Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

Ayudante: Nicholas Mc-Donnell
Email: namcdonnell@uc.cl

Ayudantía 01

Aritmética Modular

IIC3253 – Criptografía

Fecha: 2021-03-24

Definición 0.1 (Divisibilidad)**.** Para $a, b \in \mathbb{Z}$ se dice que a divide a b, denotado como $a \mid b$ si y solo si existe un $m \in \mathbb{Z}$ tal que $b = ma$.

Teorema 0.1 (Algoritmo de la división)**.** *Dados $p, q \in \mathbb{Z}$ existen únicos $d, r \in \mathbb{Z}$ tales que $p = dq + r$ y $0 \leq r < |q|$.*

Definición 0.2 (Congruencia Modulo n)**.** Dado $a, b, n \in \mathbb{Z}$ se dice que $a \equiv b \mod n$ si y solo si $n \mid b - a$.

Teorema 0.2. *La congruencia modulo n es una relación de equivalencia.*

Demostración.

Simétrica: Sean $a, b \in \mathbb{Z}$ tales que $a \equiv b \mod n$, entonces se tiene que $n \mid b-a$ por lo que $n \mid a-b$, con lo que se tiene que $b \equiv a \mod n$.

Refleja: Sea $a \in \mathbb{Z}$ se tiene que $n \mid 0 = a - a$

Transitiva: Sean $a, b, c \in \mathbb{Z}$ tales que $a \equiv b \mod n$ y $b \equiv c \mod n$, entonces se tiene que $n \mid b - a$ y $n \mid c - b$, por lo que $n \mid (b - a) + (c - b) = c - a$, y con eso se concluye que $a \equiv c \mod n$.

□

Ejemplo: 0.1. Se tiene que $3 \equiv 15 \mod 12$, ya que $15 - 3 = 12$ y $12 \mid 12$. Esto es un ejemplo que es clásico, ya que uno puede verlo en el reloj, pero hay varios otros:

- $4 \equiv 17 \mod 13$
- $21 \equiv 201 \mod 10$
- $-5 \equiv 20 \mod 25$
- $-1 \equiv n-1 \mod n$
- Dado $k \not\equiv 0 \mod 5$, $k^4 \equiv 1 \mod 5$ (Ejercicio: usando esta ayudantía demuestre esto.)

Definición 0.3 (Representante Modulo n)**.** Dado $a \in \mathbb{Z}$, se dice que $r \in \{0, \ldots, |n|-1\}$ es un representante de a modulo n si y solo si $a \equiv r \mod n$. Se nota que dado a r es único por el algoritmo de la división.

Lema 0.3. *Dados $a, b \in \mathbb{Z}$ tales que $a \equiv b \mod n$, se tiene que los representantes de a y b modulo n, r_a, r_b, cumplen que $r_a = r_b$.*

Demostración. Sean $a, b \in \mathbb{Z}$ tales que $a \equiv b \mod n$, y sean r_a y r_b sus representantes modulo n, entonces se tiene que $n \mid a - r_a$ y $n \mid b - r_b$, con lo que se tiene que $n \mid (b-a) + (r_b - r_a)$, y como $n \mid b - a$, entonces se tiene que $n \mid r_b - r_a$. Notemos además que $r_b - r_a \in \{-(|n|-1), \ldots, (|n|-1)\}$, y como el único $x \in \{-(|n|-1), \ldots, (|n|-1)\}$ tal que $n \mid x$ es $x = 0$, se tiene que $r_b - r_a = 0$, por lo que $r_a = r_b$. □

Teorema 0.4. *Dados $a, b, c, d \in \mathbb{Z}$ tales que $a \equiv b \mod n$ y $c \equiv d \mod n$,*

1) $a + c \equiv b + d \mod n$.

2) $a \cdot c \equiv d \cdot d \mod n$.

Demostración. 1) Recordando el lema ya demostrado, sabemos que $r_a = r_b$ y $r_c = r_d$, por lo que $r_a + r_c = r_b + r_d$, más aún se tiene que $a + b \equiv r_a + r_c \equiv r_b + r_d \equiv b + d \mod n$, ya que $n \mid (r_a - a) + (r_c - c)$ y $n \mid (r_b - b) + (r_d - d)$, con lo que por transitividad se tiene que $a + b \equiv c + d \mod n$.

2) Queda como ejercicio. □

Teorema 0.5 (Criterios de Divisibilidad)**.** *Dado $a = \sum_{i=0}^{n} a_i \cdot 10^i$*

1) $3 \mid a$ *si y solo si* $3 \mid \sum_{i=0}^{n} a_i$

2) $9 \mid a$ *si y solo si* $9 \mid \sum_{i=0}^{n} a_i$

3) $11 \mid a$ *si y solo si* $11 \mid \sum_{i=0}^{n} (-1)^i a_i$

Demostración. 1) Se nota que $3 \mid a$ si y solo si $a \equiv 0 \mod 3$, por lo que $\sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i 1^i \equiv \sum_{i=0}^{n} a_i \mod n$, lo que es cierto si y solo si $3 \mid \sum_{i=0}^{n} a_i$.

2) Ejercicio.

3) Ejercicio.

□