Teoría elemental de números

Matemática discreta

Resultados previos

- Axioma: todo subconjunto no vacío de N tiene mínimo, con el orden usual en N.

- Toda sucesión decreciente en N converge.

Divisibilidad

- Si a,b$\in$Z, ***a* divide a *b*** , $a \mid b$, si $\exists$c$\in$Z tal que $b=a\cdot$c. Se dice también que ***b* es múltiplo de *a*** o que ***a* es divisor de *b***. En caso contrario, $a \nmid b$, ***a* no divide a *b***.

Propiedades de divisibilidad

$\forall a, b, c \in Z$

- $1 \mid a \qquad a \mid a \qquad a \mid 0$
- Si $a \mid b$ y $b \mid a$, entonces $a = \pm b$
- $a \mid b$, entonces $a \mid b \cdot c$
- $a \mid b$ y $a \mid c$, entonces $a \mid bx+cy \quad \forall x,y \in Z$
- Si $x=y+z$, $a \mid x$, $a \mid y$, entonces $a \mid z \qquad \forall x,y,z \in Z$

División euclídea

Dados $a,b \in Z$ siendo $b \neq 0$, existen únicos $q,r \in Z$ tales que $a=b \cdot q+r$, con $0 \leq r < |b|$.

a: dividendo

b: divisor

q: cociente

r: resto

Números primos

- Dado $p \in N$, $p>1$, **p es primo** si

$$\forall n \in N \; n \mid p \Rightarrow n=p \text{ ó } n=1$$

- Todo natural mayor que 1 es divisible por, al menos, un número primo.

Teorema fundamental de la aritmética

- $\forall n \in N$, $n>1$, existen únicos $p_1, .., p_r \in N$ y existen únicos $\alpha_1, .., \alpha_r \in N^*$ tales que

$$n = p_1^{\alpha_1} ... p_r^{\alpha_r}$$

Todo natural se descompone de manera única como producto de potencias de números primos.

Máximo común divisor

Dados $a,b \in Z$ no simultáneamente nulos.

- d es **divisor común** de a y b si $d \mid a$ y $d \mid b$.
- El máximo común divisor de a y b, **mcd(a,b)**, es el mayor de los divisores comunes de a y b.
- a y b son **primos relativos** si mcd(a,b)=1.
- Si $b \neq 0$ y r es el resto de la división euclídea entre a y b, entonces:
  - Los divisores comunes de a y b son divisores de r.
  - Los divisores comunes de b y r son divisores de a.

Algoritmo de Euclides

- Dados $a,b \in Z^*$ y r el resto de la división euclídea entre a y b, entonces

$$mcd(a,b) = mcd(b,r)$$

- Nos proporciona un algoritmo para calcular el **mcd** utilizando la división euclídea.

- $mcd(a,b) = mcd(|a|,|b|)$

Algoritmo de Euclides 2

- Sean $a,b \in Z^+$ con $a \geq b > 0$, llamamos $r_0=a$ y $r_1=b$.

Aplicamos sucesivas veces la división euclídea:

$$r_0 = q_1 \cdot r_1 + r_2. \qquad 0 < r_2 < r_1$$
$$r_1 = q_2 \cdot r_2 + r_3. \qquad 0 < r_3 < r_2$$
$$\ldots\ldots\ldots\ldots$$
$$r_{n-2} = q_{n-1} \cdot r_{n-1} + r_n \qquad 0 < r_n < r_{n-1}$$
$$r_{n-1} = q_n \cdot r_n + r_{n+1} \qquad r_{n+1} = 0$$

Entonces, el $mcd(a,b)=r_n$

ejemplo

- mcd(6,9)=3
  9=**6**·1+3
  6=**3**·2+0

El último resto distinto de 0 es 3, el mcd.

- mcd(24,62)=2
  62=**24**·2+14
  24=**14**·1+10
  14=**10**·1+4
  10=**4**·2+2
  4=**2**·2+0

El último resto distinto de 0 es 2, el mcd.

Teorema de Bezout

Dados $a,b \in N^*$ y $mcd(a,b)=d$, entonces

$\exists x,y \in Z$ tales que $d=ax+by$

Identidad de Bezout

$mcd(a,b)=1 \Leftrightarrow \exists x,y \in Z$ tales que $1=ax+by$

- Dados $a,b \in Z$ se verifica
  - Si $p \mid a \cdot b$ y p es primo, entonces $p \mid a$ ó $p \mid b$.
  - Si $p \mid a \cdot b$ y $mcd(a,p)=1$, entonces $p \mid b$.

Ecuaciones diofánticas

- Buscamos soluciones enteras de una ecuación.
- Ecuación diofántica lineal en dos variables

$$ax+by=c \qquad a, b, c \in Z$$

- Diofanto, s. III a.C.

Ecuaciones diofánticas 2

- Dados $a,b,c \in Z$, $mcd(a,b)=d$, y dada la ecuación $ax+by=c$
  - Si $d \nmid c$ la ecuación no tiene soluciones enteras.
  - Si $d \mid c$ la ecuación tiene infinitas soluciones enteras. A partir de una solución particular (x_0,y_0) calculamos el resto de las soluciones

$$x = x_0 + (b/d)\cdot n \qquad n \in Z$$

$$y = y_0 - (a/d)\cdot n$$

Ecuaciones diofánticas 3

- Para calcular una solución particular:
  - dividimos ax+by=c por mcd(a,b)=d y obtenemos a´x+b´y=c´
  - como mcd(a´,b´)=1, por la identidad de Bezout a´x+b´y=1 tiene solución.
  - Encontramos la solución (x_1,y_1) de a´x+b´y=1 por el algoritmos de Euclides.
  - Una solución particular es $(c´x_1,cý_1)$.

ejemplo

(1) $6x+4y=10$. Como $\mcd(6,4)=2 \mid 10$, dividimos la ecuación por 2

(2) $3x+2y=5$. Como $\mcd(3,2)=1$, la ecuación (3) $3x+2y=1$ tiene solución (identidad de Bezout).

$3=2\cdot 1+1$, luego $(1,-1)$ es solución de (3) y $(5,-5)$ es solución particular de (2)

$$x= 5+(4/2)\cdot n=5+2\cdot n$$

$$y=-5-(6/2)\cdot n=-5-3n$$

$$n \in Z$$

Aritmética modular

Dado $m \in N$

- ***a* es congruente con *b* módulo m**, $a \equiv b \pmod m$, si $m \mid b-a$, es decir, $\exists q \in Z$ tal que $b=a+qm$.
- $a \equiv b \pmod m \Leftrightarrow \exists q_a, q_b \in Z$ y $\exists r \in Z$ que verifican

$$a = q_a m + r$$

$$b = q_b m + r$$

- $\forall z \in Z$, z es congruente módulo m forzosamente con un elemento del conjunto $\{0, 1, ..., m-1\}$.

Clases de equivalencia

- La relación $\equiv \pmod m$ es de equivalencia.
  - Reflexiva $a \equiv a \pmod m$
  - Simétrica $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$
  - Transitiva $a \equiv b \pmod m$ y $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$
- Dado $k \in Z$, se define la clase de equivalencia de k como $[k] = \overline{k} = \{x \in Z / x \equiv k \pmod m\}$.

ejemplo: $\equiv \pmod 3$

$[0] = \overline{0} = \{0,3,6,9,12,...,-3,-6,-9,-12,...\}$.

$[1] = \overline{1} = \{1,4,7,10,...,-2,-5,-8,-11...\}$.

$[2] = \overline{2} = \{2,5,8,11,...,-1,-4,-7,-10,...\}$.

Conjunto cociente

- $Z/\equiv \pmod m = \{\ \overline{k} / \ k \in Z\}$.
- $\equiv \pmod m$ define en Z una partición llamada Z_m que está formada por m clases de equivalencia $Z_m = \{\ \overline{0},\ \overline{1}, ...,\ \overline{m-1}\}$.

ejemplo:

En Z, $\equiv \pmod 3$ induce la partición $Z_3 = \{\ \overline{0},\ \overline{1},\ \overline{2}\}$

Propiedades

$a,b,c,d \in Z$, $m \in N^*$

- Si en Z_m $[a]=[b]$ y $[c]=[d]$, entonces la clase de la suma y el producto es independiente del representante que elijamos de cada clase.
  - $[a+c]=[b+d]$
  - $[a \cdot c]=[b \cdot d]$
- Propiedad cancelativa: si en Z_m $[a \cdot c]=[b \cdot c]$ y $mcd(m,c)=1$, entonces $[a]=[b]$

Aritmética en Z_n

- Suma de clases

$$\oplus: Z_n x Z_n \rightarrow Z_n : [a] \oplus [b] = [a+b]$$

Cumple las propiedades:

- Asociativa: $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$
- Conmutativa: $[a] \oplus [b] = [b] \oplus [a]$
- Elemento neutro: $[0] \oplus [a] = [a] \oplus [0] = [a]$
- Elemento opuesto: $-[a] \oplus [a] = [a] \oplus (-[a]) = [0]$

ejemplo 1

Tabla de la suma de clases en Z_4

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

ejemplo 2

En Z_7

- $-[2]=[-2]=[5]$ $-2-5=-7$
- $[5] \oplus (-[10])=[5]\oplus[-10]=[5]\oplus[4]=[9]=[2]$

  $-10= -2\cdot 7+4, -10-4 \in 7^{\cdot}$

  $[5] \oplus (-[10])=[5-10]=[-5]=[2]$

  $-5= -1\cdot 7+2,\ -5-2 \in 7^{\cdot}$
- $3\cdot[5]=[5]\oplus[5]\oplus[5]=[3\cdot 5]=[15]=[1]$
- $-3\cdot[5]=-[5]\oplus(-[5])\oplus(-[5])=[-3\cdot 5]=[-15]=[6]$

Aritmética en Z_n

- Producto de clases

$$\odot: Z_n x Z_n \rightarrow Z_n : [a] \odot [b] = [a \cdot b]$$

Cumple las propiedades:

- Asociativa: $[a] \odot ([b] \odot [c]) = ([a] \odot [b]) \odot [c]$
- Conmutativa: $[a] \odot [b] = [b] \odot [a]$
- Elemento neutro: $[1] \odot [a] = [a] \odot [1] = [a]$
- Elemento inverso: si mcd(a,n)=1

$[a]^{-1} \odot [a] = [a] \odot [a]^{-1} = [1]$

(si n es primo, existe el inverso $\forall [a] \in Z_n$)

ejemplo 1

Tabla del producto de clases en Z_4

$\odot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

ejemplo 2

En Z_7

- como mcd(7,2)=1, por la identidad de Bezout $\exists\ \alpha,\beta \in Z$ / $\alpha\cdot 2+\beta\cdot 7=1$, por tanto $[\alpha\cdot 2+\beta\cdot 7]=[1] \Rightarrow [\alpha\cdot 2] \oplus [\beta\cdot 7]=[1] \Rightarrow$
$\Rightarrow [\alpha\cdot 2] \oplus [0]=[1] \Rightarrow [\alpha] \odot [2] =[1] \Rightarrow$
$\Rightarrow [2]^{-1} =[\alpha]$
Para que se cumpla $\alpha\cdot 2+\beta\cdot 7=1$ basta tomar $\alpha=4$ y $\beta=-1$, luego $[2]^{-1}=[4]$. Efectivamente, $[2]\odot[4]=[8]=[1]$

ejemplo 3

En Z_6. Como $mcd(6,2)\neq 1$, $\nexists\ [2]^{-1}$, es decir, $\nexists\ \alpha$ tal que $[2]\odot[\alpha]=[1]$. Efectivamente, basta observar la tabla del producto de clases en Z_6

$\odot$	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]
[2]	[2]	[4]	[0]	[2]	[4]
[3]	[3]	[0]	[3]	[0]	[3]
[4]	[4]	[2]	[0]	[4]	[2]
[5]	[5]	[4]	[3]	[2]	[1]

Propiedad distributiva del producto respecto de la suma de clases

$\forall n \in \mathbb{N}^*$ y $\forall [a],[b],[c] \in \mathbb{Z}_n$

$$[a] \odot ([b] \oplus [c]) = ([a] \odot [b]) \oplus ([a] \odot [c])$$

Ecuaciones modulares

Dados $a,b \in Z$, en Z_n si $mcd(a,n)=d$ la ecuación $[a]\cdot[x]=[b]$

- no tiene solución si $d \nmid b$
- tiene d soluciones en Z_n si $d \mid b$

- $[a]\cdot[x]=[a\cdot x]=[b]$ existe $\Leftrightarrow$ $a\cdot x-b$ es múltiplo de n, es decir, si $\exists\ k \in Z$ / $ax-b=kn$. La ecuación $ax+kn=b$ tiene solución $\Leftrightarrow$ $mcd(a,n) \mid b$. Entonces, si x_0 es solución particular de $ax+kn=b$, las soluciones en Z_n vienen dadas por $[x_0]$, $[x_0+n/d]$, $[x_0+2\cdot n/d]$, ..., $[x_0+(d-1)\cdot n/d]$.

ejemplo

Las soluciones de $[5]\cdot[x]=[6]$ son:

En Z_4: como $[5]=[1]$ y $[6]=[2]$ tenemos $[1]\cdot[x]=[2]$ como $mcd(1,4)=1$ y $1 \mid 2$, hay una única solución. Consideramos la ecuación $1\cdot x+4\cdot k=1$ que tiene solución particular $x=5$ y $k=-1$, por tanto una solución particular de $1\cdot x +4\cdot k=2$ es $x=10$. Como $[10]=[2]$, la única solución es $[2]$.

En Z_{10}: como $mcd(5,10)=5$ y $5 \nmid 6$, no hay solución.

ejemplo

Las soluciones de $[5]\cdot[x]=[6]$ son:

En Z_4: como $[5]=[1]$ y $[6]=[2]$ tenemos $[1]\cdot[x]=[2]$ como $mcd(1,4)=1$ y $1 \mid 2$, hay una única solución. Consideramos la ecuación $1\cdot x+4\cdot k=1$ que tiene solución particular $x=5$ y $k=-1$, por tanto una solución particular de $1\cdot x +4\cdot k=2$ es $x=10$. Como $[10]=[2]$, la única solución es $[2]$.

En Z_{10}: como $mcd(5,10)=5$ y $5 \nmid 6$, no hay solución.

Diofanto de Alejandría

- *“Dios le concedió el ser un muchacho durante una sexta parte de su vida, y añadiendo a esto una doceava parte, El pobló de vello sus mejillas; Le iluminó con la luz del matrimonio después de una séptima parte, y cinco años después de su matrimonio Le concedió un hijo. Pero ¡ay! Infeliz niño nacido tarde; después de alcanzar la mitad de la medida de la vida de su padre, el frío destino se lo llevó. Después de consolar sus penas con la ciencia de los números durante cuatro años más, finalizó su vida”.*