Matemática Discreta 2

- Presentación del curso:

¿Qué es la matemática discreta?

Idea general: podemos decir que es el área de la matemática que estudia los conjuntos discretos.

Conjunto discreto →
- conjuntos finitos.
- conjuntos numerables (en biyección con los naturales)

MD1

Estudio de los números naturales $\mathbb{N}$ y de procedimientos que dependen de $\mathbb{N}$:

- Inducción
- Conteo
- Grafos

etc

MD2

El conjunto principal a estudiar son los números enteros.

mpenez@fing.edu.uy
sites.google.com/view/mapenez

Algo de notación:

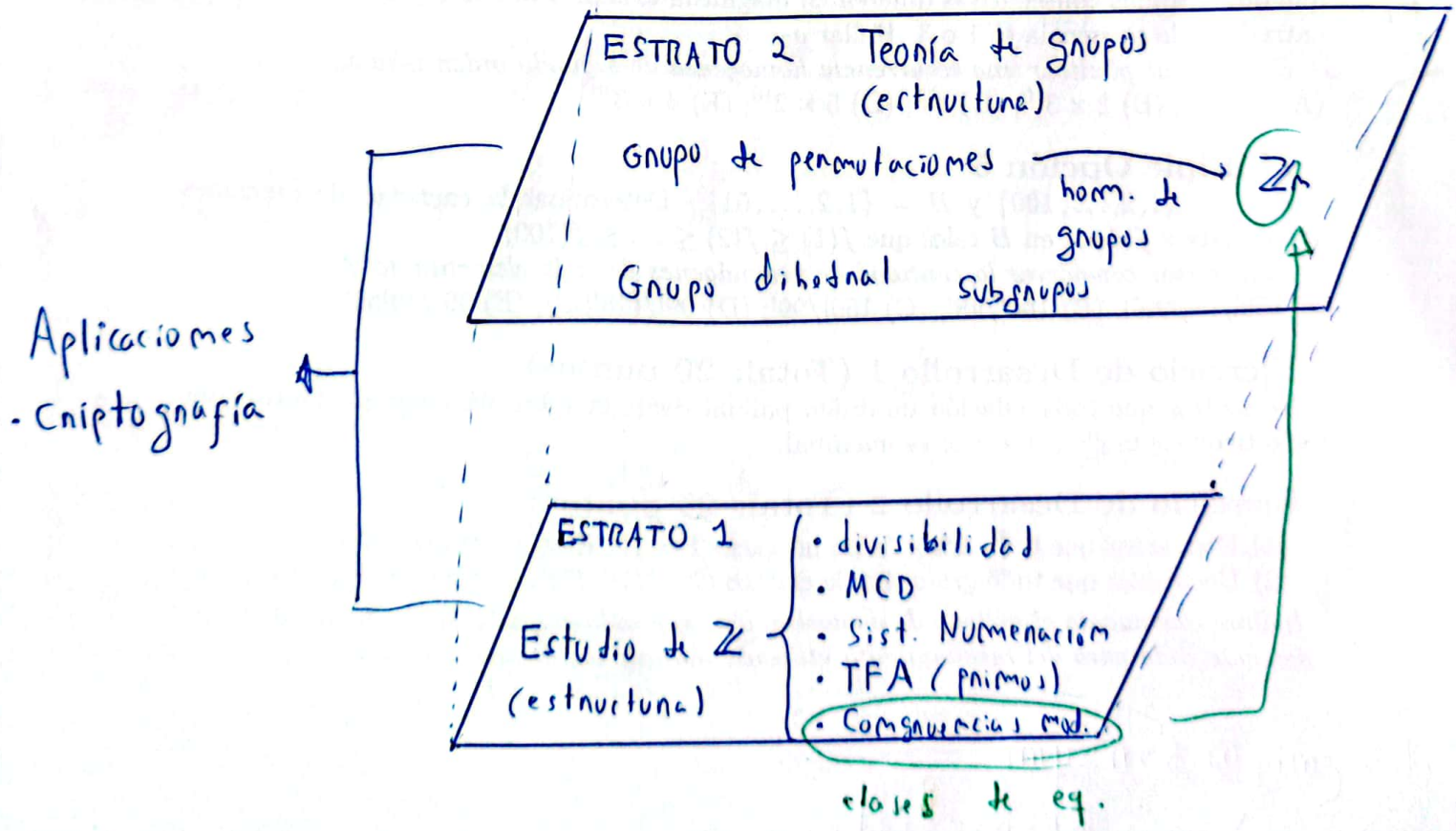
- $\mathbb{N} = \{0, 1, 2, \dots\}$ conjunto de los números naturales

Para propósitos de este curso, el cero es natural.

- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ conjunto de los números enteros

- $\mathbb{Z}^+ = \{z \in \mathbb{Z} : z > 0\} = \{1, 2, 3, \dots\}$

denota el conjunto de los enteros positivos.



- Estructura en $\mathbb{Z}$

$(\mathbb{Z}, +, \cdot)$

- $(\mathbb{Z}, \cdot)$:
  - conmutatividad
  - asociatividad
  - distributividad respecto a $+$
  - neutro ($1 \in \mathbb{Z}$)
- $(\mathbb{Z}, +)$:
  - conmutatividad
  - asociatividad
  - neutro ($0 \in \mathbb{Z}$)
  - opuesto

Si bien no siempre es posible inventar números enteros respecto a la multiplicación (y dentro de $\mathbb{Z}$), sí es posible hablar de división en $\mathbb{Z}$.

Definición: Sean $a, b \in \mathbb{Z}$. Diremos que b divide a a (denotado por $b \mid a$) si existe $q \in \mathbb{Z}$ tal que

$$a = q \cdot b.$$

$a \to$ dividendo $q \to$ cociente

$b \to$ divisor

Ejemplos:

① $a = 16$, $b = 4$

$4 \mid 16$ ya que $16 = 4 \cdot 4$

② $a = -16$, $b = 8$

$8 \mid -16$ ya que $-16 = (-2) \cdot 8$

③ $a = 21$, $b = -3$

$-3 \mid 21$ ya que $21 = (-7) \cdot (-3)$

④ $a = -121$, $b = -11$

$-11 \mid -121$ ya que $-121 = 11 \cdot (-11)$.

Observaciones:

1) b no puede ser cero. Si $a \neq 0$, ya que se tendría $a = q \cdot 0 = 0$.

2) $0 \mid 0$ ya que $0 = q \cdot 0$ para cualquier $q \in \mathbb{Z}$.

3) $b \mid 0$ para todo $b \in \mathbb{Z}$, ya que

$$0 = 0 \cdot b$$

4) Si $0 < a < b$, entonces $b \nmid a$ (b no divide a a).

5) $1 \mid a$ para todo $a \in \mathbb{Z}$, ya que

$$a = a \cdot 1$$

6) $a \mid a$ para todo $a \in \mathbb{Z}$, ya que $a = 1 \cdot a$.

Definición: Si $a \in \mathbb{Z}^+$ y $a \neq 1$, diremos que a es primo si 1 es el único divisor positivo de a menor que a

$$b \mid a \text{ y } a > b > 0 \Longrightarrow b = 1.$$

De lo contrario, diremos que a es compuesto.

Ejemplos:

① 2 es primo (es el único primo par).

Definición: Diremos que $a \in \mathbb{Z}$ es par si $2 \mid a$. De lo contrario, diremos que a es impar.

② Por definición, 1 no es primo.

③ 3, 5, 7, 11, 13, 17, 19, 23 son primos.

④ Primos de Fermat. $F_m = 2^{2^m} + 1$

con $m = 0, 1, 2, 3$ y 4

⑤ Números de Mersenne

$M_p = 2^p - 1$ con p primo.

$M_{82.589.933} = 2^{82.589.933} - 1$ (24.862.048 cifras)

es el primo más grande conocido.

Proposición (propiedades de la divisibilidad):

1) Si $a|b$ y $b|c$, entonces $a|c$ (transitividad).
2) Si $a|b$ y $b|a$, entonces $b = \pm a$.
3) Si $b|a_1$ y $b|a_2$, entonces $b|(m_1 \cdot a_1 + m_2 \cdot a_2)$ para todo $m_1, m_2 \in \mathbb{Z}$.

· Demostración:

1) $a|b \Rightarrow b = q \cdot a$ para algún $q \in \mathbb{Z}$.
$b|c \Rightarrow c = p \cdot b$ para algún $p \in \mathbb{Z}$.
Luego, $c = p \cdot (q \cdot a) = (pq)a$, $pq \in \mathbb{Z}$.
$\therefore a|c$.

2) $a|b \Rightarrow b = q \cdot a$ para algún $q \in \mathbb{Z}$.
$b|a \Rightarrow a = p \cdot b$ para algún $p \in \mathbb{Z}$.
Luego, $b = q(pb) = (qp)b$
$b - (qp)b = 0$
$b(1 - qp) = 0$

→ $b = 0$, en cuyo caso $a = 0$ ya que $a = p \cdot b$.
o
→ $qp = 1$, de donde $q = p = 1$ o $q = p = -1$
$b = 1 \cdot a$ $\quad b = -1 \cdot a$

3) $b \mid a_1 \Rightarrow a_1 = q_1 \cdot b$ para algún $q_1 \in \mathbb{Z}$.

$b \mid a_2 \Rightarrow a_2 = q_2 \cdot b$ para algún $q_2 \in \mathbb{Z}$.

Luego, $m_1 a_1 = (m_1 q_1) b$

$m_2 a_2 = (m_2 q_2) b$

Así, $m_1 a_1 + m_2 a_2 = \underbrace{(m_1 q_1 + m_2 q_2)}_{\in \mathbb{Z}} b$

Por lo tanto, $b \mid (m_1 a_1 + m_2 a_2)$. ∎

¿Qué más podemos decir si $b \nmid a$?

Teorema de la división entera:

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Entonces existen $q \in \mathbb{Z}$ y $r \in \mathbb{Z}$ con $0 \leq r < |b|$, únicos, tales que

$$a = q \cdot b + r.$$

Ejemplos:

1) $a = 13$, $b = 2$

$13 = 6 \cdot 2 + 1$

2) $a = -13$, $b = 2$

$-13 = (-6) \cdot 2 - 1 = (-6) \cdot 2 - 2 + 2 - 1 = (-7) \cdot 2 + 1$

3) $a = 21, \quad b = -5$

$21 = (-4)(-5) + 1$

4) $a = -33, \quad b = -7$

$-33 = 4 \cdot (-7) - 5 = 4 \cdot (-7) - 7 + 7 - 5$

$-33 = 5 \cdot (-7) + 2.$

Observaciones del teorema:

1) ¿Por qué b no puede ser cero?

Se pierde la unicidad de q.

$$a = q \cdot 0 + a, \quad \forall q \in \mathbb{Z}$$

2) Basta probar el resultado para $a \geq 0$ y $b > 0$.

- Caso $a \geq 0$ y $b < 0$:

Usando el teorema para $a \geq 0$ y $-b > 0$, se tiene que existen $q, r \in \mathbb{Z}$ con $0 \leq r < |-b| = |b|$ tales que

$$a = q \cdot (-b) + r$$

$$a = (-q) \cdot b + r. \quad \blacksquare$$

- Caso $a < 0$ y $b > 0$:

Usando el teorema para $-a > 0$ y $b > 0$, se tiene que existen $q, r \in \mathbb{Z}$ con $0 \leq r < |b| = b$ tales que

$$-a = q \cdot b + r$$

$$a = (-q) \cdot b - r = (-q) \cdot b - b + b - r$$

$$a = (-q-1) \cdot b + (b - r) \text{ con } 0 \leq b - r < |b|$$

- Caso $a<0$ y $b<0$:

Usando el teorema para $-a>0$ y $-b>0$, se tiene que existem $q, r \in \mathbb{Z}$ com $0 \leq r < |-b| = |b| = -b$ tales que

$$-a = q\cdot(-b) + r$$
$$a = q\cdot b - r$$
$$a = q\cdot b + b - b - r$$
$$a = (q+1)\cdot b + (-b-r)$$

donde $0 \leq -b-r < |b|$, ya que

$$0 \leq r < |-b| = -b$$
$$0 \geqslant -r > b$$
$$-b \geqslant -b-r > 0$$
$$\| $$
$$|b|$$

∎

Para demostrar el teorema, necesitamos la siguiente propiedad:

<u>Principio del elemento máximal</u>: Todo subconjunto $S \subseteq \mathbb{Z}$, $S \neq \emptyset$, y acotado superiormente posee un elemento maximal, es decir, existe $m \in S$ tal que

$$s \leq m \text{ para todo } s \in S.$$

• Demostración del teorema de la división entera para $a \geq 0$ y $b > 0$:

- Paso 1: Prueba de la existencia de q y r.

Necesitaremos considerar el siguiente subconjunto auxiliar de $\mathbb{Z}$:

$$S = \{ x \cdot b \ / \ x \in \mathbb{Z} \text{ y } x \cdot b \leq a \}$$

Ejemplo: $a = 13$ y $b = 2$

$$S = \{ 2x \ / \ x \in \mathbb{Z} \text{ y } 2x < 13 \}$$
$$= \{ \ldots, -6, -4, -2, 0, 2, 4, 6, 8, 10, 12 \}$$

(números pares < 13).

Volviendo a la prueba:

⍟ $S \neq \emptyset$ ya que $0 = 0 \cdot b$ y $0 \leq a$

⍟⍟ S está acotado superiormente, ya que

$$x b \leq a \text{ para todo } x b \in S.$$

Por el principio del elemento maximal, existe $q \cdot b \in S$ tal que $x b \leq q \cdot b$ para todo $x \cdot b \in S$.

Por otro lado, sea $r = a - q \cdot b$. Entonces:

⍟ $a = q \cdot b + r$.

⍟⍟ $r \geq 0$: ya que $q b \leq a$ (pues $q \cdot b \in S$).

⍟⍟⍟ $r < b$: Supongamos lo contrario, es decir, $r \geq b$

Luego, $a - q \cdot b \geq b$

$a \geq (q+1) \cdot b$.

De acá se tiene que $(q+1) \cdot b \in S$. Como $q \cdot b$ es el elemento maximal de S, obtenemos

$$(q+1) \cdot b \leq q \cdot b$$

$b \leq 0$, lo cual es una contradicción.

- <u>Paso 2</u>: Prueba de la unicidad de q y de r.

Supongamos además que $a = q' \cdot b + r'$ con $0 \leq r' < b$.

Basta probar que $q = q'$, ya que

$$q = q' \Rightarrow q \cdot b = q' \cdot b \Rightarrow a - q \cdot b = a - q' \cdot b$$

(es decir, $r = r'$).

Si $q' > q$, entonces

$r - r' = a - q \cdot b - (a - q' \cdot b) = (q' - q) \cdot b \geq b$

(Note que como $q' - q > 0$ y $q, q' \in \mathbb{Z}$, se tiene que $q' - q \geq 1$).

Luego, $r - r' \geq b$.

Por otro lado, $r < b$ y $-r' \leq 0$, de donde $r - r' < b$. Tenemos entonces una contradicción.

De manera similar, $q' < q$ arroja una contradicción.

Por lo tanto, $q = q'$ y $r = r'$. ∎

Sistemas de enumeración (una aplicación del teorema de la división entera):

Ejemplo: 1001101 es un número en sistema binario o en base 2, el cual representa el siguiente número:

$$1\cdot 2^6 + 0\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0$$

$$\| $$

$$64 + 0 + 0 + 8 + 4 + 0 + 1 = 77$$

78 es un número expresado en el sistema usual o decimal (base 10), note que

$$78 = 7\cdot 10^1 + 8\cdot 10^0$$

$7\cdot 10^1$ ↓ decena; $8\cdot 10^0$ ↓ unidad

Se puede representar cualquier número en el sistema decimal en cualquier base b, con $b \in \mathbb{Z}$ y $b \geq 2$. Esto es una consecuencia del teorema de la división entera, lo enunciaremos y demostraremos a continuación.

Proposición (sistema de numeración en base b):
Sea $b \in \mathbb{N}$ con $b \geq 2$ y $x \in \mathbb{N}$. Entonces existen $a_0, a_1, \dots, a_m \in \mathbb{Z}$ tales que

$$x = a_m b^m + a_{m-1} \cdot b^{m-1} + \cdots + a_1 \cdot b^1 + a_0 \cdot b^0$$

donde $0 \leq a_i < b$ para todo $i \in \{0, 1, \dots, m\}$ y con $a_m \neq 0$. (se toma $a_m = 0$ para $x = 0$).

Notación: $(a_m a_{m-1} \cdots a_1 a_0)_b$ denota a x en base b.

- **Demostración:** Para $x = 0$ la demostración es trivial, ya que basta notar que

$$x = 0 \cdot b^0.$$

Podemos asumir entonces que $x > 0$.
Usamos inducción sobre x.

- $x = 1 = 1 \cdot b^0$ con $a_0 = 1$.
- H.I.: Supongamos que se cumple el resultado para todo entero entre 1 y $x-1$.

Para x y b, por el teorema de la división entera existen $q, r \in \mathbb{Z}$ únicos tales que

$$x = q \cdot b + r \quad \text{con} \quad 0 \leq r < b.$$

Como $0 \leq q < x$, por la hipótesis inductiva existem $a_0, a_1, \ldots, a_m \in \mathbb{Z}$ tales que

$$q = a_m \cdot b^m + \cdots + a_1 \cdot b + a_0$$

com $0 \leq a_i < b$ para todo $i \in \{0, 1, \ldots, m\}$, y $a_m \neq 0$.

Luego,

$$\begin{aligned} x &= (a_m b^m + \cdots + a_1 \cdot b + a_0) \cdot b + r \\ &= a_m b^{m+1} + \cdots + a_1 b^2 + a_0 b + r \\ &= a'_{m+1} b^{m+1} + \cdots + a'_2 b^2 + a'_1 b + a'_0 \end{aligned}$$

donde
$$\begin{aligned} a'_{m+1} &= a_m \\ &\vdots \\ a'_2 &= a_1 \\ a'_1 &= a_0 \\ a'_0 &= r . \end{aligned}$$

Note que $0 \leq a'_i < b$ para todo $i \in \{0, 1, \ldots, m+1\}$ y $a'_{m+1} \neq 0$. ■

Ejemplos:

① Hallan la representación de 77 em base 2. La idea es aplican el método de la demostración anterion.

- $77 = 38 \cdot 2 + 1$

$= 19 \cdot 2^2 + 1$

$= (9 \cdot 2 + 1) \cdot 2^2 + 1$

$= 9 \cdot 2^3 + 1 \cdot 2^2 + 1$

$= (2^3 + 1) \cdot 2^3 + 1 \cdot 2^2 + 1$

$= 1 \cdot 2^6 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1$

$= 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$

$\Rightarrow 77 = (1001101)_2$

Otra forma: $77 = 7 \cdot 10 + 7$

$= (2^2 + 2 + 1) \cdot 2 \cdot (2^2 + 1) + (2^2 + 2 + 1)$

$= (2^2 + 2 + 1)(2^3 + 2) + (2^2 + 2 + 1)$

$= (2^2 + 2 + 1)(2^3 + 2 + 1)$

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

$= 2^5 + 2^4 + 2 \cdot 2^3 + 2 \cdot 2^2 + 2 \cdot 2 + 1$

$= 2^5 + 2 \cdot 2^4 + 2^3 + 2^2 + 1$

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

$= 2^6 + 2^3 + 2^2 + 1$

(mismo resultado anterior)

(2) Hallan las representaciones de 6342 en bases 5 y 7.

$$6342 = 6340 + 2 = 1268 \cdot 5 + 2$$
$$= (1265 + 3) \cdot 5 + 2$$
$$= (253 \cdot 5 + 3) \cdot 5 + 2$$
$$= 253 \cdot 5^2 + 3 \cdot 5 + 2$$
$$= (250 + 3) \cdot 5^2 + 3 \cdot 5 + 2$$
$$= (2 \cdot 5^3 + 3) \cdot 5^2 + 3 \cdot 5 + 2$$
$$= 2 \cdot 5^5 + 3 \cdot 5^2 + 3 \cdot 5 + 2$$
$$= (200332)_5$$

$$6342 = 906 \cdot 7 = (129 \cdot 7 + 3) \cdot 7$$
$$= 129 \cdot 7^2 + 3 \cdot 7$$
$$= (18 \cdot 7 + 3) \cdot 7^2 + 3 \cdot 7$$
$$= 18 \cdot 7^3 + 3 \cdot 7^2 + 3 \cdot 7$$
$$= (2 \cdot 7 + 4) \cdot 7^3 + 3 \cdot 7^2 + 3 \cdot 7$$
$$= 2 \cdot 7^4 + 4 \cdot 7^3 + 3 \cdot 7^2 + 3 \cdot 7$$
$$= (24330)_7$$

③ Hallan la Representación de 50317 en base 13.

$$\begin{aligned}
50317 &= 3870 \cdot 13 + 7 \\
&= (297 \cdot 13 + 9) \cdot 13 + 7 \\
&= 297 \cdot 13^2 + 9 \cdot 13 + 7 \\
&= (22 \cdot 13 + 11) \cdot 13^2 + 9 \cdot 13 + 7 \\
&= 22 \cdot 13^3 + 11 \cdot 13^2 + 9 \cdot 13 + 7 \\
&= (1 \cdot 13 + 9) \cdot 13^3 + 11 \cdot 13^2 + 9 \cdot 13 + 7 \\
&= 1 \cdot 13^4 + 9 \cdot 13^3 + 11 \cdot 13^2 + 9 \cdot 13 + 7 \\
&= (19\underline{11}97)_{13}
\end{aligned}$$

La notación anterior es inadecuada, ya que puede interpretarse erróneamente como:

$$(191197)_{13} = 1 \cdot 13^5 + 9 \cdot 13^4 + 1 \cdot 13^3 + 1 \cdot 13^2 + 9 \cdot 13 + 7 > 50317.$$

Por tal razón, el cociente 11 se sustituye por la letra "B".

$$50317 = (19B97)_{13}.$$

En base 13, los cocientes 10, 11 y 12 corresponden a las letras A, B y C, respectivamente.