Álgebra. Curso 2010-2011

Ejercicios del Tema 1.Teoría de números y Criptografía.

1. Demuestra, por inducción, que para todo número natural n se cumple:

   I) $1 \cdot 3 + 2 \cdot 4 + \cdots + n(n+2) = \dfrac{n(n+1)(2n+7)}{6}$

   II) $1^2 + 2^2 + 3^2 + \cdots + n^2 = n(n+1)(2n+1)/6$

   III) $\displaystyle\sum_{i=1}^{n}(-1)^{i-1}i^2 = (-1)^{n-1}\frac{n(n+1)}{2}$ IV) $\displaystyle\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4} = \left(\sum_{i=1}^{n} i\right)^2$

2. Obtén una fórmula para calcular $\sum_{i=0}^{n} \frac{1}{2^i}$ y demuéstrala utilizando el método de inducción.
3. Demuestra que para cada entero $n \geq 1$ el número $n^3 - n$ es múltiplo de 3.
4. Demuestra que la sucesión definida recursivamente por $a_2 = 20$ y $a_n = 5 \cdot 4^{n-1} - a_{n-1}$, para $n \geq 3$, verifica que $a_n = 4 \cdot (-1)^n + 4^n$ para todo natural $n \geq 2$.
5. Calcula el menor número entero positivo n_0 que cumple la desigualdad $n_0! \geq 2^{n_0}$, y utilízalo como base de inducción para comprobar que la desigualdad también se cumple para cualquier entero $n \geq n_0$.
6. Demuestra que la suma de los n primeros términos de una progresión geométrica es $\sum_{i=0}^{n} ar^i = \frac{ar^{n+1}-a}{r-1}$.
7. Demuestra que:

   I) Todo número entero al cuadrado se puede escribir de la forma $4k$ o $4k+1$.

   II) Todo número entero al cubo se puede escribir de la forma $9k$, $9k+1$ o $9k+8$.

8. Jorge tiene dos recipientes no marcados. La capacidad de un recipiente es de 17 litros y la del otro de 55 litros. ¿Cómo puede usar Jorge los dos recipientes para medir exactamente un litro?
9. Utiliza el Algoritmo de Euclides para calcular el $\text{mcd}(1492, 1776)$ y exprésalo de la forma $r \cdot 1492 + s \cdot 1776$.
10. Sean a, b y c números enteros tales que $a \mid (b+c)$.

    I) Demuestra que si $a \mid b$, entonces también debe cumplirse que $a \mid c$.

    II) Demuestra mediante un contraejemplo que $a \mid b \cdot c$ puede ser falso.

    III) Demuestra mediante un contraejemplo que $a \mid \text{mcd}(b, c)$ puede ser falso.

11. Sean a, b y c números enteros tales que $\text{mcd}(a, b) = 1$ y c divide a $a+b$. Demuestra que $\text{mcd}(a, c) = \text{mcd}(b, c) = 1$.
12. Prueba que para todo número entero p impar y no múltiplo de 5 se cumple que $p^2 - 1$ ó $p^2 + 1$ es divisible por 10.
13. Calcula las soluciones enteras de las ecuaciones diofánticas:

    I) $28x + 36y = 44$. II) $66x + 550y = 88$.

14. Repartimos 470 caramelos en un aula de 31 alumnos de modo que cada niña recibe 7 caramelos más que cada niño. Un cierto grupo de alumnos de la clase recibe 74 caramelos.¿Cuántos niños y niñas forman ese grupo?

Álgebra. Área de Álgebra
Universidade da Coruña

15. i) Demuestra que los números enteros $\{n,\ 2 \leq n \leq 9\}$ se pueden clasificar en pares tales que cada par (n, m) cumple que $nm \equiv_{11} 1$.

    ii) Utiliza el apartado anterior para probar que $10! \equiv_{11} -1$.

16. Resuelve las congruencias siguientes:

    i) $4x \equiv_{23} 1$

    ii) $2x \equiv_{10} 5$

17. Calcular n para que la última cifra de $37^{219} \cdot n$ sea 8.

18. Halla las cuatro últimas cifras binarias de 1993^{1994}.

19. Calcula el resto de dividir $1579^{1907} + 50 \cdot 52 + 49!$ entre 51.

20. Calcula el número de valores enteros x, $1 \leq x \leq 92$, para los cuales hay algún entero y tal que $xy \equiv_{92} 1$.

21. Estudia si 157 es primo (razona la respuesta).

22. Resuelve las ecuaciones

    i) $331_{(x} = 106_{(11}$ ii) $274_{(8} = x_{(2}$

23. Calcula, teniendo en cuenta que los números están en base 5,

    a) $13 + 23 + 33$ b) $43 \cdot 21$

24. Si el código ISBN de un libro es $x_1, x_2, \cdots, x_9, x_{10}$ se sabe que

$$1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + \ldots + 9 \cdot x_9 + 10 \cdot x_{10}$$

    es múltiplo de 11 y al dígito x_{10} se le llama dígito de control. Calcula dicho dígito para el código $007053065x_{10}$.

25. Halla los criterios de divisibilidad por 13 y por 9. Aplícalos para hallar el valor de x tal que el número $624x46$ sea divisible por 117.

26. Si la clave privada para el método RSA de una persona es $(13, 23, 175)$, calcula cual debe ser su clave pública.

27. Noemí codificó un mensaje mediante un cifrado afín, con $a = 8$ y $b = 11$ en $\mathbb{Z}_{27}$ para enviárselo a Ignacio. Ignacio recibió el mensaje HDAAMHPD. ¿Qué le quiere decir Noemí?

    A continuación, Ignacio quiso enviarle este mismo mensaje a Raquel, para lo que utilizó otro cifrado afín con $a = 9$ y $b = 6$. Calcula el mensaje que recibió Raquel. ¿Será capaz de desencriptarlo?

    Nota: Para escribir el mensaje de forma numérica se ha seguido la siguiente tabla:

Letra	Cifra	Letra	Cifra	Letra	Cifra	Letra	Cifra
A	01	H	08	Ñ	15	U	22
B	02	I	09	O	16	V	23
C	03	J	10	P	17	W	24
D	04	K	11	Q	18	X	25
E	07	L	12	R	19	Y	26
F	06	M	13	S	20	Z	27
G	07	N	14	T	21		

Álgebra. Área de Álgebra
Universidade da Coruña

28. Sabemos que la clave pública de Tomasa para el método de Merkle-Hellman es

$$B = \{2828, 2834, 30, 1471, 1549, 264, 3344, 3872, 3529, 4224\}.$$

Por otro lado, tenemos una tabla de conversión de caracteres a código binario, donde cada uno ocupa 5 bits (ver tabla).

i) Encripta el mensaje "LO SABES?" utilizando el método de Merkel-Hellman, para enviárselo a Tomasa.

ii) Una vez que Tomasa ha recibido el mensaje, recibes de vuelta lo siguiente:

$$(32460, 31177, 24366)$$

Si tu clave privada es

$$((16, 21, 39, 80, 159, 316, 634, 1266, 2537, 5070), 10139, 216),$$

- ¿qué te ha respondido Tomasa?
- ¿cuál es tu clave pública?

Nota: Debes tener en cuenta, a la hora de encriptar y desencriptar, que cada caracter se representa en código binario según se muestra el la tabla siguiente:

A	00000	G	00110	M	01100	R	10010	X	11000
B	00001	H	00111	N	01101	S	10011	Y	11001
C	00010	I	01000	Ñ	01110	T	10100	Z	11010
D	00011	J	01001	O	01111	U	10100	?	11011
E	00100	K	01010	P	10000	V	10110		
F	00101	L	01011	Q	10001	W	10111		

Álgebra. Área de Álgebra
Universidade da Coruña