

# Matemática Discreta Aplicada

Notas de clase

David Gabriel Corzo Mcmath

2019-08-03 02:29

# Índice general

I Notas de Clases del semestre	4
1. Clase del Día: 2019-07-22; clase introductoria, ¿qué es la matemática discreta?, juegos de lógica fáciles	5
2. Clase del Día: 2019-07-24; Lógica proposicional, juegos de lógica más complejos, ejemplos de juegos de lógica	8
3. Clase del Día: 2019-07-29; Equivalencias lógicas, tautología, contradicción, contingencia, jerarquías operacionales lógicas	12
4. Clase del Día: 2019-07-31; Inferencia, reglas de inferencia,	17
5. Clase del Día: 2019-08-05; Primer laboratorio de lógica proposicional, equivalencias lógicas, reglas de inferencia	22
6. Clase del Día: 2019-08-07; Técnicas de demostración, prueba directa, sets de números	25
7. Clase del Día: 2019-08-12; Continuación de técnicas de demostración, prueba directa, prueba por contra-recíproca, prueba por casos(exhaustión), prueba por contradicción	28
8. Clase del Día: 2019-08-14; Más ejemplos de técnicas de demostración, introducción a la inducción matemática	33
9. Clase del Día: 2019-08-19; Continuación inducción matemática, más ejemplos con las técnicas de demostración presentadas hasta el momento, técnicas de conteo, principio de la suma, principio del producto	38
10. Clase del Día: 2019-08-21; definición de P.S. \$ P.P., ejemplos, ¿cómo complementan estos principios a las técnicas de demostración?, Permutaciones	44
11. Clase del Día: 2019-08-26; Combinatoria, ejercicios con Álvaro	49
12. Clase del Día: 2019-08-28, Combinaciones, ejemplos	52
13. Clase del Día: 2019-09-02; Permutaciones y combinatoria generalizada	56
14. Clase del Día: 2019-09-16; Teoría de números, teorema de euclides, teorema fundamental de la aritmética, interesante: numeros primos, mcd(a,b)	61
15. Clase del Día: 2019-09-18; Continuación, refutación del método mcd(a,b) de la mis, mínimo común multiplo (mcm(a,b)),	65
16. Clase del Día: 2019-09-23; Identidad de Bézout	70

17.Clase del Día: 2019-09-25; Ecuación Diofantiana	74
18.Clase del Día: 2019-09-30; Aritmética modular	76
19.Clase del Día: 2019-10-07 ; Continuación de aritmética modular	80
20.Clase del Día: 2019-10-09 ; Cálculo de inversos multiplicativos módulo $n$	84
21.Clase del Día: 2019-10-09 ; 2019-10-16	87
22.Clase del Día: 2019-10-09 ; Cálculo de inversos	91
23.Clase del día: 2019-10-30 ; Cifrado Vigenirer	96
24.Clase del día: 2019-11-06 ; RSA, teoría	98
25.Clase del día: 2019-11-11 ; RSA, ejemplo	102

# Parte I

## Notas de Clases del semestre

# Capítulo 1

Clase del Día: 2019-07-22; clase introducción, ¿qué es la matemática discreta?, juegos de lógica fáciles

CS041; Mario Castillo; macastillom@utm.edu

¿Qué es?

Es la manipulación numérica de elementos contables.

Es la matemática de los números enteros.

Ej Conjeturas y pruebas: una conjectura es una idea, en matemática, es una idea que no se ha probado para todos los números, es una aproximación

$$1 = 1^2$$

$$1 + 3 = 2^2$$

$$1 + 3 + 5 = 3^2$$

$$1 + 3 + 5 + 7 = 4^2$$

$$1 + 3 + 5 + 7 + 9 = 5^2$$

$$\underbrace{1 + 3 + 5 + \dots + n}_{n \text{ números}} = n^2$$

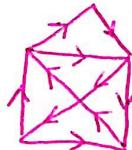
$$\sum_{i=1}^n (2i - 1) = n^2$$

cuando son 20,000,000  
de números

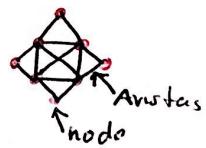
■ La forma que se deriva de observar el patrón es una con

■ Un flap es un círculo de retazos  
■ no hay que generalizar

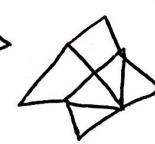
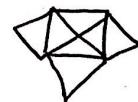
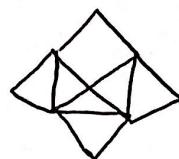
Ej: la casita



Tiene solución



Ej. La casita reloaded



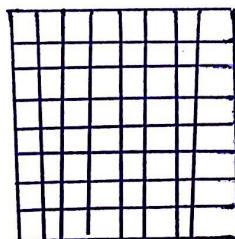
No tiene solución

Teoría de grafos

Lo que sale del nodo se llama grado, no tiene solución porque el grado de los nodos tienen que ser

Ej Ajedrez

tomar en cuenta los cuadros negros y blancos, no se puede quitar uno negro y solo uno blanco.



## E8: Teoría de números

Encryptación (cryptografía)  
oculta escritura

- Ceasar's shift

0	1	2	3	4	5	...	23	24	25
A	B	C	D	E	F	...	X	Y	Z
2	3	4	5	6	7		25	0	1

$$\text{def } \text{Encrypt}(x) = x + 2 \pmod{26}$$

No es inmune a un ataque de fuerza bruta

Enigma

RSA

ECC

# Capítulo 2

Clase del Día: 2019-07-24; Lógica proposicional, juegos de lógica más complejos, ejemplos de juegos de lógica

# Logica Proposicional

24/07/2017

Juegos de lógica:

Premisas = condicionales preexistentes

Proposición abierta  $\Rightarrow P(x) : x > 4$

$P \wedge q$  conjunción (and)

$P \vee q$  disyunción (or)

$\neg P$  no (not)

$P \Rightarrow q$  (si  $P$ , entonces  $q$ ), implicación

$P \Leftrightarrow q$  doble implicación ( $P$  si y solo si  $q$ )

o conectivos 2 proposiciones  
o atómico 1 proposición

Tablas de verdad

$P$	$q$	$P \Rightarrow q$	$P \Leftrightarrow q$
0	0	1	1
0	1	1	0
1	0	0	0
1	1	1	1

Si estudio mate discreta

entonces aprueba el curso.

Proposiciones:

m: el mayordomo dice la verdad

c: el cocinero dice la verdad

j: el jardinero dice la verdad

e: el empleado está diciendo la verdad

Premisas:

$$1. m \rightarrow c$$

$$2. \neg(c \wedge j)$$

$$3. \neg(\neg j \wedge \neg e)$$

$$4. e \rightarrow \neg c$$

Argumento:

$$5. \text{Suponemos } c = 0$$

$$6. m = 0 \text{ (porque } \neg c \text{ es verdad)}$$

$$7. j = 0 \text{ o } j = 1$$

$$8. e = 0 \text{ o } e = 1 \quad \text{y } e \neq 0 \text{ y } j \neq 0$$

conclusión parcial

$$10. c = 0, m = 0 \text{ para } \neg e \wedge \neg j = 0$$

		m	c	$m \rightarrow c$
0	0	[0]		1
0	1	[1]		1
1	0		[0]	0
1	1		[1]	1

		e	c	$e \rightarrow \neg c$
0	0			1
0	1			1
1	0			1
1	1			0

		c	j	$c \wedge j$	$\neg(c \wedge j)$
0	0			0	1
0	1			0	1
1	0			0	1
1	1			1	0

		j	e	$\neg j \wedge \neg e$	$\neg(\neg j \wedge \neg e)$
0	0			1	0
0	1			0	1
1	0			0	1
1	1			0	1

$$5'. \text{Suponemos } c = 1$$

$$6'. j = 0 \text{ (porque } 2 \text{ es verdad)}$$

$$7'. e = 1 \text{ (porque } 3 \text{ es verdad)}$$

$$8'. e = 0 \text{ (contradicción)}$$

$$\therefore m = 0$$

$$c = 0$$

$$\neg e \wedge \neg j = 0$$

1º en esta habitación hay una dama y en la otra hay un tigre.

2º en una de estas habitaciones hay una dama y en una un tigre

1.

D	T	D $\wedge$ T
0	0	0
0	1	0
1	0	0
1	1	1

2

D	T	D $\vee$ T
0	0	0
0	1	1
1	0	1
1	1	1

1	2	1 1 2
0	0	
0	1	
1	0	
1	1	

$$P \Rightarrow Q$$

# Capítulo 3

Clase del Día: 2019-07-29; Equivalencias lógicas, tautología, contradicción, contingencia, jerarquías operacionales lógicas

# Equivalecias lógicas

29/07/2019

## Definiciones preliminares

- Tautología = una proposición compuesta que siempre es verdadera.
- Contradicción = proposición compuesta que siempre es falsa.
- Contingencia = una proposición compuesta que no es tautología ni contradicción.

- 
- $P$  y  $Q$  son lógicamente equivalentes si la bicondicional es una tautología

$$\frac{P_1 \wedge (P_2 \wedge P_3)}{P \leftrightarrow Q}$$

•  $P$  y  $Q$  son lógicamente equivalentes:

$$P \equiv Q$$

- 
- Ej. Probemos que  $\neg(\neg P) \equiv P$ :

- construimos una tabla

P	$\neg P$	$\neg(\neg P)$	$\neg(\neg P) \leftrightarrow P$
0	1	0	1
1	0	1	1

tautología

Por lo tanto  $\neg(\neg P) \equiv P$ ; doble negación

Ej.: Propiedad identidad

$$P \wedge V \equiv P$$

P	V	$P \wedge V$	$P \wedge V \leftrightarrow P$
0	1	0	1
1	1	1	1

tautología

$$\underline{P \wedge V \equiv P} \text{ es verdadero}$$

• Equivalencias lógicas

- logical equivalences involving conditional statements
- logical equivalences involving biconditional statements

Ej.: Sin usar tablas de verdad, mostrar:

$$\neg(\neg P \wedge Q) \equiv P \vee \neg Q$$

Prueba: (Algebra de booleana)

$$\begin{aligned} \neg(\neg P \wedge Q) &\equiv \neg(\underbrace{\neg P}_{P}) \vee \neg Q \quad \left. \right\} \text{ De Morgan} \\ &\equiv P \vee \neg Q \quad \left. \right\} \text{ Doble negación} \end{aligned}$$

Ej.:  ~~$\neg(P \wedge (\neg P \wedge Q)) \equiv \neg(P \wedge Q)$~~

$$\text{Ej.: } \neg(P \vee (\neg P \wedge q)) \equiv \neg(P \vee q)$$

Prueba:

$$\begin{aligned} \neg(P \vee (\neg P \wedge q)) &\equiv \neg([P \vee \neg P] \wedge [P \vee q]) \text{ Distributatividad} \\ &\equiv \neg(\top \wedge [P \vee q]) \text{ Negación} \\ &\equiv \neg(P \vee q) \text{ Identidad} \end{aligned}$$

Se trabaja desde adentro  
hacia afuera.

Tener en cuenta de operaciones

$$\text{Ej.: } \neg(P \rightarrow q) \equiv P \wedge \neg q$$

2do

① $\neg$ ② $\wedge$ ③ $\vee$ ④ $\rightarrow$ ⑤ $\leftrightarrow$	<b>Ej.:</b> mostrar que $[\neg P \wedge (P \rightarrow q)] \rightarrow q$ es tautología	$P \rightarrow q \equiv \neg P \vee q$ <u>1ero</u> $\neg(P \rightarrow q) \equiv \neg(\neg P \vee q)$ $\equiv [\neg P \wedge (\neg P \vee q)] \rightarrow q$ Equivalencia → $\neg(\neg P) \wedge \neg q$ doble $\equiv P \wedge (\neg P \vee q) \rightarrow q$ Distributiva $\equiv P \wedge \neg q$ $\equiv (\neg P \wedge P) \vee (P \wedge q) \rightarrow q$ Negación $\equiv F \vee (P \wedge q) \rightarrow q$ Identidad
--	--	--

Regla de inferencia  
*modus ponens*

$$\begin{aligned} P \wedge (P \rightarrow q) &\rightarrow q \\ P \rightarrow q &\equiv \neg P \vee q \\ \text{equiva. } \rightarrow &\quad \equiv \neg P \vee q \rightarrow q \text{ Equiv. } \rightarrow \\ &\quad \equiv \neg P \vee \neg q \vee q \text{ De Morgan} \\ \equiv q \vee \neg P &\quad \text{comutativa} \quad \equiv \vee \quad \text{Dominación} \\ \equiv \neg q \rightarrow \neg P &\quad \left. \begin{array}{l} \text{Contradicción} \\ \text{P} \rightarrow q \quad \equiv \neg q \rightarrow \neg P \end{array} \right\} \text{Contradicción} \\ \text{Equiv. } \rightarrow & \end{aligned}$$

## Validación de Argumentos:

# Capítulo 4

Clase del Día: 2019-07-31; Inferencia, reglas de inferencia,

# Inferencia

31/07/2019

- Deducción
- Conclusión a partir de información conocida.

- ↳ Descubrir el razonamiento que se utiliza para demostrar o probar un argumento
- ↳ Validar un argumento → usar equivalencias lógicas y reglas de inferencia para determinar si la conclusión de dicho argumento es V o F.
- Buen Argumento = debe de ser correcto pero fácil que los demás entiendan. "Orden", "Claro".
- Un argumento puede ser falso si la conclusión es verdadera
- A raíz de lo tedioso que es hacer tablas o álgebra booleana surgen las reglas de inferencia

$$(P_1 \wedge P_2 \wedge \dots \wedge P_n) \rightarrow q$$

ó cómo hacer tablas o álgebra aquí?

▲ Reglas de inferencia son TAV TOLOGÍAS

• modus ponens

ejo:  $P \wedge (P \rightarrow q) \rightarrow q$

• Resolución

$$\begin{array}{c} p \vee q \\ \neg p \vee r \\ \hline q \vee r \end{array}$$

Plantea:

$$\begin{aligned} & (p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r) \\ & p \wedge (q \wedge r) = (p \wedge q) \vee (p \wedge r) \\ & [(p \wedge q) \wedge \neg p] \vee [(p \wedge q) \wedge \neg q] \rightarrow \text{que} \end{aligned}$$

$$(P \vee q) \wedge (\neg P \vee r) \rightarrow (q \vee r)$$

$$\boxed{[P \vee q]}$$

$$P \wedge (q \vee r) \equiv (P \wedge q) \vee (P \wedge r)$$

P q r	P ∨ q	$\neg P \vee r$	$\textcircled{1} \wedge \textcircled{2}$	q ∨ r	$\textcircled{3} \rightarrow \textcircled{4}$
0 0 0	0	1	0	0	1
0 0 1	0	1	0	1	1
0 1 0	1	1	1	1	1
0 1 1	1	1	1	1	1
1 0 0	1	0	0	0	1
1 0 1	1	1	1	1	1
1 1 0	1	0	0	1	1
1 1 1	1	1	1	1	1

Premisas

- Ej:
- $\textcircled{1} (\neg P \vee q) \rightarrow r \quad \textcircled{2} r \rightarrow (s \vee t) \quad \textcircled{3} \neg s \wedge \neg t \quad \textcircled{4} \neg t \rightarrow \neg s$
  - $\textcircled{5} (\neg P \vee q) \rightarrow (s \vee t) \quad \textcircled{6} \neg s \quad \textcircled{7} \neg t \quad \textcircled{8} \neg s$
  - $\textcircled{9} \neg s \wedge \neg t \quad \textcircled{10} \neg (\underbrace{s \vee t}_{s \vee t \text{ es falso}}) \quad \textcircled{11} \neg (P \wedge \neg q) \quad \textcircled{12} P$
  - $\textcircled{13} P \quad \textcircled{14} \neg s \wedge \neg t \quad \textcircled{15} \neg (\neg P \vee q) \quad \textcircled{16} P \wedge \neg q$
- lectura*
1.  $(\neg P \vee q) \rightarrow r$  // silogismo hipotético
2.  $r \rightarrow (s \vee t)$  // simplificación 3
3.  $\neg s \wedge \neg t$  // modus ponens con 1, 2
4.  $\neg t \rightarrow \neg s$  // simplificación 3
5.  $\neg s \wedge \neg t$  // conjunción 7 y 8
6.  $\neg (\underbrace{s \vee t}_{s \vee t \text{ es falso}})$  // De Morgan
7.  $P \wedge \neg q$  // De Morgan
8.  $P$  // simplificación 12.
9.  $\neg (\neg P \vee q)$  // por  $(s \vee t) = F$  entonces en la 5

## Validación de argumentos

- $P$ : La banda toca  
 $q$ : Las bebidas  
 $r$ : La fiesta se cancela  
 $s$ : Alice se enoja  
 $t$ : El dinero se gasta

identificación

Previsas:

$$1. (\neg P \vee q) \rightarrow (r \wedge s)$$

$$2. r \rightarrow t$$

$$3. \neg t$$

$$\frac{}{\therefore P}$$

$$4. \underbrace{(\neg P \vee q)}_{P \rightarrow q} \rightarrow r \wedge s \quad \text{equiv.}$$

$$5. (P \rightarrow q) \rightarrow \underbrace{(r \wedge s)}_r \quad \text{simplificación}$$

$$6. \underbrace{(P \rightarrow q)}_{(P \rightarrow q) \rightarrow r} \rightarrow r \quad \text{equiv.}$$

$$\underbrace{(\neg P \vee q)}_{(\neg P \vee q) \rightarrow r} \rightarrow r$$

$$7. (\neg P \vee q) \vee r \quad \text{equiv.}$$

**TABLE 8** Logical Equivalences Involving Biconditional Statements.

$$\begin{aligned} p \leftrightarrow q &\equiv (p \rightarrow q) \wedge (q \rightarrow p) \\ p \leftrightarrow q &\equiv \neg p \leftrightarrow \neg q \\ p \leftrightarrow q &\equiv (p \wedge q) \vee (\neg p \wedge \neg q) \\ \neg(p \leftrightarrow q) &\equiv p \leftrightarrow \neg q \end{aligned}$$

**TABLE 1** Rules of Inference.

Rule of Inference	Tautology	Name
$\frac{p}{\therefore p \rightarrow q}$	$(p \wedge (p \rightarrow q)) \rightarrow q$	Modus ponens
$\frac{\neg q}{\neg q \wedge (p \rightarrow q)} \quad p \rightarrow q$ $\therefore \neg p$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$	Modus tollens
$\frac{p \rightarrow q \quad q \rightarrow r}{\therefore p \rightarrow r}$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$\frac{p \vee q \quad \neg p}{\therefore q}$	$((p \vee q) \wedge \neg p) \rightarrow q$	Disjunctive syllogism
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification
$\frac{p \quad q}{\therefore p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\frac{p \vee q \quad \neg p \vee r}{\therefore q \vee r}$	$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$	Resolution

**TABLE 6** Logical Equivalences.

Equivalence	Name
$p \wedge T \equiv p$	Identity laws
$p \vee F \equiv p$	
$p \vee T \equiv T$	Domination laws
$p \wedge F \equiv F$	
$p \vee p \equiv p$	Idempotent laws
$p \wedge p \equiv p$	
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$	Commutative laws
$p \wedge q \equiv q \wedge p$	
$(p \vee q) \vee r \equiv p \vee (q \vee r)$	Associative laws
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	Distributive laws
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	De Morgan's laws
$\neg(p \vee q) \equiv \neg p \wedge \neg q$	
$p \vee (p \wedge q) \equiv p$	Absorption laws
$p \wedge (p \vee q) \equiv p$	
$p \vee \neg p \equiv T$	Negation laws
$p \wedge \neg p \equiv F$	

**TABLE 7** Logical Equivalences Involving Conditional Statements.

$$\begin{aligned} p \rightarrow q &\equiv \neg p \vee q \\ p \rightarrow q &\equiv \neg q \rightarrow \neg p \\ p \vee q &\equiv \neg p \rightarrow q \\ p \wedge q &\equiv \neg(p \rightarrow \neg q) \\ \neg(p \rightarrow q) &\equiv p \wedge \neg q \\ (p \rightarrow q) \wedge (p \rightarrow r) &\equiv p \rightarrow (q \wedge r) \\ (p \rightarrow r) \wedge (q \rightarrow r) &\equiv (p \vee q) \rightarrow r \\ (p \rightarrow q) \vee (p \rightarrow r) &\equiv p \rightarrow (q \vee r) \\ (p \rightarrow r) \vee (q \rightarrow r) &\equiv (p \wedge q) \rightarrow r \end{aligned}$$

# Capítulo 5

Clase del Día: 2019-08-05; Primer laboratorio de lógica proposicional, equivalencias lógicas, reglas de inferencia

$$\textcircled{1} [(p \rightarrow q) \wedge (\neg r \vee s) \wedge (p \vee r)] \rightarrow (\neg q \rightarrow s)$$

$$(\neg p \vee q) \wedge (p \vee r) \wedge (\neg r \vee s) \quad \text{resolution}$$

$$(q \vee r) \wedge (\neg r \vee s) \quad \text{resolution}$$

$$(r \vee q) \wedge (\neg r \vee s) \quad \text{resolution}$$

$$p \rightarrow q$$

$$\neg r \vee s$$

$$p \vee r$$

$$\therefore \neg q \rightarrow s$$

$$(q \vee s) \quad \text{equivocación}$$

$$(\neg q \rightarrow s)$$

$$\textcircled{2} [(p \wedge \neg q) \wedge r] \rightarrow (p \wedge r) \vee q$$

$$\textcircled{1} p \wedge \neg q$$

$$\textcircled{2} r$$

$$\therefore (p \wedge r) \vee q$$

$$\textcircled{3} p \quad \text{simplificación 1.}$$

$$\textcircled{4} p \wedge r \quad \text{conjunción 2 y 3}$$

$$\textcircled{5} (p \wedge q) \vee q \quad \text{adicción}$$

$$\textcircled{3} \quad [P \wedge (P \rightarrow q) \wedge (\neg q \vee r)] \rightarrow r$$

\textcircled{1} P

\textcircled{2}  $P \rightarrow q$

\textcircled{3}  $\neg q \vee r$

# Capítulo 6

Clase del Día: 2019-08-07; Técnicas de demostración, prueba directa, sets de números

# Técnicas de demostración

07/08/2019

Def: Demostración es una validación lógica de un teorema.  
Proposiciones

- Prueba o demostración directa
  - Prueba o demostración recíproca
  - Prueba o demostración por contradicción
  - Prueba o demostración por casos
  - Prueba por inducción matemática
- 

Prueba Directa: (usa modus ponens)

Queremos demostrar la implicación:

$$P \rightarrow q$$

La estrategia: 1) suponer  $P$   
2) Comprobamos  $q$

Ej: La suma de dos números pares  
es un número par.

Si  $n$  y  $m$ , entonces  $m+n$  es par.

Gregor Cantor

$\mathbb{Z}$ : Zahlen | Prueba: Supongamos  $m = 2k_1$  y  $n = 2k_2$

$\mathbb{N}$ : Naturliche

para  $k_1, k_2 \in \mathbb{Z}$

$\mathbb{Q}$ : Quotienten

Luego,  $m+n = 2k_1 + 2k_2 = 2(\underbrace{k_1+k_2}_{\mathbb{Z}}) = 2k_3$

$\mathbb{R}$ : Reelle

$\mathbb{C}$ : Komplexe

□ ◇ Q.E.D.

Ej: Si  $a$  es par y  $b$  es impar, entonces  $a \cdot b$  es par

Nota: Los impares tienen la forma  $2k+1$

Prueba:

Suponemos,  $a = 2k_1$        $b = 2k_2 + 1$  para  $k_1, k_2 \in \mathbb{Z}$

$$\begin{aligned} \text{Luego, } a \cdot b &= 2k_1 \cdot (2k_2 + 1) = 4k_1 \cdot k_2 + 2k_1 \\ &= 2(2k_1 \cdot k_2 + k_1) = \underline{\underline{2k_3}} \end{aligned}$$

# Capítulo 7

Clase del Día: 2019-08-12; Continuación de técnicas de demostración, prueba directa, prueba por contra-recíproca, prueba por casos(exhaustión), prueba por contradicción

## Prueba directa

$$P \rightarrow q$$

✓) Asumimos p verdadero

v) Demostremos q

$$\therefore p \rightarrow q$$

## Demostración

Er:

$P_1 \wedge P_2$

$$q: \text{m+n par} \quad m+n = 24$$

$$q = 1$$

Prueba por contrareciproca

La proposición  $\neg q \rightarrow \neg p$  se llama contrarecíproca (o contrapositiva) de la proposición  $p \rightarrow q$

$$P \rightarrow q \equiv {}^1q \rightarrow {}^1p$$

Ej: Para cualquier  $n \in \mathbb{Z}^+$ , si  $n^2$  es par, entonces  $n$  es par.

Si asumimos p, tendriamos:

tiene que ser  
binario no por  
casos  $n^2 = 2m$ , para algún número entero positivo  
 $\therefore n = 2k$ , es imposible inferir

Prueba: Por contrapositiva

• Asumimos  $7q = n$  impar;  $n = 2m+1$  entonces,

$$n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2[2m^2 + 2m] + 1$$

$$= 2K + 1$$

四

$P$ :  $n$  par y no impar

$q$ :  $m \cdot n$  par

Si  $n$  par y  $m$  impar, entonces  $m \cdot n$  Par,  
 $\frac{P}{q}$

$$\frac{n \wedge m}{\text{Par} \quad \text{impar}} \longrightarrow m \cdot n \text{ par}$$

Si  $m \cdot n$  impar, entonces  $n$  impar o  $m$  par.

$m \cdot n$  impar,  $\neg(n \wedge m)$  demorgan

$$\frac{\neg(m \cdot n)}{\neg(n \vee \neg m)}$$

Prueba por casos (exhaustión)

La proposición:

$$(p_1 \vee p_2 \vee \dots \vee p_k) \rightarrow q$$

es equivalente a  $\equiv (p \vee q) \rightarrow r \equiv (p \rightarrow r) \wedge (\neg r \rightarrow q)$

$$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_k \rightarrow q)$$

Ej: Si  $n$  no es divisible por 5, entonces  $n^2$  tiene residuo 1 o 4 al ser dividido por 5.

$$n = 97 \rightarrow n^2 = 9409 = 1881 \cdot 5 + 4$$

$$n = 18 \rightarrow n^2 = 324 = 64 \cdot 5 + 4$$

$$n = 6 \Rightarrow n^2 = 36 = 7 \cdot 5 + 1$$

Un número no múltiplo de 5 tiene forma

$$\underbrace{5k+1}_P_1 \circ \underbrace{5k+2}_P_2 \circ \underbrace{5k+3}_{P_3} \circ \underbrace{5k+4}_{P_4}$$

Queremos probar:

$$(P_1 \vee P_2 \vee P_3 \vee P_4) \rightarrow q$$

en donde  $q: \underbrace{5m+1}_{q_1} \circ \underbrace{5m+4}_{q_2}$

Prueba por casos:

Caso 1:  $n = 5k+1$

$$\begin{aligned} \text{Luego, } n^2 &= 25k^2 + 10k + 1 \\ &= 5(5k^2 + 2k) + 1 \\ &= 5m + 1 \end{aligned}$$

Caso 2:  $n = 5k+2$

$$\begin{aligned} \text{Luego, } n^2 &= 25k^2 + 20k + 4 \\ n &= 5(5k^2 + 4k) + 4 \\ &= 5m + 4 \end{aligned}$$

Caso 3:

$$\begin{aligned} n &= 5k+3 \\ \text{Luego } n^2 &= 25k^2 + 30k + 9 \\ &= 5(5k^2 + 6k) + 9 \equiv 5(5k^2 + 6k + 1) + 4 \\ &= 5k + 4 \end{aligned}$$

Caso 4:  $n = 5k+4$

$$\begin{aligned} \text{Luego } n^2 &= 25k^2 + 40k + 16 = n^2 = 25k^2 + 15 + 1 \\ &= 5(5k^2 + 8k + 3) + 1 \\ &= 5m + 1 \end{aligned}$$

□

## Prueba por contradicción

La proposición  $p \rightarrow q$  puede probarse de la siguiente manera:

v) Asumimos  $P$

v) Asumimos  $\neg q$

v) Demostremos que  $\underbrace{(p \wedge \neg q)}_{\text{es una contradicción}} \rightarrow F$

$$(p \wedge \neg q) \rightarrow F$$

$\therefore q$  es verdad.

Ej: Si  $a \geq 2$  y  $b \in \mathbb{Z}$ , entonces  $a \nmid b$  o  $a \nmid (b+1)$

$a = 8 ; b = 11$
$8 \nmid 11 \quad \circ \quad 8 \nmid 12 \quad \checkmark$
$a = 8 ; b = 15$
$8 \nmid 15 \quad 8 \mid 16$

Prueba: por contradicción

Asumimos  $a \geq 2$  y  $b \in \mathbb{Z}$ . Asumimos también, para fines de contradicción, que  $a \mid b$  y  $a \mid (b+1)$ .

Esto es:

$$b = m_1 \cdot a \quad y \quad b+1 = m_2 \cdot a$$

# Capítulo 8

Clase del Día: 2019-08-14; Más ejemplos  
de técnicas de demostración, introduc-  
ción a la inducción matemática

# Matemática Discreta

2019-08/14

Probar que  $a \geq 2$ , entonces  $a \nmid b$  o  $a \nmid b+1$

supongamos  $a \mid b$  y  $a \mid b+1$

$$\Rightarrow b = m_1 \cdot a \quad y \quad b+1 = m_2 \cdot a$$

sustituimos  $b = m_1 \cdot a$  en  $b+1 = m_2 \cdot a$ :

$$\begin{aligned}m_1 \cdot a + 1 &= m_2 \cdot a \\1 &= m_2 \cdot a - m_1 \cdot a \\1 &= (m_2 - m_1) \cdot a\end{aligned}$$

$\uparrow$   
 $\geq 2$

Entonces,  $\frac{1}{m_2 - m_1} = a \rightarrow a \leq 1$

$a \geq 2$  y  $a \leq 1$  ( $\rightarrow \leftarrow$ )  
contradicción

En conclusión,  $a \nmid b$  o  $a \nmid (b+1)$

□

Ej:  $\sqrt{2}$  es irracional

todos los números que no se pueden escribir como la división de dos enteros son irracionales.

Prueba: supongamos, para fines de contradicción,  $\sqrt{2}$  es racional.

$$\sqrt{2} = \frac{\underbrace{a}_{\text{fracción reducida}}}{b}, b \neq 0 \quad y \quad \text{mcd}(a, b) = 1$$

elevamos al cuadrado ambos lados

$$((2)^{\sqrt{2}})^2 = (a/b)^2 \Rightarrow 2 = \frac{a^2}{b^2} \Rightarrow a^2 = 2b^2$$

$a$  es par.

Luego,  $a = 2k$ . Entonces,

$$a^2 = (2k)^2 = 4k^2 = 2b^2$$

$$b^2 = 2k^2 \quad b^2 = 2k^2, b^2 \text{ es par} \rightarrow b \text{ es par}$$

$a$  es par y  $b$  es par ( $\rightarrow \leftarrow$ )

En conclusión,

$\sqrt{2}$  es irracional

□

---

Inducción Matemática Es una técnica de demostración para propiedades de los números enteros

Analogía: Dáminas

① Paso base tengo que demostrar que puedo botar el primero.

..... ② tengo que demostrar que si cae el primero se va a botar el que sigue  
validar argumento en el procedimiento de lógica. ③ paso inducción

③ conclusión todos se caen

Formalmente, si  $p(n)$  es una proposición abierta y  $n \in \mathbb{Z}^+$ , entonces el argumento

1.  $P(n_0)$  es verdad (para algún  $n_0 \in \mathbb{Z}^+$ )

2.  $P(n) \rightarrow P(n+1)$  es verdad

Entonces,  $p(n)$  es cierta para toda  $n \in \mathbb{Z}^+$

La suma de los primeros  $n$  impares (positivos) consecutivos es un cuadrado perfecto, en particular  $n^2$ .

matematizar:

$$\sum_{i=1}^n (2i - 1) = n^2$$

$2k+1$ , si  $k$  arranca en 0

$2k-1$ , si  $k$  arranca en 1

Paso base:  $n = 1$

$$\sum_{i=1}^1 (2i - 1) = 1 = 1^2$$

Paso induutivo: Asumimos (prueba dirigida)  $\sum_{i=1}^n (2i - 1) = n^2$

$$\begin{aligned} \sum_{i=1}^{n+1} (2i - 1) &= \underbrace{1 + 3 + 5 + 7 + \dots + (2n - 1)}_n + \underbrace{2(n+1) - 1}_{n+1} \\ &= \underbrace{\sum_{i=1}^n (2i - 1)}_{n^2} + 2n + 1 \\ &= n^2 + 2n + 1 \quad \text{factorizo} \\ &= (n + 1)^2 \end{aligned}$$

□

Ej: La suma de los primeros  $n$  consecutivos es  $\frac{n(n+1)}{2}$

# Capítulo 9

Clase del Día: 2019-08-19; Continuación inducción matemática, más ejemplos con las técnicas de demostración presentadas hasta el momento, técnicas de conteo, principio de la suma, principio del producto

# Matemática Discreta Aplicada

2019-08/19

Ej:  $\sum_{i=1}^n i = \frac{n(n+1)}{2}$  La Suma de los primeros  $n$  consecutivos es  $\frac{n(n+1)}{2}$ :

Prueba: por inducción

Paso Base: Probamos  $n=1$

$$\sum_{i=1}^1 i = \frac{1(1+1)}{2} = 1$$

Paso inductivo: Asumimos  $\sum_{i=1}^n i = \frac{n(n+1)}{2}$

Luego,  $\sum_{i=1}^{n+1} i = \underbrace{(n+1)}_{\text{lo saco de la suma para reemplazar.}} + \underbrace{\sum_{i=1}^n i}_{\text{reemplazo}}$

$$= n+1 + \frac{n(n+1)}{2} = \frac{2(n+1) + n(n+1)}{2}$$

$$= \frac{(n+1)(n+2)}{2} \quad \square$$

- 
- Se necesita probar por inducción matemática para ser válido.

Ej: Pruebe que si  $n \geq 2$ , entonces  $n^3 - n$  es un múltiplo de 3.

Prueba por inducción:

Prueba: Probamos  $n=2$

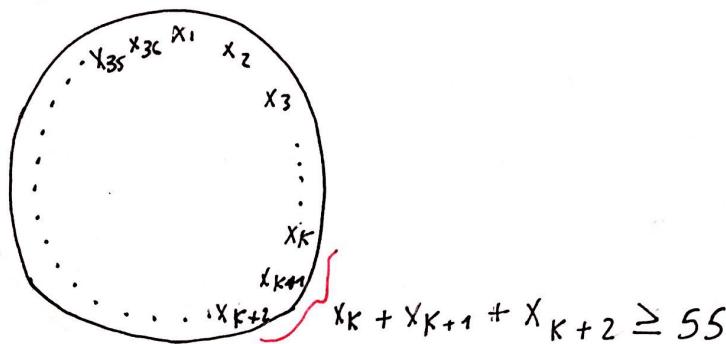
$$(2)^3 - (2) = 6 = \underbrace{2 \cdot 3}_{\text{se probó que es un múltiplo de 3.}}$$

Paso inductivo:  $n^3 - n = 3m$ ;  $m$  es un entero positivo.  $m \in \mathbb{Z}^+$

Entonces,

$$\begin{aligned}(n+1)^3 - (n+1) &= n^3 + 3n^2 + 3n + 1 - n - 1 \\&= (\underbrace{n^3 - n}_{3m}) + 3n^2 + 3n \\&= 3m + 3n^2 + 3n \\&= 3(m + n^2 + n) \\&\quad \text{esta es un entero arbitrario} \\&= 3K \quad \square\end{aligned}$$

Ej: Prueba que en una ruleta con los números de 1 a 36, dispuestos de forma aleatoria, siempre existen 3 consecutivos cuya suma es 55 o más.



Solución: Escribir los números de la ruleta en un listado hacia abajo.

$$\begin{aligned} &x_1 + x_2 + x_3 < 55 \\ &x_2 + x_3 + x_4 < 55 \\ &x_3 + x_4 + x_5 < 55 \\ &x_4 + x_5 + x_6 < 55 \\ &\vdots \quad \vdots \quad \vdots \\ &x_{35} \quad x_{36} \quad x_1 < 55 \\ &\underbrace{x_{36}}_{1-36} \quad \underbrace{x_1}_{1-36} \quad \underbrace{x_2}_{1-36} < 55 \end{aligned}$$

Se contempla prueba de contradicción por que

aquí están dispuestas todas las combinaciones posibles.

Para finir de contradicción se asume entonces que la suposición es falsa, entonces

$$x_k + x_{k+1} + x_{k+2} < 55$$

Sumamos las 36 desigualdades

$$3 \cdot \sum_{i=1}^{36} i < 36 \cdot 55$$

$$\sum_{i=1}^n i = \frac{n(n+1)}{2}$$

$$3 \cdot \left( \frac{36 \cdot 37}{2} \right) < 1980$$

$$1980 < 1980$$

(→←)

Si escoges de forma aleatoria 25 días del año, almenos 3 de esos 25, son del mismo mes

## Técnicas de conteo

Contar: asignar es la acción de asignar a un conjunto de objetos uno y solo uno, de los números naturales.

Def: Los números naturales son los enteros positivos.

$$\mathbb{N} = \mathbb{Z}^+$$

Entonces al "contar" hacemos:

$$S = \{a, e, i, \theta, u\}$$

■ Cuando se cuenta lo que se dice es el último número.

■ hay 5 números en el conjunto.

Técnica de conteo: Principio de la suma (P.S.)

- consiste en contar el número de elementos en la unión de dos conjuntos disjuntos.
- Def. Cardinalidad de un conjunto = es el número de elementos en un conjunto (finito) es su cardinalidad.
- Notación: Si A es un conjunto, su cardinalidad es  $|A|$

$$|A \cup B| = |A| + |B|, \text{ si } \underbrace{A \cap B = \emptyset}_{\text{conjuntos disjuntos}}$$

## Técnica de conteo: Principio de producto (P.P)

- Contamos el número de elementos en el producto cartesiano de dos conjuntos.
- Def. Producto Cartesiano

$$A \times B = \{(a, b) : a \in A \text{ y } b \in B\}$$

Ej:  $A = \{1, 2\}$  y  $B = \{x, y, z\}$

$$A \times B = \{(1, x), (1, y), (1, z), (2, x), (2, y), (2, z)\}$$

$$|A \times B| = |A| \times |B|$$

# Capítulo 10

Clase del Día: 2019-08-21; definición de P.S. \\$ P.P., ejemplos, ¿cómo complementan estos principios a las técnicas de demostración?, Permutaciones

$$\underline{P.S.} \quad |A \cup B| = |A| + |B|$$

$$A \cap B \neq \emptyset$$

Contamos algo que se puede hacer por casos

$$\text{P.P. } |A \times B| = |A| \cdot |B|$$

Contamos algo por pasos.

Ej.: Se tienen 10 libros de mate discreta y 250 de economía, si se quiere escoger un libro, entonces el número de maneras de poderlo hacer es:

Caso: libros de discreta: 10

Casa: Libro de economía: 250

∴ En total, por el P.S. hay 260 formas distintas de elegir un libro.

El abecedario tiene 26 letras. Se desea formar palabras usando 5 letras (no es posible repetir letras)

$$V = \{a, e, i, o, u\}$$

La tarea puede dividirse en 5 pasos:

$$V \times V = \{(a,a), (a,e) \dots (u,u)\}$$

$$|v \times v| = 25$$

$$\begin{array}{c}
 \text{J} \\
 \frac{26}{L_1} \quad \frac{25}{L_2} \quad \frac{24}{L_3} \quad \frac{23}{L_4} \quad \frac{22}{L_5} = \\
 \boxed{\begin{array}{l}
 \text{de cuantos pueden elegir} \\
 \text{de } 26. \quad \boxed{\text{elegir de } 25} \quad \boxed{\text{elegir de } 24} \\
 \text{elegir } 23 \quad \text{elegir}
 \end{array}}
 \end{array}$$

Si las letras se pudieran repetir sería:

$$\frac{26}{L_1} \cdot \frac{26}{L_2} \cdot \frac{26}{L_3} \cdot \frac{26}{L_4} \cdot \frac{26}{L_5} = 17,881,376$$

- El problema anterior consistió en una selección ordenada de 5 elementos de un conjunto con 26 "porque el orden es importante"

- FCUK

- Dunkin doognuts

Notación: Factorial

sea  $n \in \mathbb{Z}^+ \{0\}$ , entonces a la multiplicación consecutiva

$$1 \cdot 2 \cdot 3 \cdot 4 \cdots n = n!$$

Por "definición"  $0!$  está definido como  $1$ .

Con esta notación, podemos escribir la respuesta anterior como:

$$\frac{26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 \cdot \cancel{21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdots 2 \cdot 1}}{\cancel{21 \cdot 20 \cdot 19 \cdots 2 \cdot 1}} = \frac{26!}{21!}$$

$$= \frac{26!}{(26-5)!}$$

En general, una selección ordenada de  $r$  elementos de un conjunto con  $n$  elementos distintos, se llama:

$r$  - permutación de  $n$

y se calcula como:

calculadora:  
shift +  $\boxed{x}$  = permutación

26 P 5

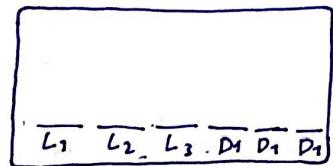
$$\frac{n!}{(n-r)!} = P(n, r)$$

Si se seleccionan los  $n$  elementos, esto se llama:  
permutación de  $n$  y se calculan como:

caso que  $r = n$

$$\frac{n!}{46} = P(n, n)$$

Ej.: Placas de correo en GT



Paso 1: escoger las letras

Paso 2: escoger los números

\* En GT no se usan vocales

\* Suponemos que hay placa 000

$$P(21,3) \cdot P(10,3) = 5,745,600$$

Ej.: Direcciones IP, internet protocol

$$\boxed{256} \cdot \boxed{256} \cdot \boxed{256} \cdot \boxed{256} = 4,294,967,296 \text{ posibles combinaciones}$$

Si se fuese a hacer por P.S.

$$\text{Caso 1} = L_1 A$$

$$\longrightarrow \text{Caso 1.1} = L_1 A$$

$$\longrightarrow \text{Caso 1.1.1} = L_3 A$$

:

$$\text{Caso 26} = L_1 Z$$

$$\longrightarrow \text{Caso 26.1} = L_2 Z$$

:

$$= 5,745,600 \text{ se hace por P.P. por que}$$

son muchas casas.

Ej.: ¿Cuántos números entre 1 y 999 no llevan el dígito 7?

Estrategia A: Por casos

Caso:  $1 \leq n \leq 9$

∴ Hay 8 dígitos entre 1 y 9 sin el 7

Caso:  $10 \leq n \leq 99$

Para saber cuántos números hay en "conjunto es el [último extremo - primer extremo + 1]"  
 $\frac{8}{D_1} \cdot \frac{9}{D_2} = 72$  números sin 7

Caso:  $100 \leq n \leq 999$

$$\frac{8}{D_1} \cdot \frac{9}{D_2} \cdot \frac{9}{D_3} = 648 \text{ números sin 7.}$$

Por el p.s. tenemos 728 números sin 7.  $\square$

Estrategia B: armar un número sin 7; por pasos

Paso 1: Elegir  $D_1$

Paso 2: Elegir  $D_2$

Paso 3: Elegir  $D_3$

$$\frac{9}{D_1} \cdot \frac{9}{D_2} \cdot \frac{9}{D_3} = 9^3 = 729$$

A los 729 números sin 7 entre 0 y 999, le restamos el 0 y terminaremos con 728 números sin 7 entre 1 y 999.  $\square$

# Capítulo 11

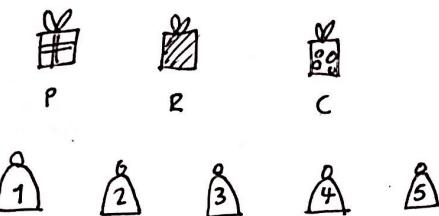
Clase del Día: 2019-08-26; Combinatoria,  
ejercicios con Álvaro

# Matemática Discreta - Combinatoria

2019-08-26

① Se distribuyen 3 regalos entre cinco chicos. De cuántas formas pueden hacerlo si:

a) cada chico solo puede recibir 1 regalo



• Cuando importa el orden usar permutación

1P	2R	3C
1P	2R	4C
:	:	

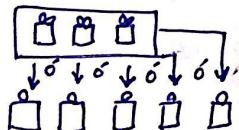
• Cuando no importa usar combinatoria

$${}^5P_3 = \frac{5!}{(5-3)!} = \frac{5!}{2!} = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1} = \cancel{\underline{60}} \quad \text{X}$$

b) a cada chico le puede tocar más de un regalo.

Por casos:

2: es como que si fuerse un paquete de 3 regalos



① un regalo a cada uno = 60  
② tres regalos solo a uno = 5

③ dos a uno y uno a otro = 60

problema de la uno:

125 X

3: losas de agrupación



$${}^5P_2 = \frac{5!}{(5-2)!} = 4 \cdot 5 = 20$$

como tenemos 3 casos se multiplica la permutación por 3

60

- c) cada chico sólo puede recibir un regalo pero los tres son idénticos.

NO IMPORTA ORDEN

$${}^n_r C = \frac{n!}{(n-r)! r!}$$

$${}^5_3 C = \frac{5!}{(5-3)! 3!} = \cancel{10}$$

- ② Una persona tiene 6 chaquetas y 10 pantalones. ¿De cuántas formas distintas puede combinar?

$$\begin{matrix} |A \times B| \\ C P \end{matrix} = |A| \times |B|$$

6	10
---	----

$$= |6| \times |10| = \cancel{60}$$

seis posibilidades de una chaqueta de 10 posibilidades diferentes de un pantalón.

\* Cuando solo hay dos conjuntos, se puede utilizar permutaciones pero cuando son 3 conjuntos se usa  $|A \times B|$

- ③ Un amigo le quiere regalar a otro dos libros, los quiere elegir entre 15 que le gustan. ¿Cuántas formas distintas puede combinar? NO IMPORTA = COMBINATORIA

$${}^{15}_2 C = \frac{15!}{(15-2)! 2!} = \cancel{105}$$

# Capítulo 12

Clase del Día: 2019-08-28, Combinaciones, ejemplos

## Combinaciones:

2019-08-28

Una selección no ordenada de  $r$  elementos de un conjunto  $n$  elementos, se llama  
 $r$ -combinación

Ej: Supongamos que tenemos un estuche con 5 lapiceros de colores:  $S = \{a, r, v, n, c\}$  y queremos escoger 3 de ellos, ¿de cuántas formas diferentes podemos hacerlo?

Si el orden fuese importante, sería:

$$P(S, 3) = \frac{5!}{2!} = 60$$

Por lo tanto:

Del total de 3-Permutaciones de 5 descontamos  $3!$  permutaciones.

$$\frac{5!}{(5-3)! 3!} = 10$$

En este caso la selección, por ejemplo:

- a, v, c
- a, c, v
- c, a, v
- c, v, a
- v, a, c
- v, c, a

es la misma selección no ordenada  
 $6 = 3!$   
 $P(3,3)$

- En general, de  $r$ -permutaciones de  $n$ , descontamos  $r!$  permutaciones

$$\frac{n!}{(n-r)! r!} = C(n, r)$$

- esto es  $r$ -combinación de  $n$  objetos

### Ej: Cadenas de bits

a) ¿Cuántas cadenas de 4 bits tienen dos ceros?

- Esta cadena tiene dos unos.

$$6 = C(4,2) \cdot \frac{4!}{2! \cdot 2!}$$

0 1 0 1      }  
 1 0 1 0      }  
 0 0 1 1      }  
 1    1 0 0      } 4!  
 1 0 0 1  
 0 1    1 0

$P(4,4)$   
 (se asume todos distintos)

$\begin{cases} 1100 \\ 1100 \end{cases}$  doble conteo  
 $\begin{cases} 1100 \\ 1100 \end{cases}$  doble conteo

b) Cadenas de 8 bits con 2 unos (6 ceros)

- suponiendo 8 símbolos distintos:

$$8! = 40320$$

- suponiendo que los 2 unos son iguales

$$\frac{8!}{2!}$$

- Suponemos que los 6 ceros son iguales:

$$\frac{8!}{2! \cdot 6!} = \underbrace{C(8,2)}_{2^8} = \underbrace{C(8,6)}_{2^8}$$

■ Propiedad de simetría:

$$C(n,r) = C(n,n-r)$$

c) Cadenas de ocho bits al menos con 3 unos.

- Contamos el complemento, es decir, cadenas de 8 bits con al menos 3 unos (0,1,2)

$$\text{Cadenas con cero unos} = C(8,0) = 1$$

$$\text{Cadenas con un uno} = C(8,1) = 8$$

$$\begin{array}{r} \text{Cadenas con dos unos} = C(8,2) = 28 \\ + \\ \hline 37 \end{array}$$

$$2^8 - 37 = 219$$

posibles combinaciones de 3 unos

Ej: Cartas

- 52 cartas en una baraja.

a) ¿Cuántas manos diferentes existen?

- 4 palos diferentes:

$$C(52,5) = 2,598,960$$



- Denominaciones:

A, 2-10, J, Q, K

b) ¿Cuántas manos de póker contiene sólo corazones?

$$C(13,5) = 1,287$$

c) ¿Cuántas manos de póker contienen al menos un corazón?

complemento sin corazones:

$$\text{sin corazón} = C(39,5) = 575,757$$

$$C(52,5) - C(39,5) = 2,023,255$$

d) opcional  
los números para sacar cada denominación:

$$\left. \begin{array}{l} \text{descontar: A, J, Q, K} \\ \text{descontar: 3, 5, 7, 9} \end{array} \right\} 13 - 8 = 5$$

$$C(20,5) = 15,504$$

# Capítulo 13

Clase del Día: 2019-09-02; Permutaciones  
y combinatoria generalizada

- Remover el factor de repetición:

ahora sí puedo repetir

(todos distintos)

- Dado un conjunto de  $n$  elementos, la selección ordenada de  $r$  de ellos con repetición puede hacerse de:

$$n \cdot n \cdot n \cdot n \cdot \dots \cdot n = n^r$$

- Ej. el número de cadenas binarias de  $K$  bits es:

El conjunto de opciones para cadenas binarias es  $\{0,1\}$

- Seleccionamos ordenadamente  $K$  opciones  $\underline{2^K}$

- Cuantas permutaciones de la palabra ball en inglés hay.

\* Toma la premisa de tener todos diferentes, las letras L aparece 2 veces, son indistinguibles, es decir

$$B \cdot A \cdot L_1 \cdot L_2 = B \cdot A \cdot L_2 \cdot L_1$$

- ① Contar todos como si todos los objetos fueran distintos.

$$P(4,4) = 4!$$

- ② Descontamos las permutaciones de L:

$$P(2,2) = 2!$$

En total  $(4!) - 2!$ :

$$\frac{4!}{2!} = 12 \text{ palabras distintas}$$

Ej: Permutaciones de la palabra:

PATATA

1) Todas distintas:

$$P(6,6) = 6! = 720$$

2) descontamos:

2.1) 3 letras A:  $P(3,3) = 3!$

2.2) 2 letras T:  $P(2,2) = 2!$

En total hay:

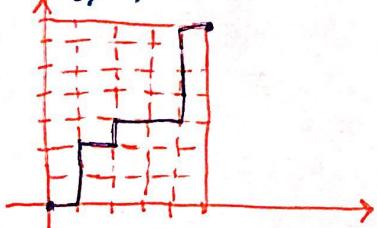
$$\frac{6!}{3! \cdot 2!} = 60 \text{ palabras distintas}$$

En general: de un conjunto de  $n$  elementos de los cuales hay  $n_1$  elementos tipo 1,  $n_2$  elementos tipo 2, ...,  $n_k$  elementos tipo K. Podemos de este conjunto elegir de forma ordenada. (permutación):

$$\frac{n!}{n_1! \cdot n_2! \cdot \dots \cdot n_k!}$$

Ej: Cuantos posibles caminos hay desde el punto (0,0) hasta el punto (5;7), si los únicos movimientos permitidos son 1 unidad a la derecha o 1 unidad hacia arriba?

ejemplo



- El camino de operaciones:

$\{R, U\}$

↑      ↑  
arriba  
derecha

- Un camino desde  $(0,0)$  hasta  $(5,7)$  incluye 12 movimientos:

5. a la derecha y

7 hacia arriba

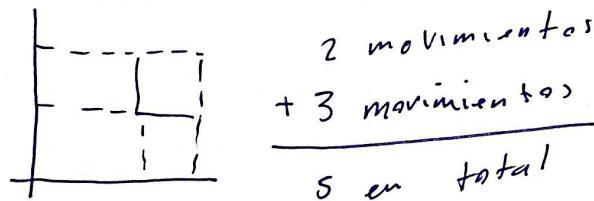
- Por ejemplo, la ruta del dibujo es:

R U U R U R R U U U U R  
 1 2 3 4 5 6 7 8 9 10 11 12

una palabra de tamaño 12 con 5 R's indistinguibles y  
 7 U's indistinguibles:

$$\frac{12!}{5! 7!} = 792$$

- Variante Comenzamos en  $(3,4)$



R U U R U  
 1 2 3 4 5

$$\frac{5!}{2! 3!} = 10 \text{ rutas}$$

Variante 2: Cuántos caminos hay de  $(0,0)$  a  $(5,7)$  que no pasan por  $(3,4)$

$$\frac{7!}{5!} \cdot \frac{9!}{10} = 782$$

$$\frac{7!}{5!} = \frac{7 \cdot 6 \cdot 5!}{5!} = 42$$

$$\frac{9!}{10} = \frac{9 \cdot 8 \cdot 7 \cdot 6 \cdot 5!}{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5!} = 36$$

### ▲ Permutaciones y combinaciones generalizadas:

Una tienda de donas tiene cinco sabores diferentes de donas: cuántas opciones diferentes tenemos para elegir 6 donas?

- glaseada
- chocolate
- crema bararia
- café
- maple

\*Consideraciones:

- selección no ordenada
- podemos repetir un sabor.

La estrategia es asociar este problema como una conocida, el de las cadenas binarias.

5 sabores 4 separadores

	*	*	*	*
G	CH	CB	C	M

Analogía: cadenas binarias

# Capítulo 14

Clase del Día: 2019-09-16; Teoría de números, teorema de euclides, teorema fundamental de la aritmética, interesante: numeros primos,  $\text{mcd}(a,b)$

## Teoría de Números

orientada a C.S.

- def. el estudio de los enteros y sus propiedades

- def. divisibilidad: dados dos enteros  $a, b$  decimos " $a$ " divide a " $b$ " ( $a \mid b$ ), si existe un entero  $q$  tal que:

$$b = a \cdot q$$

! entendemos a la división como restas sucesivas

$$b - aq = 0$$

$$b - \underbrace{a - a - \dots - a}_{q \text{ veces}} = 0$$

a " $b$ " le quito " $q$ " veces " $a$ " hasta llegar a  $0$ , si no es exacto y hay un residuo

- cuando no termina en  $0$ :

$b - qa = \underbrace{r}_{r > 0}$  } se le conoce como "algoritmo de la división de Euclides"

∴  $b$  se puede escribir como:

Indefinición  
 $b = \square \cdot 0 + 0$

$b = r + qa$ , donde " $q$ " y " $r$ " son únicos y  $0 \leq r < a$

! Cuando  $r \neq 0$ , decimos " $a$ " no divide a " $b$ " o ( $a \nmid b$ )

Def: Número Primo: un número entero positivo que tiene exactamente dos divisores.

- alterna: número que solo se divide por 1 o por sí misma

$$\text{ID Primos} = \{1, \infty\}$$

$$\text{ID Compuesto} = \{1, \infty\}$$

■ Los divisores tienen que ser distintos.

- UNO es un compuesto

- un número compuesto tiene más de dos divisores

- Los números primos son la clave de la criptografía.

### ▲ Teorema de Euclides:

“Hay infinitos números primos”

### ▲ Teorema fundamental de la aritmética:

“un número entero es primo o es un producto de potencias de números primos” • inducción fuerte

Ej:

31 es primo,

$\sqrt{31} \approx 5$  par de 1 - 5

$$2 \nmid 31 ; 3 \nmid 31 ; 5 \nmid 31$$

$$72 = 2^3 \cdot 3^2$$

▲ Def. El máximo común divisor: dados dos enteros positivos “a” & “b”, si existe un entero positivo “c” que cumple ambas:

1)  $(c | a) \wedge (c | b)$  2) cualquier otro divisor de “a” y “b”, d cumple:  $(d | c)$  propiedad del

Entonces,  $c$  es el <sup>63</sup>máximo común divisor de a y b

escrito ( $mcd$ ) de ( $a, b$ )

$$mcd(a, b) = c$$

Ej el ejemplo de la mis o profe:

$$\begin{array}{r|l} 48 & 2 \\ 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array}$$

$$\begin{array}{r|l} 84 & 2 \\ 42 & 2 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array}$$

$$mcd(2, 2, 3) = 12$$

# Capítulo 15

Clase del Día: 2019-09-18; Continuación,  
refutación del método  $\text{mcd}(a,b)$  de la mis,  
mínimo común multiplo ( $\text{mcm}(a,b)$ ),

## Continuación

$$\begin{array}{c|c} 48 & 2 \\ 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array}$$

$$\begin{array}{c|c} 84 & 2 \\ 42 & 2 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array}$$

$$48 = 2^4 \cdot 3 \quad 84 = 2^2 \cdot 3 \cdot 7$$

$$\text{mcd}(48, 84) = 2^2 \cdot 3 = 12$$

Observación: Dados  $a, b \in \mathbb{Z}^+$ , tenemos (por TFA):

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \& \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r}$$

Entonces,

$$\text{mcd}(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdot p_2^{\{\alpha_2, \beta_2\}} \cdots p_r^{\{\alpha_r, \beta_r\}}$$

Este procedimiento es muy complicado los números son grandes:

$$\text{mcd}(4517, 8633)$$

Para ello usaremos un método llamado "el algoritmo euclídeo", el cual está basado en la siguiente observación

Dados dos enteros  $a, b \in \mathbb{Z}^+$ , el algoritmo de la división de euclídeo dice que:

$$a = q \cdot b + r, \quad 0 \leq r \leq b$$

Resulta que se cumple lo siguiente:

$$\text{mcd}(a, b) = \text{mcd}(b, r)$$

Ej:

$$\frac{8}{a} = \frac{1 \cdot 6}{q} + \frac{2}{r}$$

$$\frac{b}{a} = \frac{3 \cdot 2}{q} + \frac{0}{r}$$

$$\text{mcd} \left( \frac{8}{a}, \frac{6}{b} \right) = \text{mcd} \left( \frac{\frac{a}{q} \cdot b}{b}, \frac{6}{b} \right) = \text{mcd} \left( \frac{2}{b}, 0 \right) = 2$$

forma

$$\text{mcd} \left( \boxed{\text{algo}}, 0 \right)$$

"algo" es

Ojo siempre  $b$  es más grande

$$\frac{b}{a} = q \cdot a + r$$



Ej: Calcular el  $\text{mcd}(4517, 8633) \equiv \text{mcd}(8633, 4517)$

$$8633 = 1 \cdot 4517 + 4116$$

$$\Rightarrow \text{mcd}(4517, 4116)$$

$$\Rightarrow \text{mcd}(9, 5)$$

$$9 = 1 \cdot 5 + 2$$

$$4517 = 1 \cdot 4116 + 401$$

$$\Rightarrow \text{mcd}(5, 2)$$

$$5 = 2 \cdot 2 + 1$$

$$\Rightarrow \text{mcd}(4116, 401)$$

$$\Rightarrow \text{mcd}(2, 1)$$

$$2 = 1 \cdot 1 + 1$$

$$4116 = 10 \cdot 401 + 106$$

$$\Rightarrow \text{mcd}(1, 1)$$

$$1 = 1 \cdot 1 + 0$$

$$\Rightarrow \text{mcd}(401, 106)$$

$$\Rightarrow \text{mcd}(1, 0)$$

HALT

$$\Rightarrow \text{mcd}(83, 23)$$

$$83 = 3 \cdot 23 + 14$$

$$\Rightarrow \text{mcd}(23, 14)$$

$$23 = 1 \cdot 14 + 9$$

$$\Rightarrow \text{mcd}(14, 9)$$

$$14 = 1 \cdot 9 + 5$$

! Cuando  $\text{mcd}(a, b) = 1$  decimos que  $a$  y  $b$  son primos relativos (coprimos). Por ejemplo:

$$a = 14, \quad b = 15$$

$$\text{mcd}(14, 15)$$

$$15 = 1 \cdot 14 + 1$$

$$14 = 1 + 0$$

$$\text{mcd}(1, 0)$$

### Mínimo Común Múltiplo:

Def.  $MCM$  = Dados  $a, b \in \mathbb{Z}^+$ , decimos:

1) " $d$ " es común múltiplo de " $a$ " y " $b$ " si:

$$a | d \quad \& \quad b | d$$

! hay infinitos comunes múltiplos.

2) " $d$ " es el mínimo común múltiplo de " $a$ " y " $b$ " si cualquier otro común múltiplo " $c$ " cumple

$$d | c$$

$$\text{Entonces } d = \text{mcd}(a, b)$$

$$\begin{array}{r|c} 48 & 2 \\ \hline & 2 \\ & 2 \\ & 2 \\ & 3 \end{array}$$

$$\begin{array}{r|c} 84 & 2 \\ \hline & 2 \\ & 3 \\ & 7 \end{array}$$

• de potencia máxima

$$\text{mcm}(84, 48) = 2^4 \cdot 3 \cdot 7$$

Observación: Dados  $a, b \in \mathbb{Z}$ , por TFA:

$$a = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_r^{\alpha_r} \quad \& \quad b = P_1^{\beta_1} P_2^{\beta_2} \dots P_r^{\beta_r}$$

Entonces,

$$\text{mcm}(a, b) = P_1^{\max\{\alpha_1, \beta_1\}} \cdot P_2^{\max\{\alpha_2, \beta_2\}} \cdot \dots \cdot P_r^{\max\{\alpha_r, \beta_r\}}$$

!  $\text{mcm}(a, b) \mid \text{cd}(a, b)$

# Capítulo 16

Clase del Día: 2019-09-23; Identidad de  
Bézout

## Identidad de Bézout

Dados  $a, b \in \mathbb{Z}^+$ , existen  $x, y \in \mathbb{Z}$  tales que :

$$\text{mcd}(a, b) = ax + by$$

Ej: Sabemos  $\text{mcd}(5, 3) = 1$ . Por la identidad de Bézout sabemos que existen  $x, y \in \mathbb{Z}$  con :

$$1 = 5x + 3y$$

por ejemplo :  $x = -1 ; y = 2$

$$1 = 5(-1) + 3(2)$$

$$1 = 5(-1+3) + 3(2-5)$$

$$1 = 5(-1) + 5 \cdot 3 + 3 \cdot 2 - 3 \cdot 5$$

$$1 = 5(-1+6) + 3(2-10)$$

$$1 = 5(-1) + 5 \cdot 6 + 3 \cdot 2 - 3 \cdot 10$$

- ! • Bézout dice que existen  $x, y \in \mathbb{Z}$ , pero no dice cómo encontrarlos.
- De hecho los números  $x, y \in \mathbb{Z}$ , no son únicos.

Ej: El algoritmo de Euclides extendido :

$$a = 328 \quad b = 500$$

$$\text{mcd}(500, 328)$$

Por Bézout, sabemos que existen  $x, y \in \mathbb{Z}$  tales que :

• agarramos la última ecuación con residuo  $\text{mcd}(172; 156)$

$$16 = 12 + 4$$

$$172 = 156 + 16 \quad (3) \quad (3)$$

$$16 - 12 = 4$$

$$\text{mcd}(156, 16)$$

$$4 = 500x + 328y$$

$$156 = 9 \cdot 16 + 12 \quad (4) \quad (2)$$

∴ ¿Cómo encontramos x e y?

$$\text{mcd}(16, 12)$$

$$16 = 12 + 4 \quad (5) \quad (1)$$

$$\text{mcd}(12, 4)$$

$$12 = 4 \cdot 3 + 0$$

$$\text{mcd}(4, 0)$$

$$16 - 1 \cdot 12 = 4 \quad (1)$$

master

• De la ecuación  $(2)$  despejo el residuo:

$$156 - 9 \cdot 16 = 12 \quad (2)$$

**! no desarrollar las multiplicaciones**

• sustituyo el  $12$  en  $(1)$  y remplazo en la  $(1)$

$$16 - (156 - 9 \cdot 16) = 4$$

master

De la ecuación  $(3)$  despejamos:  $16 = 172 - 156$  sustituimos en master:

$$(3) 172 - 156 = 16$$

$$16 - 156 + 9 \cdot 16 = 4$$

$$10 \cdot 16 - 156 = 4$$

$$10(172 - 156) - 156 = 4$$

(3)  
master

$$(4) 328 - 1 \cdot 172 = 156$$

$$10(172 - 156) - 156 = 4$$

$$(5) 500 - 328 = 172$$

$$10 \cdot 172 - 10 \cdot 156 - 156 = 4$$

$$10 \cdot 172 - 11 \cdot 156 = 4$$

$$10 \cdot 172 - 11 \underbrace{(328 - 172)}_{(4)} = 4$$

$$10 \cdot 172 - 11 \cdot 328 + 11 \cdot 172 = 4$$

$$21 \cdot 172 - 11 \cdot 328 = 4$$

$$21(500 - 328) - 11 \cdot 328 = 4$$

$$21 \cdot 500 - 21 \cdot 328 - 11 \cdot 328 = 4$$

$$21 \cdot 500 - 32 \cdot 328 = 724$$

$$\downarrow \\ 21 \cdot \underbrace{500}_b - 32 \cdot \underbrace{328}_a = 4$$

$$x = 21 \text{ ; } y = 32$$

es una de las infinitas soluciones

Encontramos las demás soluciones tienen la forma siguiente:

$$\begin{aligned} x &= 21 + K_1 \\ y &= -32 - K_2 \end{aligned}$$

Los escogemos de forma inteligente

Recordemos:

$$\text{mcd}(a, b) \cdot \text{mcm}(a \cdot b) = a \cdot b$$

Si escogemos  $K_1 = \frac{328}{4}$        $K_2 = \frac{500}{4}$

master

$$\begin{aligned} 4 &= 500 \cdot \left(21 + \frac{328}{4}\right) + 328 \left(-32 - \frac{500}{4}\right) \\ &= 500 \cdot 21 + \cancel{\frac{500 \cdot 328}{4}} + 328(-32) - \cancel{\frac{328 \cdot 500}{4}} \\ &\quad \text{mcm}(500, 328) \\ &= 500 \cdot 21 + 328(-32) \end{aligned}$$

En general una solución tiene la forma para  $x$ :

$$x = 21 + \frac{328}{4} \cdot K \quad K \in \mathbb{Z}$$

$$y = -32 - \frac{500}{4} K$$

En resumen:

■ Bézout:  $\text{mcd}(a, b) = ax + by$

• Euclides extendido:

Encuentre soluciones  $x = x_0$  &  $y = y_0$

• La solución general:

$$x = x_0 + \frac{b}{\text{mcd}(a, b)} \cdot K$$

donde  $K \in \mathbb{Z}$

$$y = y_0 - \frac{a}{\text{mcd}(a, b)} \cdot K$$

# Capítulo 17

Clase del Día: 2019-09-25; Ecuación Diofantiana

## Ecuación Diofantina

2019-09-25

Def. Ecuación diofantina, una ecuación de la forma:

$$ax + by = c$$

con  $a, b, c \in \mathbb{Z}^+$ , se llama ecuación diofantina.

- Las soluciones  $x, y \in \mathbb{Z}$  pueden, o no existir.

Γ

$$3x + 5y = \underbrace{1}_{\text{mcm}}$$

$$x = 2 \quad \checkmark$$

$$y = -1$$

$$3x + 5y = 2$$

$$x = 4, \quad x = -1$$

$$y = -2, \quad y = 1$$

¿relación?

son el doble

$$3x + 5y = 7$$

$$x = -21$$

$$y = 14$$

son el  
doble

! Esta ecuación tiene solución si y solo si,

$$c = K(\text{mcd}(a, b))$$

# Capítulo 18

Clase del Día: 2019-09-30; Aritmética modular

## Aritmética Modular

Definición: Congruencia módulo  $n$ .

“Dados dos enteros  $a, b$  & un entero positivo  $n$ , decimos que  $a$  &  $b$  son congruentes módulo  $n$ , si es solo si,

$$a \mid (a-b) \quad "$$

Esto lo representamos como:

$$a \equiv b \pmod{n} \quad ó,$$

$$a \equiv_n b$$

■  $n \mid (a-b)$ , quiere decir también que  $a$  &  $b$  tienen el mismo residuo al ser dividido por  $n$ .

Observación:

$$\begin{aligned} a &= q_1 \cdot n + r \\ - b &= q_2 \cdot n + r \\ \hline a - b &= n(q_1 - q_2) + r \xrightarrow{\quad r \neq 0 \quad} \end{aligned}$$

$$\frac{a-b}{n} = (q_1 - q_2) \iff n \mid (a-b)$$

\* Por eso  $n \neq 0$

Ej: El módulo 3.

- Tomemos el conjunto de todos los posibles residuos al dividir un entero por tres:

$$\{0, 1, 2\}$$

- Cada número entero puede relacionarse con uno y solo uno de los enteros en:

$$\{0, 1, 2\}$$

- Por ejemplo: relacionados con el residuo 0 están:

$$\dots -6, -3, 0, 3, 6, \dots$$

Dominio  
 $3\mathbb{Z}$

$\underbrace{-3}_{-3} \quad \underbrace{3}_{3}$   
esto es por el módulo en  
el que estamos trabajando.

- estos son representados por el cero (ya que ese es su residuo al ser divididos por 3).

En otras palabras:

$$0 \equiv_3 \dots, -9, -6, -3, 0, 3, 6, 9$$

- Por otro lado, los que están relacionados con el uno son:

$$1 \equiv_3 \dots -5, -2, 1, 4, 7, 10, \dots$$

Dominio  
 $3\mathbb{Z} + 1$

$\underbrace{-3}_{-3} \quad \underbrace{+3}_{+3}$

■ Finalmente, los que están relacionados con el dos son:

$$2 \equiv_3 \dots -4, -1, 2, 5, 8, 11 \dots \quad 3 \mathbb{Z} + 2$$

$\uparrow$        $\uparrow$        $\uparrow$   
 $-3$        $+3$

∴ Al conjunto de todos los residuos que resultan al dividir por 3, se les llama enteros módulo 3 y se les representa por  $\mathbb{Z}_3$  (se lee "zeta tres")

$$\mathbb{Z}_3 = \{0, 1, 2\}$$

En general:

• Def: Enteros modulo n: Dado n un entero positivo, le llamamos enteros módulo n al conjunto de residuos posibles al dividir un entero por n; se le representa como  $\mathbb{Z}_n$ .

$$\mathbb{Z}_n = \{0, 1, 2, \dots, (n-1)\}$$

"uno es el regalado por que"

$$\mathbb{Z}_1 = \{0\}$$

1

Ej: ¿Quién es 117 en  $\mathbb{Z}_6$ ?

Queremos r en la ecuación:

$$117 = \square 6 + r$$

$$\left[ \frac{117}{6} \right] \approx 19$$

$$r = 117 - 19 \cdot 6 = 3, \text{ en conclusión } 117 \equiv_6 3$$

# Capítulo 19

Clase del Día: 2019-10-07 ; Continuación  
de aritmética modular

## Aritmética Modular (Continuación)

2019-10-07

- Para sacar ventaja de las propiedades de los enteros módulo  $n$  ( $\mathbb{Z}_n$ ) es necesario redefinir las operaciones de suma & multiplicación:
- Dados  $a, b \in \mathbb{Z}_n$ , La suma módulo n se define de la siguiente manera.

Aritmética Modular  $\equiv$  Aritmética de residuos

$$a +_n b \equiv (a+b) \pmod{n}$$

Ej:  $a = 11$      $b = 7$     &  $n = 5$

$$\begin{array}{c} \text{Residuo de} \\ \cancel{11} \cancel{\& 5} \\ 11 +_5 7 \equiv 1 \cancel{+}_5 2 \equiv 3 \end{array}$$

Residuo de  
 $\cancel{7} \cancel{\& 5}$

Esto equivale a:

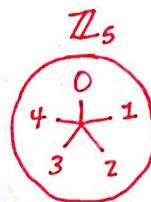
$$\underbrace{(11 + 7)}_{\text{La suma habitual}} = 18 \equiv_5 3$$

de enteros.

Ej:  $a = 11, b = 9, n = 5$

$$11 +_5 9 \equiv_5 1 +_5 4 \equiv_5 0$$

$\frac{5}{5} = 1 + 0$



$$(11 + 9) = 20 \equiv_5 0$$

$\frac{20}{5} = 4 + 0$

De forma similar se define la multiplicación módulo n:

$$a \cdot_n b = (a \cdot b) (\bmod n)$$

### Caesar's shift:

- Un sistema criptográfico cuyo funcionamiento fue entenderse usando aritmética modular.

Cripto - grafia  
oculta escritura  
criptología

- Requiere identificar cada letra del abecedario con uno y sólo uno de los enteros módulo n. En este ejemplo usaremos mod 26 para tener 26 letras. Por ejemplo:

$$\begin{aligned} A &\rightarrow 0 \\ B &\rightarrow 1 \\ C &\rightarrow 2 \\ &\vdots \\ Z &\rightarrow 25 \end{aligned}$$

} diccionario

Asociada al sistema criptográfico existe dos funciones:

1) Función encriptación: *Caesar's shift*:

$$E(x) = x + \underbrace{d}_{\text{shift}}$$

... en donde  $d \in \mathbb{Z}_{26}$

Por ejemplo, si  $d \equiv_{26} 3$

A, B, C, ..., Y, Z  
↓ ↓ ↓      ↓ ↓  
0 1 2      24 25

E(x)						
3	4	5	...	1	2	
↓	↓	↓		↓	↓	
D	E	F	...	B	C	

Ej: Para encryptar el mensaje: CAZ usando  $\mathbb{Z}$

C	A	Z
2	0	26

E(x)		
6	4	3
G	E	D

Enviamos el mensaje GED:

Función decriptación:

$$D(x) = x - d$$

G	E	D
6	4	3

D(x)		
2	0	25
C	A	Z

### Observaciones finales:

- Ventaja: implementación es simple.
- Desventaja: susceptible al análisis de frecuencias; siempre se repite la misma letra.

# Capítulo 20

Clase del Día: 2019-10-09 ; Cálculo de inversos multiplicativos módulo  $n$

## Cálculo de inversos multiplicativos módulo n

Def: neutro multiplicativo: dado un elemento  $\hat{e} \in \mathbb{Z}_n$ , este se llama neutro multiplicativo si cumple:

$$a \cdot \hat{e} = a$$

para todo  $a \in \mathbb{Z}_n$

! Siempre en  $\mathbb{Z}_n$ , el neutro es 1.

Observación = existe un "neutro aditivo que es el 0."

■ Por ejemplo, redefinimos  $\circ$ :

! Filosofía

$$a \circ b \rightarrow a^b$$

$$2 \circ 3 \rightarrow 2^3 \rightarrow 8$$

$$a \circ b \rightarrow a^b \rightarrow a$$

en neutro es 1

$$a \Delta b \rightarrow b - a$$

$$2 \Delta 3 \rightarrow 3 - 2 \rightarrow 1$$

$$a \Delta \hat{e} \rightarrow \hat{e} - a \rightarrow a$$

$$a \oplus b \rightarrow a^2 - 2ab + b^2$$

$$a \oplus b \equiv a^2 - 2a\hat{e} + \hat{e}^2 \equiv a$$

el  $\Delta$  &  $\circ$  son operaciones inventadas

Def de "inverso multiplicativo", Un elemento  $b \in \mathbb{Z}_n$ , se llama inverso multiplicativo de  $a \in \mathbb{Z}$  si se cumple:

$$a \cdot b \equiv_{\mathbb{Z}_n} 1$$

el neutro multiplicativo

! En este caso  $a$  &  $b$  son inversos multiplicativos entre sí.

! Notación:  $b \equiv a^{-1}$

Observación:

$$2x \equiv 7 \pmod{11} \Rightarrow$$

$$2x \equiv 7 + 11 \equiv 18$$

$$\begin{array}{c} \downarrow \\ \rightarrow q \end{array}$$

$$E(x) = x + d \quad x = q$$

$$E(x) = m \cdot x + d$$

Ej: Encuentre el inverso de  $a$  módulo  $n$ .

a)  $n = 5$  &  $a = 2$

$$a^{-1} \equiv 3 \text{ ya que:}$$

$$a \cdot a^{-1} = 2 \cdot 3 \equiv_5 1$$

b)  $n = 7$  &  $a = 6$

$$a^{-1} \equiv 6 \text{ ya que:}$$

$$a \cdot a^{-1} = 6 \cdot 6 \equiv_7 1$$

c)  $n = 23$  &  $a = 17$

$$a^{-1} \equiv_{23} 19 \quad \text{mod}(23)$$

$$a \cdot a^{-1} \equiv 17 \cdot 19 = 323 \equiv_{23} 1$$

Un número va a tener inverso si son primos relativos.

El 0 & el 1 no son respuesta.

1 A veces la inversa multiplicativa no existe.

• Si elijo mal "m" no puedo desencriptar.

(1)  $6x = 5 \rightarrow x = \frac{5}{6}$

"pasar a dividir el 6"

$$\frac{1}{6}6x = 5 \cdot \frac{1}{6}$$

$$x = \frac{5}{6}$$

"multiplicamos por el inverso multiplicativo de 6")

# Capítulo 21

Clase del Día: 2019-10-09 ; 2019-10-16

## Continuación encryptación

$$E(x) = 3x + 5$$

A T T A C K

0	19	19	0	2	10
$E(x)$					
5	19	10	5	11	9

↓ ↓ ↓ ↓ ↓

...

Entonces:

$$\begin{aligned} D(x) &= (x - 5) \cdot 9 \\ &= 9x - 9 \cdot 5 \\ &= 9x - 45 \\ &\xrightarrow{\mathbb{Z}_{26}} 9x + 7 \end{aligned}$$

F	K	K	F	L	J
S	10	10	5	11	9
$D(x)$					
0	19	19	0	2	10

↓ ↓ ↓ ↓ ↓

A T T A C K

*n*-grama

■ telegrama de mexico.

Definimos la función de desencriptado  $D(x)$  como:

$$D(x) = (x - 5) \cdot 3^{-1}$$

Buscamos  $3^{-1}$  en  $\mathbb{Z}_{26}$ :

# Procedimiento:

$$a = 3 \quad n = 26$$

$$\text{mcd}(26, 3)$$

$$26 = 3 \cdot 8 + 2$$

$$\text{mcd}(3, 2)$$

$$3 = 2 \cdot 1 + 1$$

$$\text{mcd}(2, 1)$$

$$2 = 1 \cdot 2 + 0$$

# Bézout:

$$3 - 2 \cdot 1 = 1$$

$$3 - (26 - 3 \cdot 8) \cdot 1 = 1$$

$$3 - 26 - 8 \cdot 3 = 1$$

$$-26 + 9 \cdot 3 = 1$$

$$1 \equiv_{26} 9 \cdot 3$$

$$\therefore 3^{-1} \equiv_{26} 9$$

...

Resumen: Estos son códigos tipo césar (shift & ponderado) son sistemas criptográficos de sustitución; un carácter  $x$  siempre será sustituido por un mismo carácter  $y$ .

Esto representa la principal debilidad de dicho sistema, pues es altamente vulnerable a un ataque por análisis de frecuencia.

En el ataque por fuerza bruta:

C. Shift  $E(x) = x + d$

Diccionario  $26!$  y por la "d"  $26 \cdot 26!$

C. Ponderado  $E(x) = kx + d$

Diccionario  $26!$  y contando  $k$  solo puede tener

$k: 26 - 1 - 1 - \text{floor}(\frac{25}{2}) = 12$  en total  $12 \cdot 26 \cdot 26!$

Exponenciación modular: es hacer cálculo con números grandes usando aritmética modular; Un algoritmo que permite evaluar de forma eficiente, cantidades como:

$$a^b \bmod(n)$$

Ej: Calcule  $2^{100} \bmod(91)$

Primero escribimos el exponente en binario

$$100_2 = 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0$$
$$\quad \quad \quad 2^6 \ 2^5 \ 2^4 \ 2^3 \ 2^2 \ 2^1 \ 2^0$$

$$\begin{array}{r} 100 \\ - 2^6 \\ \hline 36 \\ - 2^5 \\ \hline 4 \\ - 2^2 \\ \hline 0 \end{array}$$

$$100 = 2^6 + 2^5 + 2^2$$

...

... Queremos calcular  $2^{100}$ :

$$2^{2^6 + 2^5 + 2^4} = 2^{2^6} \cdot 2^{2^5} \cdot 2^{2^4}$$

Bits	$a^{2^n}$	$a^{2^{n+1}} \bmod(n)$
lsb 0	2	4
0	4	16
* → 1	16	$256 \equiv_{q_1} 74$
0	74	$5476 \equiv_{q_1} 16$
0	16	$256 \equiv_{q_2} 74$
* → 1	74	$5476 \equiv_{q_1} 16$
* → msb 1	16	$256 \equiv_{q_2} 74$

... me voy a quedar sólo con los unos

$$\text{finalmente, } 2^{100} = 2^{2^6} \cdot 2^{2^5} \cdot 2^{2^4} \xrightarrow{\mathbb{Z}_{q_1}} \overline{16} \cdot \overline{74} \cdot \overline{16}$$

$$\equiv_{q_1} 16^2 \cdot 74 \equiv_{q_1} 74 \cdot 74$$

$$\equiv_{q_1} \underline{16}$$

# Capítulo 22

Clase del Día: 2019-10-09 ; Cálculo de inversos

## Cálculo de inversos multiplicativos de módulo n

Dado  $a \in \mathbb{Z}$ ,  $n \geq 2$ , buscamos un entero  $a^{-1} \in \mathbb{Z}_n$  que satisface:

$$a \cdot a^{-1} \equiv_n 1$$

Consideremos nuevamente el ejemplo

$$a = 17 \quad \& \quad n = 23$$

$$a \cdot a^{-1} = q_1 \cdot n + 1$$

$$\underbrace{a \cdot a^{-1}}_{\text{conocido}} - \underbrace{q_1 \cdot n}_{\text{conocido}} = 1$$

en términos conocidos:

$$a^{-1} \equiv x \quad q_1 \equiv y$$

$$\underbrace{a \cdot x - y \cdot n}_{\text{identidad de Bézout.}} = 1$$

① Primero calculamos  $\text{mcd}(23, 17)$ :

$$23 = 1 \cdot 17 + 6$$

$$17 = 2 \cdot 6 + 5$$

$$6 = 1 \cdot 5 + 1$$

$$5 = 5 \cdot 1 + 0$$

$$\text{mcd}(23, 17) = 1$$

coprimos

Observación: para que la inversa exista se tiene que trabajar con co-primos.

② Luego resolvemos Bézout:

$$\begin{array}{rcl} 6 - 5 & = 1 \\ 17 - 2 \cdot 6 & = 5 \end{array}$$

$$\begin{array}{rcl} 6 - (17 - 2 \cdot 6) & = 1 \\ 3 \cdot 6 - 17 & = 1 \end{array}$$

$$3(23 - 17) - 17 = 1$$

$$3 \cdot 23 - 4 \cdot 17 = 1$$

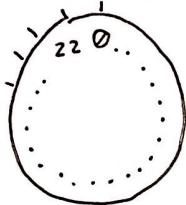
Entonces ...

$$3 \cdot 23 - 4 \cdot 17 = 1$$

$\mathbb{Z}_{23}$

$$\begin{array}{c}
 3 \cdot 23 - 4 \cdot 17 = 1 \\
 \text{+ traducir todo a mod}_{23} \\
 3 \cdot 0 - 19 \cdot 17 = 1
 \end{array}$$

$$19 \cdot 17 \equiv_{23} 1$$



En conclusión, el inverso multiplicativo de  
17 en  $\mathbb{Z}_{23}$  = 19.

Ej:  $n = 28$  &  $a = 5$

$$\text{mcd}(28, 5)$$

$$28 = 5 \cdot 5 + 3$$

$$\text{mcd}(5, 3)$$

$$5 = 3 \cdot 1 + 2$$

$$\text{mcd}(3, 2)$$

$$3 = 2 \cdot 1 + 1$$

$$\text{mcd}(2, 1)$$

$$2 = 2 \cdot 1 + 0$$

$$3 - 2 \cdot 1 = 1$$

$$5 - 3 \cdot 1 = 2 \quad ; \quad 28 - 5 \cdot 5 = 3$$

$$3 - (5 - 3) \cdot 1 = 1$$

$$3 - 5 + 3 = 1$$

$$2 \cdot 3 - 5 = 1$$

$$2(28 - 5 \cdot 5) - 5 = 1$$

$$2 \cdot 28 - 10 \cdot 5 - 5 = 1$$

$$2 \cdot 28 - 11 \cdot 5 = 1$$

$$\underline{\hspace{10em}} \mathbb{Z}_{28}$$

$$\begin{array}{r} 2 \cdot 28 - 11 \cdot 5 = 1 \\ \hline 2 \cdot \cancel{0} \quad 17 \cdot 5 \equiv_3 1 \end{array}$$

El inverso multiplicativo de 5 en  $\mathbb{Z}_{28}$   
es 17.

Vemos que en ambos casos, a & n son primos relativos:

$$\text{mcd}(n, a) = 1$$

Entonces podemos concluir que:

- ! a  $\in \mathbb{Z}_n$  tiene inverso módulo n, si y solo si, el máximo común divisor de a y n es 1.

Ej: Cifrado Cesar ponderado:

Def: Definimos un diccionario:

$$\begin{matrix} A, B, C, D \dots, X, Y, Z \\ \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\ 0 \quad 1 \quad 2 \quad 3 \quad 23 \quad 24 \quad 25 \end{matrix}$$

mod 26 ya que estamos trabajando con 26 caracteres.

Función de encriptación:

$$E(x) = k \cdot x + d$$

Por ejemplo  $K=3$  &  $d=5$

$$m = \begin{matrix} A & T & T & A & C & K \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \end{matrix}$$

$$\boxed{E(x)}$$
$$\begin{matrix} 5 & 10 & 10 & 5 & 11 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \end{matrix}$$

$$c = F \ K K F L J$$

Función de desencriptación:

$$D(x) = (x - d) \cdot K^{-1}$$

# Capítulo 23

Clase del día: 2019-10-30 ; Cifrado Vigénirer

## Cifrado Vigenère

2019-10-30

Un sistema criptográfico polialfabético.

Def polialfabético: para cada letra se usa un alfabeto diferente.

Sistema criptográfico:

- Un diccionario:  $\sum'$
- Una clave: AGUACATE
- Un mensaje:

COMER FIAMBRE SIN JAMÓN  
AGUACATE AGUA CAT EAGUA

■ tabula recta:

	A	B	C	D	...	Z	Mensaje
A							
B							
C							
:							
Z							

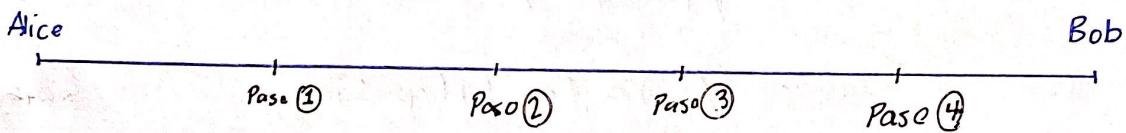
Clave

# Capítulo 24

Clase del día: 2019-11-06 ; RSA, teoría

## Systema criptográfico RSA:

- Inventado en 1978
- Mas ampliamente utilizado
- Rivest, Shamir, Adleman



Paso 1: Generación de llaves

Paso 2: Distribución

Paso 3: Encriptación

Paso 4: Desencriptación

### Generación de la llave:

- Elegimos dos números primos  $p$  &  $q$ .  
# Estos los elige Alice, solo ella lo sabe.
- Se mantienen en secreto. # Eligen numeros de 1024 bits.
- Calculamos:  $n = p \cdot q$  (parte de la clave)
- Encontrar  $p$  &  $q$  a partir de  $n$  es computacionalmente inviolable.

■ Calculamos  $\phi(n) = (p-1)(q-1)$

toiente de Euler

[1]

[1] devuelve el número de primos relativos con  $n$  menores que  $n$ .

$$\{1, 2, 3, 4\}$$

$$\phi(5) = 4$$

$$\phi(11) = 10$$

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

$$\therefore \phi(n) = (p-1)(q-1)$$

Elegimos un entero  $e$ :

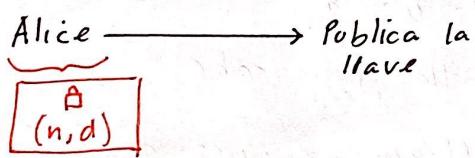
$$1) e < \phi(n)$$

#  $e$  &  $n$  es la llave pública.

$$2) \text{mcd}(e, \phi(n)) = 1$$

• La clave pública  $(n, e)$  . Calculamos otro entero  $d$ :

$$e \cdot d \equiv 1 \pmod{\phi(n)}$$



! "d" es el inverso multiplicativo de  $e \cdot \text{mod}(\phi(n))$ .  
• Clave privada  $(n, d)$ .

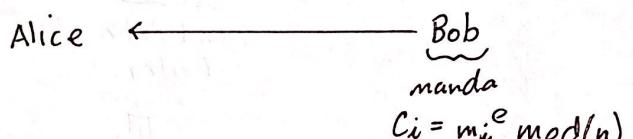
### Encryptación:

$$\underbrace{M}_{\text{mensaje}} = m_1, m_2, m_3, m_4, \dots, m_K$$

Calcula (Bob):

$$c_i = (m_i)^e \pmod{n}$$

$$\underbrace{C = c_1, c_2, c_3, \dots, c_K}_{\text{Mensaje encriptado}}$$



## Desencripta:

$$C = c_1 c_2 c_3 \dots c_k$$

# Calculamos (Alice):

$$m_i = (c_i)^d \bmod(n)$$

$$M = m_1 m_2 m_3 \dots m_k$$

$$\# ed \equiv 1 \pmod{\phi(n)} \rightarrow ed \equiv 1 \pmod{n}$$

■ Dado un diccionario:

$$\Sigma = (0: \text{L}, 1: \text{A}, 2: \text{B} \dots 27: \text{Z})$$

- Si el mensaje  $M$  se descompone en monograma (letra por letra) se escogen "p" y "q" de modo que  $n = p \cdot q$  sea mayor que el monograma más grande en  $\Sigma$ .
- Si son bigramas  $m_1 m_2$  (letras de dos en dos)

Z A N A H O R I A  
 ↓  
 2701

# El bigrama más grande será 2727.

# Capítulo 25

Clase del día: 2019-11-11 ; RSA, ejemplo

## Ejemplo: RSA

① Llaves:

$$\Sigma = (0:\square, 1:A, 2:B, \dots, 26:Z)$$

Monogramas  $\rightarrow$  máx. 26

Elegimos  $p$  y  $q$ , tal que  $n=p \cdot q > 26$ :

$$p=5 \quad y \quad q=7$$

$$\text{Calculamos: } \phi(35) = (5-1)(7-1) = 24$$

Elegimos un  $e$ , tal que:

$$1) \quad e < \phi(n)$$

$$2) \quad \text{mcd}(e, \phi(n)) = 1$$

Por ejemplo,  $e=11 \rightarrow (11, 35)$

public key

Calculamos  $d$ , tal que:

$$e \cdot d \equiv 1 \pmod{\phi(n)}$$

$$11d \equiv 1 \pmod{24}$$

$$\therefore d \equiv 11 \pmod{24} \rightarrow (11, 35)$$

private key

③ Encriptación: Bob

Mensaje  $M = \text{HIDE}$   
 $\underline{08} \underline{09} \underline{04} \underline{05}$

$$c_i = m_i^e \pmod{n}$$

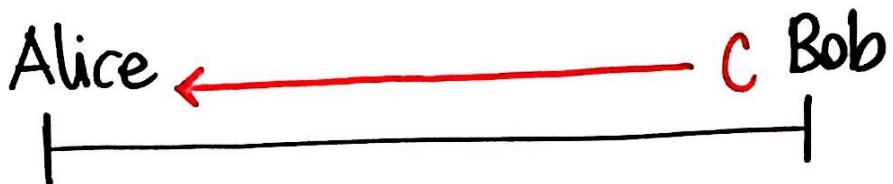
$$H: 08^{11} \pmod{35} \equiv_{35} 22$$

$$I: 09^{11} \pmod{35} \equiv_{35} 04$$

$$D: 04^{11} \pmod{35} \equiv_{35} 09$$

$$E: 05^{11} \pmod{35} \equiv_{35} 10$$

Cipher:  $C = 2204 \quad 0910$



④ Desencriptar: Alice

Cipher:  $C = 2204 \quad 0910$

$$m_i = c_i^d \pmod{n}$$

$$22 : 22^{11} \pmod{35} \equiv_{35} 08 \rightarrow H$$

$$04 : 04^{11} \pmod{35} \equiv_{35} 09 \rightarrow I$$

$$09 : 09^{11} \pmod{35} \equiv_{35} 04 \rightarrow D$$

$$10 : 10^{11} \pmod{35} \equiv_{35} 05 \rightarrow E$$

① Bigramas  $\longrightarrow$  máx. 2626

$$p = 53 \quad y \quad q = 89$$

$$\begin{aligned} \text{Calculo } \phi(4717) &= (53-1) \cdot (89-1) \\ &= 4576 \end{aligned}$$

Elijo  $e$ , tal que:

$$1) \quad e < 4576$$

$$2) \quad \text{mcd}(e, 4576) = 1$$

$$e = 3041 \longrightarrow (3041, 4717)$$

public key

Calculo  $d$ :

$$3041d \equiv 1 \pmod{4576}$$

$$d = 2209 \longrightarrow (2209, 4717)$$

private key

③  $M = \underline{\text{PIZZAS}}$

$$P1 : 1609^{3041} \pmod{4717} \equiv 0993$$

$$Z2 : 2626^{3041} \pmod{4717} \equiv 0064$$

$$AS : 0119^{3041} \pmod{4717} \equiv 0738$$

Cipher:  $C = 099300640738$

④ Cipher:  $C = \underline{\underline{0993}} \underline{\underline{0064}} \underline{\underline{0738}}$

$$0993 : 993^{2209} \pmod{4717} \equiv 1609 \rightarrow P1$$

$$0064 : 64^{2209} \pmod{4717} \equiv 2626 \rightarrow Z2$$

$$0738 : 738^{2209} \pmod{4717} \equiv 0119 \rightarrow AS$$