UNIVERSIDAD DE SANTIAGO DE CHILE **ÁLGEBRA 2001**
FACULTAD DE CIENCIA **INGENIERÍA CIVIL**
DEPTO. MATEMÁTICA Y C.C. **Prof. Gabriel Rabanales R.**

EJERCICIOS
MATEMÁTICA DISCRETA

1. Demuestre que si $a|b \;\wedge\; b \neq 0 \;\Rightarrow\; |a| \leq |b|$

Solución:

$$a|b \;\Rightarrow\; \exists\, p \in Z:\; b = ap \qquad (1)$$

$$(1) \wedge \mathrm{b} \neq 0 \;\Rightarrow\; \mathrm{p} \neq 0 \;\Rightarrow\; |\mathrm{p}| \geq 1\;,\quad \text{porque } p \in Z$$

Entonces:

$$\begin{aligned} |p| \geq 1 \quad /|a| &\Rightarrow |a||p| \geq |a| \\ &\Rightarrow |ap| \geq |a| \;, \text{ y usando (1)} \\ &\Rightarrow |b| \geq |a| \end{aligned}$$

2. Demuestre que si $a \in Z$, y es impar, entonces: $a^2 \cong 1 \bmod (8)$

Solución:

Consideremos los enteros módulo 4, es decir: $Z_4 = \left\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\right\}$

Entonces, cualquier $a \in Z$, impar, se escribe en la forma:

$$a = 4k + 1 \quad \vee \quad a = 4k + 3$$

y, en consecuencia:

$$\text{(i)} \quad \left\{ \begin{aligned} a = 4k+1 \Rightarrow a^2 &= (4k+1)^2 = 16k^2 + 8k + 1 = (16k^2 + 8k) + 1 \\ &\Rightarrow a^2 - 1 = 8(2k^2 + k) = 8 \cdot m\,,\quad m \in Z \\ &\Rightarrow a^2 \cong 1 \bmod (8) \end{aligned} \right.$$

$$\text{(ii)} \quad \left\{ \begin{aligned} a = 4k+3 \Rightarrow a^2 &= (4k+3)^2 = 16k^2 + 24k + 9 = (16k^2 + 24k + 8) + 1 \\ &\Rightarrow a^2 - 1 = 8\left(2k^2 + 3k + 1\right) = 8 \cdot m\,,\quad m \in Z \\ &\Rightarrow a^2 \cong 1 \bmod (8) \end{aligned} \right.$$

con lo cual queda demostrado.

Nota
¿Por qué tomamos enteros módulo 4, y no otro valor?

3. Encuentre (389, 167) , y expréselo en la forma: 389p + 167q.

4. Demuestre que: $ac \cong bc \mod(n) \;\wedge\; (c,n)=1 \;\Rightarrow\; a \cong b \mod(n)$

Solución:

$$ac \cong bc \mod(\mathrm{n}) \Rightarrow \exists\, k \in Z:\; ac - bc = kn \;\Rightarrow\; c(a-b) = kn \;\Rightarrow\; n \mid c(a-b) \qquad (1)$$

Entonces:

$$n \mid c(a-b) \wedge (c,n)=1 \Rightarrow n \mid (a-b) \Rightarrow \exists\, p \in Z:\; a-b = np \Rightarrow a \cong b \mod(\mathrm{n}) \qquad (2)$$

Explicación complementaria

Usando lenguaje primario, podemos decir que:
En (1) aplicamos la definición de congruencia e hicimos una factorización.
En (2) usamos el teorema (2.5.4 en la guía) que establece que si un número, n, divide a un producto de dos números, c y (a-b) en este caso, y “n” es primo con uno de ellos, con “c”, entonces necesariamente divide al otro, es decir a (a-b); en consecuencia procede aplicar la definición de congruencia y la demostración pedida queda establecida.
Debe recordarse que: (c,n) =1, significa que el **máximo común divisor** de “c” y “n” es “1”; en otras palabras, “c” y “n” son **números primos entre si.**

Aplicando lo anterior a un **ejemplo numérico**, consideremos:

$$21 \cong 9 \mod(2) \Rightarrow 3\cdot 7 \cong 3 \cdot 3 \mod(2) \wedge (3,2)=1 \Rightarrow 7 \cong 3 \mod(2)$$
$$\text{Obviamente}: \exists\, \mathrm{p} \in \mathrm{Z}:\; 7-3 = 2\mathrm{p} \Leftrightarrow 4 = 2\cdot 2, \quad \text{con } \mathrm{p}=2$$

5. Demuestre que: $a \mid b \;\wedge\; a \mid c \;\Rightarrow\; a^2 \mid bc$

Solución:

$$\left.\begin{array}{r} a \mid b \Rightarrow \exists\, p \in Z:\; b = ap \\ a \mid c \Rightarrow \exists\, q \in Z:\; c = aq \end{array}\right\} \Rightarrow bc = a^2 pq = a^2 \cdot (pq) = a^2 \cdot m,\; m \in Z \Rightarrow a^2 \mid bc$$

6. Determine si es verdadero o falso que: $a \mid (b+c) \Rightarrow a \mid b \;\vee\; a \mid c$

Solución:

Falso, y usamos un contraejemplo: $4 \mid (3+5) \wedge \neg(4 \mid 3) \wedge \neg(4 \mid 5)$

Intente usted ahora resolver los cuatro problemas siguientes:

7. Demuestre que: $a \mid b \Leftrightarrow ac \mid bc,\; c \neq 0$

8. Demuestre que el cubo de cualquier número $a \in Z$, es de la forma:

$$a^3 = 9k \;\vee\; a^3 = 9k+1 \;\vee\; a^3 = 9k+8$$

9. Demuestre que: $a \mid b \wedge a \mid c \;\Rightarrow\; a \mid (bx+cy),\; x,y \in Z$

10. Demuestre que: $a \mid b \;\wedge\; b \mid a \;\Rightarrow\; b = a \;\vee\; b = -a$

11. Demuestre que: $(n!+1,\ (n+1)!+1) = 1,\quad \forall n \in N$

Solución:

Se trata de demostrar que el máximo común divisor de "n!+1" y "(n+1)!+1" es "1", para todo número natural.

Sea $d = (n!+1,\ (n+1)!+1)$. Entonces: $d \mid n!+1 \ \wedge\ d \mid (n+1)!+1$, y tenemos que:

(i) $\quad d \mid n!+1 \Rightarrow \exists\, p \in Z : n!+1 = dp \Rightarrow n! = dp - 1 \qquad (*)$

(ii)
$$\begin{cases} d \mid (\mathrm{n}+1)!+1 \Rightarrow \exists\, q \in Z:\ (n+1)!+1 = dq & \Rightarrow n!(n+1)+1 = dq \\ & \Rightarrow (dp-1)(n+1)+1 = dq, \quad \text{usando } (*) \\ & \Rightarrow dp(\mathrm{n}+1) - n - 1 + 1 = dq \\ & \Rightarrow dp(n+1) - dq = n \\ & \Rightarrow d\big(p(n+1) - q\big) = n \\ & \Rightarrow d \cdot m = n, \quad m \in Z \\ & \Rightarrow d \mid n, \quad \forall n \in N \\ & \Rightarrow d \mid 1 \\ & \Rightarrow d = 1 \quad (d > 0) \end{cases}$$

12. Demuestre que si $a \in Z$, y es de la forma "6k+5", entonces es de la forma "3k+2".

Solución:

$$\begin{aligned} a \in Z \wedge a = 6k+5 &\Rightarrow a = 6k+3+2 = (6k+3)+2 = 3(2k+1)+2 = 3k'+2 \\ &\Rightarrow a = 3k'+2, \quad k' \in Z \end{aligned}$$

Ahora un problema para usted:

13. Demuestre que si $a \in Z$, entonces a^2 tiene resto "0" o "1" al dividirlo por "4".

Ayuda:

Considere congruencias módulo 2, con a = 2k ó a = 2k + 1.

14. Resuelva la ecuación: $2x \cong 3 \ \mathrm{mod}(4)$

Solución:

Las congruencias módulo 4 determinan el conjunto de "enteros módulo 4": $Z_4 = \left\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\right\}$

Ahora bien:
$$\begin{cases} 2 \cdot 0 - 3 = -3, & \text{no es divisible por 4} \\ 2 \cdot 1 - 3 = -1, & \text{no es divisible por 4} \\ 2 \cdot 2 - 3 = 1, & \text{no es divisible por 4} \\ 2 \cdot 3 - 3 = 3, & \text{no es divisible por 4} \end{cases} \Rightarrow \text{No hay solución}$$