**Exercice Type Cryptographie**

Table des matières

[1. Théorème des restes chinois 2](#_Toc486371794)

[Exercice 1 : Soldats de plomb (2 lignes) 2](#_Toc486371795)

[Exercice 2 : Armée de César (3 lignes) 3](#_Toc486371796)

[2. Bachet-Bézout 5](#_Toc486371797)

[Exercice 1 : 11200 et 15092 5](#_Toc486371798)

[Exercice 2 : 16558 et 10506 7](#_Toc486371799)

[3. Indicatrice d’EULER 8](#_Toc486371800)

[Exercice 1 : 97300 8](#_Toc486371801)

1. Théorème des restes chinois

## Exercice 1 : Soldats de plomb (2 lignes)

Si je place mes soldats de plomb par rangées de 12, il m’en reste cinq. Mais si je les places par rangées de 11 il ne m’en reste qu’un. Combien ai-je de soldats dans ma collection ?

**Etape 1 : Trouver le système**

m1 ≡ **5** (**12**)

m2 ≡ **1** (**11**)

**Etape 2 : Trouver l’univers**

M=**12**\***11**=132

**Etape 3 : On trouve la formule pour le système**

N=**12**\***1** \*u+**5**\***11**\*v

N=12u+55v

**Etape 4 : Bachet-Bezout pour trouver les 2 inconnues u et v**

**12**u+**11**v = 1

Trouver u et v via élément inversible :

**12**u ≡ 1 (11) ; u = 1

**11**v ≡ 1 (12) ; v = 11 ou -1

Bon là c’est simple pour trouver quand ça boucle.

Sinon faire les manipulations via une des deux méthodes :

Méthode 1 : Calculatrice

Méthode 2 : Lister nombres jusqu’à bouclage à la mano

**Etape 5 : Remplacer dans la formule trouvée juste avant**

On reprend notre équation à 2 inconnues et on remplace nos u et v :

Si on prend v=11

N=12u+55v = 12\*1 + 55\*11 = 617 (132)

N=617-132=485

…

N=89

Si on prend v=-1

N=12u+55v = 12\*1 + 55\*(-1) = -43

N=-43 (132) = -43 + 132 = 89

## Exercice 2 : Armée de César (3 lignes)

L’armée de César comptait plus de 1000 hommes et moins de 3000. Lorsqu’il voulut la dénombrer par groupe de **9**, il restait **5** soldats, par groupes de **13**, il en restait **8**. En revanche, il pouvait faire des groupes de **11** **sans qu’il ne reste de soldats**. Combien y avait-il d’hommes dans son armée ?

**Etape 1 : Trouver le système**

**m1** ≡ **5** (**9**)

**m2** ≡ **8** (**13**)

**m3** ≡ **0** (**11**)

**Etape 2 : Trouver l’univers**

M = **9**\***13**\***11** = **1287**

**Etape 3 : Trouver les grands M**

M1=**1287**/**9**= 143

M2=**1287**/**13**= 99

M3=**1287**/**11** = 117

**Etape 4 : Trouver les y**

y1\*143 ≡ 1 (**9**) ; y1 = **8**

Avec la calculatrice 🡪 mod(143,9) = 8

On travaille avec 8 pour trouver la valeur de bouclage = 1

Méthode 1 : Calculatrice

mod(8\*1,9)=8

mod(8\*2,9)=7

…

mod(8\*5,9) =1 🡪 **8** est ainsi notre valeur de bouclage pour arriver à 1

Méthode 2 : Liste à la mano

8 = -1 dans l’univers 9

Donc -1 + 9 = **8** (On retrouve ici notre valeur de bouclage)

|  |  |
| --- | --- |
| **Univers 9** | **Valeur 8** |
| 9 | 8 |
| 18 | 16 |
| … | … |

y2\*99 ≡ 1 (**13**) ; y2 = 5

y3\*117 ≡ 1 (**11**) ; y3 = 8

**Etape 5 : Remplacer dans la formule du théorème des restes chinois**

Théorème :





Ainsi : x=5\*143\*8 + 8\*99\*5 + 0\*117\*8 = 9680 (**1287)**

Pour que le résultat soit cohérent avec l’énonce nous faisons :

x = 9680 – 1287 = 8393

x = 8393 – 1287 = 7106

….

**x = 1958**

*Il y avait ainsi 1958 soldats dans son armée.*

1. Bachet-Bézout

## Exercice 1 : 11200 et 15092

1. Calculer PGCD de 11200 et 15092 :

Méthode par division :

|  |  |
| --- | --- |
| 15092 | 11200 |
| 3892 | 1 |

3892 = 15092 (-1 \* 11200)

|  |  |
| --- | --- |
| 11200 | 3892 |
| 3416 | 2 |

3416 = 11200 (-2 \* 3892)

|  |  |
| --- | --- |
| 3892 | 3416 |
| 476 | 1 |

476 = 3892 (-1 \* 3416)

|  |  |
| --- | --- |
| 3416 | 476 |
| 84 | 7 |

84 = 3416 (- 7 \* 476)

|  |  |
| --- | --- |
| 476 | 84 |
| 56 | 5 |

**56 = 476 (-5 \* 84)**

|  |  |
| --- | --- |
| 84 | 56 |
| 28 | 1 |

28 = 84 (– 1 \* **56**)

|  |  |
| --- | --- |
| 56 | 28 |
| 0 | 2 |

0 =

Méthode par tableau :

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 15092 | 11200 | 3892 | **3416** | **476** | **84** | 56 | 28 |
|  | 11200 | 3892 | 3416 | 476 | 84 | 56 | 28 | 0 |
| Diviseur | 1 | 2 | 1 | **7** | **5** | **1** | 2 | 1 |
| Reste | 3892 | 3416 | 476 | 84 | 56 | 28 | 0 | 0 |

* Notre PGCD est ainsi 28 (chiffre avant le 0 dans notre tableau).

1. En déduire une identité de Bézout entre 11200 et 15092 :

Avant de commencer nous devons savoir à partir de ou remonter. Grâce au reste nous pouvons déterminer que nous attaquerons à partir de 84, car son reste n’est pas égal à 0 contrairement à 56.

28 = **84**-**1**\*(**476**-**5**\***84**) = -**1**\*(**476**) + 6\*(84)

28 = -1\*(476) + 6(**3416**-**7**\***476**) = 6(3416) – 43(476)

28 = 6(3416) – 43(3892–1\*3416) = -43(3892) + 49(3416)

28 = -43(3892) + 49(11200-2\*3892) = 49(11200) -141(3892)

28 = 49(11200) -141(15092-1\*11200) = -141(15092) + 190(11200)

1. En déduire l’ensemble des solutions de chacun des 2 équations diophantienne linéaires suivantes :

11200x+15092y=252 et 11200x+15092y=90

Il faut avant tout vérifier si 252 et 90 sont des multiples de notre PGCD :

Pour ceci, effectuer :

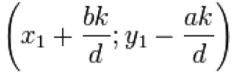
90/28 = 45/14 🡪 N’est pas un multiple de 28, donc solution = 0

252/28 = 9 🡪 252 est un multiple de 28, ainsi nous faisons :

x1=190\*9 = 1710

y1=-141\*9=-1269

Donc en appliquant la formule :



x1 et y1 sont les valeurs calculés juste au-dessous.

ak est 11200 bk est 15092.

d est notre pgcd.

x=1710+(15092/28) = 1710 + 539k

y=1260-(11200/28) = 1260-400k

## Exercice 2 : 16558 et 10506

1. Calculer PGCD de 16558 et 10506:

Méthode par tableau :

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 16558 | 10506 | 6052 | 4454 | 1598 | 1258 | 340 | 238 | 102 | 34 |
|  | 10506 | 6052 | 4454 | 1598 | 1258 | 340 | 238 | 102 | 34 | 0 |
| Diviseur | 1 | 1 | 1 | 2 | 1 | 3 | 1 | 2 | 3 | 0 |
| Reste | 6052 | 4454 | 1598 | 1258 | 340 | 238 | 102 | 34 | 0 | 0 |

PGCD (16558,10506) = 34

1. En déduire une identité de Bézout entre 16558 et 10506:

34=238-2\*(340-1\*238) = -2(340) + 3(238)

34= -2(340) + 3(1258-3\*340) = 3(1258) -11(340)

34= 3(1258) -11(1598-1\*1258) = -11(1598) + 14(1258)

34= -11(1598) + 14(4454-2\*1598) = 14(4454) – 39(1598)

34= 14(4454) – 39(6052-1\*4454) = -39(6052) + 53(4454)

34= -39(6052) + 53(10506-1\*6052) = 53(10506) – 92(6052)

34= 53(10506) – 92(16558-10506) = -92(16558) + 145(10506)

* x=-92
* y=145

1. En déduire l’ensemble des solutions de chacune des 2 équations diophantiennes linéaires suivantes :

16558 x + 10506 y = 126 ; 16558 x + 10506 y = 544

126/34 = 63/17 🡪 Pas de solution

544/34 = 16 🡪 Solution donc :

x1=-92\*16= -1472

y2=145\*16 = 2320

x=-1472+(10506/34) = -1472 + 309k

y= 2320-(16558/34) = 2320 – 487k

1. Indicatrice d’EULER

## Exercice 1 : 97300

1. Calculer la décomposition de 97300 en facteur premiers.

Avec la calculatrice faire : factor(97300) = **2**²\***5**²\***7**\***139**

Notre décomposition est alors : **2²\*5²\*7\*139**

1. En déduire que φ (97300) (=quantité de nombres premiers avec 97300 entre 1 et 97300).

On applique la formule :



φ (97300) = 97300\*(1-1/**2**)\*(1-1/**5**)\*(1-1/**7**)\*(1-1/**139**) = 33120

La quantité de nombre premier sera alors de **33120.**

1. Utiliser le petit théorème de Fermat pour trouver un exposant k tel que 3k = 1 mod 97300.

Le petit théorème de fermat dit :

A φ (n) ≡ 1 (n)

Donc : A φ (97300) ≡ 1 (97300) or φ (97300) = 33120 donc :

A33120 ≡ 1 (97300)

Sachant que 3k ≡ 1 (97300), alors A33120 = 333120

Il faut ensuite vérifier que 3 est divisible par 97300 : 3/97300 = pas divisible

Donc on conclue que **333120 ≡ 1 (97300)**

1. En déduire la valeur de **3**165603 mod 97300.

On a vu tout à l’heure que **333120 ≡ 1 (97300)**, donc la puissance qui ramène à 1 est 33120 ;

|  |  |
| --- | --- |
|  | 165603 |
|  | 33120 |
| Diviseur | **5** |
| Reste | **3** |

Alors, **3165603** ≡ **3165603\*5+**3

≡ (**3**165603)**5**\***33**

≡ 1**5**\***33**

≡ 1\***3**3

≡ 27