Introduction to Algebra

Shu Sasaki

13th February 2024

1 Introduction

2 Revising bits and bobs from NSF

2.1 Integer division

2.2 GCD and Euclid's algorithm

2.3 Euclid's algorithm extended

2.4 Prime numbers

3 Modular arithmetic

3.1 Equivalence relations and partitions

Suppose that S is a set. In NSF, a relation $\mathcal{R}$ on S is defined to be a property which may, or may not, hold for each ordered pair of elements in S (i.e. an element of the set $S \times S$ of ordered pairs in S).

A relation $\mathcal{R}$ is said to be

- reflexive if $a\mathcal{R}a$ for every element a of S,
- symmetric if $a\mathcal{R}b$ implies $b\mathcal{R}a$ for all elements a, b of S,
- anti-symmetric if $a\mathcal{R}b$ and $b\mathcal{R}a$ implies $a = b$ for all elements a, b of S,
- transitive if $a\mathcal{R}b$ and $b\mathcal{R}c$ implies $a\mathcal{R}c$ for all elements a, b, c of S,

A reflexive, symmetric and transitive relation is said to be an equivalence relation.

Examples/Exercises. Which of the following are equivalence relations?

(1) $S = \mathbb{R}$ and $a\mathcal{R}b$ if and only if $a = b$ or $a = -b$. (2) $S = \mathbb{Z}$ and $a\mathcal{R}b$ if and only if $ab = 0$. (3) $S = \mathbb{R}$ and $a\mathcal{R}b$ if and only if $a^2 + a = b^2 + b$. (4) $S = \{\text{people in the world}\}$ and $a\mathcal{R}b$ if and only if a lives within 100km of b. (5) $S = \{\text{the points in the plane}\}$ and $a\mathcal{R}b$ if and only if a and b are of

the same distance from the origin. (6) $S = \{\text{positive integers}\}$ and $a\mathcal{R}b$ if and only if ab is a square (of positive integers). (7) $S = \{1, 2, 3\}$ and $a\mathcal{R}b$ if and only if $a = 1$ or $b = 1$. (8) $S = \mathbb{R} \times \mathbb{R}$ and $p\mathcal{R}q$ (where $p = (x(p), y(q))$ and $q = (x(q), y(q))$) if and only if $x(p)^2 + y(p)^2 = x(q)^2 + y(q)^2$.

(1), (3), (5), (6) and (8) are equivalence relations.

Remark. The hardest to verify is the transitivity of $\mathcal{R}$ in (6): if a, b and c are positive integers and ab and bc are respectively squares of positive integers, then can ac be a square of positive integers? Yes! To see this, suppose that $ab = r^2$ and $bc = s^2$ for some positive integers r and s. Multiplying them together, we obtain $ab^2c = (rs)^2$. It suffices to establish that b divides rs, as if this is the case, then ac is a square of $(rs)/b$. How do we prove this? Recall from Proposition 8 that b is a product of prime factors of the form $\prod_p p^{r_p}$ where p ranges over the prime numbers and r_p is a non-negative integer for every p. If p^{r_p} and q^{r_q} are prime factors of b at distinct primes p and q, and if each of them divides rs, then the product $p^{r_p}q^{r_q}$ divides rs (this follows from the 'correct' definition of prime numbers). If we repeat the argument, then we may conclude that $\prod_p p^{r_p}$, i.e., b divides rs. To sum up, it boils down to showing that, for every prime number p that divides b (i.e. $r_p \geqslant 1$), the prime factor p^{r_p} of b divides rs. Since p^{r_p} divides b, it follows that p^{2r_p} divides b^2 and therefore that p^{2r_p} divides $(rs)^2$. If p^{s_p} is the prime factor of rs at p, then p^{2r_p} divides p^{2s_p}, i.e. $2r_p \leqslant 2s_p$, i.e. $r_p \leqslant s_p$. This manifests that p^{r_p} divides rs.

If $\mathcal{R}$ is a relation on S and a is an element of $\mathcal{R}$, we denote by $[a]_\mathcal{R}$, or simply $[a]$ if it is clear which relation we are considering from the context, the set

$$\{b \in S \mid a\mathcal{R}b\}$$

of all elements b in S which are 'in relation to' b with respect to $\mathcal{R}$. If $\mathcal{R}$ is an equivalence relation, we refer to $[a]$ an equivalence class (represented by a).

Examples/Exercises For those relations (1)-(8) above, describe the equivalence classes.

Remark. By definition, if $\mathcal{R}$ is an equivalence relation, then $a\mathcal{R}b$ if and only if $[a]_\mathcal{R} = [b]_\mathcal{R}$. To see 'only if', let c be an element of $[a]_\mathcal{R}$. By definition, this means that $a\mathcal{R}c$. Since $\mathcal{R}$ is reflexive, $c\mathcal{R}a$ holds. Since $a\mathcal{R}b$ by assumption, it follows from the transitivity of $\mathcal{R}$ that $c\mathcal{R}b$. By the reflexivity (again!), it then follows that $b\mathcal{R}c$, i.e. c is a element of $[b]_\mathcal{R}$. To sum up, we have established that $[a]_\mathcal{R} \subseteq [b]_\mathcal{R}$. Swapping the roles, it is also possible to prove $[b]_\mathcal{R} \subseteq [a]_\mathcal{R}$ (exercise!). Combining, we have $[a]_\mathcal{R} = [b]_\mathcal{R}$ as desired.

In preparation of a theorem to follow, we need:

Definition. Let S be a set. A partition of S is a set $\mathcal{P}$ of subsets of S, whose elements are called its parts, having the following properties:

- $\varnothing$ is not a part of $\mathcal{P}$.
- If A and B are distinct parts of $\mathcal{P}$, then $A \cap B = \varnothing$,

- The union of all parts of $\mathscr{P}$ is S.

Examples.

$S = \mathbb{Z}$, $\mathscr{P} = \{\{\text{even integers}\}, \{\text{odd integers}\}\}$.

$S = \{1, 2, 3, 4, 5\}$. $\{\{1, 2\}, \{3, 4\}, \{5\}\}$ and $\{\{1\}, \{2, 3, 4, 5\}\}$ are partitions but $\{\{1, 2\}, \{2, 3\}, \{4, 5\}\}$ is not.

Theorem 9 (Equivalence Relation Theorem).

- Let $\mathscr{R}$ be an equivalence relation on a set S. Then the set $[a]_{\mathscr{R}}$, as a ranges over S, form a partition of S.
- Conversely, given any partition $\mathscr{P}$ of S, there is a unique equivalence relation $\mathscr{R}$ on S such that the parts of $\mathscr{P}$ are the same as the sets $[a]_{\mathscr{R}}$ for a in S. This $\mathscr{R}$ is defined as: $a\mathscr{R}b$ if a and b lies in the same part defined by $\mathscr{P}$.

Proof. (a) We need to check the definitions one by one.

- No element of $\{[a]_{\mathscr{R}}\}$ is $\varnothing$. To see this, observe that, since $a\mathscr{R}a$ (since $\mathscr{R}$ is reflexive), a lies in $[a]_{\mathscr{R}}$; therefore $[a]_{\mathscr{R}}$ is non-empty.
- If $[a]_{\mathscr{R}}$ and $[b]_{\mathscr{R}}$ are distinct, then $[a]_{\mathscr{R}} \cap [b]_{\mathscr{R}} = \varnothing$; or equivalently, if $[a]_{\mathscr{R}} \cap [b]_{\mathscr{R}} \neq \varnothing$, then $[a]_{\mathscr{R}} = [b]_{\mathscr{R}}$. To prove the latter, let c be an non-trivial element of $[a]_{\mathscr{R}} \cap [b]_{\mathscr{R}}$ (made possible by assumption). By definition, this means that $a\mathscr{R}c$ and $b\mathscr{R}c$, or equivalently $c\mathscr{R}b$ (because $\mathscr{R}$ is symmetric). Because $\mathscr{R}$ is transitive, it follows from $a\mathscr{R}c$ and $c\mathscr{R}b$ that $a\mathscr{R}b$. From the remark above, it follows that $[a]_{\mathscr{R}} = [b]_{\mathscr{R}}$.
- The union T of $[a]_{\mathscr{R}}$, as a ranges over S, equals S. Since $[a]_{\mathscr{R}} \subseteq S$ as sets, $T \subseteq S$. Therefore it suffices to prove $S \subseteq T$. Let a be an element of S. Then a lies in $[a]_{\mathscr{R}}$ (see the proof for the first part). Since $[a]_{\mathscr{R}} \subseteq S$, it follows that a lies in S.

(b) We check the conditions of an equivalence relation one by one, following the definition of $\mathscr{R}$ given in the statement.

- reflexive. Since a and a (!) both lie in the same part, $a\mathscr{R}a$ holds.
- symmetric. If a and b lies in the same part, then so do b and a. So the reflexivity follows.
- transitive. Suppose that a and b lies in a part A of $\mathscr{P}$, i.e. a subset A of S. Similarly, suppose that b and c lie in a part B of $\mathscr{P}$. Since b lies in both A and B, it follows from the second condition of the definition of a partition that A and B are *not* distinct, i.e. $A = B$. Therefore a and c both lie in the same part $A = B$, i.e. $a\mathscr{R}c$.

By definition, $[a]_{\mathscr{R}}$ is the set of elements b in S which lie in the same part, say A, as a does. This set is nothing other than A! Hence $[a]_{\mathscr{R}} = A$. So the partition $\mathscr{P}$ of S is the subsets of the form $[a]_{\mathscr{R}}$.

To see the uniqueness ($\mathscr{R}$ is the only equivalence relation whose parts are the subsets $[a]_{\mathscr{R}}$), suppose that $\mathscr{R}$ and $\mathscr{R}'$ are equivalence relations giving rise to the partition $\mathscr{P}$. Since the parts

$\{b \mid a\mathcal{R}b\} = [a]_{\mathcal{R}}$ and $\{b \mid a\mathcal{R}'b\} = [a]_{\mathcal{R}'}$ both contain a, they are the same subsets of S. □

Remark. The theorem asserts that every element a of S belongs to exactly one equivalence class $[a]$.

Example. Let $S = \{1, 2, 3\}$.

Partition	Relations	Equivalence classes
$\{1, 2, 3\}$	$a\mathcal{R}b$ for all $a, b \in \{1, 2, 3\}$	[1]
$\{1\}, \{2, 3\}$	$1\mathcal{R}1$, $a\mathcal{R}b$ for all $a, b \in \{2, 3\}$	[1], [2]
$\{2\}, \{1, 3\}$	$2\mathcal{R}2$, $a\mathcal{R}b$ for all $a, b \in \{1, 3\}$	[2], [1]
$\{3\}, \{1, 2\}$	$3\mathcal{R}3$, $a\mathcal{R}b$ for all $a, b \in \{1, 2\}$	[3], [1]
$\{1\}, \{2\}, \{3\}$	$1\mathcal{R}1$, $2\mathcal{R}2$, $3\mathcal{R}3$	[1], [2], [3]

3.2 Congruence mod n

Let n be a positive integer.

Definition. We define a relation $\equiv$ on the set $\mathbb{Z}$ as follows:

if a and b are elements of $\mathbb{Z}$ (i.e. integers), then $a \equiv b$ if and only if $b - a$ is divisible by n.

Proposition 10. $\equiv$ on $\mathbb{Z}$ is an equivalence relation.

Proof. We need to check that it is reflexive, symmetric and transitive.

- $a \equiv a$.

  Since $a - a = 0$ and this is divisible by n (or any integer, for that matter), $a \equiv a$.

- If $a \equiv b$, then $b \equiv a$.

  Since $a \equiv b$, there exists $b - a$ is divisible by n, i.e., there exists an integer r such that $b - a = rn$. It then follows that $a - b = (-r)n$, i.e. $a - b$ is divisible by n, hence $b \equiv a$.

- If $a \equiv b$ and $b \equiv c$, then $a \equiv c$.

  By assumption, there exist integers r and s such that $b - a = rn$ and $c - b = sn$. It then follows that $c - a = (c - b) + (b - a) = rn + sn = (r + s)n$, hence $a \equiv c$. □

This means that the set of integers is partitioned into equivalence classes by $\equiv$.

Definition. We write $\mathbb{Z}_n$ for the set of equivalence classes modulo n. Personally, I prefer to write $\mathbb{Z}/n\mathbb{Z}$. When n is a prime number p, we write $\mathbb{F}_p$ instead of '$\mathbb{Z}_p$'.

Examples

$$\mathbb{Z}_5 = \left\{ \begin{array}{ccccc} \vdots & \vdots & \vdots & \vdots & \vdots \\ [-5] & [-4] & [-3] & [-2] & [-1] \\ || & || & || & || & || \\ [0] & [1] & [2] & [3] & [4] \\ || & || & || & || & || \\ [5] & [6] & [7] & [8] & [9] \\ || & || & || & || & || \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array} \right\}$$

In a standard clock, keeping track of hours $= \mathbb{Z}_{12}$ while minutes $= \mathbb{Z}_{60}$.

Proposition 11. The cardinality of $\mathbb{Z}_n$ is n, i.e. there are exactly n equivalence classes with respect to $\equiv$ modulo n, namely $[0], [1], \ldots, [n-1]$.

Proof. Firstly, we show that every integer s belongs to one of the congruence classes $[0], \ldots, [n-1]$. Indeed, there exist integers q and $0 \leqslant r \leqslant n-1$ such that $s = nq+r$, i.e. $s \equiv r \bmod n$. Therefore s lies in $[r]$.

Suppose r and s are integers satisfying $0 \leqslant r < s \leqslant n-1$. If $[r] = [s]$, then it would follow that $r - s$ is divisible by n. But this contradicts $0 < r - s < n - 1$. □

3.3 Arithmetic with congruence classes

We define addition, subtraction and multiplication on $\mathbb{Z}_n$ as follows:

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

What about 'division'? Can we make sense of it? It is NOT true that when we divide $[a]$ by $[b]$, we get $\left[\frac{a}{b}\right]$. In the first place, $\frac{a}{b}$ might not even be an integer! Would it be surprising if I tell you, for example, that when $n = 11$, we can even divide $[1]$ by $[3]$ to get $[4]$! This is because $[3][4] = [12] = [1]$.

Examples

$\mathbb{Z}_3 = \mathbb{F}_3 = \{[0], [1], [2]\}$. Then $[1] + [2] = [1 + 2] = [3] = [0]$ while $[2][2] = [2 \times 2] = [4] = [1]$.

$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$. Then $[2] + [5] = [2 + 5] = [7] = [1]$ while $[2][3] = [2 \times 3] = [6] = [0]$. Since 2 divides 6, we know very well that $\frac{6}{2} = 3$ but $\frac{[6]}{[2]} = [3]$? In the first place, $[6] = [0]$, so this should mean the same thing as $\frac{[0]}{[2]} = [3]$ but if we allowed $\frac{[0]}{[2]} = [\frac{0}{2}] = [0]$, then we would get $[0] = [3]$ which is evidently false!

It is necessary to check that these definitions do not depend on our choice of representatives. For example, we've seen $[1]+[2]=[0]$ in $\mathbb{Z}_3$ but we could have had $[4]$ instead of $[1]$, as $[1]=[4]$. In this case, $[4]+[2]=[6]=[0]$, so it does not matter whether we choose 1 or 4 (or any integer congruent to 1 mod 3 for that matter) as a representative of the equivalence class $[1]$.

More rigorously, suppose that a, b and c are integers and that $a \equiv b \bmod n$. To show that the definition of 'addition' does not depend on choice of representatives, we need to show $[a]+[c]=[b]+[c]$. Since the LHS (resp. RHS) is defined to be $[a+c]$ (resp. $[b+c]$), this is equivalent to showing that $[a+c]=[b+c]$. However, it follows from $a \equiv b \bmod n$ that $(a+c)-(b+c)$ is divisible by n and therefore that $(a+c) \equiv (b+c) \bmod n$. It follows that $[a+c]=[b+c]$.

Similarly, it is necessary to check that $[a][c]=[b][c]$, i.e. $[ac]=[bc]$. Since n divides $a-b$, it also divides $c(a-b)=ac-bc$. Therefore $ac \equiv ab$, i.e. $[ac]=[ab]$.

3.4 Modular inverses

Let n be a fixed positive integer. Throughout this section, $\equiv$ denotes the 'congruence modulo n' and $[a]$ denote the congruence class of integers congruent to a modulo n.

Definition. We say that $[a]$ has a multiplicative inverse if there exists an integer b such that $[a][b]=[1]$.

Remark. The multiplicative inverse, if exists, is unique. Indeed, if $[b]$ and $[c]$ are elements of $\mathbb{Z}_n$ satisfying $[a][b]=[1]$ and $[a][c]=[1]$, then mutiplying $[b]$ on both sides of $[c][a]=[1]$ yields $[c][a][b]=[1][b]$, i.e. $[c][1]=[b]$, i.e. $[c]=[b]$.

Theorem 12. The elements $[a]$ of $\mathbb{Z}_n$ has a multiplicative inverse if and only if $\gcd(a,n)=1$.

Proof. Suppose that $[a]$ has a multiplicative inverse, i.e. $[b]$ such that $[a][b]=[1]$, i.e. $[ab]=[1]$. This means that $ab-1$ is divisible by n, hence there exists an integer c such that $ab+(-c)n=1$. As $\gcd(a,n)$ divides the LHS, it does so the RHS, i.e. 1. The only non-negative integer diving 1 is 1, so $\gcd(a,n)=1$.

Conversely, suppose $\gcd(a,n)=1$. By Bezout, there exist integers b and c such that $ab+nc=1$. Since $ar \equiv 1 \bmod n$, it follows that $[a][b]=[ab]=[1]$. The multiplicative inverse of $[a]$ is therefore $[b]$. □

Examples.

What is the multiplicative inverse of $[4]_{21}$? Since $\gcd(4,21)=1$, the theorem assures us of the multiplicative inverse. How do we compute it? The proof indeed explains how. Since $\gcd(4,21)=1$, Euclid's algorithm (backed up by Bezout) gives us a pair of integers r and s such that $4r+21s=\gcd(4,21)=1$. Indeed, $(r,s)=(-5,1)$ does the job. In particular, $4r \equiv 1 \bmod 21$ and it therefore follows that $[4][r]=[4r]=[1]$. So $[-5]=[16]$ is the multiplicative inverse of $[4]$.

What is the multiplicative inverse of $[23]_{2023}$? Firstly, we compute $\gcd(23,2023)$ by Euclid's algorithm:

$$\begin{aligned} 2023 &= 23 \cdot 87 + 22 \\ 23 &= 22 \cdot 1 + 1. \end{aligned}$$

Hence $1 = 23 - 1 \cdot 22 = 23 - 1 \cdot (2023 - 23 \cdot 87) = (-1) \cdot 2023 + 88 \cdot 23$ and $[88]$ is the multiplicative inverse of $[23]$.

What is the multiplicative inverse of $[17]_{2023}$? Since $2023 = 119 \cdot 17$ and 17 is a prime number, $\gcd(2023, 17) = 17$. It follows from the theorem above that $[17]$ has no multiplicative inverse.

If p is a prime number, then $\mathbb{Z}_p = \{[0], [1], \ldots, [p-1]\}$ and, by the theorem, it follows that $\gcd(a, p-1) = 1$ if and only if a is prime to p. Therefore the congruence classes $[1], \ldots, [p-1]$ all have inverses.

Proposition 13. Suppose $n > 1$. The element $[a]$ of $\mathbb{Z}_n$ has no multiplicative inverse if and only if there exists an integer b, not congruent to 0 modulo n, such that $[a][b] = [0]$.

Proof. Suppose that $[a]$ has no multiplicative inverse. It then follow from the theorem above that $c = \gcd(a, n) > 1$. If we let $b = n/c$, then b is a positive integer not congruent to 0 mod n (if it were congruent to 0 mod n, then b would be n and force $c = 1$). By definition, $ab = an/c = (a/c)n$ is divisible by n, for a/c is an integer. It follows that $ab \equiv 0 \bmod n$, hence that $[a][b] = [ab] = [0]$.

To prove the converse, suppose that $[a]$ has a multiplicative inverse– we aim at establishing that no integer b, not congruent to n, satisfies $[a][b] = [0]$. By assumption, there exists an integer c such that $[a][c] = [1]$. Let b be an integer not congruent to 0 mod n. Multiplying the both sides of $[a][c] = [1]$ by $[b]$, we obtain $[b] = [b][a][c] = [c]([a][b])$. If $[a][b] = [0]$, then the RHS is $[0]$, hence the LHS $[b]$ is $[0]$, in other words, b is divisible by n. However this contradicts the assumption that b is not. □

Remark. Proposition 13 is paraphrasing $\gcd(a, n) > 1$.

Given a positive integer n, how many elements in $\mathbb{Z}_n$ has multiplicative inverses? In theory, we ask, for every $0 \leq a \leq n - 1$, whethere $\gcd(a, n) = 1$ (or not) to compile a list. For example, if $n = 24$, $\{1, 5, 7, 11, 13, 17, 19, 23\}$ (incidentally they are all prime numbers!) is the set of integers $0 \leq a \leq n - 1 = 23$ such that $\gcd(a, 24) = 1$. Hence there are 8 elements in total.

What about $n = 108$? That seems to entail a lot of computations. There is a formula!– it goes by the name of Euler's totient function. Recall from the fundamental theorem of arithmetic that n may be written as the product $\prod_p p^{r_p}$ of prime factors. Then the number we are looking for is computed by

$$\phi(n) = \prod_p (p-1)p^{r_p - 1}.$$

For example, $24 = 2^3 \cdot 3$, so $\phi(24) = (2-1)2^2 \cdot (3-1) = 8$ which is consistent with the computation above. Similarly, $108 = 3^3 \cdot 2^2$, so $\phi(108) = (3-1) \cdot 3^2 \cdot (2-1) \cdot 2 = 36$. Is this consistent with your computation?

What are multiplicative inverses useful for? They are useful in solving linear congruence equations.

Example. Solve $7X \equiv 1 \bmod 11$, or equivalently $[7]_{11}[X]_{11} = [1]_{11}$ in $\mathbb{F}_{11}$.

The first approach: Since $\mathbb{F}_{11} = \{[0], [1], \ldots, [10]\}$, we do trial and error.

$[X]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$
$[7][X]$	$[0]$	$[7]$	$[3]$	$[10]$	$[6]$	$[3]$	$[9]$	$[5]$	$[1]$	$[8]$	$[4]$
$[7][X]-[1]$	$[10]$	$[6]$	$[2]$	$[9]$	$[5]$	$[2]$	$[8]$	$[4]$	$[0]$	$[7]$	$[3]$

so $[X] = [8]$ is the solution.

The second approach: Firstly, we find the multiplicative inverse of [7] by Euclid's algorithm

$$\begin{aligned} 11 &= 7 \cdot 1 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 \end{aligned}$$

hence $1 = 4 - 1 \cdot 3 = 4 - 1 \cdot (7 - 1 \cdot 4) = 2 \cdot 4 - 1 \cdot 7 = 2 \cdot (11 - 1 \cdot 7) - 1 \cdot 7 = 2 \cdot 11 - 3 \cdot 7$. So $[-3] = [8]$ is the multiplicative inverse of [7]. Multiplying the both sides of $[7][X] = [1]$ by [8], we then get

$$[8][7][X] = [8][1].$$

The LHS, [8][7] is [1], without computing as $[8 \cdot 7] = [56] = [1]$, because we know that [8] is the multiplicative inverse of [7] so by definition $[8][7] = [1]$. The RHS is [8]. Putting these together, we see that $[X] = [8]$.

The second approach suggests it should be possible to solve equations of the form $[a][X] + [b] = [c]$ if $\gcd(a, n) = 1$ (or equivalently the liner congruence equation $aX \equiv c \bmod n$). Indeed, the equation is equivalent to $[a][X] = [c - b]$. By Theorem 12, there exists a multiplicative inverse, denoted $[a]^{-1}$, of $[a]$. Multiplying $[a][X] = [c - b]$ by $[a]^{-1}$, we obtain

$$[X] = [c - b][a]^{-1}$$

(not that the RHS is NOT $[c - b]/[a]$!).

It is possible to solve equations as above, even if $\gcd(a, n) > 1$ but we shall not touch upon these in this module. Go to Number Theory in Year 2, if you are interested.