FCEyN - UBA - Segundo Cuatrimestre 2013

# Álgebra I
## Práctica 4 - Números enteros (Parte 2)

**1**. i) Si $a \equiv 22\ (14)$, hallar el resto de dividir a $a$ por 14, por 2 y por 7.

ii) Si $a \equiv 13\ (5)$, hallar el resto de dividir a $33a^3 + 3a^2 - 197a + 2$ por 5.

iii) Hallar, para cada $n \in \mathbb{N}$, el resto de la división de $\sum_{i=1}^{n} (-1)^i \cdot i!$ por 36.

**2**. i) Hallar todos los $a \in \mathbb{Z}$ tales que $a^2 \equiv 3\ (11)$.

ii) Probar que no existe ningún entero $a$ tal que $a^3 \equiv -3\ (13)$.

iii) Probar que $a^2 \equiv -1\ (5) \Leftrightarrow a \equiv 2\ (5)$ ó $a \equiv 3\ (5)$.

iv) Probar que $a^7 \equiv a\ (7)$ para todo $a \in \mathbb{Z}$.

v) Probar que $7 \mid a^2 + b^2 \Leftrightarrow 7 \mid a$ y $7 \mid b$.

vi) Probar que $5 \mid a^2 + b^2 + 1 \Rightarrow 5 \mid a$ ó $5 \mid b$.

**3**. Enunciar y demostrar criterios de divisibilidad por 8, 9 y 11.

**4**. i) Probar que $2^{5n} \equiv 1\ (31)$ para todo $n \in \mathbb{N}$.

ii) Hallar el resto de la división de $2^{51833}$ por 31.

iii) Sea $k \in \mathbb{N}$. Sabiendo que $2^k \equiv 39\ (31)$, hallar el resto de la división de $k$ por 5.

iv) Hallar el resto de la división de $43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999}$ por 31.

**5**. Probar que cualquiera sea $n \in \mathbb{N}$, $(2^n + 5^{n+1} : 2^{n+1} + 5^n) = 3$ ó 9, y dar un ejemplo para cada caso.

**6**. *Ternas Pitagóricas, S. VI A.C.* Son las ternas $(a, b, c)$ de números naturales que satisfacen

$$a^2 + b^2 = c^2,$$

o sea que se corresponden con las longitudes de los catetos e hipotenusa de triángulos rectángulos con lados enteros.

i) Probar que si $(a, b, c)$ es una terna pitagórica, entonces $(ka, kb, kc)$ es una terna pitagórica, $\forall\, k \in \mathbb{N}$.

ii) Probar que si existe $k \in \mathbb{N}$ que divide a dos de los términos, entonces divide también al tercero.

iii) Probar que existen infinitas ternas pitagóricas *primitivas* (aquellas donde $a$, $b$ y $c$ son coprimos) que satisfacen que $c = b + 1$, como por ejemplo $(3, 4, 5)$, $(5, 12, 13)$ y $(7, 24, 25)$. (Sug: Probar que el conjunto $\{1^2 - 0^2, 2^2 - 1^2, 3^2 - 2^2, \ldots\}$ coincide con el conjunto de los números naturales impares, y considerar en él los cuadrados de los impares.)

iv) Sean $m > n \in \mathbb{N}$. Probar que la siguiente es una terna pitagórica

$$a = m^2 - n^2,\ b = 2mn,\ c = m^2 + n^2,$$

y que es primitiva si y solo si $m$ y $n$ son coprimos y uno de los dos es impar y el otro par.

v) Caracterización de todas las ternas pitagóricas *primitivas*:

(a) Probar que $c$ tiene que ser impar obligatoriamente (sug: tomar congruencia módulo 4), y que entre $a$ y $b$ hay uno que es par y el otro que es impar.

(b) Sea $a$ el impar y $b$ el par. Probar que $(c - a : c + a) = 2$ y de $b^2 = c^2 - a^2$, deducir que $c - a = 2n^2$ y $c + a = 2m^2$ para algún $n < m \in \mathbb{N}$, y concluir.

**7**. Escribir las tablas de suma y producto en $\mathbb{Z}/n\mathbb{Z}$ para 5, 6, 7 y 8. ¿Cuáles de estos anillos son cuerpos?

**8**. Un elemento $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ es un *cuadrado* (de $\mathbb{Z}/n\mathbb{Z}$) si existe $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ tal que $\overline{a} = \overline{b}^2$ en $\mathbb{Z}/n\mathbb{Z}$.

i) Calcular los cuadrados de $\mathbb{Z}/n\mathbb{Z}$ para $n = 2$, 3, 4, 5, 6, 7, 8, 9, 11 y 13. ¿Cuántos hay en cada caso?

ii) Probar que si $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ son cuadrados, entonces $\overline{a} \cdot \overline{b}$ es un cuadrado también.

iii) Probar que si $\overline{a}$ es un elemento inversible de $\mathbb{Z}/n\mathbb{Z}$ tal que $\overline{a} = \overline{b}^2$, entonces $\overline{b}$ es inversible también en $\mathbb{Z}/n\mathbb{Z}$ y $(\overline{a})^{-1}$ es un cuadrado también.

iv) Sea $p$ primo positivo. Probar que, en $\mathbb{Z}/p\mathbb{Z}$, si $\overline{a}^2 = \overline{b}^2$ entonces $\overline{a} = \overline{b}$ ó $\overline{a} = -\overline{b}$. Deducir que si $p$ es impar, entonces hay exactamente $\frac{p-1}{2}$ cuadrados no nulos en $\mathbb{Z}/p\mathbb{Z}$.

**9**. *Test de primalidad de Wilson,* por el mátemático inglés John Wilson, 1741-1793. Este test era conocido mucho antes por los árabes, y fue de hecho probado por primera vez por el matemático italiano Joseph-Louis Lagrange en 1771. Dice que si $n \in \mathbb{N}$ es distinto de 1, entonces

$$(n-1)! \equiv -1 \pmod{n} \iff n \text{ es primo .}$$

i) Probar que si $n$ es compuesto, entonces $(n-1)! \equiv 0 \pmod{n}$. ¿Qué se prueba con esto?

ii) Sea $p$ un primo positivo. Se recuerda que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo. Probar que $\overline{a} = (\overline{a})^{-1}$ en $\mathbb{Z}/p\mathbb{Z}$ si y solo si $\overline{a} = \pm\overline{1}$. Deducir que $(p-1)! \equiv -1 \pmod{p}$.

**10**. Determinar, cuando existan, todos los $a, b \in \mathbb{Z}$ que satisfacen

i) $5a + 8b = 3$, ii) $24a + 14b = 7$, iii) $39a - 24b = 6$.

**11**. Si se sabe que cada unidad de un cierto producto A cuesta 39 pesos y que cada unidad de un cierto producto B cuesta 48 pesos, ¿cuántas unidades de cada producto se pueden comprar con 135 pesos?

**12**. Hallar, cuando existan, todas las soluciones de las siguientes ecuaciones de congruencia

i) $17X \equiv 3\ (11)$, ii) $56X \equiv 28\ (35)$, iii) $56X \equiv 2\ (884)$, iv) $33X \equiv 27\ (45)$.

**13**. Hallar el resto de la división de un entero $a$ por 18, sabiendo que el resto de la división de $7a$ por 18 es 5.

**14**. Hallar todos los $a \in \mathbb{Z}$ para los cuales $(7a + 1 : 5a + 4) \neq 1$.

**15**. Describir los valores de $(5a + 8 : 7a + 3)$ en función de los valores de $a \in \mathbb{Z}$.

**16**. Hallar, cuando existan, todos los enteros $a$ que satisfacen simultáneamente:

i) $\begin{cases} a \equiv 0 & (8) \\ a \equiv 2 & (5) \\ a \equiv 1 & (21) \end{cases}$ ii) $\begin{cases} a \equiv 3 & (10) \\ a \equiv 2 & (7) \\ a \equiv 5 & (9) \end{cases}$

iii) $\begin{cases} a \equiv 1 & (6) \\ a \equiv 2 & (20) \end{cases}$ iv) $\begin{cases} a \equiv 1 & (12) \\ a \equiv 7 & (10) \\ a \equiv 4 & (9) \end{cases}$

**17**. i) ¿Existe algún entero $a$ cuyo resto en la división por 15 sea 2 y cuyo resto en la división por 18 sea 8?

ii) ¿Existe algún entero $a$ cuyo resto en la división por 15 sea 13 y cuyo resto en la división por 35 sea 22?

**18**. i) Hallar el menor entero positivo $a$ tal que el resto de la división de $a$ por 21 es 13 y el resto de la división de $6a$ por 15 es 9.

ii) Hallar un entero $a$ entre 60 y 90 tal que el resto de la división de $2a$ por 3 es 1 y el resto de la división de $7a$ por 10 es 8.

**19**. Hallar el resto de la división de $a$ por $p$ en los casos

i) $a = 33^{1427}$, $p = 5$,
ii) $a = 71^{22283}$, $p = 11$,
iii) $a = 5 \cdot 7^{2451} + 3 \cdot 65^{2345} - 23 \cdot 8^{138}$, $p = 13$.

**20**. i) Resolver la ecuación de congruencia $7^{13}X \equiv 5\ (11)$,
ii) Resolver la ecuación de congruencia $2^{94}X \equiv 7\ (97)$.

**21**. *Seudoprimos o números de Carmichael (Robert Carmichael, 1879-1967, matemático estadounidense).* Se dice que $n \in \mathbb{Z}$ es un número de Carmichael si satisface el pequeño Teorema de Fermat sin ser primo, es decir, si $a$ es un entero coprimo con $n$, entonces $a^{n-1} \equiv 1 \pmod{n}$. Probar que 561 es un número de Carmichael. En 1994 se probó finalmente que hay infinitos números de Carmichael, luego de que esta conjetura quedara abierta por muchos años.

**22**. Probar que para todo $a \in \mathbb{Z}$ vale

i) $728 \mid a^{27} - a^3$ ,

ii) $\dfrac{2a^7}{35} + \dfrac{a}{7} - \dfrac{a^3}{5} \in \mathbb{Z}$.

**23**. Hallar el resto de la división de

i) $3 \cdot 7^{135} + 24^{78} + 11^{222}$ por 70,
ii) $3^{385}$ por 400,
iii) $\displaystyle\sum_{i=1}^{1759} i^{42}$ por 56.

**24**. Hallar todos los $a \in \mathbb{Z}$ tales que

i) $539 \mid 3^{253}a + 5^{44}$,

ii) $a^{236} \equiv 6\ (19)$.

**25**. i) Describir el conjunto $\{\overline{3}^n;\ n \in \mathbb{N}\}$ en $\mathbb{Z}/7\mathbb{Z}$ y en $\mathbb{Z}/11\mathbb{Z}$. Observar la diferencia que hay en el primer caso con respecto al segundo caso, y hallar si se puede un elemento $\overline{a} \in \mathbb{Z}/11\mathbb{Z}$ que cumpla que $\{\overline{a}^n;\ n \in \mathbb{N}\} = \mathbb{Z}/11\mathbb{Z} - \{\overline{0}\}$.
ii) Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 1\ (7)$ y todos los $n \in \mathbb{N}$ tales que $3^n \equiv 4\ (7)$.
iii) Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 1\ (11)$ y todos los $n \in \mathbb{N}$ tales que $3^n \equiv 9\ (11)$.
iv) Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 53\ (77)$.

**26**. Hallar el resto de la división de $2^{2^n}$ por 13 para cada $n \in \mathbb{N}$.

**27**. Hallar todos los divisores positivos de $25^{70}$ que sean congruentes a 2 módulo 9 y a 3 módulo 11.

**28**. Sea $n \in \mathbb{N}$. Probar que $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ es inversible si y solo si $a$ es coprimo con $n$.

**29**. Sea $p$ un primo. Probar que en $\mathbb{Z}/p\mathbb{Z}$ vale que $(\overline{a} + \overline{b})^p = \overline{a}^p + \overline{b}^p$, $\forall\, \overline{a}, \overline{b} \in \mathbb{Z}/p\mathbb{Z}$ (sug: ver Ej. 32 Práctica 3). ¿Vale lo mismo en $\mathbb{Z}/n\mathbb{Z}$ si $n$ no es primo?

**30**. *El problema del logaritmo discreto.* Sea $p$ un número primo y sea $\overline{g} \in \mathbb{Z}/p\mathbb{Z}$ tal que

$$\{\overline{g}^k; 0 \leq k < p-1\} = \mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$$

(se puede probar que un tal $\overline{g}$ siempre existe, se llama *generador* de $\mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$, c.f. por ejemplo Ej. 25(i)): para $p = 7$ se puede tomar $\overline{g} = \overline{3}$. ¿Quién se puede elegir para $p = 11$?)

i) Probar que si $\overline{g}^k = \overline{a} \in \mathbb{Z}/p\mathbb{Z}$ con $0 \leq k < p-1$, entonces $g^n \equiv a\,(p) \Leftrightarrow n \equiv k\,(p-1)$.
ii) Dado $\overline{a} \in \mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$, el problema del logaritmo discreto consiste en determinar cuál es el $k$ con $0 \leq k < p-1$ tal que $\overline{g}^k = \overline{a}$ en $\mathbb{Z}/p\mathbb{Z}$. Ese $k$ siempre existe por ser $\overline{g}$ un generador.
En ese caso, $k$ se llama el *logaritmo discreto* de $a$ (en base $g$ módulo $p$) y se nota

$$k = \log_g(a) \,(\mathrm{mod}\, p).$$

O sea $k = \log_g(a) \Leftrightarrow 0 \leq k < p-1$ y $g^k \equiv a \,(\mathrm{mod}\, p)$.
Calcular $\log_3(4) \,(\mathrm{mod}\, 7)$, $\log_3(5) \,(\mathrm{mod}\, 7)$ y $\log_3(12) \,(\mathrm{mod}\, 17)$.

iii) Armar un programa que calcule $\log_g(a) \pmod p$ dados $p$ primo, $g$ generador de $\mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$ y $a$. No se conoce ningún algoritmo eficiente para calcular logaritmos discretos en general: un importante problema abierto es ¿Existe un algoritmo polinomial para calcular el logaritmo discreto en una computadora clásica? (donde esto significa que la cantidad de operaciones "bit" que realiza el algoritmo tiene que ser a lo sumo polinomial en la cantidad de bits del primo $p$).

**31**. *El algoritmo de intercambio de clave de Diffie-Hellman, 1976.* Este es un algoritmo para que dos personas Alice y Bob, puedan intercambiar una clave secreta sin que ningun espía pueda determinar cuál es, aún oyendo las comunicaciones entre Alice y Bob. Se basa en lo difícil que es calcular el logaritmo discreto de un número módulo un primo $p$ (se usan primos de 300 dígitos al menos).

i) Alice y Bob concuerdan públicamente en un primo $p$ (grande) y en $g \in \mathbb{Z}$ tal que

$$\{\overline{g}^k; 0 \leq k < p-1\} = \mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$$

(hay algoritmos que calculan un tal $g$ en forma más rápida que intentar con todos los elementos de $\mathbb{Z}/p\mathbb{Z}$).
Por ejemplo para fijar ideas $p = 23$ y $g = 5$.

ii) Alice elije secretamente un número $k$, y le manda publicamente a Bob el número $\overline{A} = \overline{g}^k$ en $\mathbb{Z}/p\mathbb{Z}$, y Bob elije secretamente un número $j$, y le manda públicamente a Alice el número $\overline{B} = \overline{g}^j$ en $\mathbb{Z}/p\mathbb{Z}$. Por ejemplo si Alice elije el 6 y Bob elije el 15, se tiene $\overline{A} = \overline{5}^6 = \overline{8}$, y $\overline{B} = \overline{5}^{15} = \overline{19}$ en $\mathbb{Z}/23\mathbb{Z}$.

iii) Alice calcula $\overline{B}^k$ y Bob calcula $\overline{A}^j$ en $\mathbb{Z}/p\mathbb{Z}$, y resulta que estos dan el mismo elemento $\overline{s} \in \mathbb{Z}/p\mathbb{Z}$, con $1 \leq s \leq p-1$. Tal $s$ es la clave secreta que Alice y Bob compartirán. Aquí $\overline{19}^6 = \overline{2} = \overline{8}^{15}$ en $\mathbb{Z}/23\mathbb{Z}$, o sea $s = 2$.

Justificar por qué siempre da el mismo $s$, y explicar por qué con los datos $p$, $g$, $\overline{A}$ y $\overline{B}$ un espía no puede encontrar $s$ facilmente.

**32**. *La función $\varphi$ de Euler* (por el matemático suizo Leonhard Euler, 1707-1783, que introdujo esta función en 1760) es la función $\varphi : \mathbb{N} \to \mathbb{N}$ definida como

$$\varphi(n) = \#\{m \in \mathbb{N} : m \leq n \text{ y } (m : n) = 1\},$$

es decir $\varphi(n)$ cuenta la cantidad de números menores (o iguales) que $n$ que son coprimos con $n$. Por ejemplo $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6, \varphi(8) = 4, \ldots$

Sea $p$ un primo. Probar que $\varphi(p) = p - 1$ y que $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$, $\forall\, k \in \mathbb{N}$.

Resulta que la función $\varphi$ también cumple que $\varphi(mn) = \varphi(m)\varphi(n)$ si $m, n \in \mathbb{N}$ son coprimos (se puede probar por ejemplo usando el Teorema Chino del Resto).

Esto permite calcular $\varphi(n)$, $\forall\, n \in \mathbb{N}$, *dada la factorización de $n$ en números primos!*

$$\text{Si } n = p_1^{k_1} \cdots p_r^{k_r}, \text{ entonces } \varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_r^{k_r}) = (p_1 - 1)p_1^{k_1 - 1} \cdots (p_r - 1)p_r^{k_r - 1}.$$

Nadie sabe hasta la fecha calcular $\varphi$ de una forma más económica que utilizando la factorización. Esto es un factor esencial del que depende la seguridad del sistema criptográfico RSA:
Mostrar que si $n = pq$ con $p$ y $q$ primos desconocidos, y uno además de $n$ conoce $\varphi(n)$ entonces puede recuperar con facilidad quiénes son $p$ y $q$...