100n \mod 97)$.

The test is passed if [number with check digits]$_{97} = [1]_{97}$

This is the case:

$$[100n+98-(100n \mod 97)]_{97} = [[100n]_{97}+98-[100n]_{97}]_{97} = [98]_{97} = [1]_{97}.$$

NOW SUPPOSE WE SWAP TWO CONSECUTIVE DIGITS:

$$m = 212ba123407$$

$$\downarrow$$

$$\tilde{m} = 212ab123407$$

NOW SUPPOSE WE SWAP TWO CONSECUTIVE DIGITS:

$$n = 212\,ba\,123407$$

$$\tilde{n} = 212\,ab\,123407$$

$$= n - 10^6(a+10b) + 10^6(b+10a)$$

NOW SUPPOSE WE SWAP TWO CONSECUTIVE DIGITS:

$$m = 212\,ba\,123407$$

$$\downarrow$$

$$\tilde{m} = 212\,ab\,123407$$

$$= m - 10^6(a+10b) + 10^6(b+10a)$$

WE ARE CHECKING

$$\tilde{m} \mod 97 = 1 \quad (?)$$

$$\tilde{m} \mod 97$$

$$= \left[m - 10^6 (a + 10b) + 10^6 (b + 10a) \right] \mod 97$$

$\tilde{m} \mod 97$

$= \left[m - 10^6 (a + 10b) + 10^6 (b + 10a) \right] \mod 97$

$= \underbrace{m \mod 97}_{=1} + \left(- 10^6 (a + 10b) + 10^6 (b + 10a) \right) \mod 97$

FOR THIS TO BE EQUAL TO 1, WE MUST HAVE

$\left(- 10^6 (a + 10b) + 10^6 (b + 10a) \right) \mod 97 = 0$

HENCE: CHECK IS PASSED IFF

$$\left[-10^6(a+10b)+10^6(b+10a)\right]_{97}=[0]_{97}$$

HENCE : CHECK IS PASSED IFF

$$\left[-10^6(a+10b)+10^6(b+10a)\right]_{97}=[0]_{97}$$

$$\left[10^6\left[-a-10b+b+10a\right]\right]_{97}$$

$$=\left[10^6\cdot 9\cdot(a-b)\right]_{97}=[0]_{97}$$

FOR THIS TO HAPPEN, WE NEED:

$[10^6]_{97} = [0]_{97}$ ← CANNOT HAPPEN $[10^k]_{97} \neq [0]_{97}$

OR

$[9]_{97} = [0]_{97}$ ← DOES NOT HOLD

OR

$[a-b]_{97} = [0]_{97}$ ← THIS HAPPENS IF AND ONLY IF $a = b$

Two consecutive digits ba of a decimal number are worth $10^k(a+10b)$ for some nonnegative integer k.

After we transpose them they are worth $10^k(b+10a)$.

The check detects the transposition, unless

$$[10^k(b+10a) - 10^k(a+10b)]_{97} = [0]_{97}$$

$$\Leftrightarrow\ [10^k(9a-9b)]_{97} = [0]_{97}$$

$$\Leftrightarrow\ [10^k 9(a-b)]_{97} = [0]_{97}$$

$$\Leftrightarrow\ ([10]_{97})^k [9]_{97} [a-b]_{97} = [0]_{97}$$

$$\Leftrightarrow\ [a-b]_{97} = [0]_{97}$$ (all non-zero elements of $\mathbb{Z}/97\mathbb{Z}$ have an inverse)

We conclude that the transposition is not detected iff $a = b$, i.e., if there is no transposition.

NOW SUPPOSE WE SWAP TWO CONSECUTIVE DIGITS:

$$m = 212\,ba\,123407$$

$$\downarrow$$

$$\tilde{m} = 212\,ab\,123407$$

$$= m - 10^6(a+10b) + 10^6(b+10a)$$

WE ARE CHECKING

$$\tilde{m} \mod 97 = 1 \quad (?)$$

NOW SUPPOSE WE SWAP TWO NON-CONSECUTIVE DIGITS:

$$m = 212b5123a07$$

$$\downarrow$$

$$\tilde{m} = 212a5123b07$$

NOW SUPPOSE WE SWAP TWO NON-CONSECUTIVE DIGITS:

$$m = 212b5123a07$$

$$\downarrow$$

$$\tilde{m} = 212a5123b07$$

$$= m - 10^2(a + 10^5 b) + 10^2(b + 10^5 a)$$

WE ARE CHECKING

$$\tilde{m} \mod 97 = 1 \quad (?)$$

$$\left(10^{2} \left(10^{5} - 1 \right) (a-b) \right) \bmod 97 = 0$$

IN GENERAL:

$$\left(10^{k} \left(10^{n} - 1 \right) (a-b) \right) \bmod 97 = 0$$

$$\left(10^{2} \left(10^{5} - 1 \right) (a-b) \right) \bmod 97 = 0$$

IN GENERAL:

$$\left(10^{k} \left(10^{n} - 1 \right) (a-b) \right) \bmod 97 = 0$$

QUESTION: DOES THERE EXIST n

$$\left[10^{n} - 1 \right]_{97} = [0]_{97}$$

YESTERDAY

- COMPUTATIONS WITH EQUIVALENCE CLASSES.

$[a]_m$

<u>Ex</u>: $m = 3$

$[2]_3 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$

$[2]_3 + [2]_3 = \{\ldots, -2, 1, 4, 7, 10, 13, \ldots\}$

$= [1]_3$

$\mathbb{Z}/n\mathbb{Z}$

$+$	$[0]_n$	$\cdots$	$[n-1]_n$
$[0]_n$	$[0]_n$		
$[1]_n$			$[0]_n$
$\vdots$			
$[n-1]_n$			

$\cdot$	

- MULTIPLICATIVE INVERSE

$$ax \equiv 1 \pmod{m}$$

$$[a]_m x = [1]_m$$

EXISTS IF AND ONLY IF

$$\gcd(a, m) = 1.$$

PROOF : TODAY.

EX: IF $\gcd(a,m) = 1$

THEN YOU CANNOT FIND

$k \in \mathbb{Z}_+$ s.t. $[a]_m^k = [0]_m$

EX: IF $\gcd(a,n) = 1$ & $\gcd(b,n) = 1$

THEN: $[a]_n [b]_n = [0]_n$

IF AND ONLY IF

$[a]_n = [0]_n$ OR $[b]_n = [0]_n$

What for?

- Recall that $[a]_m$ has an inverse (in $\mathbb{Z}/m\mathbb{Z}$) iff $\gcd(a, m) = 1$.
- The Euclidean algorithm is a technique for quickly finding the gcd of two integers. (Much faster than via the prime factor decomposition, which is hard to do for large numbers.)
- When $\gcd(a, m) = 1$, Bézout's identity gives us the inverse of $[a]_m$.

$a \mid b$

a divides b

if $\exists\ u \in \mathbb{Z}$ s.t. $a \cdot u = b$

a divides b

if $\exists\ u \in \mathbb{Z}$ s.t. $a \cdot u = b$

Does a divide 0 ?

YES!

PROPERTIES OF THE GCD

0) $\gcd(a, 0) = a$

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

Hence: W.l.o.g assume $a \geq b$.

2) $\gcd(a, b) = \gcd(-a, b)$

3) $\gcd(a, b) = \gcd(a - kb, b)$

PROOF:

IF d DIVIDES a AND b,
THEN d ALSO DIVIDES $a - kb$ AND b.

IF d DIVIDES $a - kb$ AND b
THEN d ALSO DIVIDES a AND b
BECAUSE IF d DIV. $a - kb$ AND b
THEN d DIVIDES $a - kb + lb$ AND b.

3) $\gcd(a, b) = \gcd(a - kb, b)$

Proof: For any $d \in \mathbb{Z}$:

d divides <u>both</u> a and b

if and only if

d divides <u>both</u> $a - kb$ and b

3) $\gcd(a, b) = \gcd(a - kb, b)$

4) Let $a = bq + r$. with $r \in \{0, 1, \ldots, b-1\}$

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

4) Let $a = bq_1 + r_1$.

$$\gcd(a, b) = \gcd(b, r_1)$$

→ **EUCLIDEAN ALGORITHM**

Let $b = r_1 q_2 + r_2$

$$\Rightarrow \gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2)$$

EXAMPLE:

$$\gcd(150, 27)$$
$$= \gcd(27, 15)$$
$$= \gcd(15, 12)$$
$$= \gcd(12, 3)$$
$$= \gcd(3, 0)$$

$150 = 27 \times 5 + 15$

$27 = 15 \times 1 + 12$

$15 = 12 \cdot 1 + 3$

$12 = 3 \times 4 + 0$

$\Rightarrow \gcd(150, 27) = 3$

EXAMPLE:

$\gcd(150, 27)$

$= \gcd(27, 15)$

$= \gcd(15, 12)$

$= \gcd(12, 3)$

$= \gcd(3, 0) = 3$

$150 = 5 \times 27 + 15$

$27 = 1 \times 15 + 12$

EXAMPLE:

$$\gcd(12345678906, 12345678901)$$

$$= \gcd(12345678901, 5)$$

$$= \gcd(5, 1)$$

$$= \gcd(1, 0)$$

EXAMPLE:

$$\gcd(12345678906, 12345678901)$$

$$= \gcd(12345678901, 5)$$

$$= \gcd(5, 1)$$

$$= \gcd(1, 0) = 1$$

THEOREM (EUCLID, TEXTBOOK THM 8.3)

Let a and b be integers, not both zero. Then, for any integer k

$$\gcd(a, b) = \gcd(b, a - kb)$$

THEOREM (EUCLID, TEXTBOOK THM 8.3)

Let a and b be integers, not both zero. Then, for any integer k

$$\gcd(a, b) = \gcd(b, a - kb)$$

Proof:

If d divides a and b, then it divides b and $a - kb$.

Similarly, if d divides both b and $a - kb$, then it divides b and $a - kb + kb = a$.

Since the set of divisors of a and b is the same as the set of divisors of b and $a - kb$, the greatest divisor is the same in both cases. □

Basic ingredients to compute the gcd

- $\gcd(a, b) = \gcd(\pm a, \pm b) = \gcd(b, a)$.
- Hence we can focus on the computation of $\gcd(a, b)$ with $0 \leq b \leq a$.
- If $a = qb + r$ is the Euclidean division, then

$$\gcd(a, b) = \gcd(b, a - qb) = \gcd(b, r),$$

  with $0 \leq r < b$. This is progress.

- Hence $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_n, 0) = r_n$, where

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 \leq r_1 < b \\ b &= r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1 \\ r_i &= r_{i+1} q_{i+2} + r_{i+2}, \quad 0 \leq r_{i+2} < r_{i+1}. \end{aligned}$$

Example

$\gcd(a,b)$	$a = bq + r$
$= \gcd(b,r)$	
$= \gcd(122,22)$	$122 = 22 \times 5 + 12$
$= \gcd(22,12)$	$22 = 12 \times 1 + 10$
$= \gcd(12,10)$	$12 = 10 \times 1 + 2$
$= \gcd(10,2)$	$10 = 2 \times 5 + 0$
$= \gcd(2,0)$	
$= 2$	

EUCLIDEAN ALGORITHM (RECURSIVE)

Algorithm 1 gcd(a, b : positive integers)

1: **if** $a < b$ **then**
   return gcd(b, a)
2: **else if** $b = 0$ **then**
   return a
3: **else**
   return gcd($b, a \% b$)
4: **end if**

EXERCISE

Compute $\gcd(12345678906, 12345678901)$

EXERCISE

Compute $\gcd(12345678906, 12345678901)$

SOLUTION

$$\begin{aligned}\gcd(12345678906, 12345678901) &= \gcd(12345678901, 5)\\ &\overset{(*)}{=} \gcd(5, 1)\\ &= \gcd(1, 0)\\ &= 1,\end{aligned}$$

where in $(*)$ we use the fact that a number $xxxxxxx0$ is divisible by 5.

THEOREM (BÉZOUT'S IDENTITY (TEXTBOOK THEOREM 8.4))

Let a and b be integers, not both zero.

There exist integers u and v, such that

$$\gcd(a, b) = au + bv$$

$$\gcd(4, 6) = 2 = 4 \cdot u + 6 \cdot v$$

$$u = -1, \quad v = 1.$$

UNIQUENESS ?

$$\gcd(a,b) = au + bv$$

$$= a(u + \ell b) + b(v - \ell a)$$

$$= au' + bv'$$

$\Rightarrow$ u and v are <u>not</u> unique

(In fact, there are infinitely many choices)

We prove Bézout's identity by means of the extended Euclidean algorithm, which finds solutions to Bézout's identity

$$\gcd(a, b) = au + bv,$$

where a and b are given, and u, v and $\gcd(a, b)$ are returned by the algorithm.

Note: if $\gcd(a, b) = au + bv$, then $\gcd(-a, b) = au + bv$ and $\gcd(a, -b) = au + bv$.

Hence it suffices that we consider nonnegative numbers a, b, not both zero.

EXTENDED EUCLID ALGORITHM

OBS: $\gcd(a,b) = \gcd(b,r)$, $a = bq + r$

$\downarrow$

suppose we have $\tilde{u}, \tilde{v}$ such that

$$\gcd(b,r) = b\tilde{u} + r\tilde{v}$$

$\Downarrow$

$$\gcd(b,r) = b\tilde{u} + (a - bq)\tilde{v}$$

$$= a\tilde{v} + b(\tilde{u} - q\tilde{v})$$

$\Lleftarrow$

$$\gcd(a,b) = a\tilde{v} + b(\tilde{u} - q\tilde{v})$$

USE THIS RECURSIVELY!

$\gcd(a,b)$	$a = bq + r$	q	$\tilde{u}$	$\tilde{v}$	$u = \tilde{v}$	$v = (\tilde{u} - q\tilde{v})$
$(150, 33)$	$150 = 33 \times 4 + 18$	4			2	-9
$(33, 18)$	$33 = 18 \times 1 + 15$	1	-1	2	-1	2
$(18, 15)$	$18 = 15 \times 1 + 3$	1	1	-1	1	-1
$(15, 3)$	$15 = 3 \times 5 + 0$	5	0	1	0	1
$(3, 0)$		0	1	0		

$\gcd(150, 33) = 3 = 2 \times 150 - 9 \times 33$

$\gcd(a,b)$	$a = bq + r$	q	$\tilde{u}$	$\tilde{v}$	$u = \tilde{v}$	$v = (\tilde{u} - q\tilde{v})$

Proof:

- Iteration step: Suppose $a \geq b$.
  - $\gcd(a, b) = \gcd(b, r)$, where $a = bq + r$;
  - suppose we have found $\tilde{u}$ and $\tilde{v}$ such that $\gcd(b, r) = b\tilde{u} + r\tilde{v}$;
  - use $r = (a - bq)$ to rewrite

    $$\gcd(a, b) = \gcd(b, r) = b\tilde{u} + r\tilde{v} = b\tilde{u} + (a - bq)\tilde{v} = a\tilde{v} + b(\tilde{u} - q\tilde{v}) \stackrel{!}{=} au + bv;$$

  - comparing terms: $u = \tilde{v}$ and $v = (\tilde{u} - q\tilde{v})$.

- Final step: $\gcd(a, 0) = a \Rightarrow \tilde{u} = 1$, $\tilde{v} = 0$.
  Note: in this last step, $\tilde{v}$ is not unique.

- Via successive applications of the above iteration, eventually we reach the form $\gcd(a, b) = au + bv$. □

Example

$\gcd(a,b)$	$a = bq + r$	$u = \tilde{v}$	$v = (\tilde{u} - q\tilde{v})$
$\gcd(122, 22)$	$122 = 22 \times 5 + 12$		
$\gcd(22, 12)$	$22 = 12 \times 1 + 10$		
$\gcd(12, 10)$	$12 = 10 \times 1 + 2$		
$\gcd(10, 2)$	$10 = 2 \times 5 + 0$		
$\gcd(2, 0) = 2$			

Example (cont.)

$\gcd(a, b)$	$a = bq + r$	$u = \tilde{v}$	$v = (\tilde{u} - q\tilde{v})$
$\gcd(122, 22)$	$122 = 22 \times 5 + 12$		
$\gcd(22, 12)$	$22 = 12 \times 1 + 10$		
$\gcd(12, 10)$	$12 = 10 \times 1 + 2$		
$\gcd(10, 2)$	$10 = 2 \times 5 + 0$	0	1
$\gcd(2, 0) = 2$		1	0

Example (cont.)

$\gcd(a, b)$	$a = bq + r$	$u = \tilde{v}$	$v = (\tilde{u} - q\tilde{v})$
$\gcd(122, 22)$	$122 = 22 \times 5 + 12$		
$\gcd(22, 12)$	$22 = 12 \times 1 + 10$		
$\gcd(12, 10)$	$12 = 10 \times 1 + 2$	1	$(0 - 1 \times 1) = -1$
$\gcd(10, 2)$	$10 = 2 \times 5 + 0$	0	1
$\gcd(2, 0) = 2$		1	0

Example (cont.)

$\gcd(a, b)$	$a = bq + r$	$u = \tilde{v}$	$v = (\tilde{u} - q\tilde{v})$
$\gcd(122, 22)$	$122 = 22 \times 5 + 12$		
$\gcd(22, 12)$	$22 = 12 \times 1 + 10$	-1	$(1 - 1(-1)) = 2$
$\gcd(12, 10)$	$12 = 10 \times 1 + 2$	1	-1
$\gcd(10, 2)$	$10 = 2 \times 5 + 0$	0	1
$\gcd(2, 0) = 2$		1	0

Example (cont.)

$\gcd(a, b)$	$a = bq + r$	$u = \tilde{v}$	$v = (\tilde{u} - q\tilde{v})$	sporadic checks
$\gcd(122, 22)$	$122 = 22 \times 5 + 12$	2	$-1 - 5 \times 2 = -11$	
$\gcd(22, 12)$	$22 = 12 \times 1 + 10$	-1	2	$-22 + 12 \cdot 2 \overset{\checkmark}{=} 2$
$\gcd(12, 10)$	$12 = 10 \times 1 + 2$	1	-1	$12 - 10 \overset{\checkmark}{=} 2$
$\gcd(10, 2)$	$10 = 2 \times 5 + 0$	0	1	
$\gcd(2, 0) = 2$		1	0	

$$\gcd(122, 22) = 122 \times 2 + 22 \times (-11)$$

Extended Euclidean algorithm (recursive)

Algorithm 2 Euclid(a, b : nonnegative integers, not both zero)

1: **if** $a < b$ **then**
   $(u, v, d) = \text{Euclid}(b, a)$
   return (v, u, d)
2: **else if** $b = 0$ **then**
   return $(1, 0, a)$
3: **else**
   $(q, r) \leftarrow$ quotient & remainder
   $(u, v, d) = \text{Euclid}(b, r)$
   return $(v, u - v * q, d)$
4: **end if**

Now we are in the position to prove the following result (stated earlier without proof).

THEOREM

Let $m > 1$ be integer.

The element $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ has a multiplicative inverse iff $\gcd(a, m) = 1$.

PROOF:

Claim (1): $\gcd(a, m) = 1 \Rightarrow \left([a]_m\right)^{-1}$ exists.

$\gcd(a, m) = 1$

$\Rightarrow \exists\ u, v$ s.t. $1 = au + mv$

$\Rightarrow [1]_m = [au]_m + [mv]_m$

$\Rightarrow [1]_m = [a]_m [u]_m$

PROOF:

Claim (2): $([a]_m)^{-1}$ exists $\Rightarrow \gcd(a, m) = 1$.

Let us define $[u]_m \triangleq ([a]_m)^{-1}$.

$\Rightarrow [a]_m [u]_m = [1]_m$

or $[au]_m = [1]_m$

which means $au + mv = 1$ for <u>some</u> $v \in \mathbb{Z}$

$\Downarrow$

$\frac{a}{d} u + \frac{m}{d} v = \frac{1}{d}$ for <u>some</u> $v \in \mathbb{Z}$

But suppose that d divides <u>both</u> a and m.

Proof: $\gcd(a, m) = 1$ implies the existence of integers u and v such that $1 = au + mv$ (Bézout). Hence

$$[1]_m = [au + mv]_m = [au]_m = [a]_m[u]_m,$$

proving that $[u]_m$ is the inverse of $[a]_m$ in $\mathbb{Z}/m\mathbb{Z}$.

For the other direction, if $[u]_m$ is the inverse of $[a]_m$ in $\mathbb{Z}/m\mathbb{Z}$, then $[a]_m[u]_m = [1]_m$ or, equivalently, $[au]_m = [1]_m$. This implies that

$$au + mv = 1$$

for some integer v. If d is a divisor of both a and m, then we can write

$$\frac{a}{d}u - \frac{m}{d}v = \frac{1}{d}.$$

The left hand side is an integer, whereas the right hand side is an integer iff $d = \pm 1$. Hence 1 is the greatest integer that divides a and m. □

Corollary

$\gcd(a, m) = 1$ iff there exist integers u and v such that $1 = au + mv$.

Proof:

If $\gcd(a, m) = 1$, by Bézout, there exist integers u and v such that $1 = au + mv$.

For the other direction, suppose that $1 = au + mv$, where u and v are integers. Then $[1]_m = [au + mv]_m = [au]_m = [a]_m[u]_m$, showing that $[u]_m$ is the inverse of $[a]_m$ in $\mathbb{Z}/m\mathbb{Z}$.

By the theorem that we just proved, $\gcd(a, m) = 1$. □