Ejercicios Tema 1

1. Calcular el máximo común divisor de los siguientes pares de números:

   a) 1312, 800.
   b) 1034, 999.
   c) 312, 120.
   d) 13012, 300.

   $\mathrm{mcd}(1312, 800) = 12$, $\mathrm{mcd}(1034, 999) = 1$, $\mathrm{mcd}(312, 120) = 24$, $\mathrm{mcd}(13012, 300) = 4$

2. Para cada uno de los siguientes pares de números, encontrar x e y que satisfagan la Identidad de Bezout:

   a) 1312, 800.
   b) 1034, 999.
   c) 312, 120.
   d) 13012, 300.

   $\mathrm{mcd}(1312, 800) = 12 = 11 * 1312 - 18 * 800$
   $\mathrm{mcd}(1034, 999) = 1 = 314 * 1034 - 325 * 999$
   $\mathrm{mcd}(312, 120) = 24 = 2 * 312 - 5 * 120$
   $\mathrm{mcd}(13012, 300) = 4 = -8 * 13012 + 347 * 300$

3. 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 $k \in \mathbb{Z}$

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

   No tiene solución.

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

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

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

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

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

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

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

$c = 6$

5. Resolver las siguientes ecuaciones con congruencias:

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

$x \equiv_{19} 13$

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

$x \equiv_{5} 3$

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

$x \equiv_{5} 3$

6. Resolver las siguientes ecuaciones con congruencias:

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

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

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

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

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

$x \equiv_{725} 63$

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

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

7. Resolver las siguientes ecuaciones con congruencias:

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

   $x \equiv_{38} 33$

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

   No tiene solución.

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

   $x \equiv_{60} 10$

8. 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) $3x + 2y \equiv 2 \bmod 7$
   $5x - y \equiv -3 \bmod 7.$

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

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

11. Resolver las siguientes ecuaciones con congruencias:

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

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

12. 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

13. 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.

14. 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

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

1,10,10,...

16. 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: $5+3+2+8+6 \equiv_8 0$

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

2, 2, 7

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

2, 0, 1

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

4, 14, 0

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

Problemas Tema 1

1. Sean $a, b \in \mathbb{Z}$. Probar que, si $\mathrm{mcd}(a,b) = 1$ entonces, o bien $\mathrm{mcd}(a+b, a-b) = 1$, o bien $\mathrm{mcd}(a+b, a-b) = 2$.

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. 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?.

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

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

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

6. 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: $0^5 - 0 \equiv_5 0$, $1^5 - 1 \equiv_5 0$, $2^5 - 2 \equiv_5 0$, $3^5 - 3 \equiv_5 0$, $4^5 - 4 \equiv_5 0$.

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

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

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

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

11. 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) $57|7^{n+2} + 8^{2n+1}$.

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

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

    (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)

14. 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.

15. 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.