

Résumé

Ce devoir est une synthèse de nos travaux depuis plusieurs mois sur la reconstitution du théorème des restes chinois. Grace au soutiens de notre professeur MR ZEMOR, nous avons appris a reconstruire le théorème des restes chinois en présence d'erreur ; Dans un premier temps, nous avons pris connaissance de ce théorème, puis dans un second temps, nous l'avons corrigé grace à plusieurs méthode, tel que du brut force ou une méthode de fractions continues.

Table des matières

Nous tenons tout d'abord à remercier Mr CASTAGNOS Guillaume d'avoir été le professeur principale de cette matière et, en ayant bien expliqué le fonctionnement pour partir sur de bonne base. Nous remercions par la suite Mm ZEMOR Gilles pour nous avoir suivit, aider et tutoré durant ce semestre.
nous remercions également nos familles et nos proches, pour leurs aide et leur soutiens.

1 théorème des restes

1.1 théorème des restes chinois et son histoire

Le théorème des restes chinois viens à la base d'un livre mathématique chinois de Qin JUSHIO publié en 1247. Cependant, on avait déjà découvert ce théorème au part avant dans un livre de Sun ZI au 3° siècle. Le théorème consiste en : On pose n_1, \dots, n_k des entiers premiers 2 à 2. Pour tout a_1, \dots, a_k , il existe un entier x tel que :

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

$$x \equiv a_k \pmod{n_k}$$

Nous pouvons démontrer ce théorème de la façon suivante :

Pour illustrer ce théorème, nous allons donner un exemple, mais pas n'importe quelle exemple, celui dont Sun ZI a proposé une solution :

soient des objets, prenons des bonbons, si on les repartis pour 3 enfants, il en reste 2, si on les répartit pour les 3 enfants et leurs parents, il en reste (soit 5 personnes), il en reste 3. enfin si on partage ces bonbons avec également les 2 cousins, (soit 7 personnes) il en reste 2. On a donc :

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

La question que l'on se pose à présent est combien y a t'il de bonbons ?
grace au théorème des restes chinois, on peut trouver la réponse.

1.2 notre algorithme

L'algorithme du théorème des restes chinois étant un peu lourd, nous allons montrer et expliquer qu'une partie, l'algo en entier sera en annexe. On a ici :
-PI la liste des nombres premiers -XI la liste des modules - on a posé a prend la valeur 1 car a sera après le produit des éléments de XI

```
1 for  $i$  in  $\text{range}(\text{len}(PI))$  do
2    $a \leftarrow 1$  ;
3    $pi \leftarrow PI[i]$  ;
4   for  $j$  in  $\text{range}(\text{len}(PI))$  do
5     if  $j \neq i$  then
6        $a = a * PI[j]$ 
7     end
8      $k \leftarrow \text{xeuclid}(a, pi)$  ;
9      $b \leftarrow b + k \times a \times XI[i]$  ;
10  end
11 end
```

2 Brute force

2.1 Notre premier algo version naïve

2.2 brute force de hamming

3 Les fractions continues

```
1  $b \leftarrow 0$  ;
2  $c \leftarrow 1$  ;
3  $AI \leftarrow []$  ;
4  $NI \leftarrow []$  ;
5 for  $i$  in  $\text{range}(\text{len}(N))$  do
6   if  $A[i] \neq 0$  then
7      $c = c \times N[i]$  end
8   else
9      $AI = AI + [AI[i]]$   $NI = NI + [NI[i]]$ 
10  end
11 end
12 for do
13    $a \leftarrow 1$  ;
14    $ni \leftarrow NI[i]$  ;
15   for  $j$  in  $\text{range}(\text{len}(NI))$  do
16     if  $j \neq i$  then
17        $a = a * NI[j]$ 
18     end
19      $k \leftarrow \text{xeuclid}(a, ni)$  ;
20      $b \leftarrow b + k \times a \times AI[i]$  ;
21   end
22 end
23 return  $b \div (a \times ni)$ 
```

```

1  $xs0 \leftarrow 1$  ;
2  $xs1 \leftarrow 0$  ;
3  $ys0 \leftarrow 0$  ;
4  $ys1 \leftarrow 1$  ;
5  $s \leftarrow 1$  ;
6  $d \leftarrow b$  ;
7 while  $b \neq 0$  do
8    $(q, r) \leftarrow \text{divmod}(a, b)$  ;
9    $(a, b) \leftarrow (b, r)$  ;
10   $(x, y) \leftarrow (xs1, ys1)$  ;
11   $(rs1, ys1) \leftarrow (q \times s1 + xs0, q \times ys1 + ys0)$  ;
12   $(xs0, ys0) \leftarrow (x, y)$  ;
13   $s \leftarrow -s$  ;
14 end
15 return  $s \times xs0 + ((1 - s) \div 2) \times d$ 

```