

## Definiciones

### Algoritmos aleatorizados

#### Desigualdad de Markov

Sea  $X$  una variable aleatoria no negativa. Para cada  $a \in \mathbb{R}^+$  se tiene que:

$$\Pr(X \geq a) \leq \frac{E(X)}{a}$$

#### Desigualdad de Cebyshev

$$\Pr(|X - E(X)| \geq a) \leq \frac{Var(X)}{a^2}$$

### Aritmética modular

#### Definiciones básicas

- $b \equiv c \pmod n$ , si  $n|(c - b)$
- $a \equiv b \pmod n$ , ssi  $a \pmod n = b \pmod n$
- $a \equiv (a \pmod n) \pmod n$
- Si  $a \equiv b \pmod n$  y  $c \equiv d \pmod n$ , entonces:
  - $(a + c) \equiv (b + d) \pmod n$
  - $(a \cdot c) \equiv (b \cdot d) \pmod n$

#### Máximo común divisor

Si  $b > 0$ , entonces  $MCD(a, b) = MCD(b, a \pmod b)$

La complejidad de  $MCD(a, b)$  es  $O(\max(\log(a), \log(b)))$

#### Inverso modular

$b$  es inverso de  $a$  en módulo  $n$  si  $a \cdot b \equiv 1 \pmod n$

#### Identidad de Bézout

Para cada  $a, b \in \mathbb{N}$  tales que  $a \neq 0$  o  $b \neq 0$ , existen  $s, t \in \mathbb{Z}$  tales que:

$$MCD(a, b) = s \cdot a + t \cdot b$$

#### Existencia de inverso modular

$a$  tiene inverso en módulo  $n$ , ssi  $MCD(a, n) = 1$ . Esto también implica que  $a$  y  $n$  son primos relativos (coprimos).

### Algoritmo extendido de Euclides

Suponga que  $a \geq b$ , y defina la siguiente sucesión:

- $r_0 = a$
- $r_1 = b$
- $r_{i+1} = r_{i-1} \bmod r_i \quad (i \geq 2)$

Calculamos esta sucesión hasta un número  $k$  tal que  $r_k = 0$ . Tenemos que  $MCD(a, b) = r_{k-1}$ .

Al mismo tiempo calculamos sucesiones  $s_i, t_i$  tales que:

$$r_i = s_i \cdot a + t_i \cdot b$$

Por lo que  $MCD(a, b) = r_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot b$

### Teorema de Fermat

Sea  $p$  un número primo. Si  $a \in \{0, \dots, p-1\}$ , entonces:

- $a^p \equiv a \pmod{p}$
- $a^{p-1} \equiv 1 \pmod{p}$

### Grupos

Un conjunto  $G$  y una función (total)  $o : G \times G \rightarrow G$  forman un grupo si:

- Para cada  $a, b, c \in G$ ,  $(a \circ b) \circ c = a \circ (b \circ c)$ . (Asociatividad).
- Existe  $e \in G$  tal que para cada  $a \in G$ ,  $a \circ e = e \circ a = a$ . (Existe un elemento neutro).
- Para cada  $a \in G$ , existe  $b \in G$ ,  $a \circ b = b \circ a = e$ . (Existe un inverso).

Algunas propiedades básicas:

- El neutro es único. Si  $e_1$  y  $e_2$ , satisfacen 2, entonces  $e_1 = e_2$
- Inverso de cada elemento  $a$  es único. Si  $a \circ b = b \circ a = e$ , y  $a \circ c = c \circ a = e$ , entonces  $b = c$

### Subgrupos

$(H, o)$  es un subgrupo de un grupo  $(G, o)$ , para  $\emptyset \subsetneq H \subseteq G$ , si  $(H, o)$  es un grupo.

### Teorema de Lagrange

Si  $(G, o)$  es un grupo finito y  $(H, o)$  es un subgrupo de  $(G, o)$ , entonces  $H \subseteq G$ , entonces  $|H|$  divide  $|G|$ .

### Conjuntos para el test de primalidad

$$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} \mid \text{MCD}(a, n) = 1\}$$

$$J_n = \{a \in \mathbb{Z}_n^* \mid a^{n-1} \equiv 1 \pmod{n}\}$$

$$S_n = \{a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \pmod{n} \text{ o } a^{\frac{n-1}{2}} \equiv -1 \pmod{n}\}$$

$$S_n^+ = \{a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \pmod{n}\}$$

$$S_n^- = \{a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv -1 \pmod{n}\}$$

Si  $n \geq 3$  es primo, entonces:

- $S_n = \mathbb{Z}_n^*$
- $|S_n^+| = |S_n^-| = \frac{n-1}{2}$

Sea  $n = n_1 \cdot n_2$ , donde  $n_1, n_2 \geq 3$  y  $\text{MCD}(n_1, n_2) = 1$ . Si existe  $a \in \mathbb{Z}_n^*$  tal que  $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ , entonces  $|S_n| \leq \frac{1}{2}|\mathbb{Z}_n^*|$ . ## Función  $\phi$  de Euler

Se define la función  $\phi$  de Euler como  $\phi(1) = 1$ , y  $\phi(n) = |\mathbb{Z}_n^*|$ . Es decir, la cantidad de primos relativos de  $n$ , que son menores a  $n$ .

Se tiene que  $\phi(n) \in \Omega\left(\frac{n}{\log_2(\log_2(n))}\right)$ .

### Número de Carmichael

Un número  $n$  es un número de Carmichael si  $n \geq 2$ ,  $n$  es compuesto y  $|J_n| = |\mathbb{Z}_n^*|$ .

Existe un número infinito de números de Carmichael.

### Polinomios modulares

Sea  $p(x)$  el polinomio:

$$p(x) = \sum_{i=0}^k a_i x^i$$

$p(x)$  tiene a lo más  $k$  raíces en módulo  $n$ . Se

Dos polinomios  $p_1(x)$  y  $p_2(x)$  son congruentes en módulo  $n$  si para todo  $a \in \{0, \dots, n-1\}$ :  $p_1(a) \equiv p_2(a) \pmod{n}$ .

En tal caso,  $p_1(x) \equiv p_2(x) \pmod{n}$ .

Sea  $a$  una raíz de  $p(x)$  en módulo  $n$ . Existe un polinomio  $q(x)$  de grado  $k-1$  tal que:

$$p(x) = (x-a)q(x) \pmod{n}$$

### **Teorema chino del resto**

Suponga que  $\text{MCD}(m, n) = 1$ . Para todo  $a$  y  $b$ , existe  $c$  tal que:

- $c \equiv a \pmod{m}$
- $c \equiv b \pmod{n}$

## **Recordatorios útiles de Probabilidades**

### **Probabilidad condicional**

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

### **Teorema de Bayes**

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

### **Probabilidad de la unión**

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

### **Probabilidad de la intersección de dos sucesos independientes**

$$P(A \cap B) = P(A)P(B)$$

### **Esperanza de una serie geométrica**

Sea  $X$  una variable aleatoria que indique el número de intentos hasta el primer suceso. Si la probabilidad de éxito es  $p$ , entonces:

- $P(X = k) = p(1 - p)^{k-1}$
- $E(X) = \sum_{k=1}^{\infty} p(1 - p)^{k-1}k = \frac{1}{p}$