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 conaissance de ce théorème, puis dans un segond 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 était 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 n1,...,nk des entiers premiers 2 à 2. Pour tout a1,...,ak, il existe un entier x tel que :
$x \equiv a1 \, (mod \, n1)$
$x \equiv a2 \, (mod \, n2)$
$xk \equiv ak \, (mod \, nk)$
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 répartis 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 :
$x \equiv 2 \, (mod \, 3)$
$x \equiv 3 \, (mod \, 5)$
$xk \equiv 2 \, (mod \, 7$
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 algoritme

Pour faire l'algoritme du théorème des restes chinois, il nous a fallu faire d'autres algoritmes. Mais dans un premier temps, voici notre algoritme

```
b ← 0 ;
c ← 1 ;
AI ← [ ] ;
NI ← [ ] ;
for i in range(len(N)) do
    if A[i]==0 then
        c=c×N[i]end
        else
            AI=AI+[AI[i]] NI=NI+[NI[i]]
        end
    end
    for i in rangelenAI do
        a ← 1 ;
        ni ← NI[i] ;
        for j in range(len(NI)) do
            if j ≠ i then
                a=a*NI[j]
            end
            k ← xeuclid(a, ni) ;
            b ← b + k × a × AI[i] ;
        end
    end
    return b÷(a × ni)
```

```
xs0 ← 1 ;
xs1 ← 0 ;
ys0 ← 0 ;
ys1 ← 1 ;
s ← 1 ;
d ← b ;
while b≠ 0 do
    (q, r) ← divmod(a, b) ;
    (a, b) ← (b, r) ;
    (x, y) ← (xs1, ys1) ;
    (rs1, ys1) ← (q × s1 + xs0, q × ys1 + ys0) ;
    (xs0, ys0) ← (x, y) ;
    s ← −s ;
end
return s×xs0 + ((1 − s) ÷ 2) × d
```

2 grand 2

3 grand 3