Information Systems Security
Exercices Series 1 - Modular Arithmetic
Reminders

September 22nd, 2021

Modular Arithmetic

- $\mathbb{N}$ is the set of natural numbers (positive integers) : $\{0, 1, 2, 3, ...\}$
- $\mathbb{Z}$ is the set of relative numbers (positive and negative integers) : $\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$
- $\mathbb{Z}_n$ is the set of integers modulo n : $\{0, 1, ..., n-1\}$
- $\mathbb{R}$ is the set of real numbers.
- $\lfloor x \rfloor$ is the integer part (floor) of an $x \in \mathbb{R}$, i.e. the biggest integer y such that $y \leq x$.
- $a|b$ means a divides b (for $a, b \in \mathbb{Z}$), i.e. an integer (positive or negative) k exists such that $k \cdot a = b$.

Examples :

- $\lfloor \pi \rfloor = 3$, $\lfloor -3.2 \rfloor = -4$, $\lfloor 2.4 \rfloor = 2$.
- $4|12$, $-3|21$ (because $(-3)(-7) = 21$).

Greatest Common Divisor : Let $a, b, c \in \mathbb{Z}$, such that $c|a$ and $c|b$, then c is a *common divisor* of a and b. If $\forall d$ such that d is a common divisor of a and b, we have $d \leq c$, then c is called the *greatest common divisor* of a and b : $gcd(a, b) = c$.

Modulo : Let $a, n \in \mathbb{R}$, we define "a modulo n" as the remainder r in the division of a by n :

$$a = q \cdot n + r = \lfloor \frac{a}{n} \rfloor \cdot n + (a \mod n)$$

This creates n groups of numbers with different values modulo n (from 0 to $n-1$). When two numbers a and b have the same remainder (the same value mod n), we then say they are congruent modulo n, which is denoted :

$$a \equiv b \mod n$$

Example : $7 \equiv 15 \mod 4$ ($7 \mod 4 = 3$ and $15 \mod 4 = 3$).

Congruences and properties :

Congruences are :

- Reflexive : $a \equiv b \mod n$ if $n|(a-b)$
- Symmetric : $a \equiv b \mod n$ implies $b \equiv a \mod n$
- Transitive : $a \equiv b \mod n$ and $b \equiv c \mod n$ implies $a \equiv c \mod n$

We can then see the following mathematical simplifications :

- $[(a \mod n) + (b \mod n)] \mod n = a + b \mod n$
- $[(a \mod n) - (b \mod n)] \mod n = a - b \mod n$
- $[(a \mod n) \cdot (b \mod n)] \mod n = a \cdot b \mod n$

Let $a, b, c, n \in \mathbb{Z}$, then if $a \equiv b \mod n$, we have :

- $a + c \equiv b + c \mod n$
- $a - c \equiv b - c \mod n$
- $a \cdot c \equiv b \cdot c \mod n$

Inverses and Z_n

Multiplicative Inverse : Let $a \in \mathbb{Z}_n$. The multiplicative inverse of a modulo n, if such an inverse exists, is the integer $x \in \mathbb{Z}_n$ such that $ax \equiv 1 \mod n$.
(If such an x exists, then it is unique, and a is said to be invertible). The multiplicative inverse is noted $a^{-1} \mod n$.

Division modulo n : Let $a, b \in \mathbb{Z}_n$. The division of a by b modulo n is defined as the multiplication $a \cdot b^{-1} \mod n$, and is defined only if b is invertible modulo n.

Invertible property : Let $a \in \mathbb{Z}_n$. Then, a is invertible if and only if $gcd(a, n) = 1$.

Multiplicative Group of $\mathbb{Z}_n$: The mutiplicative Group of $\mathbb{Z}_n$ is noted $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n | pgcd(a, n) = 1\}$. Specifically, if n is prime, it means $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus 0$ (i.e. if n is prime, the multiplicative group contains all integers from 1 to $n - 1$).

Bézout Identity : If $a, b \in \mathbb{Z}$, then we can find two numbers $x, y \in \mathbb{Z}$ such as $ax + by = pgcd(a, b)$.

Euler totient function : Given a number $n \in \mathbb{Z}$, the Euler totient function (also known as Euler phi function), $\Phi(n)$, is the size of the following set : $\{x \mid 0 < x < n, pgcd(x, n) = 1\}$ (i.e. the set of number co-prime with n in $\mathbb{Z}_n \setminus 0$).
Examples : $\Phi(8) = |\{1, 3, 5, 7\}| = 4$; $\Phi(7) = |\{1, 2, 3, 4, 5, 6\}| = 6$.
We can easily see that for any prime number n, $\Phi(n) = n - 1$.

Euler theorem : For any integer $n > 0$ and any integer a co-prime with n, $a^{\Phi(n)} \equiv 1 \mod n$.

Fermat's little theorem : If p is a prime number and a is an integer such that p does not divide a, then $a^p \equiv a \mod p$.

Primitive roots : Let $n \in \mathbb{Z}, g \in \mathbb{Z}_n$. We call g a primitive root modulo n if $\forall a$ such that $pgdc(a, n) = 1, \exists k \in \mathbb{Z}$ such that $g^k \equiv a \mod n$.

Order : Let $a, n \in \mathbb{N}$, and $pgdc(a, n) = 1$. The order of a modulo n, noted $ord_n(a)$, is the smaller positive integer $x \in \mathbb{N}$ such that $a^x \equiv 1 \mod n$.

Generator : For a multiplicative group $\mathbb{Z}_n^*$ and a primitive root $g \in \mathbb{Z}_n^*$, we call g a generator of $\mathbb{Z}_n^*$ (as the powers of g generates all elements in $\mathbb{Z}_n^*$).

Remark : A generator has an order which is equal to the Euler totient function of the group : $ord_n(g) = \Phi(n)$

Groups, Rings and Fields

Group : A group is an algebraic structure defined by a set G and an operator $* : G \times G \to G$, such that :

- $\forall a, b \in G, a * b \in G$. This is the closure property.
- The operator $*$ is associative (i.e. $a * (b * c) = (a * b) * c$) for all $a, b, c \in G$).
- There is a unique neutral element $1 \in G$, such that $a * 1 = 1 * a = a$ for all $a \in G$ (note that it is not necessarily the number "1").
- Each element $a \in G$ has a unique inverse $a^{-1} \in G$, such that $a * a^{-1} = a^{-1} * a = 1$ (the neutral element defined earlier).

Abelian Group : A group is said Abelian if operation $*$ is commutative ($a * b = b * a$ for all $a, b \in G$).

Ring : A ring is an algebraic structure defined by a set A and two operators $+, * : G \times G \to G$, such that :

- $(A, +)$ is an abelian group (we note the neutral element 0 for operator $+$).
- Operator $*$ is associative.
- Operator $*$ has a unique neutral element $1 \in A, 1 \neq 0$ such that $1 * a = a * 1 = a$ for all $a \in A$.
- Operator $*$ is distributive with $+$: $a * (b + c) = (a * b) + (a * c)$ and $(a + b) * c = (a * c) + (b * c)$ for all $a, b, c \in A$.

Commutative Ring : A ring is said to be commutative if the product $*$ is commutative (i.e. $a * b = b * a$ for all $a, b \in A$).

Field : A field is a commutative ring (A,+,$*$) in which $(A \setminus 0, *)$ is a group.

Exercices

Justify all answers.

1. Compute :
   - $((11 \mod 7) + (17 \mod 7)) \mod 7$
   - $((11 \mod 7) - (17 \mod 7)) \mod 7$
   - $((11 \mod 7) \cdot (17 \mod 7)) \mod 7$
   - $(21 * 27 * 41) \mod 8$
   - $-44 \mod 7$
2. In $\mathbb{Z}_7$, compute :
   - The additive table.
   - The multiplication table.
   - The additive inverse for each number.
   - The multiplicative inverse for each number.
3. Is $(\mathbb{Z}_7, +)$ a group ?
4. Is $(\mathbb{Z}_8, \times)$ a group ?
5. Is $(\mathbb{Z}_8^*, \times)$ a group ?
6. Is $(\mathbb{Z}_n^*, \times)$ a group ?
7. Give the order of :
   - 2 mod 7
   - 3 mod 7
   - 3 mod 10
8. Find a primitive root modulo 7 (i.e. a generator of $\mathbb{Z}_7^*$).
9. Find all primitive roots modulo 11.
10. Show there is no primitive root modulo 12.