

Tema 2: TEORÍA DE NÚMEROS.

1. Probar que: $\forall a, b \in \mathbb{Z} \Rightarrow |a - b| \geq ||a| - |b||$ y $|a + b| \leq |a| + |b|$.
2. Pruébese que:
 - a) Si $a, b \in \mathbb{Z}$ con $a \neq 0$ y $a|b$ entonces $a|bx, \forall x \in \mathbb{Z}$.
 - b) Si $a, b, c \in \mathbb{Z}$ con $a \neq 0$ y $b \neq 0$ y $a|b$ y $b|c \Rightarrow a|c$.
 - c) Si $a, b, c \in \mathbb{Z}$ con $a \neq 0$ y $a|b$ y $a|c \Rightarrow a|(bx + cy), \forall x, y \in \mathbb{Z}$.
 - d) Si $a, b \in \mathbb{Z}$ con $a, b > 0$ y $a|b, \Rightarrow a \leq b$.
 - e) Si $a, b \in \mathbb{Z}$ con $a, b \neq 0$ y $a|b, \Rightarrow |a| \leq |b|$.
3. Pruébese que para cada $n \in \mathbb{N}$ se verifica que:
 - a) $\frac{n(n+1)(2n+1)}{6}$ es un número entero.
 - b) $1 + 3 + 5 + 7 + \dots + (2n - 1) = n^2$.
 - c) el número natural $4^{2n+1} + 3^{n+2}$ es múltiplo de 13.
 - d) si $n \geq 10$, entonces $n^3 < 2^n$.
4. Pruébese que para cada $n \in \mathbb{N}$ se verifica que:
 - a) $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$.
 - b) si $n \geq 3$, entonces $2n + 1 < n^2$.
 - c) $(2n)! < 2^{2n}(n!)^2$
5. Pruébese que para cada $n \in \mathbb{N}$ se verifica que:
 - a) $n^4 - 4n^2$ es divisible por 3.
 - b) $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$.
 - c) $1^3 + 2^3 + 3^3 + \dots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$.
 - d) si $n \geq 5$, entonces $n^2 < 2^n$.
6. Pruébese que:
 - a) la suma y producto de dos números enteros pares es un número entero par.
 - b) la suma de dos números enteros impares es un número entero par.
7. Pruébese que:

- a) el producto de dos números enteros impares es un número entero impar.
 - b) la suma de un número entero par y un número entero impar es un número entero impar.
 - c) el producto de un número entero par por un número entero impar es un número entero par.
8. Sean $a, b \in \mathbb{Z}$ y sea $m \in \mathbb{N}$ un divisor común de a y b . Pruébese que, si m se puede expresar como combinación lineal entera de a y b , entonces $m = \text{mcd}(a, b)$.
9. Sean a, b, c tres números naturales. Sea $d_1 = \text{mcd}(a, c)$ y $d_2 = \text{mcd}(b, c)$. Probar que, si $c|ab$, entonces, también $c|d_1d_2$.
10. Sean $a, b \in \mathbb{Z}$. Probar que, si $\text{mcd}(a, b) = 1$ entonces, o bien $\text{mcd}(a + b, a - b) = 1$, o bien $\text{mcd}(a + b, a - b) = 2$.
11. Sea p un número primo tal que $p > 3$. Demuéstrese que p se puede expresar de la forma:
- a) $4n + 1$ ó $4n + 3$, para algún $n \in \mathbb{N}$.
 - b) $6n + 1$ ó $6n + 5$, para algún $n \in \mathbb{N}$.
12. Calcular $d = \text{mcd}(1312, 800)$ y hallar los números enteros x e y tales que $d = 1312x + 800y$.
13. Calcular $d = \text{mcd}(1034, 999)$ y hallar los números enteros x e y tales que $d = 1034x + 999y$.
14. Calcular $d = \text{mcd}(312, 120)$ y hallar los números enteros x e y tales que $d = 312x + 120y$.
15. Calcular $d = \text{mcd}(13012, 300)$ y hallar los números enteros x e y tales que $d = 13012x + 300y$.
16. Calcular las soluciones enteras de las siguientes ecuaciones diofánticas:
- a) $28x + 36y = 44$.
 - b) $66x + 550y = 88$.
 - c) $x^2 - y^2 = 252$.
 - d) $x^2 - y^2 = 70$.
17. Calcular las soluciones enteras de las siguientes ecuaciones diofánticas:
- a) $21x + 6y = 34$.
 - b) $68x + 230y = 12$.
 - c) $x^2 - y^2 = 22$.
 - d) $x^2 - y^2 = 102$.

18. Calcular las soluciones enteras de las siguientes ecuaciones diofánticas:
- a) $18x + 16y = 24$.
 - b) $46x + 560y = 68$.
 - c) $x^2 - y^2 = 120$.
 - d) $x^2 - y^2 = 60$.
19. Determinar los valores de $c \in \mathbb{Z}$, con $0 < c < 10$ para los que la ecuación diofántica $84x + 990y = c$ tiene solución.
20. Los precios de dos tipos de productos son 18 y 33 euros por unidad. ¿Cuál es el número máximo y mínimo de unidades que se pueden haber vendido de cada producto si se han cobrado 639 euros?.
21. En un ordenador se ejecutan dos procesos A y B. Sabemos que el proceso A tarda 9 segundos menos que el proceso B. Un día que se ejecutan 19 procesos, el tiempo total empleado fue de 261 segundos. ¿Cuántos procesos de cada tipo se ejecutaron? ¿Cuánto tiempo tarda en ejecutarse cada proceso?
22. Demuéstrese que no existe un triángulo pitagórico cuyo área sea igual a la longitud de la hipotenusa. Encontrar un triángulo rectángulo que sí lo verifique.
23. Probar que 3, 4, 5 es la única solución de la ecuación $x^2 + y^2 = z^2$ en enteros positivos consecutivos.
24. Encontrar todos los triángulos pitagóricos cuyo área sea numéricamente igual a su perímetro.

25. Pruébese que la diferencia de dos cubos consecutivos no puede ser múltiplo de 3.
26. ¿Cuántas maneras devolver 2,30 euros con monedas de 20 y 50 cts existen? ¿Y con monedas de 10 y 50 cts?
27. De todas las maneras de obtener 3,15 euros con monedas de 5, 10, 20 y 50 cts, ¿cuál es la que tiene menos monedas? (Pista, se puede suponer que de 5 y 10 cts hay una o ninguna monedas).
28. En el diseño de una placa madre para computadores multiprocesador se consideran dos tipos de procesador, uno de 210x120 mm y otro de 175x180 mm.
- ¿Cual será el mínimo tamaño de placa para que no queden huecos en ella si la cubrimos totalmente con sólo procesadores del primer tipo o con sólo procesadores del segundo tipo.
 - Si se usan patillas de conexión equiespaciadas, ¿cual será la separación máxima entre ellas?
29. Un sistema en tiempo real recibe dos interrupciones derivadas de los tiempos de finalización de dos procesos concurrentes. La de prioridad más alta, se produce cada 36 ciclos de reloj y la de prioridad más baja cada 50 ciclos.
- Suponiendo que en el instante inicial se reciben las dos interrupciones, ¿Cada cuánto se sincronizarán?
 - Suponiendo que la primera interrupción se recibe en el instante inicial y la segunda tras 24 ciclos. ¿Cuánto tardarán en sincronizarse?.
 - Cuando se sincronizan, los datos de la de prioridad más baja se pierden, por tanto es como si no se hubiese ejecutado. Suponiendo de nuevo que en el instante inicial coinciden, ¿cómo influye al rendimiento del segundo proceso que se retrase la de prioridad más baja para que tarde 51 ciclos?
30. Un sistema en tiempo real recibe dos interrupciones derivadas de los tiempos de finalización de dos procesos concurrentes. La de prioridad más alta, se produce cada 36 ciclos de reloj y la de prioridad más baja cada 52 ciclos.
- Suponiendo que en el instante inicial se reciben las dos interrupciones, ¿Cada cuánto se sincronizarán?
 - Cuando se sincronizan, los datos de la de prioridad más baja se pierden, por tanto es como si no se hubiese ejecutado. Suponiendo que la primera se recibe en el instante inicial y la segunda en un instante t entre el inicial y el décimo ciclo. ¿Qué rendimiento medio tienen los dos procesos (número de ejecuciones por unidad de tiempo)?

31. Un sistema en tiempo real recibe dos interrupciones derivadas de los tiempos de finalización de dos procesos concurrentes. La de prioridad más baja, se produce cada 24 ciclos de reloj y la de prioridad más alta cada 46 ciclos.
- Suponiendo que en el instante inicial se reciben las dos interrupciones, ¿Cada cuánto se sincronizarán?
 - Suponiendo que la primera interrupción se recibe en el instante inicial y la segunda tras 2 ciclos. ¿Cuánto tardarán en sincronizarse?.
 - Cuando se sincronizan, los datos de la de prioridad más baja se pierden, por tanto es como si no se hubiese ejecutado. Suponiendo de nuevo que en el instante inicial coinciden, ¿cómo influye al rendimiento del segundo proceso que se retrase la de prioridad más baja para que tarde 53 ciclos?
32. Un sistema en tiempo real recibe dos interrupciones derivadas de los tiempos de finalización de dos procesos concurrentes. La de prioridad más baja, se produce cada 4 ciclos de reloj y la de prioridad más alta cada 6 ciclos.
- Suponiendo que en el instante inicial se reciben las dos interrupciones, ¿Cada cuánto se sincronizarán?
 - Cuando se sincronizan, los datos de la de prioridad más baja se pierden, por tanto es como si no se hubiese ejecutado. Suponemos que el de prioridad más baja dura al menos 2 ciclos de reloj, pero lo podemos retrasar hasta 6 ciclos de reloj. ¿Qué valor dará el rendimiento óptimo (mayor número de ejecuciones del proceso por unidad de tiempo), suponiendo que los dos se sincronizan en el instante inicial?
33. Un sistema en tiempo real recibe dos interrupciones derivadas de los tiempos de finalización de dos procesos concurrentes. La de prioridad más baja, se produce cada 4 ciclos de reloj y la de prioridad más alta cada 6 ciclos.
- Suponiendo que en el instante inicial se reciben las dos interrupciones, ¿Cada cuánto se sincronizarán?
 - Supongamos que el de prioridad más alta se recibe en el instante inicial y que podemos retrar el de prioridad más alta para que se reciba en el 2º, 3º, 4º o 5º ciclo de reloj a partir del instante inicial. De esos retrasos, ¿cuál es el que provoca que tarden más en sincronizarse? ¿Y menos?
34. Sean $m \in \mathbb{N}$ y $a, b, c, d \in \mathbb{Z}$. Probar que:
- $a \equiv a \pmod{m}, \forall a \in \mathbb{Z}$.
 - Si $a \equiv b \pmod{m}, \Rightarrow b \equiv a \pmod{m}$.
 - Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.
35. Sean $m \in \mathbb{N}$ y $a, b, c, d \in \mathbb{Z}$. Probar que:

- a) Si $a \equiv b \pmod{m}$, $\Rightarrow \forall x \in \mathbb{Z}$ se tiene que $(a+x) \equiv (b+x) \pmod{m}$ y $(a*x) \equiv (b*x) \pmod{m}$.
- b) Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m} \Rightarrow (a+c) \equiv (b+d) \pmod{m}$ y $(a*c) \equiv (b*d) \pmod{m}$.
36. Demostrar que $a^5 \equiv a \pmod{10}$, $\forall a \in \mathbb{N}$.
37. Demostrar que, si n es un entero impar, entonces, $n^2 \equiv 1 \pmod{8}$.
38. Probar que si m es un número entero, entonces $m^2 \equiv 0$ ó $m^2 \equiv 1 \pmod{4}$.
39. Demostrar que, para cada $n \in \mathbb{N}$, el número entero $23^{3n+2} - 7n + 4$ no es múltiplo de 7.
40. probar que para cada número natural n , el número $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ es un número natural.
41. Calcular qué día de la semana era el 10 de Noviembre del año 345.
42. Resolver las siguientes ecuaciones con congruencias:
- a) $3x \equiv 1 \pmod{19}$.
- b) $2x \equiv 6 \pmod{10}$.
- c) $6x + 3 \equiv 1 \pmod{10}$.
43. Resolver las siguientes ecuaciones con congruencias:
- a) $x \equiv 2 \pmod{5}$
 $2x \equiv 1 \pmod{7}$
 $3x \equiv 4 \pmod{11}$.
- b) $x + 2y \equiv 3 \pmod{7}$
 $3x + y \equiv 2 \pmod{7}$.
- c) $243x + 17 \equiv 101 \pmod{725}$.
- d) $3x + 9 \equiv 2 \pmod{5}$
 $2x - 5 \equiv 1 \pmod{3}$.
44. Resolver las siguientes ecuaciones con congruencias:
- a) $125x - 17 \equiv 42 \pmod{38}$.
- b) $2x \equiv 3 \pmod{5}$
 $6x \equiv 1 \pmod{10}$
 $x \equiv 3 \pmod{3}$.

c) $5x - 4 \equiv 2 \pmod{4}$
 $3x + 2 \equiv 2 \pmod{6}$
 $x \equiv 4 \pmod{10}$.

45. Resolver las siguientes ecuaciones con congruencias:

a) $15x + 6 \equiv 12 \pmod{34}$
 $3x - 5 \equiv 9 \pmod{10}$.

b) $x \equiv 2 \pmod{3}$
 $x \equiv 7 \pmod{5}$
 $x \equiv 2 \pmod{7}$.

c) $3x + 2y \equiv 2 \pmod{7}$
 $5x - y \equiv -3 \pmod{7}$.

46. Resolver las siguientes ecuaciones con congruencias:

a) $3x + 2y - z \equiv 2 \pmod{5}$
 $5x - y + 3z \equiv -1 \pmod{5}$
 $x + y + z \equiv 3 \pmod{5}$.

b) $x + 2y - 3z \equiv 2 \pmod{7}$
 $5x + 2y - 3z \equiv -2 \pmod{7}$
 $x - 4y + 5z \equiv 3 \pmod{7}$.

c) $3x \equiv 9 \pmod{15}$.

47. Resolver las siguientes ecuaciones con congruencias:

a) $3x - 1 \equiv 5 \pmod{7}$
 $2x \equiv 3 \pmod{11}$.

b) $3x + 1 \equiv 2 \pmod{5}$
 $x \equiv 3 \pmod{10}$.

c) $2x \equiv 4 \pmod{10}$
 $3x \equiv 1 \pmod{2}$.

48. Resolver las siguientes ecuaciones con congruencias:

a) $3x - 2y \equiv 5 \pmod{7}$
 $5x - y \equiv 3 \pmod{7}$.

b) $4x + 7y \equiv 3 \pmod{5}$
 $2x + 11y \equiv 9 \pmod{5}$.

49. Sea $a \in \mathbb{Z}$ y $m \in \mathbb{N}$. Probar que $a \equiv r \pmod{m}$, donde $r \in \mathbb{N}$ es el resto de dividir a entre m .
50. Sea $a \in \mathbb{Z}$ y $m \in \mathbb{N}$. Probar que, entonces: $a \equiv 0 \pmod{m}$, ó $a \equiv 1 \pmod{m}$, ó $a \equiv 2 \pmod{m}$, ó $a \equiv 3 \pmod{m}$, ó \dots , ó $a \equiv m - 1 \pmod{m}$.
51. Probar que para cada número natural $n \in \mathbb{N}$, se verifica que:
- $6|n^3 - n$.
 - $24|n^4 + 2n^3 - n^2 - 2$.
 - $57|7^{n+2} + 8^{2n+1}$.
52. Probar que si p es un número primo mayor que 5, entonces $p^2 - 1$ ó $p^2 + 1$ es divisible por 10.
53. Probar que si n es un número entero tal que 2 y 3 no lo dividen, entonces 24 divide a $n^2 - 1$.
54. Hallar el resto de dividir: 23^{84292} entre 7 ; 113^{34291} entre 5 ; 1249^{44725} entre 9 ; 4325^{2537} entre 9 ; 17325^{4728} entre 11 ; 1732^{2583} entre 13.

(De Wikipedia) Supóngamos que Alicia y Bob están comunicándose a través de un medio de transmisión inseguro (abierto), y Alicia quiere enviar un mensaje privado a Bob (o seguro). Usando RSA, Alicia tomará los siguientes pasos para la generación de la clave pública y privada:

- Seleccione dos números primos largos p y q de manera que $p \neq q$.
- Calcule $n = pq$.
- Calcule $\phi(n) = (p - 1)(q - 1)$.
- Seleccione un entero positivo e tal que el $1 < e < \phi(n)$ tales que e y $\phi(n)$ sean primos entre sí.
- Calcule d tal que $de \equiv 1 \pmod{\phi(n)}$.

La clave pública consiste en: n el módulo y e el exponente público.

La clave privada consiste en: n el módulo, d el exponente privado.

Alicia transmite la clave pública a Bob, y guarda la clave privada p y q son ocultos pues son los factores de n , y con éstos se podría calcular d a partir de e .

Encriptación de mensajes

Ejemplo rápido: Bob quiere enviar a Alicia un mensaje secreto que solo ella pueda leer.

Supongamos que Bob desea enviar un mensaje M a Alicia. Él cambia M en un número $m < n$. El mensaje codificado c se calcula:

$$c \equiv m^e \pmod{n}$$

Descriptación de mensajes

Alicia recibe c de Bob, y conoce su clave privada d . Ella puede recuperar m de c por el siguiente procedimiento:

$$m \equiv c^d \pmod{m}$$

(Ver justificación en Wikipedia)

55. Dados $p = 61$ y $q = 53$,
- Generar una clave pública y una clave privada y pasa la clave pública a un compañero.
 - Pide a tu compañero que codifique el mensaje 123.
 - Decodificar el mensaje que te pase tu compañero.
56. Dados $p = 29$ y $q = 53$,
- Generar una clave pública y una clave privada y pasa la clave pública a un compañero.
 - Pide a tu compañero que codifique el mensaje 123.
 - Decodificar el mensaje que te pase tu compañero.
57. Expresar:
- 1528 en base 7; 31112 en base 13 y 452128 en base 3522.
 - $(3541)_7$, $(58321)_{12}$, $(101111)_2$, en base 10.
58. Expresar:
- $(1352)_9$, $(1100111)_2$, $(340021)_5$, en base 7.
 - $(12011001)_3$; $(1000011)_2$; $(12301)_5$, en base 9.
59. Demuéstrese que $121_m = [(m + 1)^2]_{10}$ para $m \geq 3$.
60. Expresar 169_m en base 10 para $m \geq 10$.
61. Resolver las siguientes ecuaciones:
- $(124)_5 = (x)_9$.
 - $(12345)_6 = (x)_7$.
62. Resolver las siguientes ecuaciones:
- $(132)_x = (330)_5$.
 - $(10402)_5 = (23113)_x$.

63. Calcular las siguientes operaciones con números expresados en base 2: $101 + 1011$; $(111) * (101)$; $(11) * (1100 + 110)$; $(10101)^2 * (11)^3$.
64. Calcular las siguientes operaciones con números expresados en base 5: $13 + 23 + 33$; $(43) * (21)$.
65. Expresar los siguientes números en base 10: $(157'35)_8$, $(521'3421)_7$, $(34'152)_9$.
66. Expresar en base 3, 7 y 12 (respectivamente) los siguientes números: $135'28$, $25'359$, $31'5321$.
67. Obtener los criterios de divisibilidad por 4 y por 13 para un número entero expresado en base 10, y aplíquense estos criterios para determinar el menor número entero positivo de 5 cifras que es divisible por 4 y por 13.
68. Obtener los criterios de divisibilidad por 14 y por 9 para un número entero expresado en base 10, y aplíquense estos criterios para determinar el mayor número entero de 6 cifras que es divisible por 14 y por 9.
69. Obtener los criterios de divisibilidad por 9 y por 14 para número expresado en base 10 y aplíquense para obtener la cifra designada por x tal que el número $68x062$ sea divisible por 126.
70. Obtener el criterio de divisibilidad por 15 de un número expresado en base 10.
71. Obtener una generalización del criterio de divisibilidad por k de un número entero n expresado en base b y, como consecuencia, estudiar si $(53286)_9$ es divisible por 8.