MATEMÁTICA DISCRETA

TEMA 6: Congruencias. Ecuaciones diofánticas.

TEMA 7: Combinatoria.

TEMA 8: Grafos.

TEMA 6: Congruencias. Ecuaciones diofánticas.

Teorema (Algoritmo de la división)
Sean $a, b \in \mathbb{Z}$ con $a > 0$ y $b > a$ entonces existen $c, r \in \mathbb{Z}$ únicos tales que

$$b = c \cdot a + r$$

con $0 \leq r < a$.

Ejemplo.
Lo anterior no es más que dividir,

$$b = c \cdot a + r$$
$$17 = 3 \cdot 5 + 2$$

Sistemas de representación

El sistema habitual es el decimal, pero el algoritmo de la división nos permite trabajar en otras bases "g".

Para ello dividiremos el número en cuestión, A, por el mayor exponente de "g", y si el resto sigue siendo mayor a "g" seguiremos repitiendo lo anterior. Finalmente A se podrá expresar como los cocientes anteriores.

Ejemplo.

Expresar 1293 en base $g=8$.

Dividiremos 1293 por el mayor exponente de 8 posible, en este caso, $8^3 = 512$.

$$1293 = 2 \cdot 8^3 + 269$$

$8^0 = 1$
$8^1 = 8$
$8^2 = 64$
$8^3 = 512$
$8^4 = 4096$

Como el resto, 269, es mayor que $g=8$, repetimos el proceso anterior.

$$269 = 4 \cdot 8^2 + 13$$

De nuevo, el resto es mayor que 8.

$$13 = 1 \cdot 8^1 + 5$$

Entonces, juntando lo anterior:

$$1293 = 2\cdot 8^3 + 269 = 2\cdot 8^3 + 4\cdot 8^2 + 13 = 2\cdot 8^3 + 4\cdot 8^2 + 1\cdot 8^1 + 5\cdot 8^0$$
$$= 2415_8$$

En general, en un sistema de base g, tendremos las cifras $0, 1, \ldots, g-1$.

Si $g=2$, las cifras son $0, 1$

$g=8$, las cifras son $0, 1, 2, \ldots, 7$

$g=10$, las cifras son $0, 1, \ldots, 7, 8, 9$

$g=12$, las cifras son $0, 1, \ldots, 8, 9, A, B$

Ejercicio: Expresar 1293 en base 12.

Expresar 4503_6 en base 9.

Observar que: $4503_6 = 4\cdot 6^3 + 5\cdot 6^2 + 0\cdot 6^1 + 3\cdot 6^0 =$

$$= 864 + 180 + 0 + 3 = 1047$$
$$\left(= 1\cdot 10^3 + 0\cdot 10^2 + 4\cdot 10^1 + 7\cdot 10^0\right)$$

Máximo común divisor. Algoritmo de Euclides

Definición

Sean $a, b \in \mathbb{Z}$. Diremos que el máximo común divisor de a y b, $mcd(a,b) = d$, si verifica:

1) $d > 0$

Divisor común — 2) d divide a "a" y a "b". $d \mid a$ y $d \mid b$ ("d divide a a", "d divide a b")

Máximo divisor — 3) Si r es un divisor común, $r \mid a$ y $r \mid b$, entonces r divide a d, $r \mid d$

En otras palabras el máximo común divisor de dos números es el producto de los divisores comunes al menor exponente.

Ejemplo El máximo común divisor de 12 y 18:

$12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$ = divisores comunes

$18 = 2 \cdot 3 \cdot 3 = 2 \cdot 3^2$

Entonces $mcd\,(12, 18) = 2 \cdot 3 = 6$.

El problema de esta técnica es que la descomposición en números primos de un número, en general, no es tarea sencilla.

Ejemplo (Algoritmo de Euclides)

- Calcular m.c.d. (1314, 247). Aplicaremos el algoritmo de la división reiteradas veces.

$$1314 = 247 \cdot 5 + 79$$
$$247 = 79 \cdot 3 + 10$$
$$79 = 10 \cdot 7 + 9$$
$$10 = 9 \cdot 1 + \boxed{1}$$
$$9 = 1 \cdot 9 + 0$$

El m.c.d (1314, 247) = 1, el último resto anterior a 0.

- Calcular mcd (1567, 4763)

$$4763 = 1567 \cdot 3 + 62$$
$$1567 = 62 \cdot 25 + 17$$
$$62 = 17 \cdot 3 + 11$$
$$17 = 11 \cdot 1 + 6$$
$$11 = 6 \cdot 1 + 5$$
$$6 = 5 \cdot 1 + \boxed{1}$$
$$5 = 1 \cdot 5 + 0$$

El algoritmo nos da $\text{mcd}(4763, 1567) = 1$. Pero dice más:

$$\text{mcd}(4763, 1567) = \text{mcd}(1567, 62) = \text{mcd}(62, 17) =$$
$$= \text{mcd}(17, 11) = \text{mcd}(11, 6) = \text{mcd}(6, 5) = \text{mcd}(5, 1) = 1$$

Lema (de Bezout)

Sean $a, b \in \mathbb{Z}$ con $\text{mcd}(a, b) = d$. Entonces existen $x_0, y_0 \in \mathbb{Z}$ tales que $ax_0 + by_0 = d$

Bezout nos asegura que tales x_0 e y_0 existen, pero no cómo calcularlos.

Ejemplo. Sabiendo que $\text{mcd}(1314, 247) = 1$. Calcular x_0 e y_0 tales que $1314x_0 + 247y_0 = 1$.

Tras realizar el algoritmo de Euclides, empezando de abajo hacia arriba vamos despejando los

restas (SIN OPERAR) y sustituyendo en el primero:

$1314 = 247 \cdot 5 + 79 \longrightarrow 79 = 1314 - 247 \cdot 5$

$247 = 79 \cdot 3 + 10 \longrightarrow 10 = 247 - 79 \cdot 3$

$79 = 10 \cdot 7 + 9 \longrightarrow 9 = 79 - 10 \cdot 7$

$10 = 9 \cdot 1 + \boxed{1} \longrightarrow 1 = 10 - 9 \cdot 1$

$9 = 1 \cdot 9 + 0$

$1 = 10 - 9 \cdot 1 = 10 - (79 - 10 \cdot 7) = 10 - 79 + 10 \cdot 7 =$

$= 10 \cdot 8 - 79 = (247 - 79 \cdot 3) \cdot 8 - 79 =$

$= 247 \cdot 8 - 24 \cdot 79 - 79 = 247 \cdot 8 - 79 \cdot 25 =$

$= 247 \cdot 8 - (1314 - 247 \cdot 5) \cdot 25 = 247 \cdot 8 - 1314 \cdot 25 + 247 \cdot 125$

$1 = \underbrace{(-25)}_{x_0} \cdot 1314 + \underbrace{(133)}_{y_0} \cdot 247$

Ejercicio. Calcular $x_0, y_0 \in \mathbb{Z}$ tales que

$1567 x_0 + 4763 y_0 = 7$