Cryptography

Modular Arithmetic

Sandra Díaz Santiago

ESCOM-IPN

August 12, 2016

Divisibility

Definition

Let a and b be integers, then a **divides** b if there exists an integer x such that b=ax. We denote this as $a|b$.

Example

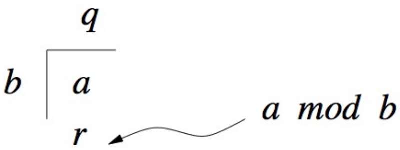
$2|8$, $7|168$, $-3|6$. Also $2 \not| 5$ y $3 \not| 14$.

Division algorithm

Definition

If a and b are integers such that $b \geq 1$ then when we divide a by b we get q (quotient) and r (remainder) such that

$$a = bq + r \quad 0 \leq r < b$$



Example

If $a = 23$ y $b = 7$ then a divided by b is equal to $q = 3$ y $r = 2$. And

$$23 = 7 \cdot 3 + 2$$

Also it is true that

$$23 \bmod 7 = 2$$

Congruences

Definition

Suppose a and b are integers and m is a positive integer. Then we write $a \equiv b \bmod m$ if m divides $b - a$. The phrase $a \equiv b \bmod m$ is called a **congruence** and it is read as a **is congruent to** b **modulo** m. The integer m is called the **modulus.**

Example

- 101 mod 7, we must find the remainder dividing 101 by 7. Then we get 3. We can also write this as $101 = 7 * 14 + 3$, since $0 \leq 3 < 7$
- -101 mod 7. In this case we have $-101 = 7 * (-15) + 4$ since $0 \leq 4 < 7$

Properties of congruences

- (*Reflexivity*) $a \equiv a \bmod m$.
- (*Symmetry*) If $a \equiv b \bmod m$ then $b \equiv a \bmod m$
- (*Transitivity*) If $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $a \equiv b \bmod m$

How can we prove these properties?

$\mathbb{Z}_m$: integers modulo m

$$\mathbb{Z}_m = \{0, 1, \dots m - 1\}$$

$$[r] = \{a | a \in \mathbb{Z}, a \equiv r \bmod n\}$$

Example If we take $m = 7$ we have:

$$\begin{aligned}
[0] &= \{\dots, -28, -21, -14, -7, 0, 7, 14, 21, 28 \dots\} \\
[1] &= \{\dots, -27, -20, -13, -6, 1, 8, 15, 22, 29 \dots\} \\
[2] &= \{\dots, -26, -19, -12, -5, 2, 9, 16, 23, 30, \dots\} \\
[3] &= \{\dots, -25, -18, -11, -4, 3, 10, 17, 24, 31 \dots\} \\
[4] &= \{\dots, -24, -17, -10, -3, 4, 11, 18, 25, 32 \dots\} \\
[5] &= \{\dots, -23, -16, -9, -2, 5, 12, 19, 26, 33 \dots\} \\
[6] &= \{\dots, -22, -15, -8, -1, 6, 13, 20, 27, 34 \dots\}
\end{aligned}$$

Addition in $\mathbb{Z}_m$

If $a, b \in \mathbb{Z}_m$, then $(a + b) \bmod m \in \mathbb{Z}_m$

Example. If we consider $m = 6$ i.e. $\mathbb{Z}_6 = \{0, 1, \ldots 5\}$ then

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	
3	3	4	5		1	
4	4	5	0	1		
5						

Remarks

In the previous example, notice that

- $(1+5) \bmod 6 = (5+1) \bmod 6 = 0$
- $(2+4) \bmod 6 = (4+2) \bmod 6 = 0$
- $(3+3) \bmod 6 = 0$

We can say that 5 is the **additive inverse** of 1, 2 is the **additive inverse** of 4 and 3 is its own additive inverse.

Can you find the additive inverses for the following elements?

1. $11 \in \mathbb{Z}_{31}$
2. $5 \in \mathbb{Z}_{48}$
3. $23 \in \mathbb{Z}_{100}$
4. $35 \in \mathbb{Z}_{53}$

Groups

Definition

A group $(G, *)$ consists of a set G with a binary operation $*$ on G satisfying the following three axioms.

1. The group operation is associative. That is, $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
2. There is an element $e \in G$, called the identity element, such that $a * e = e * a = a$ for all $a \in G$.
3. For each $a \in G$ there exists an element $a^{-1} \in G$, called the inverse of a, such that $a * a^{-1} = a^{-1} * a = 1$.

A group G is abelian (or commutative) if, furthermore, $a * b = b * a$ for all $a, b \in G$.

Questions

Is $\mathbb{Z}_m$ with the addition a group?

How can we see this ?

Is $\mathbb{Z}_m$ an abelian group?

How can we use $\mathbb{Z}_m$ in cryptography?

And what about multiplication?

Is it true that if $a, b \in \mathbb{Z}_m$, then $a * b \bmod m \in \mathbb{Z}_m$?
Let's see what happens with $\mathbb{Z}_6$

$+$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

What is wrong with this table?

What about $\mathbb{Z}_7 - \{0\}$?

+	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Everything seems fine!

What is going on?