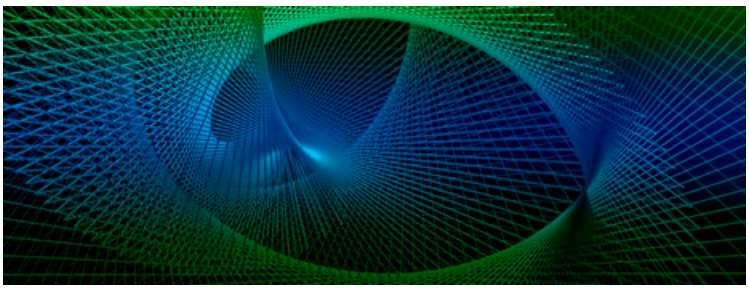

Matemática, Informática, Educación

Máximo común divisor con aritmética modular

Hasta ahora para calcular el máximo común divisor de dos números cualesquiera se suele utilizar dos métodos muy simples:

1: buscando los divisores de cada número y seleccionando los divisores comunes
2: Factorizando los números para poder obtener el máximo común divisor.

Procedimiento 1
Calcular el Máximo común divisor de 16 y 18.
Divisores de 16: $D_{16} = \{1,2,4,8,16\}$
Divisores de 18: $D_{18} = \{1,2,3,6,9,18\}$
Divisores comunes: {1,2}
Máximo común divisor = 2

Procedimiento 2

Vamos a calcular el Máximo común divisor de 16 y 21.
Factorizamos los números (15 y 21).
Escribimos en factores de cada uno de los números, 15 y 21.

$$\begin{array}{r|l} 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \qquad \begin{array}{r|l} 21 & 3 \\ 7 & 7 \\ 1 & \end{array}$$

Factores comunes: {1,3}
Máximo común divisor = 3

Algoritmo de Euclides extendido

Para calcular el máximo común divisor de dos números enteros positivos a y b, dividimos el mayor, que puede ser *a*, entre el menor, supongamos *b*. Esta división nos proporcionará un cociente y un resto. Si aplicamos recursivamente el algoritmo del cociente, se obtiene:

$$
\begin{aligned}
&Si\ definimos\ r_0 = a\ y\ r_1 = b \\
&r_0 = r_1 q_1 + r_2 && 0 < r_2 < r_1 \\
&r_1 = r_2 q_2 + r_3 && 0 < r_3 < r_2 \\
&\quad \vdots && \quad \vdots \\
&r_{n-2} = r_{n-1} q_{n-1} + r_n && 0 < r_n < r_{n-1} \\
&r_{n-1} = r_n q_n + r_{n+1} && 0 = r_{n+1}
\end{aligned}
$$

Entonces, *el máximo común divisor entre a y b es el último resto distinto de cero que obtengamos en el procedimiento anterior*.

Ejemplo:
Determinar el mcd(270, 192)

Aplicando el algoritmo de Euclides, tenemos:

$$
\begin{aligned}
270 &= 192 \cdot 1 + 78 \\
192 &= 78 \cdot 2 + 36 \\
78 &= 36 \cdot 2 + 6 \\
36 &= 6 \cdot 6 + 0
\end{aligned}
$$

$$\therefore\ mcd(270, 192) = 6$$

Ejemplo:
Determinar el mcd(231, 1820)

$$
\begin{aligned}
1820 &= 231 \cdot 7 + 203 \\
231 &= 203 \cdot 1 + 28 \\
203 &= 28 \cdot 7 + 7 \\
28 &= 7 \cdot 4 + 0
\end{aligned}
$$

$$\therefore\ mcd(231, 1820) = 7$$

Ejemplo
Utilizando el algoritmo de Euclides calcular mcd(55, 89).

En este ejemplo aplicaremos el algoritmo de Euclides sobre dos números consecutivos de Fibonacci. Este tipo de pares son los que le exigen más en el proceso de dicho algoritmo pues siempre *mcd = 1*.

$$
\begin{aligned}
89 &= 55 \cdot 1 + 34 \Rightarrow mcd(55, 89) = mcd(55, 34) \\
55 &= 34 \cdot 1 + 21 = mcd(34, 21) \\
34 &= 21 \cdot 1 + 13 = mcd(21, 13) \\
21 &= 13 \cdot 1 + 8 = mcd(13, 8) \\
13 &= 8 \cdot 1 + 5 = mcd(8, 5) \\
8 &= 5 \cdot 1 + 3 = mcd(5, 3) \\
5 &= 3 \cdot 1 + 2 = mcd(3, 2) \\
3 &= 2 \cdot 1 + 1 = mcd(2, 1) \\
2 &= 1 \cdot 2 + 0 = mcd(1, 0) = 1 \\
&\therefore mcd(55, 89) = 1
\end{aligned}
$$

El algoritmo de Euclides del menor resto

Como ya hemos visto el algoritmo de Euclides es un método para calcular el máximo común divisor (MCD) de al menos un par de números.

El algoritmo de Euclides extendido es una modificación del algoritmo de Euclides, y nos permite expresar el máximo común divisor como una combinación lineal.

Recordemos que el Máximo Común Divisor de dos números “a” y “b”, es el mayor número posible que divide a los dos.

En el algoritmo de Euclides, el resto r_i está entre 0 y r_{i-1}, si modificamos el algoritmo para que cada nuevo resto r_i esté entre 0 y $r_{i-1/2}$ obtendremos una reducción en el número de divisiones.

Como mcd(a, b) = mcd(|a|,|b|) vamos a suponer que a ≥ 0 y b > 0.

Luego

$$a = b \cdot \left\lfloor {}^{a}\!/_{b} \right\rfloor + r2 \quad 0 \leqslant r_2 < b$$

$$a = b \cdot \left(\left\lfloor {}^{a}\!/_{b} \right\rfloor + 1 \right) - r_1 \quad 0 \leqslant r_1 < b$$

El algoritmo del mínimo resto consiste en escoger en cada paso el menor resto, es decir

$$r = Mín\{r_1, r_2\} = Mín\left\{ \left| a - b \cdot \left\lfloor {}^{a}\!/_{b} \right\rfloor \right|, \left| a - b \cdot \left(\left\lfloor {}^{a}\!/_{b} \right\rfloor + 1 \right) \right| \right\}$$

$$\text{De esta manera } r \leqslant {}^{b}\!/_{2}$$

Ejemplo. Con el algoritmo del mínimo resto, obtener el *mcd* de *a = 55* y *b = 89*
Aplicando el algoritmo del mínimo resto tenemos

$$Para\ a = 89\ y\ b = 55$$

$$r = Mín\{r_1, r_2\} = Mín\left\{\left|a - b \cdot \left\lfloor {a}/{b} \right\rfloor\right|, \left|a - b \cdot \left(\left\lfloor {a}/{b} \right\rfloor + 1\right)\right|\right\}$$

$$r = Mín\left\{\left|89 - 55 \cdot \left\lfloor {89}/{55} \right\rfloor\right|, \left|89 - 55 \cdot \left(\left\lfloor {89}/{55} \right\rfloor + 1\right)\right|\right\}$$

$$r = Mín\{|89 - 55 \cdot 1|, |89 - 55 \cdot 2|\}$$

$$r = Mín\{34, 21\}$$

$$r = 21$$

$$89 = 55 \cdot 2 - 21$$

$$55 = 21 \cdot 3 - 8$$

$$21 = 8 \cdot 3 - 3$$

$$8 = 3 \cdot 3 - 1$$

$$3 = 1 \cdot 3 + 0$$

$$mcd(89, 55) = 1$$

Relación de congruencia

Si tenemos el siguiente arreglo matricial, correspondiente a los números del 1 al 25, escritos en filas de 5.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

Es posible comprobar los siguiente:

1. Si elegimos dos números cualesquiera de cualquier columna y los restamos, la diferencia es divisible por 5.
2. Los números ubicados en una misma columna, siendo esta cualquier columna tienen el mismo resto al ser divididos por 5.
3. Los residuos resultantes al dividir cualquier número por 5, corresponden consecutivamente a 1, 2, 3, 4 y 0 según la columna en que se encuentren.

El concepto de relaciones de congruencia nos permite agrupar infinitos números enteros bajo una relación de equivalencia llamada congruencia módulo n.

Los resultados comprobados pueden ser generalizados bajo la siguiente condición: Si se colocan *n* enteros consecutivos en filas constituidas por *m* elementos con *m<n*, entonces es válido en dicho arreglo:

1. Si elegimos dos números cualesquiera de cualquier columna y los restamos, la diferencia es divisible por *m*.
2. Los números ubicados en una misma columna, siendo esta cualquier columna tienen el mismo resto al ser divididos por *m*.
3. Los residuos resultantes al dividir cualquier número por *m*, corresponden consecutivamente a *1, 2, 3, … 0* según la columna en que se encuentren.

Dados dos números, *p* y *q*, decimos que *p* y *q* son congruentes módulo *n* si *(p - q)* es divisible por *n*, en tal caso el resto de dividir *p* entre *n* es igual que el resto de dividir *q* entre *n*.

Si *p* y *q* son congruentes módulo *n* entonces lo escribimos simbólicamente de la siguiente forma:

$$p \equiv q\ (mod\ n)$$

Definición: Sea *n* un número entero positivo. Dos enteros *a* y *b* son congruentes módulo *n* si *n* divide a la diferencia *a* – *b*.

$$a \equiv b \ (mod\ n),$$
$$Si\ n \mid (a-b)$$

Ejemplos:

$$27 \equiv 3 \ (mod\ 8),\ puesto\ que\ 8 \mid (27-3)$$
$$7 \equiv -1 \ (mod\ 8),\ puesto\ que\ 8 \mid (7-(-1))$$
$$37 \equiv 7 (mod\ 5),\ puesto\ que\ 5 \mid (37-7)$$
$$27 \equiv 24 (mod\ 3), ya\ que\ 3 \mid (27-24)$$

Teorema. La relación de congruencia módulo *n* cumple las siguientes propiedades

$$a)\ a \equiv a\,(mod\ n), \forall a \in \mathbb{Z}$$
$$b)\ Si\ a \equiv b (mod\ n)\ \Rightarrow b \equiv a (mod\ n),\ \forall a,b \in \mathbb{Z}$$
$$c)\ Si\ a \equiv b (mod\ n)\ y\ b \equiv c (mod\ n) \Rightarrow a \equiv c (mod\ n),\ \forall a,b,c \in \mathbb{Z}$$

Teorema. *Dados a, b, c, d y n enteros con n > 1 y*

$$a \equiv c\ (mod\ n)\ y\ b \equiv d\ (mod\ n)$$

Entonces

$$1.\ (a+b) \equiv (c+d)\ (mod\ n)$$
$$2.\ (a-b) \equiv (c-d)\ (mod\ n)$$
$$3.\ ab \equiv cd (mod\ n)$$
$$4.\ a^m \equiv c^m (mod\ n)\ \ \forall m \in \mathbb{Z}$$

Clases de equivalencia

Una clase de equivalencia es un conjunto de subconjuntos distintos del conjunto de los números enteros, bajo una relación de congruencia módulo n.

La clase de equivalencia módulo n está conformada por un conjunto infinito de elementos, números enteros congruentes entre sí bajo la relación módulo n.

Ejemplo

La relación de congruencia módulo 5, está formada por 5 clases residuales y sus elementos son números enteros de la forma *0 + 5k, 1 + 5k, 2 + 5k, 3 + 5k y 4 + 5k*, donde *k* es un entero, las cinco clases residuales o clases de equivalencia son:

$$\{\cdots, -15, -10, -5, 0, 5, 10, 15, \cdots\}$$
$$\{\cdots, -14, -9, -4, 1, 6, 11, 16, \cdots\}$$
$$\{\cdots, -13, -8, -3, 2, 7, 12, 17, \cdots\}$$
$$\{\cdots, -12, -7, -2, 3, 8, 13, 18, \cdots\}$$
$$\{\cdots, -11, -6, -1, 4, 9, 14, 19, \cdots\}$$

Cada clase residual módulo n puede ser representada por uno cualquiera de sus miembros; pero, por lo general, se representa cada clase residual por el menor entero no negativo que pertenezca a esta clase. Hay que notar que dos enteros pertenecientes a distintas clases residuales módulo n son incongruentes módulo n. Además, todo entero pertenece a una y sólo una clase residual módulo n.

Definición. Un subconjunto $[C]_n$ de los enteros se dice que es un sistema completo de residuos módulo n, si cada entero es congruente a uno y sólo uno de los elementos del conjunto C.

Ejemplos
{0, 1, 2, 3, 4} es un sistema completo de residuos módulo 5.
{-10, -4, 2, 8, 14} es otro sistema completo de residuos módulo 5.

Ejemplo
Encuentre el residuo de la división de $2^{30} \div 15$.
Solución.
El problema equivale a encontrar cuál de las quince clases residuales módulo *15*, que contienen a *{0, 1, 2, 3,…..,14}* respectivamente, contiene a 2^{30}.

Se trata de encontrar un número *a* entre *0* y *14* tal que cumpla que $2^{30} \equiv a \pmod{15}$ o lo que es lo mismo; encontrar un *a* que sea igual al residuo de dividir 2^{30} entre *15*.
Solución

$$
\begin{aligned}
&Si\ 2^{30} \div 15 \\
&Buscamos\ un\ valor\ a\ t.q.\ 2^{30} \equiv a (mod\ 15) \\
&2^4 \equiv 1 (mod\ 15)\ puesto\ que\ 15 \mid (2^4 - 1) \\
&\Rightarrow (2^4)^7 \equiv 1^7 (mod\ 15) \\
&\Rightarrow (2^4)^7 \cdot 2^2 \equiv 1 \cdot 2^2 (mod\ 15) \\
&2^{30} \equiv 4 (mod\ 15) \\
&\therefore 2^{30} \div 15\ tiene\ resto\ =\ 4
\end{aligned}
$$

Por tanto, el residuo de dividir 2^{30} entre *15* es *4*.

Ejemplo
Calcular $102^8\ mod\ 502$.

$$
\begin{aligned}
102^8\ mod\ 502 &= \left[(102^2)^2\right]^2\ mod\ 502 \\
&= \left[(102^2\ mod\ 502)^2\ mod\ 502\right]^2\ mod\ 502 \\
&= \left[(10404\ mod\ 502)^2 mod\ 502\right]^2\ mod\ 502 \\
&= \left[(364)^2\ mod\ 502\right]^2\ mod\ 502 \\
&= \left[132496\ mod\ 502\right]^2\ mod\ 502 \\
&= 470^2\ mod\ 502 \\
&= 220900\ mod\ 502 = 20
\end{aligned}
$$

Ejemplo
Calcular $12^{43}\ mod\ 713$.

Para el cálculo de expresiones de la forma a^k mod n cuando k no es una potencia de 2, se debe escribir ese exponente en binario.
Solución.

$$43 = 101011_2$$

$$43 = 2^5 + 2^3 + 2 + 1$$

$$12^{43} = 12^{32+8+2+1} = 12^{32} \cdot 12^8 \cdot 12^2 \cdot 12$$

$$12^{43} \ mod\ 713 = \{(12^{32} mod\ 713)(12^8 mod\ 713)(12^2 mod\ 713)(12\ mod\ 713)\}\ mod\ 713$$

$$12^{43} \ mod\ 713 = \{485 \cdot 629 \cdot 144 \cdot 12\}\ mod\ 713$$

$$= 527152320\ mod\ 713$$

$$= 48$$

$$(12\ mod\ 713) = 12$$

$$(12^2 mod\ 713) = (144\ mod\ 713) = 144$$

$$(12^8 mod\ 713) = [(12^2\ mod\ 713)^2 mod\ 713]^2\ mod\ 713$$

$$= [(144)^2 mod\ 713]^2\ mod\ 713$$

$$= [20736\ mod\ 713]^2\ mod\ 713$$

$$= 59^2\ mod\ 713$$

$$= 629$$

$$(12^{32} mod\ 713) = [(12^8 mod\ 713)^2\ mod\ 713]^2\ mod\ 713$$

$$= [629^2\ mod\ 713]^2\ mod\ 713$$

$$= 639^2\ mod\ 713$$

$$= 485$$

Código en C++ para obtener el residuo de una potencia dado el módulo

exponModular - exponModular.cpp

```cpp
// exponModular.cpp : Calcular el resto de una potencia dados la base,
// el exponente y el módulo

#include <iostream>
using namespace std;

long obtResto(long base, long exponente, long nMod) {
    long acum = 1, nbase, xpon;
    nbase = base; xpon = exponente;
    while (xpon != 0) {
        if (xpon & 1) {
            acum = (acum * nbase) % nMod;
        };
        xpon >>= 1;
        nbase = (nbase * nbase) % nMod;
    };
    return acum;
}

int main()
{
    long abase, expon, modulo;

    cout << "Teclee la base, el exponente y módulo de la expresión: ";
    cin >> abase >> expon >> modulo;
    cout << endl;

    cout << "El resto de " << abase << "^" << expon << " (mod "
         << modulo << ") = " << obtResto(abase, expon, modulo) << endl;

    system("pause");
    return 0;
}
```