UNIDAD III. TEORÍA DE NÚMEROS

3.1 DIVISIBILIDAD.

Un número es divisible entre otro cuando lo contiene exactamente un número entero de veces. *En otras palabras si un número divide a otro número, el cociente debe ser exacto*.

Definición : Sean *a* y *b* dos números enteros. Decimos que *a* divide a *b* (lo que simbolizamos con *a* **|** *b*) si existe un entero *c* tal que *b = (a)(c)*
Esto equivale a decir, que *b* es múltiplo de *a*. O que la división *b* ÷ *a* no deja residuo. Si *a* no divide a *b*, escribimos *a* ∤ *b*. Esto es lo mismo que decir que la división b÷ a deja residuo.

Ejemplos:
3**|**12 pues 12 = 4×3
4∤10 ya que no existe un entero c tal que 10 = 4c.
4 **|** 20 ya que si c = 5, 20 = 4c.
3**|**0 dado que 0 = 3c cuando c = 0.
1**|** 5 puesto que 5 = 1×5
5∤1 dado que 1 ≠ 5c para cualquier entero c.
Para cualquier entero *a*, *a*+ l **|** a^2 - l. Ya que a^2 - 1 = (*a*+ l)×k , con k = *a* - l.

Números primos

Un número entero *P* es primo si es un número mayor que 1 y los únicos enteros que lo dividen son 1, -1, *P* y *–P*. A los números de la forma *–P* donde es un primo les llamaremos primos negativos
Por ejemplo:

5, es divisible por (1, -1, 5, -5), primo positivo.
-5, es divisible por (1, -1, 5, -5), primo negativo.

La sucesión de los números primos, (positivos), comienza con 2, 3, 5, 7, 11, 13, 17, ...

Hay infinitos números primos, es decir, existen números primos tan grandes como se quiera. La distribución de los números primos es muy irregular. Hay algunos que son números impares consecutivos, como 3 y 5; estos se llaman ***primos gemelos***.
El MCD de dos enteros *a y b* es el mayor entero positivo que divide a *a* y *b* con resto cero. Si el MCD de dos enteros es 1, se dice que los dos números son ***primos relativos*** o ***primos entre sí***.A los números que son el producto de dos o más primos les llamaremos ***compuestos***.

Teorema Fundamental de la Aritmética

Todo entero n > 1 puede descomponerse de manera única como un producto de potencias de números primos de la siguiente manera:

$$n = p_1^{a_1} p_2^{a_2} .... p_n^{a_n}$$

donde las p_1, p_2, ..., p_n son primos tal que:
$p1 < p2 < ... < pn$ y a_1, a_2, ..., a_n son enteros positivos.
Por ejemplo:
$252 = 2^2 \times 3^2 \times 7$
$825 = 3 \times 5^2 \times 11$
$46137 = 3 \times 7 \times 13^3$

Criterios de divisibilidad

A continuación damos algunos criterios de divisibilidad que facilitan la búsqueda de los factores primos.

Divisibilidad por 2
Un número es divisible por 2 cuando termina en cero o cifra par.

Divisibilidad por 3
Un número es divisible por 3 cuando la suma de sus dígitos es un múltiplo de 3. Por ejemplo: 168351 es divisible por 3 pues 1 + 6 + 8+ 3 + 5 + 1 = 24, el cuál es múltiplo de 3.

Divisibilidad por 5
Un número es divisible por 5 cuando termina en cero o en cinco.

Divisibilidad por 7
Un número es divisible por 7 cuando separando la primera cifra de la derecha, multiplicándola por 2, restando este producto de lo que queda a la izquierda y así sucesivamente, da cero o múltiplo de 7.
Veamos un ejemplo: ¿2401 es divisible por 7?
240_1 x 2 = 2, 240 - 2 = 238, 23_8 x 2 = 16, 23 - 16 = 7.
Entonces, 2041 sí es divisible por 7. Verifiquemos:
2401 / 7 = 343.

Divisibilidad por 11
Un número es divisible por 11 cuando la diferencia entre la suma de los dígitos que ocupan un lugar impar, y la suma de los dígitos de lugar par, (puede ser de derecha izquierda ó inversamente es decir, que la diferencias pudiera dar negativa), es cero o múltiplo de 11.

Por ejemplo. Veamos si 94378 es divisible por 11:
9437, de derecha a izquierda:
Pares (subrayados): 4 y 7, 4 + 7 = 11
Impares: 9, 3 y 8, 9 + 3 = 12
Impares - Pares = 12 - 11 = 1, luego 9437 no es divisible por 11. (Verifíquelo)

Divisibilidad por 13, 17 y 19

El procedimiento para investigar la divisibilidad por 13, 17 y 19 es similar al de la divisibilidad por 7, sólo que al separar la primera cifra de la derecha, ésta se multiplica por 9, 5 y 17 respectivamente; siendo un número divisible por 13, 17 y 19 si al final del proceso sobra un cero o un múltiplo de 13, cero o un múltiplo de 17, cero o un múltiplo de 19.

Ejemplo. Investigar la divisibilidad de 1501.
Con 13:
150_1 x 9 = 9, 150 - 9 = 141, 14_1 x 9 = 9, 14 - 9 = 5.
No es divisible por 13.
Con 17:
150_1 x 5 = 5, 150 - 5 = 145, 14_5 x 5 = 25, 14 - 25 = -11.
No es divisible por 17.
150_1 x 17 = 17, 150 - 17 = 133, 13_3 x 17 = 51, 13 - 51 = -38.
Si es divisible por 19. Verifiquemos:
1501 / 19 = 79.

3.2 MÍNIMO COMÚN MÚLTIPLO (MCM) Y MÁXIMO COMÚN DIVISOR (MCD)

En ocasiones es conveniente conocer el menor de los múltiplos comunes (MCM), y el mayor de los divisores comunes (MCD) de varios números enteros. La regla de obtener dichos números es:

- Para encontrar el MCM de varios números enteros se multiplican los factores primos comunes y no comunes de los números tomados con sus mayores exponentes.
- Para encontrar el MCD de varios números enteros se multiplican los factores primos comunes de los números tomados con sus menores exponentes.

Si m es el MCD de a y b esto se denotará por m = (a, b); otra manera de calcular el MCD es usando el ***algoritmo de Euclides***, el cual se basa en la siguiente propiedad:

Si m = (a, b) y a = bq + r con $0 \leq r < b$, entonces m = (b, r).

Y consiste en lo siguiente:
Dividimos a / b obteniendo un residuo r_1, después dividimos b / r_1 y obtenemos un residuo r_2, a continuación dividimos r_1 / r_2 obteniendo un residuo r_3, y así sucesivamente hasta llegar a un residuo cero, el MCD de a y b será el último residuo diferente de cero.
El algoritmo de Euclides se incluye aquí debido a su utilidad en la demostración de algunos teoremas importantes de la divisibilidad entre enteros.

Ejemplos. Usando el ***algoritmo de Euclides***, encontrar el MCD de:

a) 328 y 1804;
b) 105 y 385

a) 1804 / 328 = 5 y resto = 164
328 / 164 = 2 y resto = 0 Por lo tanto (1804, 328) = 164

b) 385 / 105 = 3 y resto = 70
105 / 70 = 1 y resto = 35
70 / 35 = 2 y resto = 0 Por lo tanto (385, 105) = 35

Otra propiedad importante de el MCD es que:

Si $a > b$ $(a,b) = (b,a-b)$.

Ejemplo. Calcular (1001,1000)
Solución: (1001,1000) = (1000,1001 –1000) = (1000,1) = 1.

3.3 CONGRUENCIAS

Con el fin de motivar el concepto de **congruencia**, analizaremos los siguientes dos problemas.

Ejemplo 1. Se tiene un edificio de dos pisos con los cuartos numerados como en la siguiente figura:

Piso 2	2	4	6	8	.	.	.	.	.	.	.	.	.
Piso 1	1	3	5	7	.	.	.	.	.	.	.	.	.

¿En que piso localizamos el cuarto No. 98?
Solución: Localizamos el cuarto 98 en el piso 2, pues claramente observamos que en el primer piso están los cuartos con números impares y en el segundo piso los de números pares.

Ejemplo 2. Se tiene un edificio de cinco pisos con los cuartos numerados como en la siguiente figura:

Piso 5	4	9	14	19	24	…	.	.	.	.	.	.	.	.	.
Piso 4	3	8	13	18	23	…	.	.	.	.	.	.	.	.	.
Piso 3	2	7	12	17	22	…	.	.	.	.	.	.	.	.	.
Piso 2	1	6	11	16	21	…	.	.	.	.	.	.	.	.	.
Piso 1	0	5	10	15	20	…	.	.	.	.	.	.	.	.	.

¿En qué piso localizamos el cuarto No. 98?
Solución: En el problema anterior, por su sencillez, pudimos mentalmente dividir al conjunto de los enteros (positivos) en dos clases ajenas: pares e impares. En este segundo problema tenemos que dividirlos en 5 clases ajenas y ser capaces de ubicar a cualquier entero en alguna de ellas.

Si observamos detenidamente la figura, podemos ubicar a los cuartos de la siguiente manera:

No. de Piso	*Característica*	*Forma*
5	Los que exceden en cuatro unidades a un múltiplo de 5	5k+4
4	Los que exceden en tres unidades a un múltiplo de 5	5k+3
3	Los que exceden en dos unidades a un múltiplo de 5	5k+2
2	Los que exceden en una unidad a un múltiplo de 5	5k+1
1	Múltiplos de 5	5k

Nota: k = 0,1,2,3,...
Después de este pequeño análisis, podemos decir que el cuarto No. 98 se encuentra en el cuarto piso, puesto que 98 = 5(19) + 3.
Obsérvese que los del primer piso son aquellos que al dividirse entre 5 dejan residuo cero, los del segundo piso son aquellos que al dividirse entre 5 dejan residuo 1 y así sucesivamente.

Si consideramos el *conjunto de los enteros*, con este criterio podemos dividirlos en 5 clases:

C_0 = {…,-15, -10, -5, **0**, 5, 10, 15,…}
C_1 = {…, -14, -9, -4, **1**, 6, 11, 16,…}
C_2 = {…, -13, -8, -3, **2**, 7, 12, 17,…}
C_3 = {…, -12, -7, -2, **3**, 8, 13, 18,…}
C_4 = {…, -11, -6, -1, **4**, 9, 14, 119,…}.

La característica de la clase C_r es que al dividirse cualquiera de sus elementos entre cinco, deja residuo r.
Si dos enteros pertenecen a la misma clase, diremos que ellos son congruentes módulo 5 en este ejemplo.

Definición. Decimos que los enteros *a* y *b* son congruentes módulo m, m>0 si al dividirse entre m dejan el mismo residuo, y lo denotaremos como

$$a \equiv b \pmod{m}.$$

Teorema 1. $a \equiv b \pmod{m}$ si y sólo si m|b-a.

Teorema 2. La relación congruencia módulo m tiene las siguientes propiedades:

1. $a \equiv a \pmod{m}$.
2. Si $a \equiv b \pmod{m}$ entonces $b \equiv a \pmod{m}$.
3. Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$ entonces $a \equiv c \pmod{m}$.

Es de esperarse, en vista del teorema anterior, que las congruencias se comporten en muchos aspectos como igualdades. Esta semejanza queda ilustrada en el siguiente teorema:

Teorema 3. Sean a, b, c enteros y m entero positivo.

1. Si a≡ b (mod m) entonces:
   a) $a + x \equiv b + x \pmod{m}$ para todo entero *x.*
   b) $ax \equiv bx \pmod{m}$ para todo entero *x.*
2. Si a≡ b (mod $_m$) y c≡ d (mod $_m$), entonces:
   a) $a + c \equiv b + d \pmod{m}$.
   b) $a-c \equiv b-d \pmod{m}$.
   c) $ac \equiv bd \pmod{m}$.
   d) $a^n \equiv b^n \pmod{m}$ para todo entero positivo *n*.

Ejemplo.
Al dividir los números 3, 13, 23, 33 entre 10, sobra 3 por lo que decimos que ellos son congruentes modulo 10.
Para ilustrar una parte del teorema 3 utilizamos $3 \equiv 13 \pmod{10}$ y $23 \equiv 33 \pmod{10}$. Entonces podemos sumar las congruencias como lo indica el teorema y resulta otra congruencia.
Sumando obtenemos $3 + 23 \equiv 13 + 33 \pmod{10}$.
Esto es lo mismo que $26 \equiv 46 \pmod{10}$. Podemos ver que 26 y 46 son congruentes módulo 10, ya que al dividirlos entre 10 dejan residuo 6.

TEORÍA DE NÚMEROS
EJERCICIOS

1. Alicia va al club cada día, Beatriz va cada 2 días, Carlos va cada 3, Daniel cada 4, Enrique cada 5, Francisco cada 6 y Gabriela cada 7. Si hoy están todos en el club, ¿Dentro de cuántos días volverán a reunirse?

2. En un concurso de baile los jueces califican a los competidores con números enteros. El promedio de las calificaciones de un competidor es 5.625. ¿Cuál es el número mínimo de jueces para que eso sea posible?

3. La maestra distribuyó la misma cantidad de dulces entre cada uno de 5 niños y se quedó tres para ella misma. No se acuerda cuántos dulces tenía, pero se acuerda que era un múltiplo de 6 entre 65 y 100. ¿Cuántos dulces tenía?

4. 96 niños en un campamento de verano van a separarse en grupos de forma que cada grupo tenga el mismo número de niños. ¿De cuántas maneras puede hacerse la separación si cada grupo debe de tener más de 5 pero menos de 20 niños?

5. Al hacer la división de 1 entre 5^{2000}, ¿cuál será el último dígito que aparezca antes de llegar a puros ceros?

6. Un número entero positivo es múltiplo de exactamente 8 enteros positivos (incluyendo a él mismo y a la unidad). Si es múltiplo de 21 y de 35, ¿cuál es el número?

7. A Julio le dieron el número secreto de su nueva tarjeta de crédito, y observó que la suma de los cuatro dígitos del número es 9 y ninguno de ellos es 0; además el número es múltiplo de 5 y mayor que 1995. ¿Cuál es la tercera cifra de su número secreto?

8. ¿Cuántos números múltiplos de 6 menores que 1000 tienen la propiedad de que la suma de sus cifras es 21?

9. Un niño corta un cuadrado de tres días por tres días de la página de un calendario. Si la suma de las nueve fechas es divisible entre 10 y sabemos que la fecha de la esquina superior izquierda es múltiplo de 4, ¿cuál es la fecha de la esquina inferior derecha?

10. ¿Cuántas parejas de enteros positivos *a* y *b* satisfacen que $a^2 - b^2 = 15$?

11. Una sucesión se forma de la manera siguiente: el primer término es 2 y cada uno de los términos siguientes se obtiene del anterior elevándolo al cuadrado y restándole 1 (los primeros términos son 2, $2^2 - 1 = 3$, $3^2 - 1 = 8$, $8^2 - 1 = 63$, ...). La cantidad de números primos que hay en la sucesión es:

12. ¿Cuál de los siguientes números es más grande?

(a) 2^{12} (b) 4^{15} (c) 8^{11} (d) 12^8 (e) 32^6

13. ¿Cuántas cifras tiene el número $2^{1998} \times 5^{2002}$?

14. Andrés cuenta los números del 1 al 100 y aplaude si el número que dice es múltiplo de 3 o termina en 3. ¿Cuántas veces aplaudirá Andrés en total?

15. La suma de todos los dígitos del número $10^{99} - 99$ es:

16. Una "operación" consiste en multiplicar el número por 3 y sumarle 5, comenzando por el número 1. ¿Cuál es el dígito de las unidades después de aplicar la operación 1999 veces?

17. ¿Para qué valores enteros positivos de *n* la expresión $\frac{18}{n+4}$ es un entero?

18. Si *m* y *n* son enteros tales que $2m - n = 3$. Pruebe que $m - 2n$ es múltiplo de 3.

19. ¿Cuántas veces aparece el factor 2 en la descomposición en números primos de

$$1 + 2 + 3 + \ldots + 10^{11}?$$

20. Si (a, b) denota al MCD de a y b, ¿cuánto vale $(a^4 - b^4, a^2 - b^2)$?

21. Un sistema de engranes consta de tres ruedas dentadas, el engrane A tiene 4 dientes, el B tiene 6 dientes y el C tiene 8 dientes. En el engrane A se encuentra un motor que mueve todo el sistema.
    a. ¿Cuántas vueltas debe dar el engrane A para que los engranes vuelvan a su posición original?
    b. Cada engrane está conectado a una máquina que lleva el registro de cuántas vueltas completas ha dado su engrane; al momento en que la suma de los registros de las tres máquinas es 1997, ¿cuánto marca el registro de A?

22. Encuentre todas las parejas de números enteros a y b, tales que $a^2 - 10\,b^2 = 2$.

23. Encuentre dos números sin ceros y cuyo producto sea 1 000 000 000.

24. Sea a = bq + r. Si c|a y c|b, pruebe que c |r.

25. Pruebe que n es par si y sólo si n^2 es par. Nótese que los números pares son precisamente los múltiplos de 2 y por lo tanto que n sea par significa que n = 2k para algún k número entero.

26. Pruebe que $n^2 - n$ es par para todo entero n.

27. Pruebe que todo número primo de la forma 3 k + 1 también es de la forma 6 k + 1.

28. Demuestre que si n es impar entonces $8 \mid n^2 - 1$.

29. Una sala de cine tiene 26 filas con 24 asientos cada una. El total de los asientos se numera de izquierda a derecha, comenzando por la primera fila y hacia atrás. ¿En qué número de fila está el asiento número 375?

30. ¿Cuáles son los dos últimos dígitos de 7^{1998}?
    a) 01 b) 07 c) 43 d) 49

31. Una escalera tiene numerados los escalones como 0, 1, 2, 3, 4,.... Una rana está en el escalón 0, salta 5 hacia arriba al escalón 5 y luego dos para abajo hasta el escalón 3, después sigue saltando alternando 5 para arriba y dos para abajo. La sucesión de escalones que pisa la rana es 0, 5, 3, 8, 6,... ¿Cuál de los siguientes escalones *no pisa* la rana?
    a) 1997 b) 1998 c) 1999 d) 2000