CONGRUENCIAS

Por:
ANA MARCELA CHARRY HERNANDEZ
Código 2005104300
MARCO ANTONIO TRUJILLO OCAMPO
Código 2005100236

Asesor:
Magister
RICARDO CEDEÑO TOVAR

UNIVERSIDAD SURCOLOMBIANA
FACULTAD DE EDUCACIÓN
LICENCIATURA EN MATEMÁTICAS
NEIVA - HUILA
2010

CONGRUENCIAS

Por:
ANA MARCELA CHARRY HERNANDEZ
Código 2005104300
MARCO ANTONIO TRUJILLO OCAMPO
Código 2005100236

Trabajo presentado como requisito para grado

Asesor:
Magister
RICARDO CEDEÑO TOVAR

UNIVERSIDAD SURCOLOMBIANA
FACULTAD DE EDUCACIÓN
LICENCIATURA EN MATEMÁTICAS
NEIVA - HUILA
2010

Índice general

Capítulo 1

AGRADECIMIENTOS

Damos gracias a Dios quien nos dio la vida y salud para sacar adelante esta honorable carrera, a nuestros padres que por su esfuerzo y apoyo nos brindaron una educación integra, a nuestros hermanos y familiares que con su apoyo y acompañamiento nos dieron fuerzas para seguir adelante.

A la universidad surcolombiana que nos dio la oportunidad de adquirir una educación superior y de excelente calidad, específicamente al programa de Licenciatura en Matemáticas que con su admirable equipo de trabajo ayudaron a nuestra formación como profesionales.

Agradecer también a aquellos docente que dejaron una huella significativa en este proceso de formación; especialista Hernando Gutiérrez Hoyos, magister Augusto Silva que fue nuestro segundo lector y a nuestro gran profesor y amigo magister Ricardo Cedeño Tovar que aparte de ser nuestro asesor y jefe de programa nos brindo su apoyo, tiempo y dedicación para la elaboración de este trabajo.

Por ultimo a nuestros compañeros y amigos con los cuales se vivieron y compartieron buenos y malos momentos durante el transcurso de nuestra formación como docentes.

Capítulo 2
PRESENTACIÓN

A través de la historia los hombres dedicados a las ciencias naturales han planteado diversas teorías basadas en los diferentes temas que conforman las ciencias exactas, en particular las matemáticas.

Si retomamos la historia de esta ciencia podemos decir que la teoría de números se inició con el matemático griego Diofanto quien vivió en Alejandría aproximadamente 250 años $a.\ C.$ Los escritos de Diofanto parecen haber sido dedicados a la solución de varias ecuaciones algebraicas en números enteros y alguna veces en números racionales. Estos trabajos fueron continuados por otros matemáticos, que posteriormente fueron reconocidos al padre de la teoría de números Pierre Fermat.

Para Pierre Fermat la contribución que dejo Diofanto fue la que lo inspiró a convertir la teoría de números en una rama sistemática del conocimiento.

La matemática es una herramienta muy útil en nuestra sociedad y la teoría de números es una de sus ramas más importantes, la cual se encarga de estudiar los números enteros sin emplear teorías procedentes de otros campos, citando por ejemplo las propiedades de los números enteros y en ocasiones de los reales o complejos que dependen directamente de los números enteros. La teoría de números tiene gran influencia en las matemáticas puras, por eso para muchos matemáticos es considerada como la reina de las matemáticas.

En la teoría de números podemos encontrar diversos temas de mucho interés, los cuales se pueden estudiar con gran afinidad. Uno de estos temas es el de

2. PRESENTACIÓN

Congruencia Modular, que es una simplificación de muchos problemas relativos a la divisibilidad en los enteros. Dados dos números enteros ($\mathbb{Z}$); a, y, b, si ellos dejan el mismo resto al dividirlos por un número natural m, llamado *Módulo*, diremos que a es congruente con b, módulo m y lo notaron como $a \equiv b(\text{mód } m)$.

Este concepto fue introducido y estudiado principalmente por Carl Friedrich Gauss en 1.810 en su obra *Disquisitiones Arithmeticae*. La aritmética modular se aplica en: Teoría de números, Algebra abstracta y Criptografía, pero en la actualidad ésta se ve aplicada en la programación de las computadoras.

En este trabajo se pretende explicar el concepto de *Congruencia Modular* y sus principales teoremas con ejemplos prácticos y con un lenguaje más sencillo para el lector.

Capítulo 3
JUSTIFICACIÓN

Este trabajo de investigación se realiza como requisito para optar al título de Licenciado en Matemáticas de la Universidad Surcolombiana, además ponemos a prueba nuestro aprendizaje adquirido en el transcurso de nuestra carrera para un buen desarrollo de los temas aquí tratados.

Pretendemos iniciarnos como investigadores profundizando en conocimientos específicos del área de matemáticas como la *Congruencia Modular*, en este proceso de construcción se comprenderán los conceptos básicos de la teoría de números, se estudiarán algunos teoremas que complementarán el estudio sobre la congruencia modular y sus campos de aplicación.

Esto nos ha permitido profundizar en múltiples aspectos relacionados con *Congruencia Modular*, desde lo más general a lo más específico adquiriendo una idea clara y concisa, avanzando así en nuestra formación como matemáticos.

Capítulo 4
OBJETIVOS

4.1. OBJETIVO GENERAL

Profundizar, ampliar y dar a conocer todo lo referente a la *Congruencia Modular*, su manejo y utilización en situaciones teóricas y prácticas. Se presenta un trabajo completo y claro, que permite a los futuros lectores la comprensión sobre el tema.

4.2. OBJETIVOS ESPECIFICOS

1. Conocer los antecedentes relacionados a la *Congruencia Modular* con el fin de valorar y ampliar la información sobre el tema.

2. Introducir conceptos básicos de la teoría elemental de números como la *divisibilidad*, el $m.c.d$, presentar su teoría y los métodos de solución de congruencias y ecuaciones en congruencia, creando así una mentalidad de trabajo independiente.

3. Dar a conocer al programa de Licenciatura en Matemáticas y al lector la existencia de la congruencia modular en la teoría de números.

4. OBJETIVOS

4. Conocer la utilidad de la *Congruencia Modular* en los diferentes campos de aplicabilidad.

5. Capacitar al lector en el manejo teorico y en la aplicacion de los conceptos básicos de la teoría de números.

Capítulo 5

DIVISIBILIDAD

La divisibilidad en la teoría de números, es el instrumento de análisis que se usa para explorar propiedades e indagar por interrelaciones numéricas.

Si clasificamos los números enteros en pares e impares estamos averiguando si un número entero es o no divisible por dos, de igual forma podemos averiguar si un número entero es primo o no.

Consideremos a $\mathbb{Z}$ como el conjunto de números enteros. Dados dos números enteros a y b ($a \in \mathbb{Z}, b \in \mathbb{Z}$), decimos que a divide a b, lo notamos $a|b$ si existe otro número entero c tal que $b = ac$. Si a no divide a b, lo notamos $a \nmid b$.

Por ejemplo $2 \mid 4$ y $5 \mid 0$, puesto que el primer caso existe el número entero 2 tal que $4 = 2 \cdot 2$ y en el segundo caso existe el número entero 0 tal que $0 = 5 \cdot 0$.
Si $b = ac$, y, c es el número 2 decimos que b es un número par.

Un número entero n es un número par o impar, si existe un número entero k tal que $n = 2k$, ó, $n = 2k + 1$ respectivamente.

De igual manera diremos que el número entero $p > 1$ es un número primo si sus únicos divisores positivos son p y 1 (dicho de otra manera, un número entero $p > 1$ es un número primo si tiene exactamente dos divisores positivos).

El concepto de máximo común divisor se entiende como: dados dos números enteros positivos a y b, su máximo común divisor ($m.c.d.$) es el mayor de los divisores comunes de ambos números. El máximo común divisor entre a y b lo

denotaremos como $m.c.d.(a, b)$

Siempre existirá el $m.c.d.$ de dos o más números enteros positivos, puesto que el 1 siempre será un divisor común.

Por ejemplo, hallemos el $m.c.d.$ de 42 y 56. Para ello hallaremos los divisores comunes de 42 y 56, ellos son: 1, 2, 7, y 14, luego el $m.c.d.$ de 42 y 56 es 14. Es decir $m.c.d.(42, 56) = 14$.

5.1. PROPIEDADES

Sean a, b, c números enteros.

1. El número 1 divide a a, es decir $1 \mid a$. Puesto que $a = 1 \cdot a$.
   Así tenemos que $1|21$; $1|5$ y $1|0$ porque $21 = 1 \cdot 21$; $5 = 1 \cdot 5$ y $0 = 1 \cdot 0$.

2. Si $a \neq 0$ entonces a divide a a, es decir $a \mid a$. Puesto que $a = a \cdot 1$.
   Así tenemos que $-3|-3$ y $20|20$ porque $-3 = 1 \cdot (-3)$ y $20 = 1 \cdot 20$

3. Si a divide a b siendo $b \neq 0$ entonces el valor absoluto de a es menor o igual que el valor absoluto de b, es decir, si $a|b$ con $b \neq 0$, entonces $|a| \leq |b|$, por que si $a|b$ significa que existe $c \in \mathbb{Z}$ tal que $b = a \cdot c$. De aquí $|b| = |a \cdot c| = |a||c|$. Como $c \neq 0$ esto lleva a que $|c| \geq 1$, por lo tanto $|a| \leq |a||c| = |ac| = |b|$.

   Por ejemplo, $-9|27$ y es claro que $|-9| \leq |27|$.

4. Si a divide a b y b divide a a entonces el valor absoluto de a es igual al valor absoluto de b, es decir si $a|b$ y $b|a$ entonces $|a| = |b|$. Efectivamente, si $a|b$, y, $b|a$ existen enteros m, y, n tales que $b = ma$, y, $a = nb$, por lo tanto, $b = ma = m(nb) = mnb$, así que, $mn = 1$ luego $m = 1 = n$, ó, $m = -1 = n$. De aquí $b = a$, ó, $b = -a$, lo cual indica que $|a| = |b|$.

   Por ejemplo, $-7|7$, y, $7|-7$ por lo tanto $|7| = |-7|$.

5. Si a divide a b, y, b divide a c entonces a divide a c, es decir, si $a|b$ y $b|c$ entonces $a|c$. Efectivamente, si $a|b$, y, $b|c$; entonces $b = ma$, y, $c = nb$; para algún $m, n \in \mathbb{Z}$. Así que $c = nb = n(ma) = (nm)a$, de esto deducimos que $a|c$.

Por ejemplo, sabemos que 4|32, y, 32|192 por lo tanto 4|192

6. Si c divide a a y c divide a b entonces c divide a cualquier combinación lineal de a y b, es decir, si $c|a$ y $c|b$ entonces $c|(ar+bs)$ para todo r y s que pertenezcan a los enteros. En efecto, si $c|a$, y, $c|b$ entonces $a = mc$, y, $b = nc$, luego $ra+sb = r(mc)+s(nc) = (rm)c+(sn)c = (rm+sn)c$, así que $c|(ra+sb)$.

   Por ejemplo, sabemos que 6|12, y, 6|18 así que $6|12r+18t$, ya que, $12r+18t = 6(2r+3t)$.

5.2. ALGORITMO DE EUCLIDES

Al dividir a entre b (números enteros), se obtiene un cociente q y un residuo r. Es decir, si tenemos dos enteros a y b con $b \neq 0$ existen enteros únicos q y r tales que $b = aq + r$, donde $0 \leq r < |a|$.

Consideremos el siguiente conjunto $A = \{b - at : t \in \mathbb{Z}\}$. Luego $A \cap (\mathbb{N} \cup \{0\})$ es un conjunto no vacío y tiene un primer elemento por el principio del buen orden, llamaremos r a ese elemento. Como $r \in A$, existe un $q \in \mathbb{Z}$ tal que $r = b - aq$. Si $r \geq |a|$ entonces $r - |a| \geq 0$ y es un elemento de A lo que contradice que r es el elemento más pequeño de la intersección, luego $0 \leq r \leq |a|$

Para ver la unicidad, supongamos que $b = aq_1 + r_1 = aq_2 + r_2$, con, $0 \leq r_i < |a|$. Luego $|r_1 - r_2| \leq$máx $\{r_1, r_2\} < |a|$. Además $r_1 - r_2 = a(q_1 - q_2)$, así que, $a|(r_1 - r_2)$. Supongamos que $r_1 \neq r_2$ entonces $|a| \leq |r_1 - r_2|$ lo que es absurdo, con lo cual $r_1 = r_2$ y $q_1 = q_2$.

Teorema 5.1. Si a y b son enteros positivos con $a \geq b$ y si $a = qb + r$ entonces $m.c.d.(a, b) = m.c.d.(b, r)$.

Sea $d = m.c.d.(a, b)$, luego $d|a$ y $d|b$, de donde $d|(a - qb)$. Como $a - qb = r$, se tiene que $d|r$. Luego d es divisor común de b y r.

Por otra parte, si $c|b$ y $c|r$, entonces $c|(qb + r)$. Como $qb + r = a$, entonces $c|a$. De

lo anterior tenemos que c es un divisor común de a y b.

Como $d = m.c.d.(a, b)$ se tiene que $c \leq d$. Luego $d = m.c.d.(b, r)$.

Algoritmo de Euclides.

El máximo común divisor de dos enteros puede obtenerse escogiendo el mayor de todos los divisores comunes a estos. Hay un proceso más eficiente que utiliza repetidamente el algoritmo de la división. Este método se llama algoritmo de Euclides.

El algoritmo de Euclides se describe de la siguiente forma: Dados dos enteros a y b cuyo máximo común divisor se desea hallar, y asumiendo que $0 < b < a$. Se siguen los siguientes pasos:

1. Se usa el algoritmo de la división para obtener $a = q_1 b + r_1$ con $0 \leq r_1 < b$. Si $r_1 = 0$, entonces, $a = q_1 b$ así que $b|a$, por lo tanto, $m.c.d.(a, b) = b$.

2. Si $r_1 \neq 0$ se divide b por r_1 y se producen los enteros q_2 y r_2 que satisfacen $b = q_2 \cdot r_1 + r_2$ con $0 \leq r_2 < r_1$. Si $r_2 = 0$ el proceso termina, ya que $b = q_2 r_1$, y, $m.c.d - (b, r_1) = r_1$.

3. Si $r_2 \neq 0$ se procede a dividir r_2 por r_1 obteniendo $r_1 = q_3 \cdot r_2 + r_3$ con $0 \leq r_3 < r_2$.

4. Este proceso continua hasta que algún residuo cero aparece. Esto ocurre porque en la secuencia $b > r_1 > r_2 > ..... \geq 0$ no puede haber más de b enteros. Es decir, el proceso es finito.

5. En estas circunstancias, el máximo común divisor de a y b no es más que el último residuo distinto de cero del proceso anterior.

Ejemplo:

1. Para hallar el $m.c.d.(12378, 3054)$, tenemos que $12378 = 4 \cdot 3054 + 162$, y, $3054 = 18 \cdot 162 + 138$, además $162 = 1 \cdot 138 + 24$, mientras que $138 = 5 \cdot 24 + 18$,

también $24 = 1 \cdot 18 + 6$ y finalmente $18 = 3 \cdot 6 + 0$. Luego $m.c.d.(12378, 3054) = 6$ que es el último residuo distinto de cero.

Como $m.c.d.(12378, 3054) = 6$ podemos utilizar el resultado anterior para encontrar enteros x y y que cumplan la condición: $6 = 12378x + 3054y$.

Efectivamente $6 = 24 - 18 = 24 - (138 - 5 \cdot 24) = 6 \cdot 24 - 138 = 6 \cdot (162 - 138) - 138 = 6 \cdot 162 - 7 \cdot 138 = 6 \cdot 162 - 7 \cdot 3054 - 18 \cdot 162 = 132 \cdot 162 - 7 \cdot 3054 = 132 \cdot (12378 - 4 \cdot 3054) - 7 \cdot 3054 = 132 \cdot 12378 + (-535) \cdot 3054$. Así que $x = 132$; $y = -535$

Capítulo 6
CONGRUENCIAS

DEFINICIÓN. Dados los enteros a, b, m con $m > 0$, decimos que a es congruente con b módulo m, y lo escribimos como

$$a \equiv b(\text{mód } m), \text{ si } m \text{ divide a la diferencia } (a - b).$$

El número m se llama módulo de la congruencia. En otras palabras, la congruencia $a \equiv b(\text{mód } m)$ es equivalente a la relación de divisibilidad.

$$m \mid (a - b).$$

En particular, $a \equiv 0(\text{mód } m)$ si y sólo si, $m \mid a$. Por lo tanto $a \equiv b(\text{mód } m)$ si y sólo si, $a - b \equiv 0(\text{mód } m)$. Ahora si $m \nmid (a - b)$, decimos que a no es congruente con b módulo m y lo escribimos $a \not\equiv b(\text{mód } m)$

EJEMPLOS

1. $19 \equiv 7(\text{mód } 12)$, porque $12 \mid (19 - 7)$ pues $12|12$
2. $1 \equiv -1(\text{mód } 2)$, porque $2 \mid [1 - (-1)]$ pues $2|2$
3. $3^2 \equiv -1(\text{mód } 2)$, porque $2 \mid [3^2 - (-1)]$ pues $2|10$
4. Si n es un número par entonces $n = 2k$, para algún $k \in \mathbb{Z}$. Por lo tanto $2|n$ y así $n \equiv 0(\text{mód } 2)$. Por otra parte si $n \equiv 0(\text{mód } 2)$ entonces $2|n$, y, n es un número par, es decir, n es un número par si y sólo si $n \equiv 0(\text{mód } 2)$.
5. Sea n un número impar, entonces; $n = 2k + 1$, para algún $k \in \mathbb{Z}$, luego $n - 1 = 2k$, por lo tanto, $2|(n - 1)$, así que, $n - 1 \equiv 0(\text{mód } 2)$, y de esto,

$n \equiv 1(\text{mód } 2)$. Por otra parte sí, $n \equiv 1(\text{mód } 2)$, entonces, $2|(n-1)$, y de aquí, $n-1 = 2k$, para algún, $k \in \mathbb{Z}$, de esto tenemos que, $n = 2k+1$, luego n es un número impar, es decir, n es un número impar si y sólo si $n \equiv 1(\text{mód } 2)$.

6. Encontrar cinco número enteros distintos, cada uno de los cuales sea congruente con 13 módulo 11.
   Sea a cualquiera de los números buscados. Entonces, $a \equiv 13(\text{mód } 11)$, es decir, $11|(a-13)$, luego, $a-13 = 11q$, para algún $q \in \mathbb{Z}$, así que, $a = 13+11q$. Si ahora tomamos, por ejemplo, $q = -2, -1, 0, 1, 2$ tendremos los cinco números buscados ya que si remplazamos tendremos:

$$a = 13 + 11(-2) = -9$$
$$a = 13 + 11(-1) = 2$$
$$a = 13 + 11(0) = 13$$
$$a = 13 + 11(1) = 24$$
$$a = 13 + 11(2) = 35$$

   Obsérvese que estos números forman una progresión aritmética.

El símbolo de congruencia ($\equiv$) fue elegido por Gauss para sugerir una analogía con el signo de igualdad ($=$). Los dos teoremas que siguen prueban que las congruencias tienen de hecho muchas de las propiedades formales de las igualdad.

Teorema 6.1 La congruencia es una relación de equivalencia.

a) a es congruente con a módulo m, es decir, $a \equiv a(\text{mód } m)$. Porque $m|(a-a)$ esto es $m|0$. (reflexividad)

b) Si a es congruente con b módulo m, entonces b es congruente con a módulo m, es decir si, $a \equiv b(\text{mód } m)$ implica $b \equiv a(\text{mód } m)$.
   En efecto si $a \equiv b(\text{mód } m)$ entonces $m \mid (a-b) = -(b-a)$, es decir, $m|b-a$, por lo tanto, $b-a = km$, de donde, $b \equiv a(\text{mód } m)$. (simetria)

c) Si a es congruente con b módulo m, y, b es congruente con c módulo m, entonces a es congruente con c módulo m, es decir, si $a \equiv b(\text{mód } m)$, y,

$b \equiv c(\text{mód } m)$, entonces, $a \equiv c(\text{mód } m)$, puesto que, $a \equiv b(\text{mód } m)$, y, $b \equiv c(\text{mód } m)$; significa que, $m \mid (a-b)$, y, $m \mid (b-c)$, por lo tanto, $m \mid (a-b)+(b-c) = (a-c)$, de donde, $a \equiv c(\text{mód } m)$ (transitividad)

A continuación ilustraremos este teorema con algunos ejemplos.

(a) $5 \equiv 5(\text{mód } 4)$; $100 \equiv 100(\text{mód } 6)$ porque 4 y 6 dividen a 0

(b) $8 \equiv 2(\text{mód } 3)$, y, $2 \equiv 8(\text{mód } 3)$ porque $3| \pm 6$

(c) $8 \equiv -3(\text{mód } 11)$, y, $-3 \equiv -14(\text{mód } 11)$ entonces $8 \equiv -14(\text{mód } 11)$ puesto que $11|22$

Teorema 6.2 Si $a \equiv b(\text{ mód } m)$ y $\alpha \equiv \beta(\text{mód } m)$, entonces:

(a) $ax + \alpha y \equiv (bx + \beta y)(\text{mód } m)$ para todo entero x e y .

(b) $a\alpha \equiv b\beta(\text{mód } m)$.

(c) $a^n \equiv b^n(\text{mód } m)$ para cada entero positivo n.

(d) Para todo $r \in \mathbb{Z}, a + r \equiv (b + r)(\text{mód } m)$.

Demostración.

(a) Si $a \equiv b(\text{mód } m)$, y, $\alpha \equiv \beta(\text{mód } m)$, entonces, $m|(a-b)$, y, $m|(\alpha-\beta)$, por lo tanto, $m|x(a-b)$, y, $m|y(\alpha-\beta)$, así que, $m|[(ax-bx)+(\alpha y-\beta y)]$, es decir, $m|(ax+\alpha y)-(bx+\beta y)$, esto significa que, $(ax+\alpha y) \equiv (bx+\beta y)$ (mód m).

(b) Puesto que $m|(a-b)$, y, $m|(\alpha-\beta)$, entonces, $a = b + xm$, y, $\alpha = \beta + my$, así que $a\alpha = (b+xm)(\beta+ym) = b\beta + m(x\beta + by + mxy)$, de donde, $a\alpha \equiv b\beta(\text{mód } m)$.

(c) Puesto que $a = mx + b$ entonces $a^n = (mx+b)^n = b^n + mp(b, m, x)$, lo cual significa que $a^n \equiv b^n(\text{mód } m)$ donde $p(b, m, x)$ es un polinomio que depende de b, m y x.

(d) Puesto que $a = b + mx$, entonces, $a + r = b + r + mx$, así que $(a + r) \equiv (b + r)(\text{mód } m)$.

A continuación se ilustra con algunos ejemplos este teorema.

Puesto que $4 \equiv 1(\text{mód } 3)$, y, $5 \equiv 2(\text{mód } 3)$, entonces $140 \equiv 50(\text{mód } 3)$, puesto que, $140 = 4(10) + 5(20)$, y, $50 = 1(10) + 2(20)$.

Además $20 \equiv 2(\text{mód } 3)$, por que, $20 = 4(5)$, y, $2 = 1(2)$.

También $4^n \equiv 1(\text{mód } 3)$, porque, $4^n - 1$ es divisible por 3. Efectivamente supongamos que $4^n - 1 = 3m$, veamos que, $4^{n+1} - 1 = 3l$, luego, $4^{n+1} - 1 = 4(4^n) - 1 = 4(3m + 1) - 1 = 12m + 3 = 3(4m + 1) = 3l$, donde $l = 4m + 1$.

De igual forma: $4 + r \equiv (1 + r)(\text{mód } 3)$, puesto que $3|[(4 + r) - (1 + r)]$.

El **teorema 6.2** nos dice que dos congruencias respecto del mismo módulo se puede sumar, restar o multiplicar, miembro a miembro, como si fueran igualdades. El mismo resultado es verdadero para un número finito de congruencias respecto al mismo módulo.

Antes de desarrollar más propiedades de las congruencias daremos dos ejemplos que ilustran su utilidad.

Ejemplo 1
Regla de divisibilidad por 9. Un entero $n > 0$ es divisible por 9 si y sólo si, la suma de los dígitos de su expresión decimal es divisible por 9. Es decir si $n = a_0 + 10a_1 + 10^2a_2 + ... + 10^ka_k$, entonces n es divisible por 9, si y sólo si $9|(a_0 + a_1 + ... + a_k)$. Puesto que, $9|10^n - 1$, para todo número natural n, entonces, $10^n \equiv 1(\text{mód } 9)$, así que por el teorema 5.2 tendriamos que, $10^n a_n \equiv a_n(\text{mód } 9)$, también tendriamos que, $a_0+10a_1+...+10^ka_k \equiv (a_0+a_1+...+a_k)(\text{mód } 9)$, es decir $n \equiv (a_0+a_1+...+a_k)$ (mód 9).

Podemos notar también que todas estas congruencias son validas para módulo 3, luego un número es divisible por 3 si y sólo si, la suma de sus dígitos es divisible por 3. Con mayor precisión:

Un entero $n > 0$ es divisible por 3 si y sólo si, la suma de los dígitos de su expresión decimal es divisible por 3. Es decir si $n = a_0 + 10a_1 + 10^2a_2 + ... + 10^ka_k$, entonces n es divisible por 3, si y sólo si $3|(a_0 + a_1 + ... + a_k)$. Puesto que, $3|10^n - 1$, para todo número natural n, entonces, $10^n \equiv 1$(mód 3), así que, $10^n a_n \equiv a_n$ (mód 3), por lo tanto, $a_0 + 10a_1 + ... + 10^ka_k \equiv (a_0 + a_1 + ... + a_k)$(mód 3), es decir $n \equiv (a_0 + a_1 + ... + a_k)$(mód 3).

Ejemplo 2
Los números de Fermat definidos como $F_n = 2^{2^n} + 1$, donde $n \in \{0, 1, 2, 3, ...\}$. Los primeros cinco números de Fermat son primos:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad \text{y } F_4 = 65537.$$

Ahora probaremos que F_5 es divisible por 641 sin calcular explicitamente F_5. Para ello consideramos la sucesión de potencias 2^{2^n} módulo 641. Tenemos

$$2^2 = 4 \equiv 4(\text{ mod } 641)$$
$$2^4 = 16 \equiv 16(\text{ mód } 641)$$
$$2^8 = 256 \equiv 256(\text{ mód } 641)$$
$$2^{16} = 65536 \equiv 154(\text{ mód } 641), \text{ porque } 65536 = (102)(641) + 154,$$

Entonces
$2^{32} \equiv (154)^2$(mód 641), es decir $2^{32} \equiv 23716$(mód 641) y $23716 \equiv 640$(mód 641) porque $23716 = (614)(36) + 640 = (641)(37) - 1$, así que $23716 \equiv -1$(mód 641).

De aquí se puede concluir que $F_5 = 2^{32} + 1 \equiv 0$(mód 641).

Ahora, si calculamos a F_5 explícitamente tendremos:

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417.$$

Podemos concluir, que este número no es un número primo si no un número compuesto ya que tiene más de dos divisores.

En general no es posible simplificar factores comúnes no nulos de ambos miembros de una congruencia aún cuando sea posible en las igualdades.

Por ejemplo, $48 \equiv 18(\text{mód } 10)$, 48 y 18 son múltiplos de 6, pero al simplificar por 6 obtenemos, $8 \equiv 3(\text{mód } 10)$, lo cual no es cierto.

El teorema que sigue prueba que un factor común se puede simplificar si el módulo es divisible por dicho factor.

Teorema 6.3 Sea $c > 0$ entonces, $a \equiv b(\text{mód } m)$ si y sólo si, $ac \equiv bc(\text{mód } mc)$.

En efecto: $m \mid (b-a)$ si y sólo si, $cm \mid c(b-a)$.

Por ejemplo, como $18 \equiv 3(\text{mód } 15)$ entonces $6 \equiv 1(\text{mód } 5)$.

El siguiente teorema describe una regla de simplificar válida cuando el módulo no sea divisible por un factor común.

Teorema 6.4 Ley de simplificación.

Si $ac \equiv bc(\text{mód } m)$ y si $d = m.c.d.(m, c)$, entonces $a \equiv b(\text{mód } \frac{m}{d})$.

En otras palabras, un factor común c se puede simplificar si el módulo se divide por $d = m.c.d.(m, c)$. En particular, un factor común que es primo relativo con el módulo se puede simplificar siempre.

Dado que $ac \equiv bc(\text{mód } m)$ tenemos que $m|(ca-cb)$, por lo tanto, $\frac{m}{d}|\frac{c(a-b)}{d}$, sabemos que $m.c.d.(\frac{m}{d}, \frac{c}{d}) = 1$ entonces $\frac{m}{d}|(a-b)$, así que $a \equiv b(\text{mód } \frac{m}{d})$

Ejemplo:
Sean $a \equiv b(\text{mód } m)$ y $d = m.c.d.(a, b)$. Si $d|m$ y $d|a$, entonces $d|b$, por lo tanto $a \equiv b(\text{mód } \frac{m}{d})$.

Puesto que $156 \equiv 60(\text{mód } 4)$ y $m.c.d.(4, 6) = 2$, entonces $78 \equiv 30(\text{mód } 2)$.

Teorema 6.5 Supongamos que $a \equiv b(\text{mód } m)$. Si $d|m$ y $d|a$, entonces $d|b$.

$a \equiv b(\text{mód } m)$ esto significa que $m|a-b$, como $d|m$, entonces $d|(a-b)$, aqui $a-b=dk$, como $d|a$, y, $a=ld$, por lo tanto $ld-dk=b=d(l-k)$ así que $d|b$.

Ejemplo, como $26 \equiv 2(\text{mód } 4)$; $2|4$, y, $2|26$, entonces $\frac{26}{2} \equiv \frac{2}{2}(\text{mód } 4)$ es decir $13 \equiv 1(\text{mód } 4)$.

Teorema 6.6 Si $a \equiv b(\text{mód } m)$ entonces $m.c.d.(a,m) = m.c.d.(b,m)$. Con otras palabras, los números que son congruentes módulo m tienen el mismo máximo común divisor con m.

En efecto: $a \equiv b(\text{mód } m)$ si y sólo si $m|(a-b)$, de donde $a-b=mg$, para algún $g \in \mathbb{Z}$. Ahora, sea $d = m.c.d.(a,m)$ y $e = m.c.d.(b,m)$, entonces, $d|a$ y $d|m$ luego $d|mg = (a-b)$ entonces $d|[a-(a-b)]$, de aquí $d|b$, puesto que d divide a m, se tiene que d es el máximo común divisor de b, y, m, es decir $d|e$. De igual manera $e|b$ y $e|m$, de aqui $e|mg = (a-b)$, entonces $e|(a-b)+b$ de aqui $e|a$, por lo tanto e divide al máximo común divisor de a y m, luego $e|d$, por lo tanto $d=e$.

Ejemplo:
Puesto que, $50 \equiv 15(\text{mód } 35)$, y el $m.c.d.(50,35) = 5 = m.c.d(15,35)$, entonces $\frac{50}{5} \equiv \frac{15}{5}(\text{mód } \frac{35}{5})$, es decir $10 \equiv 3(\text{mód } 7)$.

Teorema 6.7 Sí $a \equiv b(\text{mód } m)$ y si $0 \leq |b-a| < m$ entonces $a=b$

Como $m|(a-b)$ tenemos $m \leq |a-b|$ y como por hipótesis $0 \leq |b-a| < m$, esto implica que $|a-b|=0$, así que $a=b$.

Teorema 6.8 $a \equiv b(\text{mód } m)$ si y sólo si a y b tienen el mismo resto cuando se dividen por m.

Puesto que $a \equiv b(\text{mód } m)$, entonces $a = b + tm$, pero por lo otro lado $a = mq + r$; así que $mq + r = b + tm$; es decir $b = m(q - t) + r$, lo cual significa que r es el residuo de dividir a b por m.

Reciprocamente, si a, y, b tienen el mismo residuo al dividirlos por m, veamos que $a \equiv b(\text{mód } m)$. Del enunciado tenemos que $a = qm + r$, y, $b = km + r$. Así que $a - b = qm - km = (q - k)m$, es decir $a \equiv b(\text{mód } m)$.

Ejemplo.
Puesto que $12 \equiv 7(\text{mód } 5)$, luego $5|(12-7) = 5$; además $12 = 5k+r_1$, y, $7 = 5q+r_2$, para algún $k, q \in \mathbb{Z}$. Si $k = 2$, y, $q = 1$, entonces, $12 = 5(2) + r_1$, y, $7 = 5(1) + r_2$, de donde $r_1 = 12 - 10 = 2$, y, $r_2 = 7 - 5 = 2$, por lo tanto $r_1 = r_2$.

6.1. CONGRUENCIAS LINEALES

Una congruencia lineal es de la forma $ax \equiv b(\text{mód } m)$, donde $a, b, m \in \mathbb{Z}, m > 1$ y x es una variable.

Teorema 6.9 La congruencia $ax \equiv b(\text{mód } m)$ tiene solución si y sólo si $d|b$ donde $d = m.c.d.(m, a)$.

De $ax \equiv b(\text{mód } m)$ se deduce que $m|(ax - b)$, así que $ax - b = mk$, por lo tanto $b = ax - mk$ con $k \in \mathbb{Z}$. Puesto que $d|a$ y $d|m$ entonces $d|ax$, y, $d|mk$, así que $d|(ax - mk) = b$.

Si $d = m.c.d.(m, a)$ entonces $d = ms + at$, y como $d|b$, entonces $b = kd = k(ms + at) = m(ks) + a(tk)$, así que $a(tk) - b = m(-ks)$, haciendo $x = tk$, tenmos que $ax - b = m(-ks)$. Por lo tanto $ax \equiv b(\text{mód } m)$.

NOTA: Una condición necesaria y suficiente para que la congruencia $ax \equiv b(\text{mod } m)$, tenga solución es que $m.c.d.(m, a)|b$ y si este es el caso entonces existen exactamente (m, a) soluciones (mód m). Si hallamos una solucion x_0 entonces podemos hallar las otras soluciones utilizando la siguiente fórmula

$x = x_0 + \frac{km}{d}$ en donde $k = 0, 1, 2, ..., d-1$.

Sí x_0 es solución de $ax \equiv b(\text{mód } m)$, es decir $ax_0 - b = ml$, entonces, $x_0 + \frac{km}{d}$; donde $k \in \mathbb{Z}$, también es solución, ya que $a(x_0 + \frac{km}{d}) = ax_0 + \frac{akm}{d} = b + lm + \frac{akm}{d} = b + m(l + \frac{ak}{d})$, puesto que $d|a$ entonces $\frac{ak}{d} \in \mathbb{Z}$, por lo tanto haciendo $g = l + \frac{ak}{d}$ tenemos que $a(x_0 + \frac{km}{d}) = b + mg$, lo que significa que $x_0 + \frac{km}{d}$, es solución.

Ejemplo: Resolver $3x \equiv 15(\text{mód } 18)$

Como el $m.c.d(3, 18) = 3$, entonces existen exactamente 3 soluciones. De $3x \equiv 15(\text{mód } 18)$, se tiene que $3x = 15 + 18k$, esto equivale a $x = 5 + 6k$, un valor para x, ocurre en $k = 0$; es decir $x_0 = 5$, luego $x = x_0 + \frac{km}{d} = 5 + \frac{18k}{3} = 5 + 6k$, donde $0 \leq k \leq (d-1)$

Si $k = 0$ entonces $x = 5$
Si $k = 1$ entonces $x = 11$
Si $k = 2$ entonces $x = 17$

Hay 3 soluciones, que son; $5, 11$ y 17.

Capítulo 7
EJERCICIOS Y APLICACIONES

7.1. EJERCICIOS

1. Tres reyes de un tablero de ajedrez, que formaban sociedad, tenían un mono. Una tarde compraron una partida de plátanos, con intención de repartírsela al día siguiente.

   Por la noche se levantó uno de ellos, se puso a contar los plátanos, e hizo tres partes iguales. Tomó para sí una de ellas y dejó el resto (otras dos partes). Como después del reparto le había sobrado un plátano se lo dio al mono.

   Poco después se despertó otro rey y se fue a contar los plátanos para coger su tercera parte. Después de tomar esa cantidad y dejar las otras dos partes, vio que sobraba un plátano y se lo dio al mono.

   Un poco más tarde se levantó el tercer rey, sin sospechar lo que habían hecho sus compañeros; al querer tomar su tercera parte vio que sobraba un plátano, y se lo dio al mono; se llevó la parte que creyó que le correspondía dejando el resto y se fue a acostar.

   A la mañana siguiente se levantaron y ninguno declaró lo que habían hecho la noche anterior. Hicieron el reparto de los plátanos que había en ese momento;

cada uno se llevó la tercera parte y sobró un plátano que le dieron al mono. ¿Cuál es el menor número posible de plátanos para realizar estas operaciones?

Solución

Primero que todo debemos analizar el problema.

- El primer rey dividió el conjunto de plátanos en tres partes iguales y le sobro uno, el rey toma su parte y el plátano que le quedo sobrando se lo dio al mono.
- El segundo rey dividió el conjunto de plátanos que quedo en tres partes iguales y le sobro uno, el rey toma su parte y el plátano que le quedo sobrando se lo dio al mono.
- El tercer rey dividió el conjunto de plátanos que quedo en tres partes iguales y le sobro uno, el rey toma su parte y el plátano que le quedo sobrando se lo dio al mono.
- La repartición que hacen los tres reyes, dividen el conjunto de plátanos que queda en tres partes iguales y les sobro un plátano, el cual se lo dieron al mono.

Bueno ahora diremos que n es el conjunto total de datos, b son las partes en que se divide el conjunto, q son las partes que toma cada rey y r es el residuo ó lo que cada rey le da al mono cuando hace las reparticiones.

$$\begin{array}{ll} n & \mid \quad b \\ \hline r & \quad q \end{array}$$

Entonces.

$$\begin{array}{ll} n & \mid \quad 3 \\ \hline 1 & \quad A \end{array} \quad ; 3A + 1 = n; \; A = \frac{n-1}{3}.$$

Luego el primer rey toma A partes del conjunto y quedan $2A$

$$\begin{array}{cc} 2A & \mid \ 3 \\ \hline 1 & B \end{array} \ ; 3B+1=2A;\ B=\frac{2A-1}{3}.$$

Luego el segundo rey toma B partes del conjunto y quedan $2B$

$$\begin{array}{cc} 2B & \mid \ 3 \\ \hline 1 & C \end{array} \ ; 3C+1=2B;\ C=\frac{2B-1}{3}.$$

Luego el tercer rey toma C partes del conjunto y quedan $2C$.

$$\begin{array}{cc} 2C & \mid \ 3 \\ \hline 1 & D \end{array} \ ; 3D+1=2C;\ D=\frac{2C-1}{3}.$$

Luego la repartición que hacen los tres reyes juntos, cada rey toma D partes del conjunto y el plátano que les sobra se lo dan al mono.

Ahora si remplazamos a C en la ecuación D luego B y por ultimo remplazamos a A.

$D=\frac{2C-1}{3}$ luego $D=\frac{2\left(\frac{2B-1}{3}\right)-1}{3}=\frac{\frac{4B-5}{3}}{3}=\frac{4B-5}{9}$

luego $D=\frac{4B-5}{9}$.

$D=\frac{4B-5}{9}$ luego $D=\frac{4\left(\frac{2A-1}{3}\right)-5}{9}=\frac{\frac{8A-19}{3}}{9}=\frac{8A-19}{27}$

luego $D=\frac{8A-19}{27}$.

$D=\frac{8A-19}{27}$ luego $D=\frac{8\left(\frac{n-1}{3}\right)-19}{27}=\frac{\frac{8n-65}{3}}{27}=\frac{8n-65}{81}$

luego $D=\frac{8n-65}{81}$.

Ahora despejamos n en la ecuación D quedando $n = \dfrac{81D + 65}{8}$. Luego 81D+65, debe ser un multiplo de 8, por lo tanto D debe ser un número impar, por lo tanto.

Sea $D = 1$ entonces $n = 8{,}25$
$D = 3$ entonces $n = 38{,}5$
$D = 5$ entonces $n = 58{,}75$
D=7 entonces **n= 79**

El menor número posible de plátanos para realizar estas operaciones es 79.

2. Encontrar el residuo de dividir 6^{1987} por 37.

Tenemos que $6^0 \equiv 1(\text{mód } 37)$, y $6^1 \equiv 6 \equiv -31(\text{mód } 37)$, $6^2 = 36 \equiv -1(\text{mód } 37)$. Ahora $6^{1987} = 6 \cdot 6^{1986} = 6(6^2)^{993}$, y tenemos que $6^2 \equiv -1$ (mód 37), entonces $6 \cdot (6^2)^{993} = 6 \cdot (-1)^{993} = -6$; $-6 \equiv 31(\text{mód}37)$, es decir $6^{1987} \equiv 31(\text{mód}37)$.

3. Probar que 7 divide $3^{2n+1} + 2^{n+2}$ para todo $n \in \mathbb{N}$.

Supongamos que $3^{2n+1} + 2^{n+2} = 7m$; si $n = 1$; $3^3 + 2^3 = 27 + 8 = 35 = 7 \cdot 5$; si $n = k$; $3^{2k+1} + 2^{k+2} = 7j$; si $n = k + 1$; $3^{2k+3} + 2^{k+3} = 7l$. Ahora como $3^{2k+3}+2^{k+3} = 3^2 \cdot 3^{2k+1}+2^{k+3} = 9(7m-2^{k+2})+2^{k+3} = 63m-9 \cdot 2^{k+2}+2 \cdot 2^{k+2} = 63m - 7 \cdot 2^{k+2} = 7[9m - 2^{k+2}]$.

4. Encuentre los cuadrados perfectos mód 13.

Primero observamos que sólo tenemos al cuadrado todos los números hasta el 6 porque $r^2 \equiv (13 - r)^2(\text{mód } 13)$, ya que $r^2 - (13 - r)^2 = 26r - 13^2 = 13(2r - 13)$, así que $r^2 \equiv (13 - r)^2(\text{mód } 7)$. Por lo tanto,

$$0^2 \equiv 0(\text{mód } 13)$$
$$1^2 \equiv 1(\text{mód } 13)$$
$$2^2 \equiv 4(\text{mód } 13)$$
$$3^2 \equiv 9(\text{mód } 13)$$
$$4^2 \equiv 3(\text{mód } 13)$$
$$5^2 \equiv 12(\text{mód } 13)$$
$$6^2 \equiv 10(\text{mód } 13)$$

Con esto podemos concluir que los cuadrados perfectos modulo 13 son $0, 1, 4, 9, 3, 12$ y 10.

5. Encuentre infinitas soluciones para $n \in \mathbb{Z}^+$ tal que $2^n + 27$ es divisible por 7.

Consideremos la sucesión 2^n y observamos que:

$$2^1 \equiv 2(\text{mód } 7)$$
$$2^2 \equiv 4(\text{mód } 7)$$
$$2^3 \equiv 1(\text{mód } 7)$$
$$2^4 \equiv 2(\text{mód } 7)$$
$$2^5 \equiv 4(\text{mód } 7)$$
$$2^6 \equiv 1(\text{mód } 7).$$

De aqui podemos concluir que $2^{3k-2} \equiv 2(\text{mód } 7)$; $2^{3k-1} \equiv 4(\text{mód } 7)$ y $2^{3k} \equiv 1(\text{mód } 7)$.
Si $n = 3k$, entonces $2^{3k} \equiv 1(\text{mód } 7)$. De aquí $2^{3k} + 27 \equiv 1 + 27 \equiv 0(\text{mód}7)$, para todo $k \in \mathbb{Z}^+$. Esto produce infinitos valores para n.
Si $n = 3k - 1$, entonces $2^{3k-1} \equiv 4(\text{mód } 7)$, de donde$2^{3k-1} + 27 \equiv 3(\text{mód } 7)$ y esto significa que $2^{3k-1} + 27$ no es divisible por 7.
Si $n = 3k - 2$, entonces $2^{3k-2} \equiv 2(\text{mód } 7)$, de donde $2^{3k-2} + 27 \equiv 1(\text{mód } 7)$ y esto significa que $2^{3k-1} + 27$ no es divisible por 7.

6. Probar que $7|(2222^{5555} + 5555^{2222})$

   Tenemos que $2222 \equiv 3(\text{mód } 7)$, y, $5555 \equiv 4(\text{mód } 7)$, porque $7|2219$, y, $7|5551$, así que $(2222^{5555} + 5555^{2222} = [(3^5)^{1111} + (4^2)^{1111}]$, pero $3^5 \equiv 5(\text{mód } 7)$, y, $4^2 \equiv -5(\text{mód } 7)$, entonces $(3^5)^{1111} + (4^2)^{1111} \equiv 5^{1111} + (-5)^{1111} = 0$. Esto significa que $7|(2222^{5555} + 5555^{2222})$

7. Hallar el residuo de dividir 4^{179} entre 5.

   Tenemos que $4 \equiv -1(\text{mód } 5)$, entonces, $4^{179} \equiv (-1)^{179}(\text{mód } 5)$, y esto equivale a $4^{179} \equiv -1(\text{mód } 5)$, luego el residuo de dividir -1 entre 5 es 4 luego el residuo de dividir 4^{179} entre 5 también es 4.

8. Hallar el residuo de dividir 15^{168} entre 13

   Sabemos que $15 \equiv 2(\text{mód } 13)$, entonces, $15^{168} \equiv 2^{168}(\text{mód } 13)$, pero como $168 = 2^3 \cdot 3 \cdot 7 = 6 \cdot 28$ luego $2^{168} = (2^6)^{28}$ y $2^6 = 12 \equiv -1(\text{mód } 13)$, entonces $2^{168} \equiv (-1)^{28}(\text{mód } 13)$, por lo tanto $2^{168} \equiv 1(\text{mód } 13)$.

9. Demostrar que $2|n(n+1)$.

   - si n es par, entonces, $n \equiv 0(\text{mód } 2)$, así que $n + 1 \equiv 1(\text{mód } 2)$, ahora $n(n+1) \equiv 0 \cdot 1(\text{mód } 2)$, y esto significa que $2|n(n+1)$.
   - si n es impar, entonces $n \equiv 1(\text{mód } 2)$, y $n + 1 \equiv 2(\text{mód } 2)$, luego $n(n+1) \equiv 1 \cdot 2(\text{mód } 2)$, y como $2 \equiv 0(\text{mod } 2)$, entonces, $n(n+1) \equiv 0(\text{mód } 2)$, luego $2|n(n+1)$.

10. Si contamos 100 días a partir de hoy ¿Qué día de la semana caerá?.

    Tenemos que $100 = 98 + 2 = 14 \cdot 7 + 2$, lo que significa que pasaran 14 semanas y 2 dias y si hoy es miércoles el cienavo día es viernes.

11. Resolver $32x \equiv 28(\text{mód } 36)$

    Aquí tenemos: $32x - 28 = 36l$, y esto equivale a $8x - 7 = 9l$.

    El $m.c.d.(8,9) = 1$, por lo tanto, la congruencia tiene solución. Podemos cambiar $8x$ por $-x$, y a -7 por -2, así tendriamos que $-x \equiv -2(\text{mód } 9)$, ó, $x \equiv 2(\text{mód } 9)$. Una solución es $x_0 = 2$ y para la congruencia inicial tendriamos 4 soluciones.

    Entonces $x_0 = 2$ este seria el primer valor y las otras soluciones son:
    $k = 0$ entonces $x_0 = 2$
    $k = 1$ entonces $2 + 1 \cdot \frac{36}{4} = 2 + 9 = 11$
    $k = 2$ entonces $2 + 2 \cdot \frac{36}{4} = 2 + 2 \cdot 9 = 20$
    $k = 3$ entonces $2 + 3 \cdot \frac{36}{4} = 2 + 3 \cdot 9 = 29$

    Las 4 soluciones son; $2, 11, 20$ y 29.

12. Expresar el $m.c.d.(44, 21)$ como combinación lineal de 44 y 21.

    Tenemos $44 = 2 \cdot 21 + 2 = 2(10 \cdot 2 + 1) + 2 = 2(10(2 \cdot 1 + 0) + 1) + 2$.
    Luego $m.c.d(44, 21) = 1$.

    Además: $1 = 21 - 10 \cdot 2 = 21 - 10(44 - 2 \cdot 21) = 21 \cdot 21 + (-10) \cdot 44$. Así que $x = 21$, y $y = (-10)$.

EJERCICIOS.

1. Muestre que 41 divide a $2^{20} - 1$.
2. Muestre que para cualquier entero a, $a^3 \equiv 0, 1$ ó $6(\text{mód } 7)$.
3. Muestre que si un entero a no es divisible por 2 y 3, entonces $a^2 \equiv 1(\text{ mód } 24)$.

4. Muestre con un ejemplo que si $a^k \equiv b^k (\text{mód } n)$ y $k \equiv j (\text{mód } n)$, no necesariamente $a^j \equiv b^j (\text{mód } n)$.

5. Resolver la congruencia $3x + 3 \equiv (6 + 2x) (\text{mód } 5)$

6. Aplicando el algoritmo euclidiano encontrar el (m, c, d) de.

   a) 7469 y 2464

   b) 2689 y 4001

   c) 2947 y 3997

   d) 1109 y 4999

7. Encontrar el máximo común divisor d de los números 1819 y 3587 y a continuación encontrar los enteros x, y, y que satisfagan $1819x + 3587y = d$.

8. ¿Cuántos enteros entre 100 y 1000 se dejan dividir por 7?

7.2. APLICACIONES

La congruencia modular se puede aplicar en diferentes campos como: La teoría de números, el algebra, las artes visuales, la música, la criptologia, funciones Hash para asignación de memoria, Números Pseudo-Aleatorios y la aplicación más frecuente es en la computación.

Enfocándonos en algunas de estas aplicaciones encontramos la **Criptologia** la cual es una disciplina que se encarga de la seguridad en la trasmisión de mensajes en clave de un emisor a un receptor.

Esta se encuentra conformada por dos ramas: la **Criptografía** y el **Criptoanálisis**.

La **Criptografía** que viene del griego "kripto"que significa ocultar y "raphos"que significa escritura. La criptografía es una de las técnicas de codificación más simple y más usada. Es un tipo de cifrado por sustitución en el que una letra

en el texto original es remplazada por otra letra que se encuentra en un número fijo de posiciones más adelante en el alfabeto.

Ejemplo

Con un cambio a partir de 3. entonces.

A-B-C-D-E-F-G-H-I-J...
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓...
D-E-F-G-H- I- J-K-L-M...
Los pasos para hacer cifrado de mensajes son:

1. Transforme cada letra en un número. Para ello, utilice su posición en el alfabeto. A es 0, B es 1, C es 3,...hasta Z es 25
2. Apliquen la función $f(x) \equiv (x+n)(\text{mod } p)$ donde x es un desplazamiento n, y, p el número de letras del alfabeto, obteniendo así a $f(x) \equiv (x+3)(\text{mod } 26)$ esta función la aplicamos a cada número.
3. Transforme cada número a letra y envíe el mensaje

Ejercicio:

$A = 0; B = 1; C = 2; D = 3; E = 4; F = 5; G = 6; H = 7; I = 8; J = 9; K = 10; L = 11; M = 12; N = 13; O = 14; P = 15; Q = 16; R = 17; S = 18; T = 19; U = 20; V = 21; W = 22; X = 23; Y = 24; Z = 25.$

Encripte los siguientes mensajes:

"HOLA" "NOS VEMOS EN EL CDU".

El **Criptoanálisis** que viene del griego "kryptós" que significa escondido y "analýein" que signifiva desatar, es el estudio de los métodos para obtener el sentido de una

información, en donde logramos descifrar el mensaje.

Para decodificar se hace de manera similar a la criptografía, aplicando la funcion $f(x) \equiv (x - n)(\text{mod } p)$

Desencripte el mensaje

"QDGLHSLHUGHGLVFUHWDV"

Capítulo 8

BIBLIOGRAFIA

- Introduction to the theory of numbers - **Leonar Eugene Dickson**- publicado por el Grupo Trillia, 2004.
- Introducción a la teoría analítica de números - **Tom Apóstol**- Editorial Reverté.S.A 1984, impreso en España.
- Introducción a la teoría de los números -**Ivan Niven** y **Herbert S. Zuckerman** - México : Limusa-Wiley : Agencia para el Desarrollo Internacional, Centro Regional de Ayuda Técnica, 1969.
- Teoría de los números - **Burton W. Jones**- Editorial Trillas, Mexico, 1969.
- Teoría de Números (Para principiantes)-**Luis Rafael Jimenéz Becerra y Gustavo Nevardo Rubiano Ortega**- Universidad Nacional Colombia -2004
- ELEMENTARY NUMBER THEORY- **W W L CHEN**- Cambridge University Press-2009
- INTRODUCTION TO NUMBER THEORY - **Franz Lemmermeyer**- Noviembrer 28, 2000- Springer, 1998.
- Teoría Elemental de los números - **Willian Judson LeVeque**- Herrero Hermanos, 1998

8. BIBLIOGRAFIA

- Fundamentos de la teoría de números - **Ivan M. Vinogradof y Emiliano A. Bernando**- Mir, 1971.
- Complementos de Matemática Discreta - **Juan Carlos Ferrando, Ana Martínez**- Ed. Univ. Politéc. Valencia , 1971.
- Disquisitiones arithmeticae - **Carl Friedrich Gauss, William C. Waterhouse**- Springer, 1986.