REPUBLICA DE CHILE
MINISTERIO DE EDUCACION
CENTRO DE PERFECCIONAMIENTO, EXPERIMENTACION
E INVESTIGACIONES PEDAGOGICAS
DEPARTAMENTO DE MATEMATICA

teoría de números

prof.: césar burgueño m.

LO BARNECHEA, AGOSTO DE 1977.

MINISTERIO DE EDUCACION

CENTRO DE PERFECCIONAMIENTO
EXPERIMENTACION E
INVESTIGACIONES PEDAGOGICAS

Departamento de Matemática

Doc. Nº 16.153.-

TEORIA DE NUMEROS

PROF. CESAR BURGUEÑO MORENO

LO BARNECHEA, JULIO 1977.

- 0 - 0 - 0 - 0 - 0 -

P R E S E N T A C I O N

"La Matemática es una manera de pensar, una forma de razonamiento. Si bien habla en números, no es verdad aquello de que los números son fríos. Los números tienen calor y color, como tienen música y poesía"

El Departamento de Matemática del Centro de Perfeccionamiento, Experimentación e Investigaciones Pedagógicas tiene el agrado de entregar a los profesores de matemática del país este material curricular complementario sobre TEORIA DE NUMEROS" y que ha sido elaborado por el integrante de este Departamento, profesor CESAR BURGUEÑO MORENO.

El propósito fundamental de este material es permitir a nuestros colegas alcanzar mejores niveles de excelencia académicos y con ello contribuir a facilitar y mejorar su acción docente a nivel de aula, en los aspectos ligados con el texto que se presenta.

Se supone comúnmente que la aritmética es la rama más sencilla de la matemática. Nada más lejos de la verdad. El tema es difícil de plantear, aunque se admite que la práctica de la aritmética elemental es bastante fácil. Lo mismo puede decirse de la mayoría de las ciencias: no es necesario comprender la teoría electromagnética para instalar una lámpara, ni estudiar física para poder reparar una bomba. Podemos contar con nuestros dedos, y no damos importancia a las dificultades que implica este acto.

De la teoría de números, E.T. BELL dice: "es el último gran continente salvaje de la matemática". En esta teoría siempre hay algo nuevo. Desde hace 2500 años, aficionados al igual que profesionales, la han explorado; sin embargo, aún hay muchas razones para esperar que los descubrimientos futuros, con o sin ayuda de máquinas, superen los del pasado.

Llama la atención que la aritmética no tiene aún a su Descartes, por no decir su Newton. Sin embargo, tiene a un FERMAT, el "príncipe de los aficionados", ya que su diversión era la matemática y se acercó a ella como un aficionado, pero que desarrolló como maestro de maestros.

Apreciaremos todas las sugerencias y críticas constructivas que acerca de este trabajo hagan llegar nuestros colegas.
El Departamento de Matemática y, en especial, su autor las acogerán de muy buen grado, considerando que las experiencias obtenidas a nivel de sala de clases son las que mejor contribuyen a enriquecer un trabajo con las características del que presentamos.

TEODORO JARUFE ABEDRABU
Jefe
Departamento Matemática

I N D I C E

Pág.

- - - - - - - -

I.- D I V I S I B I L I D A D

Definición 1: Dados dos enteros a y b, a distinto de cero, se dice que b es divisible por a si existe un entero x tal que $b = ax$ (notación $a \mid b$: se lee "a divide a b"). Si no existe tal x, entonces se dice que b no es divisible por a (notación $a \nmid b$; se lee "a no divide a b")

Definición 2: Si a divide b y $0 < a < b$ se dice que a es un divisor propio de b

Observación: $a \mid 0$ para todo entero a distinto de cero; basta tomar $x = 0$ en la definición.

Teorema 1: Sean a, b, c enteros, entonces:

1.- $a \mid b \implies a \mid bc$ para todo entero c

2.- $a \mid b$ y $b \mid c \implies a \mid c$

3.- $a \mid b$ y $a \mid c \implies a \mid (bx+cy)$, para todo par de enteros x, y; en particular $a \mid (b+c)$

4.- $a \mid b$ y $b \mid a \implies a = \pm b$

5.- $a \mid b$, $a > 0$, $b > 0 \implies a \leq b$

Demostración:

1.- $a \mid b \implies$ hay entero x tal que $b = ax \implies bc = axc = a(xc)$
luego, $a \mid bc$

2.- $a \mid b \implies$ hay x tal que $b = ax$
$b \mid c \implies$ hay y tal que $c = by$
luego, $c = by = (ax)\, y = a(xy)$. Luego, $a \mid c$

3.- $a \mid b \implies b = ax \implies bx = axx$
$a \mid c \implies c = ay \implies cy = ayy$
$\therefore bx+cy = ax^2+ay^2 = a(x^2+y^2)$. Luego, $a \mid (bx+cy)$

4.- $a \mid b \implies b = ax$
$b \mid a \implies a = by$
Luego, $b = byx \implies yx = 1 \implies x = \pm 1$, $y = \pm 1$
Luego, $b = \pm a$

5.- $a \mid b \implies b = ax \implies x > 0$, pues si no, se tendría que $b < 0$, lo que es una contradicción.
Luego, $a \leq b$

Teorema 2: (Algoritmo de división)
Dados dos enteros a, b, con $a > 0$, entonces existen enteros q y r únicos tales que $b = q\,a+r$ con $0 \leq r < a$

Demostración:

Considere la progresión aritmética
....., b-3a, b-2a, b-a, b, b+a, b+2a, b+3a, ...

En esta sucesión seleccionamos el miembro no negativo menor y lo denotamos por r (∴ $0 \leq r < a$)

Por otra parte, r es un elemento de la sucesión y es de la forma $r = b-qa$; luego, $b = qa+r$, con $0 \leq r < a$

Definición 3: Se dice que a es divisor común de b y c si $a \mid b$ y $a \mid c$

Como hay sólo un número finito de divisores de cualquier entero distinto de cero, entonces hay sólo un número finito de divisores comunes de b y c.

Definición 4: Sean b, c enteros, uno de ellos no nulo.
Sean $a_1 < a_2 < \ldots\ldots < a_n$ los divisores comunes de b y c. Entonces a_n se llama máximo común divisor de b y c (es decir es el mayor de los divisores comunes de b y c)

Notación: máximo común divisor de b y c = : (b,c)

Observación: Se desprende de la definición, que un entero a_n es el máximo común divisor de b y c (no ambos nulos) si:
i) $a_n \mid b$ y $a_n \mid c$
ii) si $k \mid b$ y $k \mid c \Longrightarrow k \mid a_n$

Teorema 3: Sea g el máximo común divisor de b y c. Entonces hay enteros x, y, tales que $g = (b,c) = (bx+cy)$.
(Demostración: ver bibliografía)

Teorema 4: El máximo común divisor de dos enteros, no ambos nulos, es único.

Demostración:

Sean g y g' dos máximos comunes divisores de b y c; luego por la parte (ii) de la observación tenemos que:

$$\left.\begin{array}{l} g' \mid b \quad y \quad g' \mid c \Longrightarrow g' \mid g \\ g \mid b \quad y \quad g \mid c \Longrightarrow g \mid g' \end{array}\right\} \Longrightarrow g = g'$$

Teorema 5: Algoritmo de Euclides (método para encontrar el máximo común divisor)

Dados los enteros b y c > 0, se hace una aplicación repetida del algoritmo de la división y obtenemos la serie de ecuaciones:

$$(*)\quad \begin{cases} b = cq_1+r_1, & 0 < r_1 < c \\ c = r_1q_2+r_2, & 0 < r_2 < r_1 \\ r_1 = r_2q_3+r_3, & 0 < r_3 < r_2 \\ \quad - - - - - - - - \\ r_{j-2} = r_{j-1}q_j+r_j, & 0 < r_j < r_{j-1} \\ r_{j-1} = r_jq_{j+1} \end{cases}$$

Entonces, $(b,c) = r_j$

Los valores de x_o, y_o en $(b,c) = (bx_o+cy_o)$ pueden obtenerse eliminando $r_1, r_2, \ldots, r_{j-1}$ en el conjunto de ecuaciones (*).

Demostración:

La cadena de ecuaciones se obtiene de la siguiente manera:

1.- Se divide b por c y se obtienen q_1, r_1 con $0 < r_1 < c$

2.- Se divide c por r_1 y se obtienen q_2, r_2 con $0 < r_2 < r_1$

3.- Se divide r_1 por r_2 y se obtienen q_3, r_3 con $0 < r_3 < r_2$

- - - - - -

El proceso se detiene cuando la división es exacta, es decir cuando el residuo es cero.

Ahora debemos probar que r_j es el máximo común divisor de b y c.

Sea $g = (b,c) = bx_o+cy_o$ Por demostrar: $g = r_j$

$g = (b,c) \Longrightarrow g \mid b \quad y \quad g \mid c$

$$g \mid b \quad y \quad g \mid c \xrightarrow{\text{ec.1}} g \mid r_1$$

$$g \mid c \quad y \quad g \mid r_1 \xrightarrow{\text{ec.2}} g \mid r_2$$

$$g \mid r_1 \quad y \quad g \mid r_2 \xrightarrow{\text{ec.3}} g \mid r_3$$

Así, sucesivamente vemos que $g \mid r_j$

Por otra parte, de la ecuación final tenemos que $r_j \mid r_{j-1}$.

Luego, de la penúltima ecuación tenemos que $r_j \mid r_{j-2}$.

Así, sucesivamente vemos que $r_j \mid b$ y $r_j \mid c$

Por lo tanto $r_j \mid g$

Luego, tenemos que: i) $g \mid r_j$ de la primera parte y

ii) $r_j \mid g$ de la última parte.

Luego, $g = r_j$

Para determinar x_o, y_o de tal manera que $r_j = bx_o + cy_o$ basta eliminar r_1 mediante las dos primeras ecuaciones, a continuación eliminar r_2 entre la ecuación resultante y la tercera.

Procediendo con las eliminaciones sucesivas de r_3, r_4, ..., r_{j-1} se obtiene r_j en la forma $(bx_o + cy_o)$

Ejemplo: Sea $b = 963$ y $c = 657$

$963 = 657 \cdot 1 + 306$ con $0 < 306 < 657$

$657 = 306 \cdot 2 + 45$ con $0 < 45 < 306$

$306 = 45 \cdot 6 + 36$ con $0 < 36 < 45$

$45 = 36 \cdot 1 + 9$ con $0 < 9 < 36$

$36 = 9 \cdot 4 + 0$

Luego, el máximo común divisor entre 963 y 657 es 9, es decir $(963, 657) = 9$

Además, eliminando 36, 45 y 306 en las ecuaciones anteriores, podemos encontrar enteros x_o, y_o tales que $9 = 657x_o + 963y_o$

En efecto:

$$\begin{aligned} 9 &= 45-36 \\ &= 45-(306-45\cdot 6) \\ &= -306+7\cdot 45 \\ &= -306+7(657-306\cdot 2) \\ &= 7\cdot 657-15\cdot 306 \\ &= 7\cdot 657-15(963-657) \\ &= 22\cdot 657-15\cdot 963 \end{aligned}$$

es decir, $x_o = 22$, $y_o = -15$

Ejercicios:

1.- Aplicando el algoritmo de Euclides, encontrar el máximo común divisor de:

a) 1272 y 84
b) 4488 y 891
c) 3244 y 292
d) 1618 y 113

2.- Encontrar el máximo común divisor de los números 1384 y 6912, y a continuación encontrar enteros x_o, y_o, que satisfagan

$$1384\, x_o + 6912 \cdot y_o = d$$

3.- Encontrar enteros x, y, de tal manera que:

a) $178x+269y = 5$
b) $224x+379y = 17$
c) $37x+49y = 15$
d) $56x+78y = 2$

Definición 5: Un entero $p > 1$ se llama número primo, si no hay divisor d de p con $1 < d < p$
Si un entero $a > 1$ no es primo, entonces se dice compuesto.
Son números primos: 2, 3, 5, 7, 11, 13, 17, 19, 23 ...
Son números compuestos: 4, 6, 8, 9, 10, 12, 14, 15, 16, ...

Definición 6: Dos enteros a y b se dicen relativamente primos, si el máximo común divisor entre ellos es uno; es decir, si $(a,b) = 1$

Teorema 6: Todo entero n mayor de 1 puede expresarse como producto de números primos.

Demostración:

Si n es primo: nada que demostrar
Si n no es primo, entonces hay $n_1 \in \mathbb{Z}$ con $1 < n_1 < n$ tal que n_1 divide a n, es decir $n = n_1 \cdot n_2$ con $1 < n_1 < n$, $1 < n_2 < n$
Si n_1 y n_2 son números primos, entonces está listo.
Si n_1 no es primo, entonces hay $n_3 \in \mathbb{Z}$ tal que n_3 divide a n_1; es decir, $n_1 = n_3 \cdot n_4$ con $1 < n_3 < n_1$, $1 < n_4 < n_1$
De la misma forma se procede con n_2 y así sucesivamente.
Este proceso termina, pues cada uno de los factores que aparecen son mayores que uno y menores que n.
Observando que los factores primos que aparecen no son necesariamente distintos, se tiene que el entero n se puede escribir de la forma:

$$n = P_1^{t_1} \cdot P_2^{t_2} \text{ ----- } P_r^{t_r} \quad \text{donde } P_1, P_2, \text{---}, P_r$$

son números primos distintos y $t_1, t_2, \text{---}, t_r$ enteros mayores o iguales que uno.

Ejemplo: $180 = 2^2 \cdot 3^2 \cdot 5$

Teorema 7: Si $p \mid ab$, con p primo, entonces $p \mid a$ o $p \mid b$.

Demostración:

Por teoremas anteriores, podemos escribir los enteros a y b en la forma

$$a = P_1^{t_1} \text{ --- } P_r^{t_r} \qquad P_i \text{ primo}, \ 1 \leq t_i \qquad i = 1,2,\ldots,r$$

$$b = q_1^{u_1} \text{ --- } q_s^{u_s} \qquad q_i \text{ primo}, \ 1 \leq u_i \qquad i = 1,2,\ldots,s$$

Supongamos $P \nmid a$; por demostrar $p \mid b$
$P \nmid a$ luego $p \neq p_1, P_2 \text{ ---}, p_r$ pues $p, p_1, p_2, \ldots p_r$ son primos.

Por otra parte, como $p \mid ab = P_1 \cdot \ldots \cdot P_r \cdot q_1 \cdot \ldots \cdot q_s$ tenemos que $p = q_i$ algún i, $1 \leq i \leq s$ luego $p \mid b$

Teorema 8: . Hay infinitos números primos.

Demostración:

Supongamos que hay sólo un número finito de números primos que designaremos por: $p_1, p_2, \ldots, p_r$ y formenos el número

$n = 1+p_1 \cdot p_2 \cdot \ldots \cdot p_r$

Si alguno de los p_i $(i = 1, \ldots r)$ divide a n entonces por teorema 1, parte 3, tenemos que $p_i \mid 1$ contradicción.

Luego, n es primo o bien es un número compuesto divisible por un primo distinto de $p_1, p_2, \ldots, p_r$

Es decir, en ambos casos obtenemos un nuevo número primo distinto de $P_1, P_2, \ldots, P_r$. Luego, hay infinitos primos.

Ejercicio:

Demuestre que es posible encontrar sucesiones, arbitrariamente grandes, de enteros consecutivos que no contienen números primos. (Por ejemplo: 40.322, 40.323 40.324, 40.325, 40.326, 40.327, 40.328 es una sucesión de siete enteros consecutivos y ninguno de ellos es primo, pues son divisibles por 2, 3, 4, 5, 6, 7, 8 respectivamente)

Ejercicios:

1.- Demuestre que cualquier primo de la forma 3k+1 es también de la forma 6k'+1 con k, k' $\in \mathbb{N}$

2.- Demuestre que la suma de un número par de enteros impares es par.

3.- Demuestre que todo entero no divisible por 3 es de la forma 3n+1 o 3n+2.

4.- Pruebe que si f(x) es un polimonio con coeficiente enteros, y si a es un entero diferente de cero, tal que f(a) = 0, entonces a divide al termino constante.

II.-C O N G R U E N C I A S

Definición 7: Sean a, b $\in$ Z. Si un entero m, distinto de cero, divide a la diferencia a-b, entonces se dice que a es congruente con b módulos m y se escribe $a \equiv b \pmod{m}$

Ejemplo: $7 \equiv 1 \pmod{3}$ pues 3 divide a 7-1 = 6

Si m no divide a la diferencia a-b, entonces se dice que a no es congruente con b módulo m y se escribe $a \not\equiv b \pmod{m}$ es decir: $a \equiv b \pmod{m}$ si y sólo si $a-b = k \cdot m$, para algún entero k.

$a \not\equiv b \pmod{m}$ si y sólo si $a-b \neq k \cdot m$, $\forall k \in Z$

Observación: Es claro que si m divide a la diferencia a-b, entonces -m también divide a la diferencia a-b. Luego, sin perdida de generalidad podemos restringirnos al estudio de módulos positivos.

Propiedades de las congruencias

Para a, b, c, m $\in$ Z cualesquiera, tenemos:

i) Propiedad refleja:

$a \equiv a \pmod{m}$ es claro pues $a-a = 0 = 0 \cdot m$

ii) Propiedad simétrica:

Debemos probar que: $a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$

$a \equiv b \pmod{m} \Longrightarrow a-b = k \cdot m$ para algún entero k

luego $b-a = (-k) \cdot m$ luego $b \equiv a \pmod{m}$

iii) Propiedad transitiva:

P.D: $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$

$a \equiv b \pmod{m} \Longrightarrow a-b = k \cdot m$ para algún $k \in Z$

$b \equiv c \pmod{m} \Longrightarrow b-c = k'm$ para algún $k' \in Z$

sumando estas igualdades tenemos:

$(a-b)+(b-c) = k \cdot m + k' \cdot m$

luego, $a-c = (k+k') \cdot m$

es decir, $a \equiv c \pmod{m}$

Así, hemos visto que la relación "ser congruente con" en Z es una relación de equivalencia.

Proposición: $a \equiv b \pmod m$ y $c \equiv d \pmod{}$ $\Longrightarrow a+c \equiv b+d \pmod m$

Demostración: se deja al lector.

Proposición: si $a \equiv b \pmod m$ y $c \equiv d \pmod m$ $\Longrightarrow ac \equiv bd \pmod m$

Demostración:

$$a \equiv b \pmod m \Longrightarrow a-b = k\cdot m \Longrightarrow ac-bc = (k\cdot c)\cdot m$$
$$c \equiv d \pmod m \Longrightarrow c-d = k'm \Longrightarrow \underline{bc-bd = (bk')\cdot m}$$
$$ac-bd = (kc+bk')\cdot m$$

luego, $ac \equiv bd \pmod m$ ya que $kc+bk' \in Z$

Solución de congruencia:

Dados a, b en Z y m un entero positivo, queremos saber cuando la congruencia $ax \equiv b \pmod m$ tiene solución, y en caso que tenga solución, cuales son explicitamente todas las soluciones.

Definición 8: Función de Φ de Euler: Es una función numérica definida por: $\Phi(1) = 1$

$\Phi(n)$ = número de enteros positivos menores que n y relativamente primos a n

por ejemplo: $\Phi(2) = 1$, $\Phi(3) = 2$, $\Phi(4) = 2$, $\Phi(5) = 4$
$\Phi(6) = 2$, $\Phi(7) = 6$, $\Phi(8) = 4$, $\Phi(9) = 6$
$\Phi(10) = 4$, $\Phi(11) = 10$, $\Phi(12) = 4$, $\Phi(13) = 12$, etc.

Definición 9: Si $x \equiv y \pmod m$ entonces y se llama residuo de x módulo m.

Un conjunto $x_1, x_2, \ldots, x_m$ es un sistema completo de residuos módulo m si para todo entero y existe un y solamente un x_j tal que $y \equiv x_j \pmod m$

Ejemplo 1: 0, 1, 2, 3, 4, 5, 6 es un sistema completo de residuos módulo 7. En efecto al dividir cualquier número entero por 7 se obtiene uno y solo uno de los elementos de 0, 1, 2, 3, 4, 5, 6 como resto.

Ejemplo 2: 0, 18, 36, 20, 38, 22, 40, 24, 42, 26, 44, 28, 46, 30, 48, 32, 50 es un sistema completo de restos módulo 17. Observar que está constituido sólo por multiplos de 2.

Ejercicio: Encontrar sistema completo de residuos módulo 19, que contenga sólo múltiplos de tres.

Definición 10: Un sistema reducido de residuos módulo m es un conjunto de enteros r_i tales que $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod m$ si $i \neq j$ y tales que todo número x primo con m es congruente módulo m a algún elemento r_i del conjunto.

Ejemplo:

i) el conjunto 1, 5, 7, 11 es un sistema reducido de restos módulo 12

ii) El conjunto 1, 2, 3, 4, 5, 6 es un sistema reducido de restos módulo 7 (compárelo con el sistema completo de restos módulo 7)

Observación: El número de elementos que contiene un sistema reducido de restos módulo m es precisamente $\Phi(m)$, donde Φ es la función de Euler (definición)

Teorema 9: Sean $a, m \in Z$, con $(a, m) = 1$
Sea $S = \{r_1, r_2, \ldots, r_n\}$ un sistema completo (respectivamente reducido) de restos módulo m. Entonces $\{ar_1, ar_2, ar_3, \ldots, ar_n\}$ es un sistema completo (respectivamente reducido) de restos módulo m.

Demostración:

Primero probaremos que si $(r_i, m) = 1$, entonces $(ar_i, m) = 1$
En efecto, si $(r_i, m) = 1$ entonces existen enteros x_1, y_1 tales que $1 = r_i x_1 + m y_1$. Además, por hipótesis $(a,m) = 1$
Luego, hay x_o, y_o en Z tales que $1 = ax_o + my_o$
Es decir, tenemos $1 = ax_o + my_o = r_i x_1 + my_1$
Luego, $ax_o \cdot r_i x_1 = (1-my_o)(1-my_1) = 1 - my_o - my_1 + my_o my_1$

$$= 1 - m(y_o - y_1 + my_o y_1)$$

$$= 1 - my_2; \quad \text{con } y_2 = y_o + y_1 + my_o y_1$$

Luego, $ar_i x_o x_1 + my_2 = 1$ y por lo tanto,
cualquier divisor de ar_i y de m debe dividir a 1
Luego, $(ar_i, m) = 1$
Luego, tenemos el mismo número de $ar_1, ar_2, \ldots, ar_n$ que de $r_1, r_2, \ldots, r_n$

Además, $ar_i \equiv ar_j \pmod m \Longrightarrow r_i \equiv r_j \pmod m$

$\Longrightarrow i = j$

Luego, ar_i no es congruente con ar_j módulo m, si $i \neq j$

Teorema de Euler:

Si $(a, m) = 1$ Entonces $a^{\Phi(m)} \equiv 1 \pmod m$

Demostración:

Sea $r_1, r_2, \ldots\ldots r_{\Phi(m)}$ un sistema reducido de restos módulo m.
Luego por teorema anterior $ar_1, ar_2, \ldots\ldots, ar_{\Phi(m)}$ también es un sistema reducido de restos módulos m.
Luego para cada r_i hay un único ar_j tal que $r_i \equiv ar_j \pmod m$.
Dicho de otra manera $r_1, r_2, \ldots\ldots, r_{\Phi(m)}$ son precisamente (salvo el orden) los residuos módulos m de $ar_1, ar_2, \ldots\ldots, ar_{\Phi(m)}$

Luego:

$(ar_1)(ar_2)\ldots\ldots\ldots\ldots(ar_{\Phi(m)}) \equiv r_1 \cdot r_2 \ldots\ldots r_{\Phi(m)} \pmod m$

$a^{\Phi(m)}(r_1 r_2 \ldots\ldots r_{\Phi(m)}) \equiv r_1 \ldots\ldots r_{\Phi(n)} \pmod m \Longrightarrow$

$\Longrightarrow a^{\Phi(m)} \equiv 1 \pmod m$

(se puede cancelar ya que $(r_i, m) = 1$)

Corolario (Teo de Fermat):

Si p es primo y $p \nmid a$
Entonces $a^{p-1} \equiv 1 \pmod p$

Demostración:

Es obvio a partir de la definición de la función Φ de Euler que $\Phi(P) = P - 1$, para todo primo p.
Además, como $P \nmid a$ se tiene que $(a,p) = 1$
Luego, podemos aplicar el teo anterior y tenemos:

$$a^{P-1} \equiv 1 \pmod p$$

Corolario: Si $(a, m) = 1$, entonces la congruencia $ax \equiv b \pmod m$ tiene una solución x_1 y más aún todas sus soluciones están dadas por $x = x_1 + jm$, donde j es un entero cualquiera (es decir $x \equiv x_1 \pmod m$, luego $ax \equiv b \pmod m$, tiene sólo una solución incongruente x_1, pues todos los demás son congruentes a x_1 módulo m)

Demostración:

$x_1 = a^{\Phi(m)-1} \cdot b$ es solución de $ax \equiv b \pmod m$

pues $a \cdot a^{\Phi(m)-1} \cdot b = a^{\Phi(m)} \cdot b \equiv 1 \cdot b \equiv b \pmod m$

Sea x una solución cualquiera de la congruencia $ax \equiv b \pmod m$ demostraremos que x es de la forma $x_1 + jm$ donde j es un entero.

En efecto, como x y x_1 son soluciones, entonces:

$ax - ax_1 \equiv b - b \equiv 0 \pmod m$

luego, $a(x - x_1) \equiv 0 \pmod m$

luego, $x - x_1 \equiv 0 \pmod m$ de donde $x = x_1 + jm$ con $j \in Z$

Ejercicios:

1.- Encuentre todas las soluciones de las congruencias

i) $5x \equiv 2 \pmod 3$

ii) $7x \equiv 2 \pmod 4$

iii) $2x \equiv 7 \pmod 9$

iv) $3x \equiv 5 \pmod{11}$

2.- Demuestre que $n^6 - 1$ es divisible por 7 si $(n, 7) = 1$

3.- Si k es un entero positivo cualquiera y $(n, 7) = 1$
Pruebe que $n^{6k} - 1$ es divisible por 7

4.- Determine el último dígito de la representación decimal de 7^{400}

5.- Usando el teorema del Binomio de Newton demuestre que
$(a+b)^p \equiv a^p + b^p \pmod p$ (donde p es un número primo)

Por corolario del teorema de Fermat sabemos que si $(a, m) = 1$, entonces la congruencia $ax \equiv b(m)$ tiene exactamente una solución $x \equiv x_1 \pmod m$.

Veamos el caso en que $(a, m) \neq 1$

Sea $g = (a, m)$. Luego, $g \mid a$ y $g \nmid m$

Supongamos que $u \in Z$ es solución de la congruencia $ax \equiv b \pmod m$.

Es decir, $au \equiv b \pmod m$.

Como, $g \mid a$ y $g \mid m$ tenemos que $a \equiv 0 \pmod g$, por lo tanto $au \equiv 0 \pmod g$, y $m \equiv 0 \pmod g$; luego, $b \equiv au \equiv 0 \pmod g$.

Es decir, para que la congruencia $ax \equiv b \pmod{m}$ tenga solución es necesario que $g \mid b$.

(o lo que es equivalente: si $g \nmid b$, entonces la congruencia $ax \equiv b \pmod{m}$ no tiene solución)

Teorema 10: La congruencia $ax \equiv b \pmod{m}$ tiene exactamente $g = (a, m)$ soluciones incongruentes si y sólo si $g \mid b$.

Demostración:

Por lo anterior, basta demostrarlo que si $g \mid b$, ces la congruencia $ax \equiv b \pmod{m}$ tiene exactamente $g = (a, m)$ soluciones incongruentes.

Supongamos entonces, que $g \mid b$ y como $g = (a, m)$ entonces también tenemos que $g \mid a$ y $g \mid m$, es decir hay $a', m', b' \in Z$ tales que:

$a = g \cdot a'$, $m = gm'$ y $b = gb'$ con $(a', m') = 1$

Reemplazando en $ax \equiv b \pmod{m}$ tenemos

$$ga'x \equiv gb' \pmod{g m'}$$

$\Longrightarrow$ $gm' \mid ga'x - gb'$ $\Longrightarrow$ $gm' \mid g(a'x - b')$

$\Longrightarrow$ $g(a'x - b') = t\, gm'$ algún $t \in Z$

$\Longrightarrow$ $a'x - b' = t\, m'$

$\Longrightarrow$ $a'x \equiv b' \pmod{m'}$

Como $(a', m') = 1$, entonces esta última congruencia tiene exactamente una solución incongruente módulo m', a saber:

$x \equiv x_1 \pmod{m'}$.

Además, es claro que toda solución de $a'x \equiv b' \pmod{m'}$ es también solución de $ax \equiv b \pmod{m}$

Es decir, las soluciones de $ax \equiv b \pmod{m}$ son los enteros u tales que $u \equiv x_1 \pmod{m'}$ luego, $u = x_1 + t\, m'$ con $t \in Z$

Puede ocurrir que no todos los enteros de la forma $x_1 + t\, m'$ sean incongruentes módulo m.

Nosotros buscamos los valores de t para los cuales los enteros $x_1 + t\, m'$ son incongruentes módulo m (estos van a ser las soluciones incongruentes módulo m de $ax \equiv b \pmod{m}$).

Descartemos primeros los valores de t para los cuales $x_1+t\ m'$ es congruente módulo m.

En efecto, si:

$$x_1+t_1\ m' \equiv x_1+t_2\ m' \pmod{m}$$

$$\Longrightarrow\ t_1\ m' \equiv t_2\ m' \pmod{m}$$

$$\Longrightarrow\ t_1 \equiv t_2 \pmod{g}$$

Luego, los valores de t que sirven son aquellos que constituyen el sistema completo de residuos módulo g, es decir 0, 1. 2, ..., g - 1

Luego, las g = (a, m) soluciones incongruentes de $ax \equiv b \pmod{m}$ son:

$$x_1,\ x_1+m',\ x_1+2m',\ \ldots,\ x_1+(g-1)\ m'$$

pero $m' = \frac{m}{g}$ luego, las soluciones incongruentes las podemos reescribir en la forma:

$$x_1,\ x_1+\frac{m}{g},\ x_1+2\frac{m}{g},\ \ldots,\ x_1+(g-1)\frac{m}{g}$$

Estas son las únicas soluciones, pues si a t se le da un valor cualquiera entonces el entero $x_1+t\frac{m}{g}$ correspondiente será congruente módulo m a uno y sólo uno de estos valores.

Ejemplo: Determinar las soluciones incongruentes de la congruencia $24x \equiv 16 \pmod{32}$

Primero observamos que (24,32) = 8 y que 8 divide a 16, luego por teorema anterior la congruencia tiene exactamente 8 soluciones incongruentes módulo 32.

$$24x \equiv 16 \pmod{32}$$
$$\therefore\ 3x \equiv 2 \pmod{4}$$
$$\therefore\ -x \equiv 2 \pmod{4} \quad \text{pues } 3 \equiv -1 \pmod{4}$$
$$\therefore\ x \equiv 2 \pmod{4} \quad \text{pues } -2 \equiv 2 \pmod{4}$$

Luego, por teorema anterior todas las soluciones incongruentes son 2+4 t con $0 \leq t \leq 7$

Es decir son: 2, 6, 10, 14, 18, 22, 26, 30

Ejemplo: Resolver $11x = 8 \pmod{33}$

Para esta congruencia no existe solución pues (11,33) = 11 y 11 no divide a 8.

Ejercicios:

I.- Encontrar todas las soluciones incongruentes de:

1.- $14x \equiv 11 \pmod 5$

2.- $6x \equiv 8 \pmod{20}$

3.- $8x \equiv 16 \pmod{12}$

4.- $23x \equiv 8 \pmod{17}$

5.- $11x \equiv -15 \pmod{10}$

6.- $22x \equiv 77 \pmod{121}$

7.- $51x \equiv 9 \pmod{54}$

8.- $353x \equiv 254 \pmod{400}$

II.- Determine el número de soluciones incongruentes para cada una de las congruencias:

1.- $15x \equiv 25 \pmod{35}$

2.- $15x \equiv 24 \pmod{35}$

3.- $15x \equiv 0 \pmod{35}$

III.- Encontrar el menor entero positivo distinto de uno que satisfaga simultáneamente las congruencias:

$$x \equiv 1 \pmod 3$$
$$x \equiv 1 \pmod 5 \quad y$$
$$x \equiv 1 \pmod 7$$

(es decir encontrar entero con la propiedad que al ser dividido por 3, 5 o 7 deje siempre resto 1)

Comentario:

Para números pequeños es fácil obtener soluciones de la congruencia $ax \equiv b \pmod m$ donde $(a, m) = 1$.

Fácil en el sentido que se puede encontrar por simple inspección o bien probando todos los enteros de un sistema completo de restos módulo m o bien utilizando la solución. $x_o = a^{\Phi(m)-1}.b$ que nos da el teorema de Euler.

En caso de números grandes, la simple inspección ya no funciona. Examinar un sistema completo de restos módulo m cuando m es grande resulta muy agotador. Por último, la solución que nos da el Teorema de Euler tampoco es muy práctica ya que $a^{\Phi(m)}$ es muy grande en general. En este último caso se puede obtener una solución pequeña reduciendo $x_o = a^{\Phi(m)-1}.b$ módulo m.

Resolvamos (I) $ax \equiv b \pmod m$ con $(a, m) = 1$
y donde a, b y m son números grandes.

Por la teoría general que ya hemos visto sabemos que hay una y sólo una solución en el intervalo 0, 1, ..., m-1 .

Método para encontrar la solución:

Partiendo de $ax \equiv b \pmod m$ (I) nos damos

$$my \equiv b \pmod a \quad \text{(II)}$$

Supongamos que encontramos solución $y = y_o$ de la congruencia (II), entonces afirmamos que

$$x_o = \frac{b-my_o}{a} \in Z, \text{ es solución de (I)}$$

En efecto, $a\left(\frac{b-my_o}{a}\right) = b - my_o \equiv b \pmod m$

Luego, x_o es solución de (I)

Ejemplo:

1.- $625x \equiv 1 \pmod{879}$ Debemos transformar esta congruencia hasta tener una que nos sea fácil saber su solución.

$879y \equiv 1 \pmod{625}$

2.- $254y \equiv 1 \pmod{625}$ pues 879 = 625+254
$625z \equiv 1 \pmod{254}$

3.- $117z \equiv 1 \pmod{254}$
$254u \equiv 1 \pmod{117}$

4.- $20u \equiv 1 \pmod{117}$
$117v \equiv 1 \pmod{20}$

5.- $17v \equiv 1 \pmod{20}$
$20w \equiv 1 \pmod{17}$

6.- $3w \equiv 1 \pmod{17}$

La congruencia 6.- tiene solución $w_o = 6$

$\therefore \quad v_o = \frac{1-20.6}{17} = \frac{-119}{17} = -7$ es solución de (5)

$\therefore \quad u_o = \frac{1-117.(-7)}{20} = 41$ es solución de (4)

$\therefore \quad z_o = \frac{1-254.41}{117} = -89$ es solución de (3)

$\therefore \quad y_o = \frac{1-625.(-89)}{254} = 219$ es solución de (2)

$\therefore \quad x_o = \frac{1-879.219}{625} = -308$ es solución de (1)

Para encontrar la solución en el intervalo 0, 1, ..., 878 basta ver a qué entero es congruente - 308 módulo 879.

Así vemos que 571 es tal solución (basta sumar -308 con 879)

Luego, $x = \{x_o + tm\}\ t \in Z = \{571 + t.879\}\ t \in Z$

son todas las soluciones de $625x \equiv 1 \pmod{879}$

Observemos que utilizando la solución que nos da el Teorema de Euler tendríamos $x = (625)^{\Phi(879)-1}$. 1 número muy grande, más adelante veremos que $625^{\Phi(879)-1}$ se puede reducir módulo 879 y obtener $x_o = 571$ como solución. Para desarrollar este método de solución necesitaremos conocer más acerca de la función Φ de Euler, más explícitamente saber cuánto vale $\Phi(a)$ si a es un entero cualquiera.

Ejercicios:

1.- Encontrar todas las soluciones de cada una de las congruencias:

a) $20x \equiv 50 \pmod{8}$

b) $353x \equiv 254 \pmod{400}$

c) $18x \equiv 36 \pmod{9}$

2.- ¿Cuántas soluciones tiene la congruencia $33x \equiv 0 \pmod{11}$?

III.- SISTEMAS DE CONGRUENCIAS

Nos interesa conocer las soluciones del sistema.

$$\left.\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &\text{-----} \\ a_kx &\equiv b_k \pmod{m_k} \end{aligned}\right\} \quad (*)$$

Condiciones para que el sistema (*) tenga solución:

i) $a_ix = b_i \pmod{m_i}$ debe tener solución para todo $i = 1, 2, \ldots, k$

ii) $(a_i, m_i) = 1$ todo $i = 1, 2, \ldots, k$

iii) $(m_i, m_j) = 1$ si $i \neq j$

La necesidad de las condiciones (i) y (ii) es natural, ya que buscamos solución del sistema (*), es decir, debe satisfacer a cada una de las congruencias de (*).

Para la condición (iii) no es tan evidente su necesidad. Nos limitaremos a dar un contraejemplo es decir un sistema en el cual $(m_i, m_j) \neq 1$ y mostrar que no tiene solución.

Consideremos:

$$\left.\begin{aligned} &1.- \quad 3x = 5 \pmod 8 \\ &2.- \quad 5x = 4 \pmod 6 \end{aligned}\right\} \quad (I)$$

Es claro que se verifican las condiciones (i) y (ii) pues $(3,8) = 1 = (5,6)$.

La condición (iii) en cambio, no se verifica pues $(8,6) = 2 \neq 1$.

Debemos mostrar que el sistema (I) no tiene solución, para esto veamos cuales son todas las soluciones de la congruencia (1) y de la congruencia (2).

Por simple inspección vemos que $x_o = 7$ es solución de la congruencia (1), por lo tanto, todas sus soluciones son $x = 7 + t \cdot 8$ con t entero. Es decir, todas sus soluciones son números impares.

Para la congruencia (2) vemos que $x_o = 2$ es solución, luego, todas sus soluciones son $x = 2+t\cdot 6$ con t entero, es decir, todas sus soluciones son números pares. Luego, no puede existir solución del sistema (I).

Teorema 11: Si el sistema (*) tiene una solución x_o, entonces todas las soluciones son:

$$x = x_o + t\cdot m_1\cdot m_2\cdot \ldots\ldots \cdot m_r \text{ con t entero}$$

Demostración:

Por inducción sobre k.

k = 1 luego, x_o solución de $a_1 x \equiv b_1 \pmod{m_1}$ y por el corolario del Teorema de Euler sabemos que todas sus soluciones son $x = x_o + t\cdot m_1$ con t entero. Luego, vale para k = 1.

Supongamos válido el teorema para sistemas con k-1 congruencias y lo demostraremos para k congruencias.

Consideremos:

$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &- - - - - \\ a_{k-1} x &\equiv b_{k-1} \pmod{m_{k-1}} \end{aligned}\right\} \quad (* \quad *)$$

La hipótesis general del teorema nos dice que hay una solución y_o de (* *). Por otra parte, la hipótesis de inducción nos dice todas las soluciones del sistema (* *) son $x = y_o + t\cdot m_1\cdot \ldots\ldots \cdot m_{k-1}$ con t entero.

Reemplazaremos esta última solución en la última congruencia del sistema (*), es decir, en la congruencia $a_k x \equiv b_x \pmod{m_k}$

$$a_k\,(y_o + t\cdot m_1 \ldots\ldots m_{k-1}) \equiv b_k \pmod{m_k}$$

luego, $a_k\, t\cdot m_1 \ldots\ldots m_{k-1} \equiv b_k - a_k\, y_o \pmod{m_k}$ (1)

Esta congruencia en t tiene solución:

t_o ya que $(a_k \cdot m_1 \cdots m_{k-1}, m_k) = 1$

Luego, todas las soluciones de (1) son : $t = t_o + t' m_k$ con t' entero.

Reemplazando t en $x = y_o + t \cdot m_1 \cdots m_{k-1}$ tenemos:

$$x = y_o + (t_o + t' m_k) m_1 \cdots m_{k-1}$$

$$x = y_o + t_o m_1 \cdots m_{k-1} + t' \cdot m_1 \cdots m_k \quad \text{con t' entero.}$$

Demostrando que $y_o + t_o \cdot m_1 \cdots m_{k-1}$ es solución particular del sistema (*) (se deja al lector como ejercicio), tenemos demostrado el teorema.

Ejemplo: Encontrar todas las soluciones del sistema:

$$\left.\begin{array}{ll} 1.- & 5x \equiv 3 \pmod 8 \\ 2.- & 9x \equiv 1 \pmod 5 \\ 3.- & 4x \equiv -1 \pmod 7 \end{array}\right\}$$

Es claro que verifica las condiciones pues:

$(5,8) = (9,5) = (4,7) = 1$ y
$(8,5) = (8,7) = (5,7) = 1$

Resolvemos primero la congruencia (1)
Vemos que -1 es solución pues $-5 \equiv 3 \pmod 8$
Luego, todas sus soluciones son: $x = -1+8y$ con y entero.
Reemplazando esta solución en la congruencia (2) tenemos

$$9(-1+8y) \equiv 1 \pmod 5$$

$$-9+72y \equiv 1 \pmod 5$$

$$72y \equiv 10 \pmod 5 \qquad y_o = 0 \text{ es solución}$$

Luego, todas sus soluciones son: $y = 0+Z.5$ con Z entero.
Luego, $x = -1+40Z$ que reemplazando en la congruencia (3) queda:

$$4(-1+40Z) \equiv -1 \pmod 7$$

$$160Z \equiv 3 \pmod 7$$

$$-Z \equiv 3 \pmod 7$$

$$z_o = -3 \text{ es solución}$$

Luego, todas las soluciones de (3) son $Z = -3+7\cdot t$ con t entero.

Reemplazando Z en $x = -1+40Z$ tenemos

$x = -1+40(-3+7\cdot t)$, t entero

$x = -121+280\ t$, t entero son todas las soluciones del sistema. Observe que $280 = 8\cdot 5\cdot 7$, es decir, tal como lo afirma el teorema, la solución general es módulo del producto de los módulos de las congruencias.

Ejercicios: Encuentre todas las soluciones de:

a.- $\left.\begin{aligned} 3x &\equiv 1 \pmod 5 \\ 2x &\equiv 1 \pmod 7 \\ 8x &\equiv 2 \pmod 3 \end{aligned}\right\}$

b.- $\left.\begin{aligned} 2x &\equiv 3 \pmod 7 \\ 5x &\equiv 2 \pmod 3 \\ 7x &\equiv 1 \pmod 4 \\ 9x &\equiv 1 \pmod 5 \end{aligned}\right\}$

Démonos el siguiente problema:

Encontrar un número entero que deje restos 1, 2 y 3, cuando se divide por 3, 4 y 5 respectivamente. Posiblemente el lector podrá encontrar una solución utilizando método de tanteo. ¿Pero cuáles son todas las soluciones del problema? Esto quizás, pueda presentar un poco más de dificultad. En forma más general podemos plantear: Encontrar todos los enteros que dejen restos $b_1, b_2, \ldots, b_k$ cuando se dividen por $m_1, m_2, \ldots, m_k$ respectivamente.

Este último problema es el que a continuación resolveremos.

Primero observamos que el problema es equivalente a resolver el sistema de congruencias:

$$\left.\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &- - - - - \\ x &\equiv b_k \pmod{m_k} \end{aligned}\right\} \qquad (*)$$

Adoptaremos como hipótesis: $(m_i, m_j) = 1$ si $i \neq j$

A continuación demostraremos que el sistema (*) tiene solución.

Sea $m_1 \cdot m_2 \cdot \cdots \cdot m_k = m_i \, n_i$ esto es siempre posible, basta tomar

$$n_i = m_1 \cdot m_2 \cdot \cdots \cdot m_{i-1} \cdot m_{i+1} \cdot \cdots \cdot m_k$$

Consideremos el sistema:

$$\left.\begin{aligned} n_1 x &\equiv 1 \pmod{m_1} \\ n_2 x &\equiv 1 \pmod{m_2} \\ &- - - - - \\ n_k x &\equiv 1 \pmod{m_k} \end{aligned}\right\}$$

Cada una de estas congruencias tiene solución pues $(n_i, m_i) = 1$ (esto se deduce de la hipótesis $(m_i, m_j) = 1$ si $i \neq j$)

Sea x_i solución de la congruencia i-ésima, es decir:

$$n_i x_i \equiv 1 \pmod{m_i} \quad \text{todo } i = 1, 2, \ldots, k$$

formemos $x_o = n_1 x_1 b_1 + n_2 x_2 b_2 + \cdots\cdots + n_k x_k b_k$

Afirmamos que x_o es solución del sistema (*)

En efecto, $x_o \equiv b_1 \pmod{m_1}$ ya que m_1 divide a

$$n_i x_i b_i = m_1 \cdot m_2 \cdots m_{i-1} \cdot m_{i+1} \cdots m_k x_i b_i \quad \text{todo } i = 2, 3 \ldots, k$$

Luego, $n_i x_i b_i \equiv 0 \pmod{m_1}$ todo $i = 2, 3, \ldots k$

Luego, $x_o \equiv n_1 x_1 b_1 \pmod{m_1}$, pero además sabemos que x_1 es solución de la congruencia $n_1 x \equiv 1 \pmod{m_1}$, es decir, que $n_1 x_1 \equiv 1 \pmod{m_1}$.

Luego, $x_o \equiv b_1 \pmod{m_1}$. De la misma forma se demuestra que:

$$x_o \equiv b_2 \pmod{m_2}$$
$$x_o \equiv b_3 \pmod{m_3}$$
$$- - - - - -$$
$$x_o \equiv b_k \pmod{m_k}$$

Por lo tanto, x_o es solución particular del sistema (※)
Luego, todas sus soluciones son:

$$x = x_o + t \cdot m_1 \cdot \ldots \cdot m_r \text{ con t entero}$$

Ejemplo: Encontrar todos los enteros que dejan restos 1, 2 y 3 al ser divididos por 3, 4 y 5 respectivamente. Es decir, se pide encontrar las soluciones del sistema:

$$\left.\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 3 \pmod 5 \end{aligned}\right\} \quad (※)$$

primero calculamos n_1, n_2, n_3: $n_1 = 20$

$n_2 = 15$

$n_3 = 12$

y formamos:

1.- $20x \equiv 1 \pmod 3$
2.- $15x \equiv 1 \pmod 4$
3.- $12x \equiv 1 \pmod 5$

y encontramos $x_1 = 2$ es solución de la congruencia 1.-

$x_2 = 3$ es solución de la congruencia 2.-

$x_3 = 3$ es solución de la congruencia 3.-

Luego, la solución particular de (※) es:
$x_o = 20 \cdot 2 \cdot 1 + 15 \cdot 3 \cdot 2 + 12 \cdot 3 \cdot 3 = 238$
Luego, todas las soluciones de (※) son

$x = 238 + t \cdot 3 \cdot 4 \cdot 5$ con t entero
$x = 238 + t \cdot 60$ con t entero

Tomando $t = -3$ tenemos $x = 58$, que es la solución positiva más pequeña.

Ejercicios:

1.- Verificar que efectivamente la solución particular y x = 58 satisfacen (*)

2.- Encontrar los enteros que satisfagan simultáneamente las congruencias $x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 5$, $x \equiv 1 \pmod 7$.

3.- Encontrar todas las soluciones del sistema

$$\left.\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 5 \pmod 7 \end{aligned}\right\}$$

IV.- SOLUCION DE CONGRUENCIAS UTILIZANDO EL TEOREMA DE EULER

Veremos ahora como encontrar soluciones a la congruencia $ax \equiv b \pmod m$ para números grandes utilizando la solución que nos da el Teorema de Euler, es decir $x_o = a^{\Phi(m)-1}.b$. Para esto necesitamos conocer el valor de $\Phi(m)$ siendo m un entero cualquiera.

En el Teorema 6 vimos que todo entero n mayor que 1 puede expresarse con producto de números primos es decir:

$$n = P_1^{t_1} \cdot P_2^{t_2} \cdots\cdots P_r^{t_r}$$

P_i primo, $1 \leq t_i \in Z$ $\qquad i = 1, \ldots\ldots, r$

$P_i \neq P_j$ si $i \neq j$

ordenando estos primos, podemos suponer que $P_1 < P_2 < \ldots\ldots < P_r$

Luego, todo entero n lo podemos escribir en la forma:

$$n = P_1^{t_1} \cdot P_2^{t_2} \cdots\cdots P_r^{t_r}, \text{ con } 1 \leq t_i \in Z$$

y

$P_1 < P_2 < \ldots\ldots < P_r$ primos

y que se llama descomposición canónica de un entero en producto de números primos.

A continuación haremos algunas afirmaciones cuyas demostraciones (que son fáciles) se dejan como ejercicio al lector.

1.- Si a es un entero distinto de ± 1 entonces existe un número primo p tal que p divide a a.

2.- Si $n = P_1^{t_1} \cdots P_k^{t_k}$ representa un entero positivo descompuesto en su forma canónica, entonces todos sus divisores son de la forma de $= P_1^{s_1} \cdot \cdots P_k^{s_k}$ con $0 \leq s_i \leq t_i$

3.- Si $n = P_1^{t_1} \cdots P_k^{t_k}$ es un entero positivo desompuesto en su forma canónica, entonces:

$$\sum_{d \mid n} d = \frac{P_1^{t_1+1} - 1}{P_1 - 1} \cdot \frac{P_2^{t_2+1} - 1}{P_2 - 1} \cdots \frac{P_k^{t_k+1} - 1}{P_k - 1}$$

(Resulta de: $\sum_{d \mid n} d = (1+P_1+\cdots+P_1^{t_1}) \cdot (1+P_2+\cdots+P_2^{t_2}) \cdots (1+P_k+\cdots P_k^{t_k})$)

4.- Si $a = P_1^{t_1} \cdots P_r^{t_r}$, $t_i \geq 0$ y

$b = P_1^{s_1} \cdots P_r^{s_r}$, $s_i \geq 0$ son enteros descompuestos en producto de primos. Entonces:

a) $(a,b) = P_1^{\text{mínimo } (t_1, s_1)} \cdot P_2^{\text{mínimo } (t_2, s_2)} \cdots P_r^{\text{mínimo } (t_r, s_r)}$

donde (a,b) designa el máximo común divisor entre a y b

a) $[a,b] = P_1^{\text{máximo } (t_1, s_1)} \cdot P_2^{\text{máximo } (t_2, s_2)} \cdots P_r^{\text{máximo } (t_r, s_r)}$

donde $[a, b]$ designa el mínimo común multiplo entre a y b

Por ejemplo, tomemos $a = 108 = 2^2 \cdot 3^3 \cdot 5^0$

$$b = 225 = 2^0 \cdot 3^2 \cdot 5^2$$

$\therefore$ $(108, 225) = 2^0 \cdot 3^2 \cdot 5^0 = 9$ y

$[108, 225] = 2^2 \cdot 3^3 \cdot 5^2 = 2.700$

Teorema 12: Si p es un número primo y $\mathfrak{D}$ denota la función de Euler, entonces:

$$\mathfrak{D}(P^t) = P^t - P^{t-1} = P^t\left(1-\frac{1}{P}\right)$$

Demostración:

Buscamos el número de enteros menores que P^t y relativamente primos a P^t.
Es claro entonces, que $\mathfrak{D}(P^t) = P^t - H$ siendo H el número de enteros menores que p^t y que no son relativamente primos a p^t. Estos enteros son P, 2 P, 3 P, ..., P^{t-1}. P es decir $H = P^{t-1}$

$$\therefore\ \mathfrak{D}(P^t) = P^t - P^{t-1} = P^t\left(1-\frac{1}{P}\right)$$

Teorema 13: $(a,b) = 1,\ a > 0,\ b > 0 \Longrightarrow \mathfrak{D}(ab) = \mathfrak{D}(a)\,\mathfrak{D}(b)$

Demostración:

Sea $C = \{0, 1, 2, ..., ab-1\}$.

Los elementos x de C se obtienen sin repetición de
$aq+r$ con $r = 0, 1, ..., a-1$ y
$q = 0, 1, ..., b-1$

Nosotros buscamos los x en C tales que $(x,ab) = 1$
pero $(x, ab) = 1 \Longleftrightarrow (x,a) = 1 = (x,b)$

Además, como $x = aq+r$, $0 \leq q \leq b-1$, $0 \leq r \leq a-1$

se tiene: $(x,a) = 1 \Longleftrightarrow (aq+r) = 1 \Longleftrightarrow (a,r) = 1$

Para r fijo consideremos la sucesión:

$0 \cdot a+r,\ 1 \cdot a+r,\ 2 \cdot a+r,\ ....,\ (b-1)\,a+r$ (*)

Demostraremos que esta sucesión contiene exactamente $\mathfrak{D}(b)$ enteros que son primos con b
Primero vemos que si $i \neq j$ entonces $i \cdot a+r \not\equiv ja+r \pmod b$
si no tendría que b divide a $j-i$ lo que es absurdo ya que
$0 \leq i,\ j \leq b-1$

Dividiendo cada elemento de la sucesión (*) por b se tiene que
$ia+r \doteq c_i b+R_i$ con $0 \leq R_i < b$, todo $i = 0, 1, ..., b-1$

y así obtenemos restos R_o, R_1, ... R_{b-1} que tienen la propiedad

$R_i \neq R_j$ si $i \neq j$ pues si $R_i = R_j$, entonces tendríamos:

$$ia+r = c_i b+R_i, \quad ja+r = c_j b+R_i$$

$$\Longrightarrow \quad i \cdot a - j \cdot a = (c_i - c_j)\, b$$

$$\Longrightarrow \quad (i-j)\, a = (c_i - c_j)\, b$$

$$\Longrightarrow \quad b \mid (i-j)\, a \overset{(a,b)=1}{\Longrightarrow} \quad b \mid i-j \quad \text{-absurdo.}$$

Luego, los R_i son todos distintos y $R_i < b$ todo $i = 0, \ldots, b-1$

Luego, los R_i son 0, 1, ..., b-1 salvo posiblemente el orden.

Por lo tanto, en la sucesión (*) hay $\Phi(b)$ elementos que son primos con b.

Es decir, para cada r ($0 \leq r \leq a-1$) hay $\Phi(b)$ elementos

Luego, $\Phi(a.b) = \Phi(a) \cdot \Phi(b)$

Corolario: Si $a > 1$ es un entero cualquiera y

$$a = P_1^{t_1} \cdot P_2^{t_2} \cdot \ldots \cdot P_r^{t_r}$$

su descomposición canónica en producto de primos (que es conocida) Entonces:

$$\Phi(a) = a\left(1-\frac{1}{P_1}\right) \cdot \left(1-\frac{1}{P_2}\right) \cdot \ldots \cdot \left(1-\frac{1}{P_r}\right)$$

Demostración:

$$\Phi(a) = \Phi\left(P_1^{t_1} \cdot P_2^{t_2} \cdots P_r^{t_r}\right)$$

$$= \Phi\left(P_1^{t_1}\right) \cdot \Phi\left(P_2^{t_2}\right) \cdots \Phi\left(P_r^{t_r}\right) \text{ pues } \left(P_i^{t_i}, P_j^{t_j}\right) = 1 \text{ si } i \neq j$$

$$= \left(P_1^{t_1} - P_1^{t_1-1}\right)\left(P_2^{t_2} - P_2^{t_2-1}\right) \cdots \left(P_r^{t_r} - P_r^{t_r-1}\right)$$

$$= P_1^{t_1} \cdot P_2^{t_2} \cdots P_r^{t_r} \left(1-\frac{1}{P_1}\right)\left(1-\frac{1}{P_2}\right) \cdots \left(1-\frac{1}{P_r}\right)$$

$$= a\left(1-\frac{1}{P_1}\right) \cdot \left(1-\frac{1}{P_2}\right) \cdots \left(1-\frac{1}{P_r}\right)$$

Ejemplo: $\Phi(360) = \Phi(2^3 \cdot 3^2 \cdot 5)$

$$= 360\left(1-\frac{1}{2}\right) \cdot \left(1-\frac{1}{3}\right) \cdot \left(1-\frac{1}{5}\right)$$

$$= 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5}$$

$$= 96$$

Volvamos ahora a la congruencia $ax \equiv b \pmod m$ con $(a, m) = 1$

Sabemos que $x_o = a^{\Phi(m)-1} \cdot b$ es solución.

Ahora ya sabemos el valor de $\Phi(m)$ para un entero cualquiera m.

El problema que aún subsiste es que en general $a^{\Phi(m)-1}$ es muy grande, por lo tanto nos interesa poder reducirlo módulo m.

Por ejemplo, resolvamos la ecuación:

$$5x \equiv 2 \pmod{26}, \quad (5,26) = 1$$

En este caso tenemos que:

$$x_o = 5^{\Phi(26)-1} \cdot 2$$

primero veamos cuanto vale $\Phi(26)$

$$\begin{aligned}\Phi(26) &= \Phi(2 \cdot 13) \\ &= \Phi(2) \cdot \Phi(13) \text{ pues } (2, 13) = 1 \\ &= 1 \cdot 12 \\ &= 12\end{aligned}$$

$\therefore \quad x_o = 5^{11} \cdot 2$

Ahora debemos reducir 5^{11} módulo 26

$$5^2 \equiv -1 \text{ (mód 26)}$$

$\therefore \quad (5^2)^5 \equiv (-1)^5 \pmod{26}$

$\therefore \quad 5^{10} \equiv -1 \pmod{26}$

$\therefore \quad 5^{11} \equiv -5 \pmod{26}$

$\therefore \quad x_o = -5 \cdot 2 = -10$ es solución

o bien $x_o = 16$ que sería la solución en el intervalo 0, 1, ..., 25 que es un sistema completo de restos módulo 26.

Luego, todas las soluciones de $5x \equiv 2 \pmod{26}$ son $x = 16 + t \cdot 26$ con t entero.

NOTA: Al reducir 5^{11} módulo 26 hemos utilizado el siguiente hecho: $a \equiv b \pmod{m} \Longrightarrow a^t \equiv b^t \pmod{m}$, t entero, esto resulta de:

$$a^t - b^t = (a-b)(a^{t-1} + a^{t-2} \cdot b + a^{t-3} \cdot b^2 + \ldots + ab^{t-2} + b^{t-1})$$

Luego, si $m \mid a-b$ entonces $m \mid a^t - b^t$

es decir, si $a \equiv b \pmod{m}$, entonces $a^t \equiv b^t \pmod{m}$

Ejercicios:

1.- Calcule:

a) $\Phi(81)$

b) $\Phi(540)$

c) $\Phi(735)$

d) $\Phi(1287)$

2.- Resolver utilizando el Teorema de Euler las ecuaciones siguientes:

a) $3x \equiv 5 \pmod{11}$

b) $7x \equiv 4 \pmod{12}$

3.- Demuestre que n^6-1 es divisible por 7 si $(n, 7) = 1$

4.- Demuestre que n^7-n es divisible por 42 para cualquier entero n.

V.- ECUACIONES DIOFANTICAS

Sea $F(x, y) \in Z[x, y]$, es decir:

$$F(x, y) = \sum_{i,j=0}^{n} a_{ij}x^i y^j \quad , \quad a_{ij} \in Z$$

Consideremos la ecuación $F(x,y) = 0$, llamada ecuación diofántica. El problema consiste en encontrar pares de enteros (x_o, y_o) tales que:

$$F(x_o, y_o) = 0$$

Caso particular $F(x,y) = f(x)+ay$ con $a \neq 0$

Luego, tenemos la ecuación diofántica $f(x)+ay = 0$ (1)
a partir de la cuál podemos escribir la congruencia:

$$f(x) \equiv 0 \pmod{a} \quad (2)$$

Es claro que si tenemos una solución de (1), entonces tenemos una solución de (2) y viceversa.

En efecto, sea (x_o, y_o) una solución de (1), entonces $f(x_o)+ay_o=0$

luego, $f(x_o) \equiv 0 \pmod a$

es decir, x_o es solución de (2)

Recíprocamente, si x_o es solución de (2)

entonces $f(x_o) = a \cdot t$, algún t en Z

$\therefore$ $(x_o, -t)$ es solución de (1) pues

$$f(x_o)+a(-t) = at+(-at) = 0$$

Consideremos la ecuación diofántica

$$ax+by = c \quad (\ast)$$

Sea $d = (a,b)$, entonces si d no divide a c la ecuación $(\ast)$ no tiene solución.

Para ver esto último supongamos que $(\ast)$ tiene una solución (x_o, y_o), es decir, $ax_o+by_o = c$ y como $d = (a,b)$, entonces hay enteros s, t tales que $a = d \cdot s$, $b = d \cdot t$

luego, $d\ s\ x_o+d\ t\ y_o = c$

luego, $d\ (s\ x_o+t\ y_o) = c$

luego, d divide a c lo que demuestra la afirmación.

Dividiendo la ecuación diofántica $(\ast)$ por d tenemos:

$$\frac{a}{d}x+\frac{b}{d}y = \frac{c}{d} \qquad \text{con } (\frac{a}{d}, \frac{b}{d}) = 1$$

Por lo tanto, basta estudiar ecuaciones diofánticas del tipo

$(\ast)$ $ax+by = c$ con $(a,b) = 1$

Para encontrar las soluciones de $(\ast)$, es suficiente resolver

$ax \equiv c \pmod b$ o $by \equiv c \pmod a$

Sea por ejemplo, x_o una solución de: $ax \equiv c \pmod b$

luego, $ax_o \equiv c \pmod b \iff ax_o = c+bt$, t entero.

Tomando $y_o = -t$ tenemos que $(x_o, -t)$ es solución de $(\ast)$

Ahora veremos cuáles son todas las soluciones de $(\ast)$

Supongamos que tenemos enteros (x_o, y_o) que son solución de $(\ast)$ (que se encuentra como arriba) es decir, tenemos

$ax+by = c$ y $ax_o+by_o = c$

luego, $a(x-x_o)+b(y-y_o) = 0$

luego, $b \mid a(x-x_o)$, $a \mid b(y-y_o)$

pero $(a,b) = 1$ luego, $b \mid x-x_o$ y $a \mid y-y_o$

Luego, $x-x_o = b \cdot t$

$y-y_o = -at$

es decir, $\{(x_o+bt, y_o-at) / t \in Z\}$ son todas las soluciones de (*)

Ejemplo: Encontrar todas las soluciones de la ecuación diofántica $7x+9y = 12$.

Primero debemos encontrar solución particular (x_o, y_o).

Para esto basta resolver la congruencia $7x \equiv 12 \pmod 9$ la cual tiene como solución $x_o = 3$ (se encuentra rápidamente por simple inspección o bien utilizando alguno de los métodos conocidos)

Como x_o es solución de $7x \equiv 12 \pmod 9$ se tiene

$7x_o = 12+t \cdot 9$ luego, $7 \cdot 3 = 12+t \cdot 9$

de donde obtenemos $t = 1$, es decir, $y_o = -1$

luego, $\{3+9 \cdot u, \ -1-7u\}$ $u \in Z$ son todas las soluciones de $7x+9y = 12$

Ejercicios:

1.- Encuentre todas las soluciones de las ecuaciones diofánticas:

a) $3x+5y = 1$

b) $10x-7y = 17$

c) $6x+8y = 2$

2.- Probar que $ax+by = c$ tiene solución si y solamente si $ax+by = c+a$ tiene solución.

3.- Probar que $ax+by = c$ tiene solución si y solamente si $(a,b) = (a,b,c)$

4.- Si $ax+by = c$ tiene dos soluciones (x_o, y_o) y (x_1, y_1) con $x_1 = 1+x_o$ y si $(a,b) = 1$ entonces pruebe que $b = \pm 1$

VI.- LA ECUACION $x^2+y^2 = z^2$

A continuación estudiaremos las soluciones de la ecuación $x^2+y^2 = Z^2$ (enteros Pitagóricos) para enteros x, y, z mayores que cero y tal que $(x, y, z) = 1$

Primero observemos que x, y, z no pueden ser todos pares ya que se tendría $(x, y, z) \geq 2$

Tampoco pueden ser todos impares pues en tal caso se tiene que x^2, y^2, Z^2 serían impares y x^2+y^2 sería par pero Z^2 impar.

De la misma forma vemos que no se puede dar el caso de dos pares y un impar.

Por lo tanto, uno de ellos debe ser par y los otros dos impares.

Pero Z no puede ser par, pues se tendría

$$z = 2k_1, \qquad x = 2k_2+1, \qquad y = 2k_3+1$$

$\therefore$ $z^2 = 4k_1^2$ es decir, $z^2 \equiv 0 \pmod 4$ y por otra parte

$$z^2 = x^2+y^2 = 4k_2^2+4k_2+1+4k_3^2+4k_3+1 \equiv 2 \pmod 4$$

lo que es absurdo.

Luego, x o y es par y los otros dos impares. Sin pérdida de generalidad podemos suponer que x es par y por lo tanto y, z son impares.

De $x^2+y^2 = z^2$ se tiene que

$$x^2 = (z^2-y^2) = (z+y)(z-y)$$

luego, $(\frac{x}{2})^2 = \frac{z+y}{2} \cdot \frac{z-y}{2}$ es un entero ya que x es par

Además se tiene que $(\frac{z+y}{2}, \frac{z-y}{2}) = 1$, pues si $(\frac{z+y}{2}, \frac{z-y}{2}) \neq 1$, entonces existe primo p tal que divide a $\frac{z+y}{2}$ y a $\frac{z-y}{2}$. Por lo tanto, p divide a $\frac{z+y}{2} + \frac{z-y}{2} = z$ y a $\frac{z+y}{2} - \frac{z-y}{2} = y$ luego, p divide a x pues $x^2 = z^2-y^2$, pero esto es absurdo ya que $(x,y,z) = 1$, luego $(\frac{z+y}{2}, \frac{z-y}{2}) = 1$

Entonces, $\frac{z+y}{2} = u^2$, $\frac{z-y}{2} = v^2$ para ciertos enteros positivos no nulos u, v tales que $(u, v) = 1$

Por lo tanto: $z = u^2+v^2$

$y = u^2-v^2 \quad \Longrightarrow \quad u > v$

$(\frac{x}{2})^2 = u^2 \cdot v^2 \quad \Longrightarrow \quad x = 2uv$

Es decir, las soluciones de la ecuación $x^2+y^2 = z^2$, son los enteros de la forma: $x = 2uv$

$y = u^2-v^2$

$z = u^2+v^2$

con u, v enteros positivos no nulos y tal que $(u, v) = 1$ y $u > v$

Efectivamente, son soluciones al problema, pues :

$(2uv)^2+(u^2-v^2)^2 = 4u^2v^2+u^4-2u^2v^2+v^4$

$= u^4+2u^2v^2+v^4$

$= (u^2+v^2)^2$

Por ejemplo, tomando $u = 2$ y $v = 1$
tenemos $x = 4$, $y = 3$, $z = 5$ que son los enteros pitagóricos más conocidos.

En general, la ecuación $x^n+y^n = z^n$ con x, y, z enteros positivos no nulos y n natural no tiene solución.

Más aún, el matemático Fermat conjeturó (hasta el momento no se ha podido demostrar) que la ecuación $x^n+y^n = z^n$ no tiene solución para $n > 2$.

El lector puede encontrar en la bibliografía las demostraciones para los casos $n = 3$ y $n = 4$, es decir, se demuestra que las ecuaciones $x^3+y^3 = z^3$ y $x^4+y^4 = z^4$ no tienen solución.

Ejercicios:

1.- Probar que si $x^2+y^2 = z^2$, entonces uno de: x, y, es múltiplo de 3 y uno de: x, y, z, es un múltiplo de 5.

Sabemos que $x = 2uv$, $y = u^2-v^2$, $z = u^2+v^2$ con $u > v > 0$ y $(u,v) = 1$

Estudie los casos $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 3$ $x \equiv 2 \pmod 3$ y $y \equiv 0 \pmod 3$, $y \equiv 1 \pmod 3$ $y \equiv 2 \pmod 3$ siendo x, y enteros cualesquiera debe ocurrir alguno de los casos anteriores. Haga lo mismo colocando 5 en lugar de 3 y tendrá demostrado el problema)

2.- Probar que todo entero n puede expresarse en la forma

$n = x^2+y^2-z^2$

3.- Demuestre que $x^2+y^2 = z^4$ tiene un número infinito de soluciones con $(x, y, z) = 1$

(Observe que $z^2 = u^2+v^2$ cuyas soluciones usted conoce)

4.- Demuestre que $x^4+y^4 = z^2$ no tiene solución para x, y, z enteros positivos no nulos con $(x, y, z) = 1$.

- - - - - - - - - - -

B I B L I O G R A F I A

- BURTON W. JONES — TEORIA DE LOS NUMEROS
- DICKSON, EUGENE — INTRODUCTION TO THE THEORY OF NUMBERS
- ANTHONY J. PETTOFREZZO, DONALD R. BYRKIT — INTRODUCCION A LA TEORIA DE LOS NUMEROS

- - - - - - -

/ecpm.