Clase 6

Teoría de Números Básica

Fernando Krell[1]

[1]Departamento de Ciencias de la Computación
Pontificia Universidad Católica de Chile

6 de Abril de 2016

Divisibilidad

- $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$
- $a, b \in \mathbb{Z}$, a divide $b \in \mathbb{Z}$ si $\exists \in \mathbb{Z},\ ak = b$
- Notación: $a \mid b$, $a \nmid$ b si $\forall k \in \mathbb{Z},\ ak \neq b$
- Ejemplos: $1 \mid b\ \forall b \in \mathbb{Z}$, $3 \mid 27$, $2 \nmid 11$
- Observación:

$$a \mid b \wedge a \mid c \Rightarrow \exists X, Y \in \mathbb{Z},\ a = Xb + Yc$$

$$\forall a, b \in \mathbb{Z}\ \exists X, Y \in \mathbb{Z},\ 1 = Xa + Yb$$

- Ejemplo: $3 = 6 \cdot 2 + -1 \cdot 15$

Divisibilidad (2)

- a es divisor de b si $a > 0$ y $a \mid b$
- a es factor de b si además $a \notin \{1, b\}$

  p es primo si no tiene factores!
- $a \in \mathbb{Z}, b \in \mathbb{Z}^+, \exists! q, r \in \mathbb{Z}, 0 \leqslant r < b$

$$a = qb + r$$

- es posible encontrar q, r en tiempo polinomial (división entera).

Máximo común divisor

MCD

- $\text{mcd}(a, b) = \text{máx}\{d,\ d \mid a \wedge d \mid b\}$
- Ejemplos: $\text{mcd}(15, 10) = 5,\ \text{mcd}(15, 0) = 15$

$$\text{mcd}(a, p) = 1 \forall p \text{ primo, } \forall a \in \{1, 2, 3..., p - 1\}$$

- a y b son primos relativos si $\text{mcd}(a, b) = 1$

Proposición 1

$\forall a, b \in \mathbb{Z}^+ \; \exists X, Y \in \mathbb{Z}$ tales que $Xa + Yb = \text{mcd}(a, b)$ y, además $\text{mcd}(a, b) = \text{mín}\{d | d = Xa + Yb > 0\}_{X,Y \in \mathbb{Z}}$

Demostración.

- Sea $I \stackrel{\text{def}}{=} \{Xa + Yb > 0\}_{X,Y \in \mathbb{Z}}$. (notar que a y $b \in I$)
- Sea $d = \text{mín}(I) = \hat{X}a + \hat{Y}b$, demostremos primero que d divide a *todo* elemento c en I.
- $c = Xa + Yb$, pero $c = qd + r$ para $r < d$
  $\Rightarrow r = Xa + Yb - q(\hat{X}a + \hat{Y}b)$
- $r = (X - q\hat{X})a + (Y - \hat{Y}q)b$
  1. $r \neq 0 \Rightarrow d$ no es mínimo en I
  2. $r = 0 \Rightarrow d \mid c$
- Nos falta demostrar que d es máximo. Sea $d' > d$ tal que $d' \mid a \wedge d' \mid b$
- $\Rightarrow d' | (\hat{X}a + \hat{Y}b) \Rightarrow d' \mid d$, lo cual es una contradicción pués $d' > d$.

Proposición 2

$c \mid ab \wedge \text{mcd}(a, c) = 1 \Rightarrow c \mid b$.
Caso especial:Si p es primo y $p \mid ab \Rightarrow p \mid a \vee p \mid b$

Demostración.

- $c \mid ab \Rightarrow \gamma c = ab$.
- $\text{mcd}(a, c) = 1 \Rightarrow \exists X, Y \in \mathbb{Z}$ tales que $1 = Xa + Yc$
- $\Rightarrow b = Xab + Ycb = X\gamma c + Ybc = (X\gamma + Yb)c$
- $\Rightarrow c \mid b$

□

Proposición 3

$a \mid N \wedge b \mid N \wedge \text{mcd}(a, b) = 1 \Rightarrow ab \mid N$.
Ejemplo, $a = 4, b = 9$, $4 \mid 36$ y $9 \mid 36$

Demostración.

- $ac = N,\ bd = N$ y $1 = Xa + Yb \Rightarrow N = XaN + YbN$.
- $N = Xabd + Ybac = ab(Xd + Yc) \Rightarrow ab|N$

$\square$

Reducción Módulo N

- r es el resto de la division entera de N por a, $a = qN + r$.
- Reducción modular: Definimos $[a \mod N]$ como el resto r, y lo denominamos esta función como reducción módulo N.
- Observación: $0 \leqslant [a \mod N] < N$.
- Congruencia. a y b son congruentes módulo N ($a = b \mod N$) si $[a \mod N] = [bmodN]$.
- Ejemplo: 25 es congruente con 4 modulo 21 (denotamos como $25 = 4 \mod 21$)

Proposición 4

$$a = b \mod N \Leftrightarrow N \mid (a - b)$$

Demostración.

$\Rightarrow$ $a - q_a N = r_a = r_b = b - q_b N \Rightarrow a - b = N(q_a - q_b)$

$\Leftarrow$ $N \mid (a-b) \Rightarrow \gamma N = a-b = q_a N + r_a - q_b N - r_b$
Pero $-N < r_a - r_b < N$, por lo tanto si $r_a \neq r_b$, N no es múltiplo de $a - b$, lo cual es una contradicción.

$\square$

Suma y multiplicación mód N

Sean $a = a' \mod N$ y $b = b' \mod N$.

1. $a + b = a' + b' \mod N$. $a = q_a N + r_a, b = q_b N + r_b$
   Por lo tanto $a + b = (q_a + q_b)N + r_a + r_b$.
2. $ab = a'b' \mod N$. Por lo tanto
   $ab = (q_a q_b)N^2 + (q_a r_b + q_b r_a)N + r_a r_b$.

Podemos reducir, luego sumar o multiplicar
Ejemplo: $(16757 \times 77789) \mod 7 = ((16757 \mod 7) \times (77789 \mod 7)) \mod 7 = 6 \times 5 \mod 7 = 2$

División mód N

- Problema: Division módulo N no necesariamente esta definida para todo entero. $ab = cb \mod N \implies a = c \mod N$.
- No necesariamente un entero tiene inverso multiplicativo.
- Ejemplo: 2 no tiene inverso multiplicativo módulo 4:
  - $2 \cdot 0 \mod 4 = 0$,
  - $2 \cdot 1 \mod 4 = 2$,
  - $2 \cdot 2 \mod 4 = 0$,
  - $2 \cdot 3 \mod 4 = 2$.

Última Proposición

$b, N \in \mathbb{Z}, b \geqslant 1, N > 1,$

b tiene inverso multiplicativo mód $N \Leftrightarrow \text{mcd}(b, N) = 1$

Demostración.

$\Rightarrow$ $b \cdot c = 1 \mod N, \Rightarrow \exists \gamma \in \mathbb{Z} bc - 1 = \gamma N \Leftrightarrow$ $bc - \gamma N = 1$ pero 1 es el positivo mas pequeño, por lo que $\text{mcd}(b, N) = 1$

$\Leftarrow$ $\text{mcd}(b, N) = 1 \Rightarrow \exists X, Y \in \mathbb{Z}$ tales que $Xb + YN = 1 \Rightarrow Xb = 1 \mod N$, por lo tanto $X = b^{-1} \mod N$

□

Ejemplo: $b = 8, N = 11, 11 \times 3 - 4 \cdot 8 = 1 \Rightarrow -4$ mód $11 = 7$ es el inverso de 8 mód 11

Grupos

Un grupo $(\mathbb{G}, \circ)$ esta comuesto por un conjunto $\mathbb{G}$ y una operación binaria $\circ$ tales que

- $\circ$ es cerrado en $\mathbb{G}$: $g \circ h \in \mathbb{G} \forall g, h \in \mathbb{G}$
- existe elemento neutro para $\circ$ (identidad). $\exists e \in \mathbb{G},\ g \circ e = e \circ g = g \forall g \in \mathbb{G}$
- Elementos tienen inverso: $\forall g \in \mathbb{G},\ \exists g' \in \mathbb{G}, g \circ g' = e$
- Asociatividad: $\forall g, h, i \in \mathbb{G},\ g \circ (h \circ i) = (g \circ h) \circ i$
- Commutatividad: $\forall g, h \in \mathbb{G},\ g \circ h = h \circ g$

Si $\mathbb{G}$ es finito, entonces decimos que el grupo es finito y su orden es $m = |\mathbb{G}|$

Exponenciacion

Sea $m \in \mathbb{N}$ y $g \in \mathbb{G}$

- Notación Aditiva: $m \cdot g = g \circ g \circ \cdots \circ g$
  Afortunadamente, tenemosi las siguientes propiedades:

$$(m + m') \cdot g = (m \cdot g) \circ (m' \cdot g)$$
$$(m \times m') \cdot g = m \cdot (m' \cdot g)$$
$$(m \cdot g) \circ (m \cdot h) = m \cdot (g \circ h)$$

- Notación Multiplicativa: $g^m = g \circ g \circ \cdots \circ g$

$$g^{m+m'} = (m \cdot g) \circ (m' \cdot g)$$
$$(m \times m') \cdot g = m \cdot (m' \cdot g)$$
$$(m \cdot g) \circ (m \cdot h) = m \cdot (g \circ h)$$

Teorema

Theorem

Si $\mathbb{G}$ es un grupo abeliano de orden m, entonces $g^m = 1 \forall g \in \mathbb{G}$ (en donde 1 es el elemento neutro para $\mathbb{G}$)

Demostración.

Sean $g_1, g_2, ..., g_m$ todos los elementos de $\mathbb{G}$. Sea g un elemento cualquiera de $\mathbb{G}$.
Notar que si $g \circ g_i = g \circ g_j$, entoces $g_i = g_j$ (podemos aplicar $\circ$ con el inverso de g a ambos lados).
Por lo tanto, $(g \circ g_1), (g \circ g_1), \ldots, (g \circ g_m)$ es una permutación de $g_1, g_2, ..., g_m$.
Entonces,

$$(g \circ g_1) \circ (g \circ g_1) \circ \ldots \circ (g \circ g_m) = g_1 \circ g_2 \circ \ldots \circ g_m$$

Y concluimos que $g^m = 1$ $\square$

Corolario 1

Corollary

Sea $\mathbb{G}$ *un grupo de orden* m*, entonces para todo* $g \in \mathbb{G}$*, y para todo* $x \in \mathbb{N}$, $g^x = g^{x \mod m}$

Demostración.

$g^x = g^{k \cdot m + x \mod m} = g^{k \cdot m} \circ g^{x \mod m}$, para algún entero k.
Pero $g^{k \cdot m} = (g^m)^k = 1^k = 1$ □

Corolario 2

Corollary

Sea $f_e : \mathbb{G} \to \mathbb{G}$ *una función definida como* $f_e(g) = g^e$. f_e *es una biyección si* $\text{mcd}(e, m) = 1$, *y más aun, si* $d = e^{-1}$ mód m, *entonces* f_d *es su función inversa.*

Demostración.

Basta con demostrar que $f_d(f_e(g)) = g$.
$f_d(f_e(g)) = f_d(g^e) = (g^e)^d = g^{e \cdot d} = g^{e \cdot d \text{ mód } m} = g^1 = g$ □