Hoja 1: Aritmética entera y modular

Opción A

1A.1 Dados a y b, dividendo y divisor respectivamente, obtener q y r, cociente y resto de la división euclídea, en cada caso:

a	17	-17	17	-17	5	-5	5	-5
b	5	5	-5	-5	17	17	-17	-17
q								
r								

1A.2 Sean $a, b \in \mathbb{Z}$. Decidir si las siguientes afirmaciones son verdaderas o falsas y demostrarlo:

1) Si $4|a$ y $5|b$ entonces $10|5a + 2b$.
2) Si $a + b|10$ entonces $a|10$ ó $b|10$.
3) Si $10|a$ ó $10|b$ entonces $10|a \cdot b$.
4) Si $a + b|c$ y $a|b$ entonces $a|c$.
5) Si $a|10$ y $b|10$ entonces $a + b|20$.
6) $3 \mid n(n+1)(n+2)$, para todo $n \in \mathbb{Z}$.

1A.3 Estudiar si $63, 73$ y 161 son primos. Para los que no lo sean, obtener todos sus divisores.

1A.4 Sean $a, b \in \mathbb{Z}$. Decidir razonadamente si es verdadera o falsa cada una de estas afirmaciones:

1) Si $15|a \cdot b$ entonces $5|a$ ó $5|b$.
2) Si $6|a \cdot b$ entonces $6|a$ ó $6|b$.
3) Si $6|a$ y $10|a$ entonces $60|a$.
4) Si $6|a$ y $5|a$ entonces $30|a$.

1A.5 Sea $m \in \mathbb{Z}$.

1) Si $m|140$ y $\mathrm{mcd}(20, m) = 1$, ¿qué valores puede tomar m?
2) Si $m|400$ y $\mathrm{mcd}(20, m) = 1$, ¿qué valores puede tomar m?

1A.6 Utilizar el algoritmo extendido de Euclides para hallar $x, y \in \mathbb{Z}$ tales que

$$126x + 72y = \mathrm{mcd}(126, 72).$$

1A.7 Resolver las siguientes ecuaciones diofánticas. Utilizar el algoritmo extendido de Euclides para hallar una solución particular.

1) $126x + 33y = 12$
2) $112x + 72y = 84$
3) $14x + 21y = 84$

1A.8 Un juego infantil consta de un palo vertical de 1.50 m de altura sujeto en una base horizontal y de unos discos que se ensartan en él. Los discos son de dos alturas diferentes: 9 cm y 21 cm, respectivamente. Justificar que es posible cubrir el palo totalmente sin rebasarlo usando estos dos tipos de discos y dar todas las formas de hacerlo.

1A.9 Una persona tiene un presupuesto entre 250 y 300 euros para comprar dos tipos de productos. Una unidad del primer tipo cuesta 15 euros y una unidad del segundo cuesta 24 euros. Determinar la menor cantidad de dinero, dentro del presupuesto, que esa persona puede gastar y para esa cantidad, dar todas las formas de gastarlo.

1A.10 Calcular el representante canónico de:

1) $\overline{20}, \overline{-4}, \overline{31}$ en $\mathbb{Z}_5$ y $\mathbb{Z}_{12}$.
2) $\overline{8}+\overline{3}$, $\overline{4}-\overline{8}$, $\overline{3}\cdot\overline{5}$, $\overline{5}\cdot\overline{20}$ en $\mathbb{Z}_5$ y $\mathbb{Z}_{12}$.
3) $\overline{53}^2$, $\overline{53}^5$ y $\overline{53}^{182}$ en $\mathbb{Z}_5$ y $\mathbb{Z}_{12}$.
4) $\overline{27}^n$, $n \in \mathbb{N}$ en $\mathbb{Z}_5$ y $\mathbb{Z}_{12}$.

1A.11 En $\mathbb{Z}_{14}$ y $\mathbb{Z}_{20}$,

1) Obtener todos los elementos inversibles.
2) Utilizar el algoritmo extendido de Euclides para hallar el inverso de $\overline{9}$ y de $\overline{19}$.
3) ¿Hay algún elemento distinto de $\overline{1}$ que sea inverso de sí mismo?

1A.12 Resolver la ecuación $\overline{10}\cdot x = \overline{6}$ en $\mathbb{Z}_2$, $\mathbb{Z}_5$, $\mathbb{Z}_{21}$ y $\mathbb{Z}_{26}$.

1A.13 Plantear y resolver en cada caso una ecuación de la forma $\overline{a}\cdot x = \overline{b}$ con $\overline{a}, \overline{b}, x \in \mathbb{Z}_{35}$ de modo que verifique las siguientes condiciones o justificar que no puede existir.

1) Tiene una única solución.
2) No tiene solución.
3) Tiene tres soluciones.
4) Tiene cinco soluciones.

1A.14 Para cada caso, indicar razonadamente qué valores de $n \in \mathbb{N}$ hacen que la ecuación modular $\overline{14}\cdot x = \overline{21}$ con $x \in \mathbb{Z}_n$ verifique:

1) Tiene una única solución.
2) No tiene solución.
3) Tiene tres soluciones.
4) Tiene siete soluciones.

1A.15 Se considera la función $f : \mathbb{Z}_{14} \to \mathbb{Z}_{14}$ definida por

$$f(x) = \overline{3}x + \overline{5}$$

1) Probar que es válida como función de cifrado y obtener la función de descifrado.
2) Dar el cifrado de la cadena $[\overline{2}, \overline{0}, \overline{1}, \overline{4}]$ y descifrar $[\overline{3}, \overline{1}, \overline{4}]$.
3) Estudiar cuántas funciones $f : \mathbb{Z}_{14} \to \mathbb{Z}_{14}$, de la forma $f(x) = \overline{a}x + \overline{b}$ con $\overline{a}, \overline{b} \in \mathbb{Z}_{14}$, son válidas como función de cifrado.

Nota: Para facilitar o revisar las cuentas de los siguientes problemas, se pueden usar las funciones de WxMaxima:

- `mod(a,n)` que devuelve un representante de $\overline{a}$ en $\mathbb{Z}_n$.
- `inv_mod(a,n)` que devuelve un representante de $\overline{a}^{-1}$ en $\mathbb{Z}_n$.
- `makelist(f(x),x,L)` que devuelve una lista con los valores que toma la función $f(x)$ para los valores de x contenidos en la lista L.

1A.16 Isabel Corrales desconfía de su nueva compañera de piso y cifra los mensajes que envía a su novio con una función de cifrado afín, de forma que la primera y la última letra de su nombre se transforman en la primera y la última de su apellido, respectivamente. Su compañera, que ciertamente la espía, se ha enterado de esos datos y además sabe que utiliza el castellano con espacio en blanco. Toda esa información le parece suficiente para descifrar su último mensaje. ¿Cuál es el significado de ‘‘ÑYHGRW’’?

Tabla auxiliar: Equivalentes en el alfabeto castellano con espacio en blanco

Letra	*blanco*	A	B	C	D	E	F	G	H	I	J	K	L	M
Número	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Letra	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Número	14	15	16	17	18	19	20	21	22	23	24	25	26	27

1A.17 Nuestros servicios de inteligencia han interceptado el mensaje cifrado ‘‘PIB’’. Se conoce que el mensaje ha sido cifrado utilizando una función $f(x) = \overline{a}x + \overline{b}$, y que el emisor utiliza el alfabeto castellano de 27 letras, sin espacio en blanco, según la siguiente tabla:

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Número	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Letra	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Número	14	15	16	17	18	19	20	21	22	23	24	25	26	

Se sabe que la función de cifrado f transforma la letra ‘‘P’’ en sí misma y que su término independiente $\overline{b}$ toma uno de los dos valores: $\overline{8}$ o $\overline{10}$.

Se pide hallar una función de cifrado válida que verifique dichas condiciones y recuperar el mensaje original.

Opción B

1B.1 Dados a y b, dividendo y divisor respectivamente, obtener q y r, cociente y resto de la división euclídea, en cada caso:

a	23	-23	23	-23	7	-7	7	-7
b	7	7	-7	-7	23	23	-23	-23
q								
r								

1B.2 Sean $a, b \in \mathbb{Z}$. Decidir si las siguientes afirmaciones son verdaderas o falsas y demostrarlo:

1) Si $2|a$ y $3|b$ entonces $6|3a + 2b$.
2) Si $10|a + b$ entonces $10|a$ ó $10|b$.
3) Si $10|a + b$ y $10|b$ entonces $10|a$.
4) Si $10|a + b$ y $5|b$ entonces $5|a$.
5) Si $10|a$ y $5|b$ entonces $10|a + b$.
6) $2 \mid n(n + 1)$, para todo $n \in \mathbb{Z}$.

1B.3 Estudiar si $57, 99$ y 101 son primos. Para los que no lo sean, obtener todos sus divisores.

1B.4 Sean $a, b \in \mathbb{Z}$. Decidir razonadamente si es verdadera o falsa cada una de estas afirmaciones:

1) Si $5|a \cdot b$ entonces $5|a$ ó $5|b$.
2) Si $10|a \cdot b$ entonces $10|a$ ó $10|b$.
3) Si $4|a$ y $5|a$ entonces $20|a$.
4) Si $4|a$ y $6|a$ entonces $24|a$.

1B.5 Sea $m \in \mathbb{Z}$.

1) Si $m|20 \cdot 33$ y $\mathrm{mcd}(20, m) = 1$, ¿qué valores puede tomar m?
2) Si $20 \cdot 33|m$ y $\mathrm{mcd}(20, m) = 1$, ¿qué valores puede tomar m?

1B.6 Utilizar el algoritmo extendido de Euclides para hallar $x, y \in \mathbb{Z}$ tales que

$$36x + 102y = \mathrm{mcd}(36, 102).$$

1B.7 Resolver las siguientes ecuaciones diofánticas. Utilizar el algoritmo extendido de Euclides para hallar una solución particular.

1) $92x + 84y = 62$
2) $539x + 363y = 22$
3) $6x + 15y = 102$

1B.8 Un ordenador tarda 6 nanosegundos en hacer una suma y 10 nanosegundos en hacer un producto. Si ha estado haciendo estas dos operaciones sin parar durante 104 nanosegundos, ¿cuántas sumas y productos ha podido hacer?

1B.9 En un examen tipo test hay que obtener al menos 100 puntos sobre 180 para aprobar. Una serie de preguntas valen 6 puntos cada una y otras valen 15 puntos (erróneas o en blanco valen 0).

1) ¿Es posible obtener exactamente 100 puntos?
2) ¿Cuál es el menor número de puntos N que se puede obtener para aprobar? Indicar todas las formas de obtener esos N puntos.

1B.10 Calcular el representante canónico de:

1) $\overline{20}, \overline{-4}, \overline{31}$ en $\mathbb{Z}_6$ y $\mathbb{Z}_7$.
2) $\overline{8}+\overline{3}$, $\overline{4}-\overline{8}$, $\overline{3}\cdot\overline{5}$, $\overline{5}\cdot\overline{20}$ en $\mathbb{Z}_6$ y $\mathbb{Z}_7$.
3) $\overline{17}^2$, $\overline{17}^9$ y $\overline{17}^{184}$ en $\mathbb{Z}_6$ y $\mathbb{Z}_7$.
4) $\overline{16}^n$, $n \in \mathbb{N}$ en $\mathbb{Z}_6$ y $\mathbb{Z}_7$.

1B.11 En $\mathbb{Z}_{15}$ y de $\mathbb{Z}_{44}$,

1) Obtener todos los elementos inversibles.
2) Utilizar el algoritmo extendido de Euclides para hallar el inverso de $\overline{7}$ y de $\overline{43}$.
3) ¿Hay algún elemento distinto de $\overline{1}$ que sea inverso de sí mismo?

1B.12 Resolver la ecuación $\overline{6}\cdot x = \overline{15}$ en $\mathbb{Z}_3$, $\mathbb{Z}_{13}$, $\mathbb{Z}_{21}$ y $\mathbb{Z}_{22}$.

1B.13 Plantear y resolver en cada caso una ecuación de la forma $\overline{a}\cdot x = \overline{b}$ con $\overline{a}, \overline{b}, x \in \mathbb{Z}_{12}$ de modo que verifique las siguientes condiciones o justificar que no puede existir.

1) Tiene una única solución.
2) No tiene solución.
3) Tiene tres soluciones.
4) Tiene cinco soluciones.

1B.14 Para cada caso, indicar razonadamente qué valores de $n \in \mathbb{N}$ hacen que la ecuación modular $\overline{15}\cdot x = \overline{18}$ con $x \in \mathbb{Z}_n$ verifique:

1) Tiene una única solución.
2) No tiene solución.
3) Tiene tres soluciones.
4) Tiene cinco soluciones.

1B.15 Se considera la función $f : \mathbb{Z}_{18} \to \mathbb{Z}_{18}$ definida por

$$f(x) = \overline{5}x + \overline{3}$$

1) Probar que es válida como función de cifrado y obtener la función de descifrado.
2) Dar el cifrado de la cadena $[\overline{1}, \overline{3}, \overline{5}]$ y descifrar $[\overline{1}, \overline{2}]$.
3) Estudiar cuántas funciones $f : \mathbb{Z}_{18} \to \mathbb{Z}_{18}$, de la forma $f(x) = \overline{a}x + \overline{b}$ con $\overline{a}, \overline{b} \in \mathbb{Z}_{18}$, son válidas como función de cifrado.

Nota: Para facilitar o revisar las cuentas de los siguientes problemas, se pueden usar las funciones de WxMaxima:

- `mod(a,n)` que devuelve un representante de $\overline{a}$ en $\mathbb{Z}_n$.
- `inv_mod(a,n)` que devuelve un representante de $\overline{a}^{-1}$ en $\mathbb{Z}_n$.
- `makelist(f(x),x,L)` que devuelve una lista con los valores que toma la función $f(x)$ para los valores de x contenidos en la lista L.

1B.16 El agente secreto Kevin Osborne cifra todos sus mensajes con una función de cifrado afín. Lo hace transformando primero cada letra del alfabeto en su número de orden correspondiente (ver tabla adjunta) y a continuación aplicando a cada número la función $f\colon \mathbb{Z}_{27} \to \mathbb{Z}_{27}$, $f(x) = \bar{a}x + \bar{b}$ para ciertos $\bar{a}, \bar{b} \in \mathbb{Z}_{27}$. Finalmente vuelve a transformar los números en letras antes de enviar el mensaje. Además, sabemos que Kevin es muy cuidadoso y firma todos sus mensajes añadiendo sus iniciales al final.

Hemos interceptado el mensaje ‘‘WCYTE’’. Halla la función de descifrado que utiliza Kevin y desencripta el mensaje.

Tabla auxiliar: Equivalentes en el alfabeto castellano sin espacio en blanco

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Número	0	1	2	3	4	5	6	7	8	9	10	11	12	13
	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
	14	15	16	17	18	19	20	21	22	23	24	25	26	

1B.17 El jefe de Julia Zamora quiere averiguar los mensajes que envía en horas de trabajo a sus amigos. En su empeño, averigua que cifra sus mensajes con una función de cifrado afín, sobre el alfabeto inglés con espacio en blanco. También sabe que uno de los dígito de la clave es 21 y que la primera letra de su nombre se transforma en la primera de su apellido. El jefe está seguro de poder descifrar de ahora en adelante todos los mensajes de Julia. Probar que está en lo cierto y descifrar el criptograma interceptado ‘‘RAC’’.

Tabla auxiliar: Equivalentes en el alfabeto inglés sin espacio en blanco

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M
Número	0	1	2	3	4	5	6	7	8	9	10	11	12
Letra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Número	13	14	15	16	17	18	19	20	21	22	23	24	25