Ejercicios Tema 3

1. 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 $\text{mcd}(a + b, a - b) = 2$.

2. 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 $n \in \mathbb{N}$.

3. Calcular $d = \text{mcd}(1312, 800)$ y hallar los números enteros x e y tales que $d = 1312x + 800y$.

   $\text{mcd}(1312, 800) = 12 = 11 * 1312 - 18 * 800$

4. Calcular $d = \text{mcd}(1034, 999)$ y hallar los números enteros x e y tales que $d = 1034x + 999y$.

   $\text{mcd}(1034, 999) = 1 = 314 * 1034 - 325 * 999$

5. Calcular $d = \text{mcd}(312, 120)$ y hallar los números enteros x e y tales que $d = 312x + 120y$.

   $\text{mcd}(312, 120) = 24 = 2 * 312 - 5 * 120$

6. Calcular $d = \text{mcd}(13012, 300)$ y hallar los números enteros x e y tales que $d = 13012x + 300y$.

   $\text{mcd}(13012, 300) = 4 = -8 * 13012 + 347 * 300$

7. Calcular las soluciones enteras de las siguientes ecuaciones diofánticas:

   a) $28x + 36y = 44$.

   $x = 44 + 9k$
   $y = -33 - 7k$
   para todo $k \in \mathbb{Z}$

   b) $66x + 550y = 88$.

   $x = -32 + 25k$
   $y = 4 - 3k$
   para todo $k \in \mathbb{Z}$

8. Calcular las soluciones enteras de las siguientes ecuaciones diofánticas:

   a) $21x + 6y = 34$.

   No tiene solución.

b) $68x + 230y = 12$.

$x = 264 + 115k$
$y = -78 - 34k$
para todo $k \in \mathbb{Z}$

9. Calcular las soluciones enteras de las siguientes ecuaciones diofánticas:

   a) $18x + 16y = 24$.

   $x = 12 + 8k$
   $y = -12 - 9k$
   para todo $k \in \mathbb{Z}$

   b) $46x + 560y = 68$.

   $x = -2482 + 280k$
   $y = 204 - 23k$
   para todo $k \in \mathbb{Z}$

10. Determinar los valores de $c \in \mathbb{Z}$, con $0 < c < 10$ para los que la ecuación diofántica $84x+990y = c$ tiene solución.

    $c = 6$

11. Pruébese que la diferencia de dos cubos consecutivos no puede ser múltiplo de 3.

    $(n+1)^3 - n^3 = 3n^2 + 3n + 1 \equiv_3 1$

12. Demostrar que $a^5 \equiv a \mod 10$, $\forall a \in \mathbb{N}$.

    Es equivalente a probar que $a^5 - a \equiv_{10} 0$.
    Como 2 y 5 son primos entre sí, por el Teorema Chino del Resto, esto es equivalente a probar que $a^5 - a \equiv_2 0$ y $a^5 - a \equiv_5 0$.
    Módulo 2: $0^5 - 0 \equiv_2 0$, $1^5 - 1 \equiv_2 0$.
    Módulo 5: $0^5 - 0 \equiv_5 0$, $1^5 - 1 \equiv_5 0$, $2^5 - 2 \equiv_5 0$, $3^5 - 3 \equiv_5 0$, $4^5 - 4 \equiv_5 0$.

13. Demostrar que, si n es un entero impar, entonces, $n^2 \equiv 1 \mod 8$.

14. Probar que si m es un número entero, entonces $m^2 \equiv 0$ ó $m^2 \equiv 1 \mod 4$.

15. Demostrar que, para cada $n \in \mathbb{N}$, el número entero $23^{3n+2} - 7n + 4$ no es múltiplo de 7.

16. Probar que para cada número natural n, el número $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ es un número natural.

17. Resolver las siguientes ecuaciones con congruencias:

    a) $3x \equiv 1 \mod 19$.

    $x \equiv_{19} 13$

    b) $2x \equiv 6 \mod 10$.

    $x \equiv_5 3$

    c) $6x + 3 \equiv 1 \mod 10$.

    $x \equiv_5 3$

18. Resolver las siguientes ecuaciones con congruencias:

    a) $x \equiv 2 \mod 5$
    $2x \equiv 1 \mod 7$
    $3x \equiv 4 \mod 11$.

    $x \equiv_{5*7*11} 2 * 77 * 3 + 4 * 55 * 6 + 5 * 35 * 6 \equiv 5 * 7 * 112062$

    b) $x + 2y \equiv 3 \mod 7$
    $3x + y \equiv 2 \mod 7$.

    $x \equiv_7 3,\ y \equiv_7 0$

    c) $243x + 17 \equiv 101 \mod 725$.

    $x \equiv_{725} 63$

    d) $3x + 9 \equiv 2 \mod 5$
    $2x - 5 \equiv 1 \mod 3$.

    $x \equiv_{3*5} 1 * 3 * 2 + 0 * 5 * 2 \equiv_{3*5} 6$

19. Resolver las siguientes ecuaciones con congruencias:

    a) $125x - 17 \equiv 42 \mod 38$.

    $x \equiv_{38} 33$

b) $2x \equiv 3 \bmod 5$
$6x \equiv 1 \bmod 10$
$x \equiv 3 \bmod 3$.

No tiene solución.

c) $5x - 4 \equiv 2 \bmod 4$
$3x + 2 \equiv 2 \bmod 6$
$x \equiv 4 \bmod 10$.

$x \equiv_{60} 10$

20. Resolver las siguientes ecuaciones con congruencias:

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

b) $x \equiv 2 \bmod 3$
$x \equiv 7 \bmod 5$
$x \equiv 2 \bmod 7$.

c) $3x + 2y \equiv 2 \bmod 7$
$5x - y \equiv -3 \bmod 7$.

21. Resolver las siguientes ecuaciones con congruencias:

a) $3x + 2y - z \equiv 2 \bmod 5$
$5x - y + 3z \equiv -1 \bmod 5$
$x + y + z \equiv 3 \bmod 5$.

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

c) $3x \equiv 9 \bmod 15$.

22. Resolver las siguientes ecuaciones con congruencias:

a) $3x - 1 \equiv 5 \bmod 7$
$2x \equiv 3 \bmod 11$.

b) $3x + 1 \equiv 2 \bmod 5$
$x \equiv 3 \bmod 10$.

c) $2x \equiv 4 \bmod 10$
$3x \equiv 1 \bmod 2$.

23. Resolver las siguientes ecuaciones con congruencias:

    a) $3x - 2y \equiv 5 \bmod 7$
    $5x - y \equiv 3 \bmod 7$.

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

24. Probar que para cada número natural $n \in \mathbb{N}$, se verifica que:

    a) $6|n^3 - n$.
    b) $24|n^4 + 2n^3 - n^2 - 2$.
    c) $57|7^{n+2} + 8^{2n+1}$.

25. Probar que si p es un número primo mayor que 5, entonces $p^2 - 1$ ó $p^2 + 1$ es divisible por 10.

26. Probar que si n es un número entero tal que 2 y 3 no lo dividen, entonces 24 divide a $n^2 - 1$.

27. Hallar el resto de dividir: 23^{84292} entre 7 ; 113^{34291} entre 5 ; 1249^{44725} entre 9.

    2, 2, 7

28. Hallar el resto de dividir: 4325^{2537} entre 9 ; 17325^{4728} entre 11 ; 1732^{2583} entre 13.

    2, 0, 1

29. Hallar el resto de dividir: 24^{84292} entre 14 ; 114^{34291} entre 50 ; 1269^{44725} entre 9.

    4, 14, 0

30. Hallar el resto de dividir: 4325^{2537} entre 15 ; 172325^{4728} entre 15 ; 1732^{2583} entre 16.

31. 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.

    10036

32. 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.

33. 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.

    685062

34. Obtener el criterio de divisibilidad por 15 de un número expresado en base 10.

    1,10,10,...

35. Obtener el criterio de divisibilidad por 8 de un número entero n expresado en base 9 y, como consecuencia, estudiar si $(53286)_9$ es divisible por 8.

    Criterio de divisibilidad: 1,1,... Resto de dividir entre 8: $5+3+2+8+6 \equiv_8 0$

36. 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?.

37. 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?

38. ¿Cuántas maneras devolver 2,30 euros con monedas de 20 y 50 cts existen? ¿Y con monedas de 10 y 50 cts?

39. 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).

40. 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.

    a) ¿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.

    b) Si se usan patillas de conexión equiespaciadas, ¿cual será la separación máxima entre ellas?

41. 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.

    a) Suponiendo que en el instante inicial se reciben las dos interrucciones, ¿Cada cuánto se sincronizarán?

    b) Suponiendo que la primera interrupción se recibe en el instante inicial y la segunda tras 24 ciclos. ¿Cuánto tardarán en sincronizarse?.

    c) 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?

42. 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.

    a) Suponiendo que en el instante inicial se reciben las dos interrucciones, ¿Cada cuánto se sincronizarán?

    b) 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)?

43. 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.

    a) Suponiendo que en el instante inicial se reciben las dos interrucciones, ¿Cada cuánto se sincronizarán?

    b) Suponiendo que la primera interrupción se recibe en el instante inicial y la segunda tras 2 ciclos. ¿Cuánto tardarán en sincronizarse?.

    c) 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?

44. 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.

    a) Suponiendo que en el instante inicial se reciben las dos interrucciones, ¿Cada cuánto se sincronizarán?

    b) 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?

45. 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.

    a) Suponiendo que en el instante inicial se reciben las dos interrucciones, ¿Cada cuánto se sincronizarán?

b) 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?

(De Wikipedia) Supongamos 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:

a) Seleccione dos números primos largos p y q de manera que $p \neq q$.

b) Calcule $n = pq$.

c) Calcule $\phi(n) = (p-1)(q-1)$.

d) Seleccione un entero positivo e tal que el $1 < e < \phi(n)$ tales que e y $\phi(n)$ sean primos entre sí.

e) Calcule d tal que $de \equiv 1 mod(\phi(n))$.

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:

$$c \equiv_n m^e$$

Desencriptación de mensajes

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

$m \equiv_n c^d$

(Ver justificación en Wikipedia)

46. Dados $p = 61$ y $q = 53$,

a) Generar una clave pública y una clave privada y pasa la clave pública a un compañero.

b) Pide a tu compañero que codifique el mensaje 123.

c) Decodificar el mensaje que te pase tu compañero.

47. Dados $p = 29$ y $q = 53$,

a) Generar una clave pública y una clave privada y pasa la clave pública a un compañero.

b) Pide a tu compañero que codifique el mensaje 123.

c) Decodificar el mensaje que te pase tu compañero.