Maths Eggenberg

semestre 1

Conversion, changement de base

- Methode de la soustraction

1. $(78)_{10} = 64 + (78 - 64) = 64 + 8 + 6 = 64 + 8 + 4 + 2 = 2^6 + 2^3 + 2^2 + 2^1 = (1001110)_2$

2. $(7904)_{10} = 2 \cdot 60^2 + \underbrace{(7904 - 2 \cdot 60^2)}_{704} = 2 \cdot 60^2 + 11 \cdot 60^1 + \underbrace{(704 - 11 \cdot 60^1)}_{44} = 2 \cdot 60^2 + 11 \cdot 60^1 + 44 \cdot 60^0$

$= ([02][11][44])_{60}$

- Methode de la division

1. $7904 / 60 = 131$ reste 44
$131 / 60 = 2$ reste 11
$2 / 60 = 0$ reste 2

$(7904)_{10} = ([02][11][44])_{60}$

Exercice :

$(07\ 21\ 1403)_{23} = 7 \cdot 23^3 + 21 \cdot 23^2 + 13 \cdot 23 + 3 = ([03]\ [07]\ [16]\ [07])_{31}$

Représentation des entiers signés

Complément en base 2

- Si $x \geq 0$, 1^{er} bit est 0, x s'écrit sur les n-1 bits restants
- Si $x \leq 0$, 1^{er} bit est 1, x s'écrit sur les n-1 bits restants

Notation : si x est exprimé en complément en base 2 on notera $(x)_{\bar{2}n}$

Conversion simplifiée

Exemple : $(-72)_{10} = (?)_{\bar{2}8}$

1. Convertir 72 en base 2 : $(01001000)_2$
2. Inverser les bits : $(10110111)_2$
3. Ajouter 1 : $(10111000)_2$
4. Fin : $(-72)_{10} = (10111000)_2$

Reconversion en base 10

- Si 1^{er} bit $=0 \Rightarrow$ convertir normalement
- Si 1^{er} bit $=1 \Rightarrow x = -2^{n-1}$ + convertir le reste normalement

⚠ Attention aux overflow

Exemple :

$$\begin{array}{rcr} (5)_{10} & : & (0101)_{\bar{2}8} \\ + \ (5)_{10} & : & + \ (0101)_{\bar{2}8} \\ \hline (10)_{10} & \neq & (1010)_{\bar{2}8} \end{array}$$

$$(1010)_{\bar{2}8} = -2^3 + (010)_2 = -2^3 + 2 = -6$$

Binaire à virgule

on peut uniquemen travailler qu'avec des nombres à décimales finies

Représenter $(13{,}625)_{10}$ en base 2

Par tatonnement :

$$13{,}625 = 8+4+1+\frac{1}{2}+\frac{0}{4}+\frac{1}{8} = (1101{,}101)_2$$

Par multiplication

$$(13)_{10} = 8+4+1 = (1101)_2$$

$$(0{,}625)_{10} = \frac{2\cdot 0{,}625}{2} = \frac{1{,}25}{2} = \frac{1}{2} + \frac{0{,}25}{2}$$

$$\frac{2\cdot 0{,}25}{2\cdot 2} = \frac{0{,}5}{4} = \frac{0}{4} + \frac{0{,}5}{4}$$

$$\frac{2\cdot 0{,}5}{2\cdot 4} = \frac{1}{8} + 0$$

$$(13{,}625)_{10} = (1101{,}101)_2$$

Nombres à virgule flottante

Ecriture scientifique en base 10

$$\pm\, x,y \cdot 10^{z} \quad \text{avec} \quad z \in \mathbb{Z},\ y \in \mathbb{N},\ x \in \{1 \dots 9\}$$

Encodage en binaire

$x_0 \quad x_1 \dots x_8 \quad x_9 \dots x_{31}$

x_0 : signe (1 bit)

$x_1 \dots x_8$: exposant (11 bits)

$x_9 \dots x_{31}$: mantisse (en 32 bits : 23 bits, en 64 bits : 52 bits)

décalage : 127 décalage : 1023

$$(-1)^{x_0}\,(2)^{(x_1 \dots x_8)_2 - 127}\,(1, x_9 \dots x_{31})_2$$

Exemples:

1 $(1\ \ 1101011\ \ 0010 \dots 0)_{float} = (-1)^1 \cdot 2^{203-127}\left(1, \frac{1}{8}\right) = -1,125 \cdot 2^{76}$

2. $(-784)_{10} = (?)_{float}$ bit caché

$(784)_{10} = 2^9 + 2^8 + 2^4 = 110001\ 0000$

$e = 127 + 9 = 136 = 128 + 8 = 1000\ 1000$

$(-784)_{10} = (1\ \ 1000\,1000\,000\ \ 10001\ 0000\ \underbrace{0 \dots 0}_{\times 14})$

bit caché

3. $(0,07)_{10} = (0,001,000\ 111\ 01\ 00101\ 00001) = (1,00) \cdot 2^{-4}$

$e = -4 + 127 = 123 = (1111011)_2$

$(0,07)_{10} = (0\ \ 1111011\ \ 000\ 111\ 01\ 00101\ 00001\ 00000)_{float}$

PGDC et PPMC

Decomposition en facteur premier

$68 = 2 \cdot 2 \cdot 17$ $\qquad$ $PGDC = 2 \cdot 2 = 4$

$168 = 2\ 2 \cdot 2 \cdot 3 \cdot 7$ $\qquad$ $PPMC = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 \cdot 17 = 2856$

complexité : $O(n^3)$ ou pire

Euclide :

$$\begin{array}{r|l} a & b \\ \hline r & q \end{array}$$

tant que $r \neq 0$

Exemple :

$$\begin{array}{r|l} 168 & 68 \\ \hline -136 & 2 \\ \hline 32 & \end{array} \qquad \begin{array}{r|l} 68 & 32 \\ \hline -64 & 2 \\ \hline 4 & \end{array} \qquad \begin{array}{r|l} 32 & 4 \\ \hline -32 & 8 \\ \hline 0 & \end{array}$$

$\longleftarrow$ pgdc(168, 68)

complexité : $O(\log(n))$

$$\overbrace{a \cdot b}^{\text{Facile}} = \overbrace{pgdc(a,b)}^{\text{Facile}} \cdot ppmc(a,b) \Rightarrow ppmc(a,b) = \frac{a \cdot b}{pgdc(a,b)}$$

Première pierre angulaire du RSA :

Theoreme de Bachet-Bēzout :

Soit $a, b \in \mathbb{Z}^*$, $\exists x, y \in \mathbb{Z}$ t.q.

$$ax + by = \mathrm{pgdc}(a,b)$$

Euclide étendus

initialisation (toujours)

iter	r	q	x	y
0	168	0	1	0
1	68	0	0	1
2	32	2	$1 - 2 \cdot 0$	$0 - 2 \cdot 1$
3	4 (pgdc)	2	$\underbrace{-2}_{x}$	$\underbrace{5}_{y}$
4	0 ↳ STOP	8		

iter	
2	$168 = 68 \cdot 2 + 32$ (168 − 136 = 32)
3	$68 = 32 \cdot 2 + 4$ (68 − 64 = 4)
4	$32 = 4 \cdot 8 + 0$ (32 − 32 = 0)

$$x_i = x_{i-2} - q \cdot x_{i-1}$$

$$y_i = y_{i-2} - q_i \cdot y_{i-1}$$

$$r = ax + by = 168 \cdot (-2) + 68 \cdot 5 = 4$$

Exercice :

Trouver le pgdc (784, 138) avec Euclide étendus

iter	r	q	x	y
1	784	0	1	0
2	138	0	0	1
3	94	5	1	-5
4	44	1	-1	6
5	6	2	3	-17
6	2	7	-22	125
7	0	3		

le signe de x et y change à chaque ligne et signe (x) ≠ signe (y)

iter

784	138
94	5

138	94
44	1

94	44
6	2

44	6
2	7

6	2
	3

$$\text{pgdc}(784, 138) = 2$$

$$2 = (-22)\,784 + 125 \cdot 138$$

Theorie de l'arithmétique modulaire

L'opérateur modulo:

$a \bmod b = r \Rightarrow \exists q \in \mathbb{Z}$ t.q. $a + bq = r$

avec : $0 \leq r \leq b-1$

Exemple:

$3 \bmod 10 = 3 \qquad 3 + 0 \cdot 10 = 3$

$33 \bmod 10 = 3 \qquad 33 + (-3) \cdot 10 = 3$

$-7 \bmod 10 = 3 \qquad (-7) + 1 \cdot 10 = 3$

On dit que a et b sont congruent si:

$$a \bmod n = b \bmod n$$

et on note : $a \equiv_n b$

Quelques propriétées :

1. $a + b \equiv_n a \bmod n + b \bmod n$
2. $a \cdot b \equiv_n a \bmod n \cdot b \bmod n$