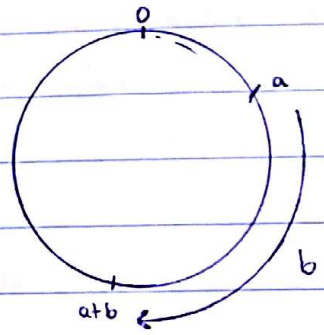
UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 11 de Abril de 2017

- Soma Modular:

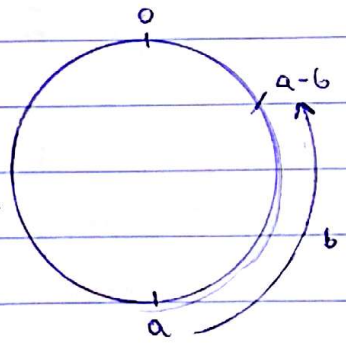
$\bar{a} + \bar{b} = 0$



$\bar{a} + \bar{b} = \overline{a+b}$

- Subtração Modular:

$\bar{a} - \bar{b}$



$\bar{a} - b = \overline{a-b}$

Se $\bar{a} = \bar{a'}$ e $\bar{b} = \bar{b'}$, então $\bar{a} - \bar{b} = \bar{a'} - \bar{b'}$.

$\bar{a} = \bar{a'} \Rightarrow a = a' + nt$

$\bar{b} = \bar{b'} \Rightarrow b = b' + nt'$ (SUBTRAIR)

$(a-b) = (a'-b') + n(t-t')$

$\Downarrow\Downarrow$

$\overline{a-b} = \overline{a'-b'}$

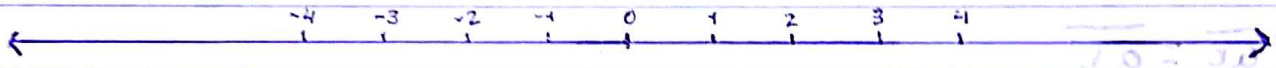
$\bar{a} - \bar{b} \quad \bar{a'} - \bar{b'}$

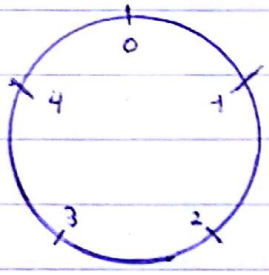
OBS: Também podemos calcular a forma reduzida módulo n de inteiros negativos

EXEMPLO: $n = 5$

$\bar{2} - \bar{3} = \overline{2-3} = \bar{-1} = 4$

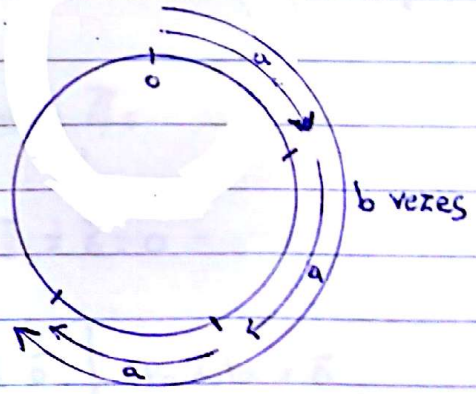
↳ QUAL A FORMA REDUZIDA DE -1?





- MULTIPLICAÇÃO MODULAR

$\bar{a} \cdot \bar{b}$



$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

Se $\bar{a} = \bar{a'}$ e $\bar{b} = \bar{b'}$

Então $\bar{a} \cdot \bar{b} = \bar{a'} \cdot \bar{b'}$

$\bar{a} = \bar{a'} \Rightarrow a = a' + n \cdot t$

$\bar{b} = \bar{b'} \Rightarrow b = b' + n \cdot t'$ (MULTIPLICA)

$(a \cdot b) = (a' + n \cdot t) + (b' + n \cdot t')$

$= a'b' + a'nt' + b'nt + n^2 tt'$

$= (a'b') + n \cdot (a't' + b't + ntt')$

↳ MULTIPLO DE N

$\overline{ab} = \overline{a'b'}$

$\bar{a} \cdot \bar{b} \quad \bar{a'} \cdot \bar{b'}$

EXEMPLO: $n = 8$

$\overline{7} \cdot \overline{3} = \overline{21} = \overline{5}$

$\overline{23} \cdot \overline{35} = \overline{805} = \overline{5}$

- PROPRIEDADES DAS OPERAÇÕES DE SOMA E MULTIPLICAÇÃO

1) Soma e multiplicação são associativas:

$\bar{a} + (\bar{b} + \bar{c}) = (\bar{a} + \bar{b}) + \bar{c}$

$\bar{a} \cdot (\bar{b} \cdot \bar{c}) = (\bar{a} \cdot \bar{b}) \cdot \bar{c}$

2) São comutativas

$\bar{a} + \bar{b} = \bar{b} + \bar{a}$

$\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$

3) Tem elementos neutros:

$\bar{a} + \bar{0} = \bar{a}$

$\bar{a} \cdot \bar{1} = \bar{a}$

4) Todo elemento $\bar{a}$ possui inverso aditivo, isto é, um elemento $-\bar{a}$ tal que $\bar{a} + (-\bar{a}) = \bar{0}$.

5) Inverso multiplicativo?

Veremos mais adiante.

6) Propriedade distributiva:

$\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$.

- PROPRIEDADE "ESTRANHA"

EXEMPLO: $\mathbb{Z}_6$

$\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$

$2 \neq \bar{0}$
$3 \neq \bar{0}$
} Produto $= \bar{0}$

Nos inteiros, se $ab = 0$, então $a = 0$ ou $b = 0$

- POTÊNCIA MODULAR

Quero calcular a^e módulo m.

$a^e = \underbrace{a \cdot a \cdot \ldots \cdot a}_{e \text{ vezes}}$

$\bar{a} \in \mathbb{Z}_m$

$e \in \mathbb{N}$

m módulo
(inteiro ≥ 2)

PRIMEIRA IDEIA: MÉTODO INGÊNUO:

MULTIPLICO $\bar{a} \cdot \bar{a}$

↓

REDUZO O RESULTADO
MÓDULO m

↓

MULTIPLICO O RESULTADO
REDUZIDO POR $\bar{a}$

↓

REDUZO NOVAMENTE

NÚMERO DE MULTIPLICAÇÕES: e
NÚMERO DE REDUÇÕES: e-1

SEGUNDA IDEIA: MÉTODO EFICIENTE, CONHECIDO COMO "DOUBLE AND ADD" (DOBRAR E SOMAR)

Vamos representar o expoente em binário (base 2):

$e = e_n \cdot 2^n + e_{n-1} \cdot 2^{n-1} + e_{n-2} \cdot 2^{n-2} + \ldots + e_2 \cdot 2^2 + e_1 \cdot 2 + e_0$

$e_i \in \{0, 1\}$, para todo $0 \leq i \leq n$.

$\bar{a}^e = \bar{a}^{e_n \cdot 2^n + e_{n-1} \cdot 2^{n-1} + e_{n-2} \cdot 2^{n-2} + \ldots + e_2 \cdot 2^2 + e_1 \cdot 2 + e_0} =$

$= \bar{a}^{e_n \cdot 2^n} \cdot \bar{a}^{e_{n-1} \cdot 2^{n-1}} \cdot \ldots \cdot \bar{a}^{e_2 \cdot 2^2} \cdot \bar{a}^{e_1 \cdot 2} \cdot \bar{a}^{e_0} =$

$= (\bar{a}^{2^n})^{e_n} \cdot (\bar{a}^{2^{n+1}})^{e_{n-1}} \cdot \ldots \cdot (\bar{a}^2)^{e_1} \cdot (\bar{a})^{e_0}$

ELEVO AO QUADRADO — ELEVO AO QUADRADO — ELEVO AO QUADRADO — ELEVO AO QUADRADO

→ A cada etapa, elevo a base anterior do quadrado para obter a nova base.

→ Expoentes e_i são 0 ou 1.

→ Como obter os expoentes e_i?

- e_0 é o resto da divisão de e por 2.
  - ↳ Se e é impar → $e_0 = 1$
  - ↳ Se e é par → $e_0 =$

Obtenho o quociente de e por 2 e repito o processo:

↳ e_1 será o resto da divisão desse resultado por 2.

e assim por diante.

O expoente e na base 2 tem $n+1$ algarismos $(e_0, e_1, e_2, \ldots, e_n)$

$n = \log_2^e$

/ /

n elevações ao quadrado

n11 divisões por 2

↓

Quantidade proporcional a $\log^{e} z$.

- ALGORITMO DE POTENCIAÇÃO MODULAR:

- ENTRADA: inteiro a, inteiro não-negativo e, inteiro maior ou igual a 2 m.
- SAÍDA: forma reduzida de a^e módulo m.
- INSTRUÇÕES:

1) R ← 1, A ← a, E ← e
2) Enquanto E ≠ 0, faça:
   2.1) Se E é impar, então:
      2.1.1) R ← (R * A) mod m
      2.1.2) E ← (E-1) /2
   2.2) Se E é par, então:
      2.2-1) E ← E/2
   2.3) A ← (A * A) mod m
3) Retorne o valor em R.

Exemplo 1:

$3^{61374236} \mod 38$

R	A	E	É IMPAR?
1	3	01374236	NÃO
1	9	30687143	
9	$81 \equiv 5$	15343571	
$45 \equiv 7$	25	7671	
$175 \equiv 23$	17		
23			