UNIT 3

Modular arithmetic

Contents

INTEGER NUMBERS

1. Integer number arithmetic

Arithmetic is understood as the study of the operations between numbers and their properties. In the set of integer numbers $\mathbb{Z}$ we consider two binary operations, the addition (+) and the product (·). All of their properties are derived from the consideration of the following axioms:

(A.1) They are **closed operations** within $\mathbb{Z}$, that is $(\forall n, m \in \mathbb{Z})(n + m \in \mathbb{Z} \wedge n \cdot m \in \mathbb{Z})$

$$+: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} | (n, m) \to n + m$$

$$\cdot: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} | (n, m) \to n \cdot m$$

(A.2) **Commutative law:** $(\forall n, m \in \mathbb{Z})(n + m = m + n \wedge n \cdot m = m \cdot n)$

(A.3) **Associative law:** $\forall n, m, k \in \mathbb{Z}\big((m + n) + k = m + (n + k) \wedge (n \cdot m) \cdot k = n \cdot (m \cdot k)\big)$

(A.4) **Existence of identity elements:** $(\exists 0,1 \in \mathbb{Z})(\forall n \in \mathbb{Z})(n + 0 = n \wedge n \cdot 1 = n)$

(A.5) **Distributive law:** $(\forall n, m, k \in \mathbb{Z})(n \cdot (m + k) = n \cdot m + n \cdot k)$

(A.6) **Existence of an inverse element:** $(\forall n \in \mathbb{Z})(\exists! (-n) \in \mathbb{Z})(n + (-n) = 0)$

(A.7) **Cancellation law:** $(\forall n \in \mathbb{Z})\Big(n \neq 0 \to \big((\forall m, k \in \mathbb{Z})(n \cdot m = n \cdot k \to m = k)\big)\Big)$

Notes:

- ✓ From the fifth axiom, we can define the subtraction operation as $n - m := n + (-m) \forall n, m \in \mathbb{Z}$
- ✓ This set of axioms enable us to prove other integer properties such as:

$$(\forall n \in \mathbb{Z})(0 \cdot n = 0)$$

$$(\forall n, m \in \mathbb{Z})(n - (-m) = n + m)$$

2. Ordering of integer numbers

We can endow integer numbers with an order relationship that has a set of properties defined by the following axioms: $(\forall n, m, k \in \mathbb{Z})$

(A.8) $(\forall n \in \mathbb{Z})(n \leq n)$

(A.9) $(\forall n, m \in \mathbb{Z})(n \leq m \wedge m \leq n \rightarrow n = m)$

(A.10) $(\forall n, m, k \in \mathbb{Z})(n \leq m \wedge m \leq k \rightarrow n \leq k)$

(A.11) $(\forall n, m, k \in \mathbb{Z})(n \leq m \rightarrow n + k \leq m + k)$

(A.12) $(\forall n, m, k \in \mathbb{Z})(n \leq m \wedge 0 \leq k \rightarrow n \cdot k \leq m \cdot k)$

(A.13) **Well-ordering principle:** $(\forall A \subseteq \mathbb{Z}^+)\big(A \neq \emptyset \rightarrow (\exists m \in A)(\forall a \in A)(m \leq a)\big)$

Notes:

✓ The well-ordering principle ensures that any subset of $\mathbb{Z}^+ = \{n \in \mathbb{Z}, 0 \leq n\} = \mathbb{N} \cup \{0\} = \{n \in \mathbb{Z}, 1 \leq n\} \cup \{0\}$ contains an infimum (minimum element).

✓ We define m s a lower bound of a set $A \subseteq \mathbb{Z}$ if $(\forall a \in A)(m \leq a)$. We define a lower bound of a set as an infimum when it belongs to the set.

✓ Through the definition of the infimum element, we can infer that the infimum must be unique. If two infimums m_1, m_2 were to exist, through the definition we would find that $m_1 \leq m_2 \wedge m_2 \leq m_1$, and by applying axiom 9 we can conclude that $m_1 = m_2$.

✓ From the $\leq$ relationship it is possible to define the $<, \geq, >$ relationships: $n < m \leftrightarrow n \leq m \wedge n \neq m$

✓ This group of axioms enable us to prove other ordering properties for integer numbers such as $n \leq m \leftrightarrow -m \leq -n$, $n \leq m \wedge k \leq 0 \rightarrow m \cdot k \leq n \cdot k$

3. Induction principle

Proposal:

Be it $S \subseteq \mathbb{N} = \{n \in \mathbb{Z}, 1 \leq n\}$ so that the following conditions are met:

1. Induction base case: $1 \in S$
2. Induction hypothesis: $(\forall k \in \mathbb{N})(k \in S \rightarrow k + 1 \in S)$

Then $S = \mathbb{N}$.

Proof *(exercise)*

Proof is achieved through *reductio ad absurdum* (reduction to absurdity):

Suppose that $S \neq \mathbb{N}$ and consider S^c.

Take m, the infimum for S^c, guaranteed to exist by the well-ordering principle.

Condition (1.) states that: $1 \in S \Rightarrow m \neq 1$ and therefore: $(m-1) \in \mathbb{N} \wedge (m-1) \notin S^c \rightarrow (m-1) \in S$

Applying the induction hypothesis, we can affirm $(m-1)+1 = m \in S$, which contradicts $m \in S^c$.

Since we have achieved a contradiction by supposing $S \neq \mathbb{N}$, we can assure that $S = \mathbb{N}$

Example *(exercise)*

From the sequence defined recursively by $a_1 = 2$ and $a_n = a_{n-1} + 2n \; \forall n \geq 2$ verify via induction that $(\forall n \in \mathbb{N})\big(a_n = n(n+1)\big)$.

Considering $S = \{n \in \mathbb{N}, a_n = n(n+1)\}$ it is enough to prove through induction that $S = \mathbb{N}$.

4. Division, quotient, and remainder

The Division Theorem

Given two integer numbers D, d with $d \in \mathbb{N}$, there are two other integer numbers $q, r \in \mathbb{Z}$ such that:

1. $D = d \cdot q + r$
2. $0 \leq r < d$

In addition, $q, r \in \mathbb{Z}$ are unique, and thus $(\forall D \in \mathbb{Z})(\forall d \in \mathbb{N})(\exists! q', r' \in \mathbb{Z})(D = d \cdot q' + r' \wedge 0 \leq r' < d)$

Proof *(exercise)*

The proof process of this theorem has two parts. Firstly, we must prove the existence of $q, r \in \mathbb{Z}$ such that conditions 1. and 2. are met. To that extent, we can consider the set $R = \{x \in \mathbb{N} \mid D = d \cdot y + x\}$, prove that is not an empty set and apply the well-ordering principle to take its infimum, r. This will also ensure the existence of $q \in \mathbb{Z}$, verifying $D = d \cdot q + r$. To prove that 2. is verified, we use *reductio ad absurdum*.

Secondly, we must prove that $q, r \in \mathbb{Z}$ are unique for each pair of integers D, d with $d \in \mathbb{N}$. To that extent, it is enough to consider the existence of $q', r' \in \mathbb{Z}$ with the same properties and prove that they are equal to $q, r \in \mathbb{Z}$.

Quotient and remainder

The elements $q, r \in \mathbb{Z}$ that verify the division theorem conditions are respectively defined as quotient and remainder.

Multiples and divisors

Definition:

Given two integer numbers $D, d \in \mathbb{Z}$, we will write $d|D$ and say that:

- ✓ d ***divides*** D, or
- ✓ d is a ***divisor*** of D, or
- ✓ d is a ***factor*** of D, or
- ✓ D is a ***multiple*** or d

If we can find $q \in \mathbb{Z}$ such that $D = d \cdot q$

Or in other words: $d|D \Leftrightarrow (\exists q \in \mathbb{Z})(D = d \cdot q)$

4.1. Greatest Common Divisor

Definition:

Given two integers $n, m \in \mathbb{Z}$, we say that $d \in \mathbb{N}$ is one of the greatest common divisors of n and m, or in other words, $d = gcd(n, m)$, if it is possible to verify that:

1. $d|n \wedge d|m$ (that is, d is a common divisor of n and m), and
2. $(\forall d' \in \mathbb{N})(d'|n \wedge d'|m \rightarrow d'|d)$ (that is, d is the greatest of the common divisors)

Proposal:

Given two integers $n, m \in \mathbb{Z}$, the greatest common divisor of n and m is unique:

$$(\forall n, m \in \mathbb{Z})\big(\exists!\, d = gcd(n, m)\big)$$

Proof *(exercise)*

This is an easy proof. It is possible to suppose that two greatest common divisors $d, d' \in \mathbb{N}$ exist, and then prove that they are equal through the definition.

Notes

It is possible to verify that $d = gcd(n, m) = gcd(-n, m) = gcd(-n, -m) = gcd(n, -m)$

For this reason, we will always calculate the greatest common divisor of positive integers.

4.1.1. Euclidean algorithm

Proposal:

Be it two integer numbers $n, m \in \mathbb{Z}$.

If $d = gcd(n, m)$, then d divides any linear combination of n and m.

That is, $(\forall a, b \in \mathbb{Z})\big(d|(am + bn)\big)$

Proof

If $d = mcd(n, m)$ then $d|n \wedge d|m$.

Through the divisor definition, we can affirm the existence of $q, q' \in \mathbb{Z}$ such that $n = q \cdot d \wedge m = q' \cdot d$.

Applying these equalities to the linear combination, we find that:

$$an + bn = a \cdot q \cdot d + b \cdot q' \cdot d = (a \cdot q + b \cdot q') \cdot d$$

Through the divisor definition, it is possible to conclude that $d|a \cdot n + b \cdot m$, as we wanted to prove.

Proposal:

Be it $D, d \in \mathbb{N}$ such that $D \geq d$, and $q, r \in \mathbb{N}$ such that $D = d \cdot q + r$, then $gcd(D, d) = gcd(d, r)$.

Proof

Be it $M = gcd(D,d)$, to prove that $M = gcd(d,r)$ we must verify the properties of the definition.

Since $M|D \wedge M|d \rightarrow M|(d \cdot q + r) \wedge M|d$, due to the prior proposal we know that M divides any linear combination of D and d, hence $M|(D - q \cdot d)$, that is, $M|r$. Therefore, $M|d \wedge M|r$.

In addition, if $M'|d \wedge M'|r$, then $M'|D$ (D being a linear combination of d and r), and therefore $M'|M$, thus proving the second property of the greatest common divisor definition.

The **Euclidean algorithm** to calculate the greatest common divisor of two numbers consists in the recursive application of the prior proposal. Given $D, d \in \mathbb{N}$, we recursively define $q_i, r_i \in \mathbb{N}$ as follows:

$$D = d \cdot q_1 + r_1, 0 \leq r_1 < d$$
$$d = r_1 \cdot q_2 + r_2, 0 \leq r_2 < r_1$$
$$r_1 = r_2 \cdot q_3 + r_3, 0 \leq r_3 < r_2$$
$$\vdots$$
$$r_i = r_{i+1} \cdot q_{i+2} + r_{i+2}, 0 \leq r_{i+2} < r_{i+1}$$
$$\vdots$$

Since $r_1 > r_2 > r_3 > \cdots > r_i > r_{i+1} > \cdots$ and $\forall i, r_i \in \mathbb{Z}^+$ we can affirm through the well-ordering principle that a $r_k = 0$ will exist. Hence, the last steps of the process will take the following form:

$$\vdots$$
$$r_{k-3} = r_{k-2} \cdot q_{k-1} + r_{k-1}, 0 \leq r_{k-1} < r_{k-2}$$
$$r_{k-2} = r_{k-1} \cdot q_k + r_k, r_k = 0$$

Observe that, in the last line, we obtained: $r_{k-2} = r_{k-1} \cdot q_k \rightarrow r_{k-1}|r_{k-2}$

And therefore: $gcd(r_{k-2}, r_{k-1}) = gcd(r_{k-1} \cdot q_k, r_{k-1}) = r_{k-1}$

Applying the prior proposal to each of the equalities we can reach $gdc(D,d) = gcd(r_{k-2}, r_{k-1}) = r_{k-1}$.

Examples

✓ Calculate $gcd(105,30)$

$$105 = 30 \cdot 3 + 15, 0 \leq 15 < 30$$
$$30 = 15 \cdot 2 + 0$$

Then $gcd(105,30) = 15$

✓ Calculate $gcd(504,396)$

$$504 = 396 \cdot 1 + 108, 0 \leq 108 < 396$$
$$396 = 108 \cdot 3 + 72, 0 \leq 72 < 108$$
$$108 = 72 \cdot 1 + 36, 0 \leq 36 < 172$$
$$72 = 36 \cdot 2 + 0$$

Then $mcd(504,396) = 36$

4.1.2. Coprime numbers and the Euler's phi function

Definition

We define two integers $n, m \in \mathbb{Z}$ as **coprime** or **mutually prime** when $mcd(n, m) = 1$

Example

Calculate $gcd(17,30)$

$$30 = 17 \cdot 1 + 13, 0 \leq 13 < 17$$
$$17 = 13 \cdot 1 + 4, 0 \leq 4 < 13$$
$$13 = 4 \cdot 3 + 1, 0 \leq 1 < 4$$
$$4 = 1 \cdot 4 + 0$$

$gcd(17,30) = 1 \rightarrow 17,30$ are coprime

Definition

Given $n \in \mathbb{Z}$, **Euler's $\Phi(n)$ function** as the function that indicates the cardinal of a set of positive coprime numbers lesser or equal than n:

$$\Phi: \mathbb{N} \rightarrow \mathbb{N}$$
$$n \rightarrow \Phi(n) = |\{x \in \mathbb{N} | mcd(x, n) = 1 \wedge 1 \leq x \leq n\}|$$

Notes

$$\Phi(1) = 1$$
$$\Phi(2) = 1$$
$$\Phi(3) = 2$$
$$\Phi(4) = 2 \text{ (Nor 2 nor 4 match the requisites)}$$
$$\Phi(5) = 4$$

4.1.3. Diophantine equations and Bézout's identity

Definition

An equation $ax + by = e$, with $a, b, e, x, y \in \mathbb{Z}$ is called **Diophantine equation**.

Theorem: Bézout's identity

Be it $a, b \in \mathbb{N}$ and $d = gcd(a, b)$. Then $\exists n, m \in \mathbb{Z}$ such that $d = n \cdot a + m \cdot b$.

Proof *(exercise)*

To prove this theorem, it is enough to go backwards in the Euclidean algorithm process.

Examples

✓ $mcd(105,30) = 17$

$$\left.\begin{matrix} 105 = 30 \cdot 3 + 15 \\ 30 = 15 \cdot 2 + 0 \end{matrix}\right\} \rightarrow \left\{ 105 - 30 \cdot 3 = 15 \rightarrow 105 \cdot \boxed{1} + 30 \cdot \boxed{(-3)} = 15 = mcd(105,30) \right.$$

✓ $gcd(504,396) = 36$

$$\left.\begin{array}{r} 504 = 396 \cdot 1 + 108 \\ 396 = 108 \cdot 3 + 72 \\ 108 = 72 \cdot 1 + 36 \\ 72 = 36 \cdot 2 + 0 \end{array}\right\} \rightarrow \left\{\begin{array}{l} 504 - 396 \cdot 1 = 108 \\ 396 - 108 \cdot 3 = 72 \\ 108 - 72 \cdot 1 = 36 \end{array}\right\} \rightarrow \left\{\begin{array}{l} 36 = 108 - 72 \cdot 1 = \\ \quad = 108 - (396 - 108 \cdot 3) \cdot 1 = 4 \cdot 108 - 396 \\ \quad = 4 \cdot (504 - 396 \cdot 1) - 396 \\ \quad = 504 \cdot \boxed{4} + 396 \cdot \boxed{(-5)} \end{array}\right.$$

Notes

Be it a Diophantine equation $ax + by = e$ with $d = gcd(a, b)$.

Through Bézout's identity we can affirm that $\exists n, m \in \mathbb{Z}$ such that $d = n \cdot a + m \cdot b$.

If we verify that d divides e, $d|e \rightarrow (\exists q)(e = q \cdot d)$, we can infer:

$$e = d \cdot q = (n \cdot a + m \cdot b) \cdot q = a \cdot (q \cdot n) + b \cdot (q \cdot m)$$

Hence $x = q \cdot n \wedge y = q \cdot m$ will be solutions to Bézout's identity and $(\exists a', b')(a = a' \cdot d \wedge b = b' \cdot d)$.

Theorem

A Diophantine equation $ax + by = e$ has a solution if and only if $gcd(a, b)|e$.

In addition, if (x_0, y_0) is a solution for $ax + by = e$, the set of solutions of the equation takes the form:

$$S = \left\{\left(x_0 + k \cdot \frac{b}{d}, y_0 - k \cdot \frac{a}{d}\right) | k \in \mathbb{Z} \wedge d = mcd(a, b)\right\}$$

Proof *(exercise)*

Prove $gcd(a, b)|e \rightarrow (\exists x, y \in \mathbb{Z})(a \cdot x + b \cdot y = e)$ and $(\exists x, y \in \mathbb{Z})(a \cdot x + b \cdot y = e) \rightarrow gcd(a, b)|e$.

To that extent, it is possible to use the prior notes. In addition, it is necessary to prove that all the elements of the set S are solutions of the Diophantine equation.

Example:

To solve the Diophantine equation, we must first calculate the greatest common divisor through the Euclidean algorithm:

$$gcd(365,72) = 1$$
$$365 = 72 \cdot 5 + 5$$
$$72 = 5 \cdot 14 + 2$$
$$5 = 2 \cdot 2 + 1$$

Since $1|18$, according to the prior theorem, the equation has a solution. We calculate Bézout's identity through the development of the Euclidean Algorithm:

$$1 \underset{5=2\cdot 2+1}{=} 5 - 2 \cdot 2 \underset{72=5\cdot 14+2}{=} 5 - 2 \cdot (72 - 5 \cdot 14) = 5 \cdot 29 - 2 \cdot 72 \underset{365=72\cdot 5+5}{=} (365 - 75 \cdot 5) \cdot 29 - 2 \cdot 72$$
$$= 29 \cdot 365 + (-147)72$$

Therefore $1 = 29 \cdot 365 + (-147)72 \Rightarrow 18 = 29 \cdot 18 \cdot 365 + (-147 \cdot 18)72 = 522 \cdot 365 + (-2646)72$

In this manner, the solution to the equation is $S = \{(522 + k \cdot 72, -2646 - k \cdot 365) | k \in \mathbb{Z}\}$

4.2. Least common multiple

Definition

Given $a, b \in \mathbb{N}$, we define $m \in \mathbb{N}$ as a least common multiple of a and b, that is, $m = lcm(a, b)$, when it is possible to verify that:

1. $a|m \wedge b|m$ (that is, m is a common multiple to a and b)
2. $(\forall m' \in \mathbb{N})(a|m' \wedge b|m' \rightarrow m|m')$ (that is, any multiple of a and b is multiple of $m = mcm(a, b)$, making m the least of the common multiples of a and b)

Proposal

Be it $a, b \in \mathbb{N}$ and $d = gcd(a, b)$.

We can verify that $m = lcm(a, b) = \frac{a \cdot b}{d}$.

Proof *(Exercise)*

It is enough to prove that conditions 1 and 2 are met for $m = \frac{a \cdot b}{d}$

Examples

- ✓ $gcd(105,30) = 15 \rightarrow lcm(105,30) = \frac{105 \cdot 30}{15} = 210$
- ✓ $gcd(504,396) = 36 \rightarrow lcm(504,396) = \frac{504 \cdot 396}{36} = 5544$

5. Prime numbers factorization

Definition

It is said that $p \in \mathbb{N}$ is a **prime number** if $p \geq 2$ and if the only integers that divide it are 1 and p

$$p \in \mathbb{N} \Leftrightarrow (\forall n \in \mathbb{Z})(n|p \rightarrow n = 1 \vee n = p)$$

Notes

If $p \in \mathbb{N}$ is a prime number, then $\Phi(p) = p - 1$

Theorem: unique factorization based on prime numbers

Every natural number $n \geq 2$ can be factorized as a unique product of prime numbers, except for the order of the factors.

Proof *(Exercise)*

For this theorem we must prove both the existence of the factorization and its uniqueness.

Existence:

To prove the existence, we proceed through *reductio ad absurdum:*

Take the set $B = \{n \in \mathbb{N} | n \geq 2 \wedge n \text{ is not factorized through prime numbers}\}$.

Proving the theorem is to prove that $B = \emptyset$, hence we suppose the opposite, $B \neq \emptyset$.

We take the infimum of the set $m = min\{n \in B\}$. We can suppose that it is not a prime number, since a prime number can be factorized by itself.

Since m is not a prime number, by definition there exist m_1 and m_2 such that

$$(m = m_1 \cdot m_2) \wedge (1 < m_1, m_2 < m).$$

$m_1, m_2 \notin B$, and hence they can be factorized as a product of prime numbers, which in turn means that m can also be factorized through prime numbers, which contradicts $m \in B$.

Then, we can conclude that $B = \emptyset$, and the existence of the factorization in prime numbers for every natural number is proven.

Uniqueness:

To prove uniqueness, we proceed similarly.

We consider the set $B = \{n \in \mathbb{N} | n \geq 2 \wedge n \text{ does not have a unique factorization in prime numbers}\}$ and prove that it is an empty set.

Theorem:

Be it $a, b \in \mathbb{N}$. The necessary and sufficient condition for $a|b$, that is, for a to divide b, is that b contains all the prime factors of a with equal or greater exponents.

Theorem:

The greatest common divider of two numbers $a, b \in \mathbb{N}$ is the product of the prime factors common to both, taking each with the lesser of the exponents with which they appear in the factorizations of the given numbers.

The least common multiple of two numbers $a, b \in \mathbb{N}$ is the product of the common and non-common prime factors of both, taking each with the greater of the exponents with which they appear in the factorization of the given numbers.

Proposal:

If $m = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_s^{n_s}$, where $\forall i \in \{1,2,\ldots s\}$ p_i is a prime number and n_i is the number of times that p_i is repeated in the factorization of m as a product of prime numbers, then:

$$\Phi(m) = \frac{m}{p_1 \cdot p_2 \cdot \ldots \cdot p_s} \cdot (p_1 - 1)(p_2 - 1) \cdot \ldots \cdot (p_s - 1)$$

6. Large prime numbers and the factorization of large numbers

When we want to verify whether a number p is a prime number, the simplest algorithm that we can use is to test whether the number is divisible by all the prime numbers lesser than $\sqrt{p}$. If there are no numbers that divide p, we can conclude that it is a prime number. If the opposite is true, we will have found a factor for its factorization in prime numbers.

However, this algorithm is not valid for large prime numbers. Should we try to use it to test whether numbers lesser than 10^{100} are prime numbers, it would take us around 200 years to achieve the solution.

In order to test whether large numbers are prime numbers, we must use primality tests that provide us with a probability on whether p is a prime number. Two of the most common tests, due to their simplicity, are the Lehmann and Miller-Rabin primality tests. These tests are based on mathematical congruences, which will be analyzed further down the road.

When the issue is to achieve the factorization of a number, we might again leverage the brute force algorithm based on testing all the prime numbers lesser than the value of the number's root. Again, this algorithm is very slow and not effective for large numbers. There are other methods that, while less efficient, are quicker when dealing with large numbers: the Fermat primality test, Pollard's p-1 algorithm, or quadratic factorization methods.

Fermat's primality test

The aim of this method is to factorize a number $n \in \mathbb{N}$ by finding two other numbers $x, y \in \mathbb{N}$ such that $n = (x+y)(x-y) = x^2 - y^2$.

This way, we would obtain a factorization $n = a \cdot b$, with $a = (x+y)$ and $b = (x-y)$.

The steps of the algorithm are as follows:

1. Take x_0, the first integer number greater than $\sqrt{n}$
2. For every $i = 1,2,\ldots$ calculate $e_i = x_i^2 - n$
3. Afterwards:
   - i. If e_i is a perfect square, take $y_i = \sqrt{e_i} \in \mathbb{N}$ and $n = (x_i + y_i)(x_i - y_i)$
   - ii. If e_i is not a perfect square take $x_{i+1} = x_i + 1$ and go back to step 2

Notes

✓ In step 3.ii, when we go back to step 2 to calculate e_{i+1}, we can use the prior iteration as follows:

$$e_{i+1} = e_i + 2x_i + 1$$

Observe that:

$$e_{i+1} = x_{i+1}^2 - n = (x_i + 1)^2 - n = \underbrace{x_i^2 - n}_{e_i} + 2x_i + 1 = e_i + 2x_i + 1$$

✓ In addition, we can only carry out this step if $x_{i+1} \leq \frac{n+1}{2}$, in other case this method will not yield a factorization.

MODULAR ARITHMETIC

7. Modular arithmetic

Definitions:

Be it $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$.

We say that a **is congruent with** b **module** m if $m|(b-a)$

And write it as: $a \equiv b \, mod \, m$ or $a = b \, mod \, m$

With $m \in \mathbb{N}$, for each $a \in \mathbb{Z}$ we define its **equivalence class** module m as:

$$[a]_m = \{b \in \mathbb{Z} | a \equiv b \, mod \, m\}$$

Exercise

With $m \in \mathbb{N}$, to be congruent module m is an equivalence relationship in $\mathbb{Z}$. To verify this, it is enough to prove that the relationship defined by that property is reflective, symmetric, and transitive.

Notes

✓ Observe that if $a \equiv b \, mod \, m$, by definition $m|(b-a)$.

Through the definition of the division relationship, this in turn means that

$$(\exists q \in \mathbb{Z})(b - a = q \cdot m) \Leftrightarrow (\exists q \in \mathbb{Z})(b = q \cdot m + a)$$

Then, a is the remainder obtained by dividing b by m.

✓ With $m \in \mathbb{N}$, the division theorem ensures that $\forall a \in \mathbb{Z}, \exists! \, q, r \in \mathbb{Z}$ so as $a = m \cdot q + r \wedge 0 \leq r < m$

If $a = m \cdot q + r \wedge 0 \leq r < m$ with $m|(a-r)$

Through the definition of the module m congruency relationship, we can write: $[a]_m = [r]_m$

Hence, given $m \in \mathbb{N}$, $\forall a \in \mathbb{Z}$ there exists a **unique** $r \in \mathbb{N}$ such that $r \in [a]_m = [r]_m$ and $0 \leq r < m$.

✓ This element is called the **canonical representative** of the equivalence class $[a]_m$

✓ Observe that given $m \in \mathbb{N}$, $\mathbb{Z}$ is divided into m disjoint sets that are the equivalence classes module m: $\mathbb{Z} = [0]_m \cup [1]_m \cup [2]_m \cup \ldots \cup [m-1]_m$

Definitions:

Be it $m \in \mathbb{N}$.

The set $\mathbb{Z}_m = \mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}$ is the set of **integers module** m.

The binary operations **addition** and **product** in the set $\mathbb{Z}_m$ are defined as:

$$+: \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m \mid ([a]_m, [b_m]) \to [a]_m + [b_m] := [a+b]_m$$

$$\cdot: \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m \mid ([a]_m, [b_m]) \to [a]_m \cdot [b_m] := [a \cdot b]_m$$

The arithmetic defined in $\mathbb{Z}_m$ by these operations is called **modular arithmetic**.

Proposal:

1. The result of the addition and product in $\mathbb{Z}_m$ do not depend on the canonical representative in the equivalence class:

$$[a]_m = [a']_m \wedge [b]_m = [b']_m \Rightarrow \begin{cases} [a]_m + [b]_m = [a']_m + [b']_m \Leftrightarrow [a+b]_m = [a'+b']_m \\ [a]_m \cdot [b]_m = [a']_m \cdot [b']_m \Leftrightarrow [a \cdot b]_m = [a' \cdot b']_m \end{cases}$$

2. These operations verify the first 6 axioms of arithmetic in $\mathbb{Z}$.

(A.14) They are **closed operations** in $\mathbb{Z}_m$.

(A.15) **Commutative law**

(A.16) **Associative law**

(A.17) **Existence of identity elements**

(A.18) **Distributive law**

(A.19) **Existence of an inverse element**

Notes

✓ One of the most important differences between $\mathbb{Z}$ and $\mathbb{Z}_m$ is that the cancellation law of integer numbers (A.7) $(\forall n \in \mathbb{Z})\left(n \neq 0 \rightarrow \left((\forall m, k \in \mathbb{Z})(n \cdot m = n \cdot k \rightarrow m = k)\right)\right)$ is not verified in the set of integers module m.

Counterexample:

$3 \cdot 1 = 3 \cdot 5 \, mod \, 6 \wedge 3 \neq 0 \, mod \, 6$ but $1 \neq 5 \, mod \, 6$

Notation

From now on, when we write $a \in \mathbb{Z}_m$ or $a \, mod \, m$ we will be taking representative a as its equivalence class $[a]_m$.

8. Invertible elements

Definitions

Given $m \in \mathbb{N}$, it is said that an element $r \in \mathbb{Z}_m$ is **invertible** if there is any $x \in \mathbb{Z}_m$ such that:

$$r \cdot x = 1 \, mod \, m$$

In that case, we will say that x is an **inverse** of r, and define it as r^{-1}

Theorem

Element $r \in \mathbb{Z}_m$ is invertible if and only if r and m are coprime.

Proof *(exercise)*

In order to prove the theorem, we must verify two implications. First, we must verify that if $r \in \mathbb{Z}_m$ is invertible then r and m are coprime. To that extent, it is enough to use the definition and characterization of coprime numbers. Secondly, we must verify that if r and m are coprime then $r \in \mathbb{Z}_m$ is invertible. To achieve that conclusion, it is necessary to use Bézout's identity.

Corollary

If p is a prime number, every element of $\mathbb{Z}_p$ different from zero is invertible.

Proof *(exercise)*

The corollary is a direct consequence of the theorem.

Example

We want to discern whether 31 has an inverse module 97, and in case it does, calculate it.

Through the theorem, 31 has an inverse module 97 if $mcd(31,97) = 1$.

Through the Euclidean algorithm, we have that:

$$97 = 31 \cdot 3 + 4$$
$$31 = 4 \cdot 7 + 3$$
$$4 = 3 \cdot 1 + \boxed{1}$$

Then, $mcd(31,97) = 1$, and we can affirm that there is an inverse of 31 module 97. We could also have applied the corollary, since 97 is a prime number. In order to calculate the inverse, we can leverage Bézout's identity:

$$1 = 4 - 3 \cdot 1 = 4 - (31 - 4 \cdot 7) = 8 \cdot 4 - 31 = 8 \cdot (97 - 31 \cdot 3) - 31 = \; 97 \cdot 8 + 31 \cdot (-25)$$
$$31 \cdot (-25) = 1 \, mod \, 97 \Leftrightarrow 31^{-1} = -25 = 72 \, mod \, 97$$

This implies that $31 \cdot (-25) = 1 \, mod \, 97$, and $31^{-1} = -25 = 72 \, mod \, 97$ is the inverse of $31 \, mod \, 97$, that is, $(31 \cdot 72 = 1 \, mod \, 97)$. Observe that we took as an inverse the canonical representative of the equivalence class of (-4) module 97. In that way, we can consider the inverse of each invertible element as unique.

9. Euler's function. Theorems of Euler and Fermat.

Let us remember the definition of Euler's function:

$\forall m \geq 1$ $\Phi(m)$ is the number of natural numbers $x \in \mathbb{N}$ such that $1 \leq x < m$ and $mcd(x,m) = 1$, that is, lesser than and coprime with m.

Through the prior theorem, the value for Euler's function $\Phi(m)$ matches the number of invertible integer numbers in $\mathbb{Z}_m$.

Euler's theorem

If $mcd(m,r) = 1$ then $r^{\Phi(m)} = 1 \, mod \, m$.

Proof *(exercise)*

To verify this theorem, we take the set composed by the invertible elements module m:

$$I_m = \{x \in \mathbb{Z}_m \mid x \text{ is invertible}\}$$

Since $mcd(m,r) = 1$, we have that $r \in I_m \Rightarrow I_m \neq \emptyset$.

In addition, the number of elements of I_m is $\Phi(m)$: $|I_m| = \Phi(m)$.

We can express I_m as $I_m = \{x_1, x_2, \ldots, x_{\Phi(m)}\}$

We define the set $r \cdot I_m = \{z \in \mathbb{Z}_m | (\exists x \in I_m)(z = r \cdot x \, mod \, m)\}$ and prove that $r \cdot I_m = I_m$

To that extent, it is enough to prove the contents in both directions *(exercise)*.

Be $x = x_1 \cdot x_2 \cdot \ldots \cdot x_{\Phi(m)} \, mod \, m$ an invertible element of $\mathbb{Z}_m$, and $x^{-1} = x^{-1}{}_{\Phi(m)} \cdot \ldots \cdot x_2^{-1} \cdot x_1^{-1} \cdot mod \, m$ its inverse $mod \, m$.

Since $I_m = r \cdot I_m$, the set $r \cdot I_m = \{r \cdot x_1, r \cdot x_2, \ldots, r \cdot x_{\Phi(m)}\}$ is nothing but a rearrangement of the set $I_m = \{x_1, x_2, \ldots, x_{\Phi(m)}\}$, hence:

$x = x_1 \cdot x_2 \cdot \ldots \cdot x_{\Phi(m)} = (r \cdot x_1) \cdot (r \cdot x_2) \cdot \ldots \cdot (r \cdot x_{\Phi(m)}) = r^{\Phi(m)} \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_{\Phi(m)} = r^{\Phi(m)} \cdot x \, mod \, m$

Multiplying both parts by x^{-1} we obtain: $1 = x \cdot x^{-1} = r^{\Phi(m)} \cdot x \cdot x^{-1} = r^{\Phi(m)} \, mod \, m$, as we wanted to prove.

Fermat's theorem

If p is a prime number and $p \nmid r$ (p does not divide r), then $r^{p-1} = 1 \, mod \, p$

Proof *(exercise)*

Proof of this theorem can be immediately achieved from the prior theorem.

10. Congruencies resolution

10.1. First degree congruencies

A first-degree congruency is an equation that takes the form: $a \cdot x = b \, mod \, m$

Where $a, b \in \mathbb{Z}_m$ and x is the unknown value.

Theorem

The congruency $a \cdot x = b \, mod \, m$ has a solution if and only if $mcd(a,m)|b$.

Proof *(exercise)*

Proof is clear from Bézout's identity and the definition of congruency. Remember that there are two implications that need to be verified.

Corollary

1. If $mcd(a,m) = 1$, the congruency $a \cdot x = b \, mod \, m$ has a single solution.
2. If $mcd(a,m) = d \neq 1$ and $d|b$, then the congruency $a \cdot x = b \, mod \, m$ has d different solutions such that, if x_0 is a solution, then $\left\{x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}\right\}$ is the set of all the solutions module m.

Proof *(exercise)*

1. It is easy to see that if $mcd(a,m) = 1$, we have $a^{-1} \, mod \, m$ so that $x = a^{-1} \cdot a \cdot x = \boxed{a^{-1} \cdot b} \, mod \, m$ is a solution for the congruency $a \cdot x = b \, mod \, m$. In addition, the solution is unique module m, since the invers is unique module m.
2. If $mcd(a,m)|b$, the prior theorem affirms that the congruency $a \cdot x = b \, mod \, m$ has a solution. Since $d|a, d|m \wedge d|b$, there are $a_0, m_0, b_0 \in \mathbb{N}$ such that $a = a_0 \cdot d, m = m_o \cdot d$ and $b = b_0 \cdot d$, verifying that $mcd(a_0, m_0) = 1$. Through step 1 of this proof, if $mcd(a_0, m_0) = 1$, congruency $a_0 \cdot x = b_0 \, mod \, m_0$ has a unique solution of the form: $x_0 = a_0^{-1} \cdot b_0 \, mod \, m_0$.

Through the definition of congruency, we have that:

$$x_0 = a_0^{-1} \cdot b_0 \, mod \, m_0 \leftrightarrow (\exists q \in \mathbb{Z})(x_0 = m_0 \cdot q + a_0^{-1} \cdot b_0) \leftrightarrow a_0 \cdot x_0 = a_0 \cdot m_0 \cdot q + b_0$$

Hence, since $m = m_0 \cdot d$:

$$x_0 - a_0^{-1} \cdot b_0 = m_0 \cdot q \underset{\cdot d}{\leftrightarrow} (x_0 - a_0^{-1} \cdot b_0) \cdot d = d \cdot m_0 \cdot q$$

$$(x_0 - a_0^{-1} \cdot b_0) \cdot d = d \cdot m_0 \cdot q \xleftrightarrow[\substack{m = m_0 \cdot d \\ b = b_0 \cdot d \\ congruency \, definition}]{} x_0 \cdot d - a_0^{-1} \cdot b = 0 \, mod \, m$$

$$x_0 \cdot d - a_0^{-1} \cdot b = 0 \, mod \, m \underset{\cdot a_0}{\leftrightarrow} a_0 \cdot x_0 \cdot d - a_0 \cdot a_0^{-1} \cdot b = 0 \, mod \, m$$

$$a_0 \cdot x_0 \cdot d - a_0 \cdot a_0^{-1} \cdot b = 0 \, mod \, m \xleftrightarrow[a_0 \cdot a_0^{-1} = 1]{a = a_0 \cdot d} x_0 \cdot a = b \, mod \, m$$

Therefore, we have that $x_0 = a_0^{-1} \cdot b_0 \, mod \, m_0$ is a solution for congruency $a \cdot x = b \, mod \, m$

In addition, if $x = x_0 + k \cdot m_0, k \in \{0,1,\ldots,(d-1)\}$ it is verified that it is also a solution for congruency

$$a \cdot x = a \cdot (x_0 + k \cdot m_0) = a \cdot x_0 + a \cdot k \cdot m_0 \underset{a=a_0 \cdot d}{=} b + a_0 \cdot k \cdot d \cdot m_0 \underset{m=m_0 \cdot d}{=} b + a_0 \cdot k \cdot m = b \, mod \, m$$

Example

Solve $12 \cdot x = 6 \, mod \, 15$.

Since $mcd(12,15) = 3 \wedge 3|6$, applying the prior theorem we can affirm that that the congruency has a solution.

$$15 = 12 + \boxed{3}\} \Rightarrow mcd(15,12) = 3$$

From Bézout's identity $3 = 15 - 1 \cdot 12$, multiplying by $2 = 12/6$ we obtain:

$$3 \cdot 2 = 2 \cdot 15 - 2 \cdot 12 \Rightarrow (-2) \cdot 12 = 3 \, mod \, 15$$

And then $x = -2 = 13 \, mod \, 15$ is a solution for the congruency. To obtain the set of all the solutions, it is enough to consider the prior corollary:

$$\left\{13, 13 + \frac{15}{3}, 13 + 2 \cdot \frac{15}{3}\right\} = \{13,18,23\} = \{13,3,8\}$$

Effectively, we can now observe that:

$$12 \cdot \boxed{13} = 156 = 15 \cdot 10 + 6 = 6 \, mod \, 15$$

$$12 \cdot \boxed{3} = 36 = 15 \cdot 2 + 6 = 6 \, mod \, 15$$

$$12 \cdot \boxed{8} = 96 = 15 \cdot 6 + 6 = 6 \, mod \, 15$$

Exercise

Solve congruency $111 \cdot x = 75 \, mod \, 321$

10.2. Linear congruency systems

A system of linear congruencies is an equation system that takes the form:

$$\begin{cases} x = a_1 \, mod \, m_1 \\ x = a_2 \, mod \, m_2 \\ \vdots \\ x = a_k \, mod \, m_k \end{cases}$$

Where $mcd(m_i, m_j) = 1$ if $i \neq j$.

Chinese remainder theorem

The congruency system $\begin{cases} x = a_1 \, mod \, m_1 \\ x = a_2 \, mod \, m_2 \\ \vdots \\ x = a_k \, mod \, m_k \end{cases}$ with $mcd(m_i, m_j) = 1$ if $i \neq j$ has a solution.

If x and x' are solutions for the congruency system, then $x = x' \, mod \, M$ with $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

Proof

Proof of this theorem is constructive. From it, it is possible to define the steps that must be followed to solve a system of congruencies.

Be it $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$ and $M_i = \frac{M}{m_i} \forall i \in \{1,2,\ldots,k\}$.

We have that $mcd(M_i, m_i) = 1, \forall i \in \{1,2,\ldots,k\}$.

Bézout's identity ensures that $\forall i \in \{1,2,\ldots,k\}$ there are $N_i, P_i \in \mathbb{Z}$ so that $M_i \cdot N_i + m_i \cdot P_i = 1$.

Having $x = \sum_{i=1}^{k} a_i \cdot M_i \cdot N_i = a_1 \cdot M_1 \cdot N_1 + a_2 \cdot M_2 \cdot N_2 + \ldots + a_k \cdot M_k \cdot N_k$ as a solution for the system, it is enough to observe that $M_i = 0 \, mod \, m_j$ if $i \neq j$ and therefore:

$x = a_1 \cdot M_1 \cdot N_1 + a_2 \cdot M_2 \cdot N_2 + \ldots + a_i \cdot M_i \cdot N_i + \ldots + a_k \cdot M_k \cdot N_k = a_i \cdot M_i \cdot N_i \, mod \, m_i \, \forall i \in \{1,2,\ldots k\}$

Since $M_i \cdot N_i + m_i \cdot P_i = 1$, we also have that $M_i \cdot N_i = 1 \, mod \, m_i$ and then:

$$x = \sum_{i=1}^{k} a_i \cdot M_i \cdot N_i = a_i \cdot M_i \cdot N_i = a_i \cdot 1 = a_i \, mod \, m_i \, \forall i \in \{1,2,\ldots k\}$$

On the other hand, if x and x' are solutions for the congruency system, $x = x' \, mod \, m_i \, \forall i \in \{1,2\ldots k\}$.

This means that $m_i | (x - x') \, \forall i \in \{1,2,\ldots,k\}$ and since $mcd(m_i, m_j) = 1$ if $i \neq j$, we can affirm that $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k | (x - x')$.

Example

Solve the following congruency system:

$$\begin{cases} 2x = 1 \, mod \, 5 \\ x = 2 \, mod \, 6 \\ x = 3 \, mod \, 7 \end{cases}$$

In order to be able to apply the Chinese remainder theorem, it is necessary for all the equation of the system to have the form $x = a \, mod \, m$, that is, x must be isolated.

In the given system, the first equation takes the form $2x = 1 \, mod \, 5$, thus, x is not isolated. In order to isolate it, it is necessary to multiply both sides of the equality by the inverse of $2 \, mod \, 5$, in this case, 3 $(2 \cdot 3 = 6 = 1 \, mod \, 5)$. Through this modification, the first equation of the system becomes $x = 3 \, mod \, 5$.

Hence, $a_1 = 3$. Through the theorem, we obtain $N_1 = -2$, $N_2 = -1$, $N_3 = -3$, and $M = 210$.

With these values, we can then build the solution as follows:

$$x = 42 \cdot (-2) \cdot 3 + 35 \cdot (-1) \cdot 2 + 30 \cdot (-3) \cdot 3 = -592 = 38 \, mod \, 210$$

References

Enderton, Herbert B. "A mathematical introduction to logic". Elsevier, 2001.

Norman L. Biggs, "Discrete mathematics". Oxford University Press, 2002.

R. Johnsonbaugh, "Discrete mathematics". Prentice Hall, 1997.

Ralph P Grimaldi, "Discrete and Combinatorial Mathematics: An Applied Introduction". Addison-Wesley, 1994.

W. K. Grassmann and J.P. Tremblay, "Logic and discrete mathematics : a computer science perspective". Prentice Hall, 1996.