Complementos de Matemática

para criptografía

Extraído de Técnicas criptográficas de protección de datos ED: Alfaomega

División Euclidea

Dados 2 números enteros "a" y "b" . Se dice que "a" divide a "b" ó lo que es lo mismo que "b" es divisible por "a" [$a|b$] si existe un entero "c" tal que $b = a.c$.
Se dice entonces que "a" es un divisor de "b".
Un divisor es *propio* si no es el propio número ni el 1.
Un número primo es aquel que no tiene divisores propios

Teorema de Euclides

Si un número primo divide a un producto divide al menos a uno de los factores

mcd y mcm.

Dado dos números "a" y "b" se llama :

- **Máximo común divisor. mcd(a,b) :** al mayor número entero que divide a "**a**" y a "**b**"
- **Mínimo común múltiplo. mcm(a,b) :** al menor número entero divisible por "a" y por "b"
- **Se demuestra que :** a.b = mcd (a,b) . mcm(a,b) →*Demostrarlo*
- **Se dice que :** dos enteros. 'a' y 'b' son primos entre si si mcd (a,b) = 1

Teorema de la división de Euclides

Dados dos números enteros $a > b > 0$, se verifica que : mcd (a,b) = mcd (b,r) siendo "r" el resto de dividir "a" entre "b" [$a = b.q + r$].

La aplicación reiterada del Teorema anterior permite calcular el mcd

Ej. :

mcd(24,10) = mcd(10,4) = mcd (4,2) = 2

Se deduce entonces que si mcd(a,b) = d, con $a > b$, existen entonces enteros "u" y "v" tales que $d = u . a + v . b$ (Es decir el mcd de dos números se puede expresar como una combinación lineal de esos números con coeficientes enteros)

Ejemplo:

b = 32 ; a=20 → mcd (32,20) = 4. Según el Teorema anterior existen deo números 'u' y 'v' tal que 32u + 20b = 4. En este caso sencillo es evidente que 'u' = 2 y 'v' = -3.

Algoritmo extendido de Euclides

Es el que permite determinar los calores de "u" y "v"

Teorema de Lagrange.

Se llama *Grupo* "G" a un conjunto provisto de una operación asociativa que tiene un elemento neutro, respecto de la cual cada elemento de G tiene un inverso.

Se llama *Orden* de un grupo finito G al número de elementos de dicho grupo.

Un *elemento* g ε G se dice que es un generador si cualquier elemento de G puede escribirse como potencia de 'g'.

Números Enteros Módulo m

Sea Z = {....,-2, -1, 0, 1, 2, ...} el conjunto de los números enteros.

Sea "m" un entero positivo y dos números a, b εZ.
"a" y "b" son congruentes módulo "m" [a ≡ b (mod m)] si su diferencia es múltiplo de "m" (a-b = k.m), o lo que es igual si "a" y "b" tienen el mismo resto al ser dividido por "m".

Se llama clase de equivalencia definida por el número *a módulo m*, denotada por [a] al conjunto de los número enteros que son congruentes con *a módulo m*.

$$[a] = \{n \ \varepsilon\ Z;\ \ n \equiv a \pmod m \}$$

El conjunto de las clases de equivalencia se denota por Z_m y es el conjunto de los números enteros módulo m.

Ejemplo :

Si m = 6 => [4] = { ..., -8, -2, 4, 10, 16, ... } = { 4 + 6k; k ε Z)

Si m = 7 => [4] = { ..., -10, -3, 4, 11, 18, ...} = {4 +7k; k ε Z)

En la práctica [a] se identifica al resto de dividir "a" entre "m". Por ejemplo la clase de 14 módulo 6 se identifica por 2 y la de 25 módulo 7 con 4.

$$Z_m = \{ 0,1,2,.....m-1\}$$

Notar que los congruencias se pueden Sumar, restar y multiplicar.

Sean :
$a \equiv b \pmod{m}$, $a' \equiv b' \pmod{m}$

Entonces :

$$\boxed{\begin{array}{l} a+a' \equiv b+b' \pmod{m} \\ a-a' \equiv b-b' \pmod{m} \\ a.a' \equiv b.b' \pmod{m} \end{array}}$$

Teorema del Resto Chino

Dado el siguiente sistemas de ecuaciones en congruencias:

$$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2},\ ....\ x \equiv a_r \pmod{m_r}$$

Si cada par de módulos son primos entre si; es decir mcd $(m_i, m_j) = 1$ para $i \neq j$, entonces existe una solución simultánea para todas las congruencias y dos soluciones cualesquiera son congruentes módulo $m = m_1 . m_2 .\ ....\ m_r$.
Uan solución ,s, para el sistema de congruencias antereior viene dad por la expresión

$$S = \sum_{i=1}^{r} a_i M_i N_i$$

Donde Mi = m/mi y Ni es el inverso de Mi módulo mi

Ejemplo :

Sea $x \equiv 15 \ (\bmod 2\ )$; $x \equiv 20\ (\bmod 3\ )$,

Entonces $m = 2 . 3 = 6$; $M_1 = 6/2$; $M_2 = 6/3$

$S = 15 . 3 . 1 + 20 . 2 . 2 =$ **125**

Comprobación :

125 / 2 → Resto = 1
15 / 2 → Resto = 1

→ $125 \equiv 15 \pmod 2$

125 / 3 → Resto = 2
20 / 3 → Resto = 2

→ $125 \equiv 20 \pmod 3$

Función de Euler

- Un elemento $a \in \mathbb{Z}_m$ es invertible si existe otro elemento $b \in \mathbb{Z}_m$, tal que :

$$\boxed{a.b \equiv 1 \pmod m.}$$

- Un elemento no nulo $a \in \mathbb{Z}_m$ es un *divisor de cero* si existe otro elemento no nulo $b \in \mathbb{Z}_m$ tal que :

$$\boxed{a.b \equiv 0 \pmod m}$$

Es evidente que todos los divisores de “m” son divisores de cero y por tanto no invertible. Además son invertibles todos los enteros positivos menores que “m” que son primos con “m’. Por tanto, si “m” es primo, todos los enteros positivos menores que el son primos con “m” y todos invertibles.

Es tambien evidente entonces que si p es primo $\Phi(p) = p-1$

Grupo de unidades $\mathbb{Z}_m$.

Se llama así al conjunto de los elementos invertibles de $\mathbb{Z}_m$ y se designa por $\mathbb{Z}^*_m$.

Es fácil ver que $\mathbb{Z}^*_m$ es un grupo para el producto, el orden de dicho grupo se representa por :

$$\boxed{\Phi(m) = \#\mathbb{Z}^*_m}$$

$\Phi(m)$ es la función *phi* de Euler.
Evidentemente, si p es un número primo, $\Phi(p) = p-1$.
Es posible demostrar dos propiedades de la función phi de Euler.

- Si p es un número primo $\Phi(p^k) = p^{k-1}(p-1)$
- Si $mcd(m,n) = 1$, entonces $\Phi(m.n) = \Phi(m).\Phi(n)$

Asi pues si $m = p_1^{k1} \ldots\ldots p_r^{kr}$ es la descomposición factorial de "m" se llega a la función phi

$$\boxed{\phi(m) = p_1^{k_1 - 1}(p_1 - 1)\ldots\ldots p_r^{k_r - 1}(p_r - 1) = m.\left(1 - \frac{1}{p_1}\right)\ldots\ldots\left(1 - \frac{1}{p_r}\right)}$$

Teorema de Euler

Para todo elemento $a \in Z_m$ se verifica : $a^{\Phi(m)} \equiv 1 \pmod{m}$

Teorema (pequeño) de Fermat

Si 'p' es un número primo se verifica para todo entero $a^p \equiv a \pmod{p}$
Si 'a' no es divisible por 'p' : $a^{p-1} \equiv 1 \pmod{p}$

Primalidad

El problema consiste en dererminar si un número es primo. En caso de números pequeños puede parecer tarea sencilla pero para números de cerca de 200 dígitos, tales como los usados en RSA el problema asume dimensiones mas que considerables.

Test de primalidad
El mas evidente es la prueba mediante divisiones sucesivas.
Suponga que 'n' es un número impar grande; Se toma un número entero impar 'm' y se prueba si divide o no a 'n'. Se deben probar todos los valores posibles desde 3 hasta el entero mas cercano a $\sqrt{n}$.

Problemas de métodos matemáticos

1. ¿ Cuantos divisores tiene 945? Lístelos

$945 = 3^3 . 5 . 7$ el numero de divisores sera 4 . 2 . 2 = 16

1 , 3, 5 ,7, 9, 15, 21, 27, 35, 45, 63, 105, 135, 189, 315, 945

2. Para cada uno de los siguientes pares de enteros encontrar su máximo común divisor (mcd = d) y expresarlo como combinación lineal de la pareja

   a. 26, 19

mcd(26,19) = 1 = -8 . 26 =11 . 19

   b. 187, 34

mcd(187,34) = 17 = 1 . 187 -5 . 34

   c. 841, 160

mcd(841,160) = 1= -39 . 841 + 205 . 160

   d. 1547, 560

mcd(1547, 560) = 7 = 21 . 1547 - 58 . 560

3. Calcular el mínimo común múltiplo de a = 2345 y b= 737 usando la fórmula :

$$a.b = mcd(a,b) . mcm(a,b)$$

mcd(2345, 737) = 67
mcm(a,b) = 2345 . 737/67 = 25795

4. Calcular el valor de la función Φ de Euler para los siguientes números

   a. 81
   b. 1960
   c. 1996
   d. 41503

$\Phi(81) = \Phi(3^4) = 3^{(4-1)}(3-1)=3^3 . 2 \quad = 54$
$\Phi(1960) = \Phi (2^3 . 5 . 7^2) = 2^2 . 4 . 7 . 6 \quad = 672$
$\Phi(1996) = \quad = 996$
$\Phi(41503)= \quad =32340$

5. Determinar el menor entero positivo que da resto 1 al dividirlo por 11, resto 2 al dividirlo por 12 y resto 3 al dividirlo por 13.

$x \equiv 1 \ (\bmod\ 11)$
$x \equiv 2 \ (\bmod\ 12)$
$x \equiv 3 \ (\bmod\ 13)$

➔ *-10*

6. Encontrar la menor solucion no negativa para :

   $x \equiv 2 \ (\text{mod } 3)$, $x \equiv 3 \ (\text{mod} 5)$, $x \equiv 4 \ (\text{mod } 11)$, $x \equiv 5 \ (\text{mod } 16)$

$x = 2 \,.\, 880 \,.\, 1 + 3 \,.\, 528 \,.\, 2 + 4 \,.\, 240 \,.5 + 5 \,.165 \,.\, 13 = 20453 \equiv 1973 \ (\text{mod } 2640)$