FCEyN - UBA - Segundo cuatrimestre 2015

Álgebra I
Práctica 4 - Números enteros (Parte 2)

Congruencia y Tablas de Restos

1. Sea a un entero impar que no es divisible por 5.

i) Probar que $a^4 \equiv 1\ (10)$.

ii) Probar que a y a^{45321} tienen el mismo resto en la división por 10.

2. 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.

3. 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.

4. 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 $3 \mid a^2 + b^2 \Leftrightarrow 3 \mid a$ y $3 \mid b$.

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

vi) Probar que $5 \mid a^2 + b^2 \Leftrightarrow a \equiv 2b\ (5)$ ó $a \equiv 3b\ (5)$.

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

viii) Probar que cualesquiera sean $a, b, c \in \mathbb{Z}$, $a^2 + b^2 + c^2 + 1$ no es divisible por 8.

5. Demostrar que ninguna de las siguientes ecuaciones tiene soluciones enteras

i) $x^3 - 2 = 7y$. ii) $15x^2 - 7y^2 = 9$. iii) $3x^2 + 2 = y^3$. iv) $7x^3 + 2 = y^3$.

6. Probar que la ecuacion $x^2 + y^2 = 3$ no tiene soluciones con $(x, y) \in \mathbb{Q}^2$.

Ecuaciones diofánticas y de congruencia

7. 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) $33X \equiv 27\ (45)$.

8. Determinar todos los $b \in \mathbb{Z}$ para los cuales existe $a \equiv 4\ (5)$ tal que $6a + 21b = 15$.

9. Hallar todos los $(a, b) \in \mathbb{Z}^2$ tales que $b \equiv 2a \pmod 5$ y $28a + 10b = 26$.

10. 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.

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

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

13. Hallar todos los $n \in \mathbb{N}$ para los cuales $n^3 + 4n + 5 \equiv n - 1\ (n^2 + 1)$.

14. Hallar todos los $n \in \mathbb{N}$ tales que $(3^{n+1} + 4^n : 4^{n+1} - 3^n) \neq 1$.

Teorema chino del resto

15. 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) $\begin{cases} a \equiv 1 & (6) \\ a \equiv 2 & (20) \\ a \equiv 3 & (9) \end{cases}$ iv) $\begin{cases} a \equiv 1 & (12) \\ a \equiv 7 & (10) \\ a \equiv 4 & (9) \end{cases}$

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

i) $\begin{cases} 3\,a \equiv 4 & (5) \\ 5\,a \equiv 4 & (6) \\ 6\,a \equiv 2 & (7) \end{cases}$ ii) $\begin{cases} 3\,a \equiv 1 & (10) \\ 5\,a \equiv 3 & (6) \\ 9\,a \equiv 1 & (14) \end{cases}$ iii) $\begin{cases} 15\,a \equiv 10 & (35) \\ 21\,a \equiv 15 & (8) \\ 18\,a \equiv 24 & (30) \end{cases}$

17. i) Sabiendo que los restos de la división de un entero a por 3, 5 y 8 son 2, 3 y 5 respectivamente, hallar el resto de la división de a por 120.

ii) Sabiendo que los restos de la división de un entero a por 6, 10 y 8 son 5, 3 y 5 respectivamente, hallar los posibles restos de la división de a por 480.

18. 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?

19. 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.

Pequeño teorema de Fermat

20. 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) $a = 5 \cdot 7^{2451} + 3 \cdot 65^{2345} - 23 \cdot 8^{138}$, $p = 13$.

21. Hallar todos los primos positivos p tales que $p \mid 2^p + 5$.

22. Resolver en $\mathbb{Z}$ las ecuaciones de congruencia

i) $7^{13}X \equiv 5\ (11)$, ii) $2^{194}X \equiv 7\ (97)$.

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

i) $728 \mid a^{27} - a^3$, ii) $\dfrac{2a^7}{35} + \dfrac{a}{7} - \dfrac{a^3}{5} \in \mathbb{Z}$.

24. *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.

25. Sean p y q dos primos positivos distintos y $a \in \mathbb{Z}$. Probar que si a es un entero coprimo con $p\,q$ entonces $p\,q \mid a^{(p-1)(q-1)} - 1$, y que para todo a vale $a \equiv a^{(p-1)(q-1)+1} \pmod{p\,q}$.

26. Sea p un primo, $p > 2$ y sea $a \in \mathbb{Z}$ tal que $p \nmid a$. Probar que $p^n \mid a^{(p-1)p^{n-1}} - 1$ para todo $n \in \mathbb{N}$.

Sugerencia: En el paso inductivo notar que $a^{(p-1)p^n} - 1 = (a^{(p-1)p^{n-1}})^p - 1^p$.

27.
i) Hallar el resto de la división de 3^{3603} por 5^3.
ii) Hallar el resto de la división de 7^{542} por 81.

28. Resolver en $\mathbb{Z}$ los siguientes sistemas lineales de ecuaciones de congruencia

i) $\begin{cases} 2^{2013}X \equiv 6 \ \ (13) \\ 5^{2013}X \equiv 4 \ \ (7) \\ 7^{2013}X \equiv 2 \ \ (5) \end{cases}$, ii) $\begin{cases} 10^{49}X \ \equiv 17 \ \ (39) \\ 5X \ \ \ \ \ \ \equiv 7 \ \ (9) \end{cases}$.

29. Hallar el resto de la división de

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

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

i) $539 \mid 3^{253}a + 5^{44}$, ii) $a^{236} \equiv 6\ (19)$.

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

32. Resolver en $\mathbb{Z}$ la ecuación de congruencia $7\,X^{45} \equiv 1 \pmod{46}$.

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

34.
i) Probar que $(3a^6 - 3 : 5a^6 + 2) = 1$ ó 7. Hallar todos los $a \in \mathbb{Z}$ para los cuales vale 7.
ii) Hallar todos los $a \in \mathbb{Z}$ tales que $(3a^7 - 3 : 5a^7 + 2) = 7$.
iii) Hallar todos los $a \in \mathbb{Z}$ tales que $(11a^6 + 1 : 90) = 5$.
iv) Sea $a \in \mathbb{Z}$ tal que $(9a^{25} + 10 : 280) = 35$. Hallar el resto de la división de a por 70.
v) Hallar todos los $a \in \mathbb{Z}$ tales que $(3a^{98} - 5a^{50} + 4 : 140\,a) = 14$.
vi) Hallar todos los enteros positivos a tales que $(4a^{62} - a : 11a) \neq a$.
vii) Para cada entero a hallar $(a^{18} + 413 : 3^2.5.7^3)$.

35. Demostrar que ninguna de las siguientes ecuaciones tiene soluciones enteras

i) $x^5 = y^2 + 4$. ii) $x^4 = y^3 + 7$. iii) $x^7 = y^4 + 2$. iv) $x^5 = y^3 + 12$.

36. *La función φ de Euler* (por el matemático suizo Leonhard Euler, 1707-1783, quién 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 $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6, \varphi(8) = 4, \ldots$

i) Sea p un primo. Probar que $\varphi(p) = p - 1$ y que $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$, $\forall\, k \in \mathbb{N}$.
ii) Sean p y q dos primos distintos. Probar que $\varphi(p\,q) = pq - p - q + 1 = (p-1)(q-1)$.
iii) Probar 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.

Nota: Resulta que la función φ 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 $\varphi(n)$ en general de una forma más económica que utilizando la factorización. Esto es un factor esencial del que depende la seguridad del sistema criptográfico RSA!

Problemas surtidos

37. Sea p un número primo impar, a y b enteros coprimos con p y n un número natural. Probar que si $p^\alpha \,||\, a - b,\ p^\beta \,||\, n$ y $\alpha \geq 1$ entonces $p^{\alpha+\beta} \,||\, a^n - b^n$.

Aclaración: La notación $p^k \,||\, m$ quiere decir que p^k es la mayor potencia de p que divide a m.

38. Vamos a probar que si $m, n \in \mathbb{N}$ son coprimos, entonces $\varphi(mn) = \varphi(m)\varphi(n)$: Para ello probaremos que hay una biyección entre $A_m \times A_n$ y A_{mn}, donde

$$A_l := \{k \in \mathbb{N} \,:\, k \leq l \text{ y } (k : l) = 1\}.$$

i) Probar que si $c \in \mathbb{N}$ es coprimo con mn y $x \equiv c \pmod{mn}$ entonces x es coprimo con m y x es coprimo con n.

ii) Por el Teorema Chino del Resto, dado $a \leq m$ y $b \leq n$, el sistema de ecuaciones de congruencia

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

determina un único $c \leq mn$ tal que $x \equiv c \pmod{mn}$ (por ser m y n coprimos). Probar que si a es coprimo con m y b es coprimo con n, entonces c es coprimo con mn.

iii) Entonces, a cada x le podemos asignar el correspondiente par $(r_m(x), r_n(x))$. Probar que dicha correspondencia es una biyección.

∗ **39**. Decimos que un punto de coordenadas enteras es *v*isible si no hay otro punto de coordenadas enteras entre él y el origen. Probar que para todo $n \in \mathbb{N}$ existe un cuadrado de $n \times n$ puntos de coordenadas enteras ninguno de los cuales es visible.

∗ **40**. i) Probar que para todo $t \in \mathbb{Q}$ el par

$$(x, y) = \left(\frac{t^2 - 4t - 1}{t^2 + 1},\ 2 - \frac{2t(2t+1)}{t^2 + 1} \right)$$

es solución de $x^2 + y^2 = 5$. Comparar con Ej. 6.

ii) Probar que, junto con $(1, -2)$, éstas son todas las soluciones racionales de $x^2 + y^2 = 5$.

∗ **41**. Sea p un número primo y $a_1, a_2, \ldots, a_{2p-1}$ una sucesión en $\mathbb{Z}$.

i) Supongamos que entre los a_i ningún resto módulo p aparece repetido más de $p - 1$ veces. Probar que para cada $k = 1, 2, \ldots, p$ existen k subsucesiones (no necesariamente disjuntas) de k elementos cada una, tales que al sumar todos los miembros de cada subsucesión se obtienen k resultados diferentes módulo p. Sugerencia: Inducción en k.

ii) Concluir que siempre existe una subsucesión de largo p de suma 0.

iii) Probar que dados $2n - 1$ números enteros, siempre se puede elegir n de ellos tales que su suma sea múltiplo de n.

∗ **42**. A un grupo de $N \geq 1$ prisioneros se le concede la oportunidad de ganarse el perdón. Saben que se los formará en fila con un sombrero cada uno, los sombreros llevarán escrito un número del 1 al k, con $k \in \mathbb{N}$ conocido, y cada uno sólo tendrá una única oportunidad para gritar un número. No pueden hablar dos o más a la vez. Serán liberados quienes digan el número de su propio sombrero.

Mostrar que pueden diseñar una estrategia que les asegure salvar a $N-1$ de ellos en el caso

i) $k = 2$.

ii) k arbitrario.

Aclaración: Cada prisionero sólo puede ver los números de los sombreros de aquellos prisioneros delante suyo en la fila. Nadie puede ver su propio sombrero.

El anillo $\mathbb{Z}/m\mathbb{Z}$

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

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

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

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

iii) Probar que si $\overline{a}$ es un elemento inversible de $\mathbb{Z}/m\mathbb{Z}$ tal que $\overline{a} = \overline{b}^2$, entonces $\overline{b}$ es inversible también en $\mathbb{Z}/m\mathbb{Z}$ 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 $\dfrac{p-1}{2}$ cuadrados no nulos en $\mathbb{Z}/p\mathbb{Z}$.

v) Probar que si $n \in \mathbb{N}$ es compuesto e impar, existen $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ con $\overline{a}^2 = \overline{b}^2$ y $\overline{a} \neq \pm\overline{b}$.

45. 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. 40 Práctica 3). ¿Vale lo mismo en $\mathbb{Z}/m\mathbb{Z}$ si m no es primo?

46. *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 $(n-1)!$ no es coprimo con n. ¿Qué implicación 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 $(p-1)! \equiv -1 \pmod{p}$.

47. 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).

48. *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. 47(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 $k = \log_g(a) \,(\mathrm{mod}\, p) \;\Leftrightarrow\; 0 \leq k < p-1$ 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) Para el taller: armar un programa que calcule $\log_g(a) \,(\mathrm{mod}\, p)$ 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).

49. *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.

∗ **50**. Sea $a > 1$ un entero y p un número primo impar.

i) Demostrar que los divisores primos impares de $a^p - 1$ dividen a $a-1$ o son de la forma $2pk+1$.

ii) Demostrar que los divisores primos impares de $a^p + 1$ dividen a $a+1$ o son de la forma $2pk+1$.

iii) Demostrar que hay una cantidad infinita de números primos de la forma $2pk + 1$.

∗ **51**. i) Demostrar que la sucesión $1, 5, 5^2, \ldots, 5^k, \ldots,\ k = 0, 1, \ldots$ recorre 2^n restos distintos módulo 2^{n+2}, para todo $n \geq 0$.

ii) Demostrar que todo número impar es congruente módulo 2^{n+2} a uno de la forma $\pm 5^k$.

∗ **52**. Sean $a, n \in \mathbb{N}$ con $a > 1$. Demostrar que $\varphi(a^n - 1)$ es multiplo de n.