POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

LOG1810

STRUCTURES DISCRÈTES

TD 7 : THÉORIE DES NOMBRES

SOLUTIONNAIRE

H2024

Exercice 1 :

Utilisez l'algorithme d'Euclide étendu pour trouver le pgcd de 3914 et 2992 (Voir le complément du cours).

Solution:

Voici le déroulement de l'algorithme d'Euclide étendu pour trouver le pgcd de 3914 et 2992, avec chaque étape montrant les coefficients de Bézout et les restes successifs :

[3914,1,0] [2992,0,1]

[922,1,−1] [2992,0,1]

[922,1,−1] [226,−3,4]

[18,13,−17] [226,−3,4]

[18,13,−17] [10,−159,208]

[8,172,−225] [10,−159,208]

[8,172,−225] [2,−331,433]

[2,1165,−1524] [2,−331,433]

À la fin de ces étapes, nous obtenons le pgcd de 3914 et 2992, qui est **2**.

Vérification à l'aide des coefficients de Bézout :

1165x3914-1524x2992=2

-331x3914+433x2992=2

Cela montre que le pgcd de 3914 et 2992 est bien 2, ce qui valide notre solution

Exercice 2 :

Dans le cadre d'un chiffrement RSA, on considère les valeurs p = 47, q = 67.

a) Calculez la base modulaire n.

La base modulaire est n = p * q = 3149

b) Calculez l'indicatrice de Carmichael i

L'indicatrice de Carmichael, calculée comme le plus petit commun multiple de p-1 et q-1, est ppcm(46, 66)= 46*66/pgcd(46,66) qui est i = 1518.

c) En considérant que la clé de chiffrement est e = 197, calculez la valeur de la clé privée d.

Pour trouver la clé privée d telle que e * d ≡ 1 (mod i), nous devons résoudre l'équation 197d + 1518a = 1, où d est la clé privée et a un entier quelconque. Pour ce faire, nous utiliserons l'algorithme d'Euclide étendu.

Nous commençons avec i = 1518 et e = 197, et les organisons comme deux vecteurs initiaux [i, 1, 0] et [e, 0, 1].

Voici les étapes de calcul avec l'algorithme d'Euclide étendu pour trouver la clé privée d, avec 197d + 1518a = 1 :

1 [i, 1, 0] [e, 0, 1]

[1518, 1, 0] et [197, 0, 1]
[139, 1, -7] et [197, 0, 1]
[139, 1, -7] et [58, -1, 8]
[23, 3, -23] et [58, -1, 8]
[23, 3, -23] et [12, -7, 54]
[11, 10, -77] et [12, -7, 54]
[11, 10, -77] et [1, -17, 131]
[1, 180, -1387] et [1, -17, 131]

pk sette ordre

a · 1518 - 1387 · 197

Vérification :
180x1518-1387x197 = 1
-17x1518+131x197 = 1

Après avoir suivi ces étapes, nous trouvons que la clé privée d peut être 131(Nous choisissons une clé positive).

Exercice 3 :

Montrez que :

a) Soit n un entier naturel, 36^n -1 est divisible par 7.

Solution :

36 ≡ 1 mod 7

(36)^n ≡ 1^n mod 7

36^n ≡ 1 mod 7

36^n -1 ≡ 0 mod 7

D'où 36^n -1 est divisible par 7.

b) Soit a un entier et n un entier naturel, $a(a^{2n}-1)$ est divisible par 3.

Solution :

Cas 1 : Si a est divisible par 3, c'est trivial.

Cas 2 : Si a n'est pas divisible par 3

3 est premier, donc d'après le petit théorème de Fermat, on a :

a^2 ≡ 1 (mod 3) donc (a^2)^n ≡ 1^n (mod 3), soit (a^2)^n ≡ 1 (mod 3)

On obtient successivement :

(a^2)^n – 1 ≡ 0 (mod 3)

(a^(2n) – 1) ≡ 0 (mod 3)

a(a^(2n) – 1) ≡ 0 (mod 3)

Des deux cas, on déduit que a(a^2n – 1) est divisible par 3 pour tout a entier et tout n entiers naturels

Exercice 4 :

Quel est le plus petit entier naturel qui divisé par 8, 15, 18 et 24 donne pour reste respectivement 7, 14, 17 et 23?

Solution :
Soit n cet entier naturel.
On a :
n ≡ 7 (mod 8)
n ≡ 14 (mod 15)
n ≡ 17 (mod 18)
n ≡ 23 (mod 24)

Soit les entiers a, b, c, d. On peut réécrire les modulos :
n + 8a = 7
n + 15b = 14
n + 18c = 17
n + 24d = 23
En combinant deux à deux ces égalités on a :
7 – 8a = 14 – 15b et 17 – 18c = 23– 24d
Ou encore -8a + 15b = 7 et -18c + 24d = 6
• Considérons l'égalité -8a + 15b = 7.
Elle peut se réécrire : 8e + 15b = 7 avec e = -a.
8 et 15 étant relativement premiers entre eux, on peut résoudre 8e + 15b = 1 et multiplier les résultats par 7.
Résolvons cette équation avec l'algorithme d'Euclide étendu.
On part donc des vecteurs [8, 1, 0] [15, 0, 1].
À la suite des manipulations successives, on obtient : [1, 2, -1] [1, -13, 7].
(2, -1) est une solution particulière de 8e + 15b = 1. On en déduit que (14, -7) est une solution particulière de 8e + 15b = 7, ou encore que (-14, -7) est une solution particulière de -8a + 15b = 7.
On peut donc écrire a = -14 + 15k et b = -7 -8k, avec k entier.
De ce résultat, on peut déduire :
n = 7 – 8a = 7 – 8(-14 - 15k) = 7 + 112 + 120k = 119 + 120k, avec k entier.
6
n = 14 – 15b = 14 – 15(-7 -8k) = 14 + 105 + 120k = 119 + 120k, avec k entier.
• Considérons à présent l'égalité -18c + 24d = 6.
Elle peut se réécrire : -3c + 4d = 1, soit 3f + 4d = 1 avec f = -c.
3 et 4 étant relativement premiers entre eux, 3f + 4d = 1 admet une solution.
Résolvons cette équation avec l'algorithme d'Euclide étendu.

On part donc des vecteurs [3, 1, 0] [4, 0, 1].
À la suite des manipulations successives, on obtient : [1, 3, -2] [1, -1, 1].
(-1, 1) est une solution particulière de 3f + 4d = 1.
On peut donc écrire f = -1 + 4p et d = 1 -3p, avec p entier.
Soit c = 1 - 4p et d = 1 -3p, avec p entier.
De ce résultat, on peut déduire :
n = 17 – 18c = 17 – 18(1 – 4p) = 17 -18 + 72p = -1 + 72p, avec p entier.
n = 23 – 24d = 23 – 24(1 -3p) = 23 - 24 + 72p = -1 + 72p, avec p entier.
En tenant compte des deux résultats précédents, soit n = 119 + 120k et n = -1 + 72p, avec k et p entiers, on obtient une nouvelle égalité : 119 + 120k = -1 + 72p, soit 120k – 72p = -120.
Elle devient après simplification :
5k – 3p = -5, soit 5k + 3g = -5 avec g = -p.
3 et 5 étant relativement premiers entre eux, 5k + 3g = 1 admet une solution.
Les résultats seront multipliés par -5 pour trouver les solutions de 5k + 3g = -5.
Résolvons cette équation avec l'algorithme d'Euclide étendu.
On part donc des vecteurs [5, 1, 0] [3, 0, 1].
À la suite des manipulations successives, on obtient : [1, 2, -3] [1, -1, 2].
(-1, 2) est une solution particulière de 5k + 3g = 1.
Ainsi, (5, -10) est une solution particulière de 5k + 3g = -5, ou encore (5, 10) est une solution particulière de 5k – 3p = -5.
On peut donc écrire k = 5 - 3t et p = 10 - 5t, avec entier.
De ce résultat, on peut déduire :
n = 119 + 120k = 119 + 120(5 - 3t) = 119 + 600p -360t = 719 -360t, avec t entier.
n = -1 + 72p = -1 + 72(10 - 5t) = -1 + 720 – 360t = 719 -360t, avec t entier.
Conclusion
On obtient la plus petite valeur de n lorsque t = 1, soit n = 359

Exercice 5 :

Démontrez que 7 divise la somme de 2222^5555 + 5555^2222. Décrivez chaque étape de votre réponse.
Note : Les calculs suivants vous sont fournis pour vous aider.

- 5555 = 6 * 925 + 5
- 2222 = 7 * 317 + 3
- 5555 = 7 * 793 + 4

Solution **:**
7 est un nombre premier et ne divise pas 2222.
D'après le petit théorème de Fermat, 2222^6 ≡ 1 (mod 7).
Puisque 5555 = 6 * 925 + 5, alors 2222^5555 = 1^925 * 2222^5 (mod 7).
Donc, 2222^5555 ≡ 2222^5 (mod 7).
Comme 2222 = 7 * 317 + 3, alors 2222 ≡ 3 (mod 7).
Ainsi, 2222^5 ≡ 3^5 (mod 7), ce qui donne 2222^5 ≡ 5 (mod 7).
Donc 2222^5555 ≡ 5 (mod 7).
De même, 7 est un nombre premier et ne divise pas 5555.
En appliquant le petit théorème de Fermat, 5555^6 ≡ 1 (mod 7).
Comme 5555 = 7 * 793 + 4, alors 5555^2222 ≡ 4^370 * 5555^2 (mod 7).
Donc, 5555^2222 ≡ 5555^2 (mod 7).
Et comme 5555 = 7 * 793 + 4, alors 5555 ≡ 4 (mod 7).
Ainsi, 5555^2 ≡ 4^2 (mod 7), ce qui donne 5555^2 ≡ 2 (mod 7).
Donc 5555^2222 ≡ 2 (mod 7).
Par conséquent, nous pouvons conclure que :
2222^5555 ≡ 5 (mod 7) et 5555^2222 ≡ 2 (mod 7).
Donc la somme (2222^5555 + 5555^2222) ≡ (5+2) (mod 7).
Puisque (5 + 2) ≡ 0 (mod 7), nous avons 2222^5555 + 5555^2222 ≡ 0 (mod 7).
Cela prouve que 7 divise 2222^5555 + 5555^2222.

Exercice 6 :

Vous souhaitez envoyer le message suivant « FURTIF ». En considérant que vous encodez chaque lettre par sa position dans l'alphabet, en 2 chiffres (ex. A↔01, B↔02, C↔03, etc.) et que vous considérez les lettres 2 par 2, encodez le message selon RSA avec la clef de chiffrement donnée précédemment et donnez les blocs à envoyer.

Solution :

On commence par découper le message en blocs de 2 : FU RT IF. En changeant chaque lettre par sa position, on obtient les blocs à crypter : 0621 1820 0906.
On encode chaque bloc m_i de m tel que $c_i \equiv m_i^e \pmod{n}$

$0621^{197} \equiv 2757 \pmod{3149}$
$1820^{197} \equiv 1177 \pmod{3149}$
$0906^{197} \equiv 2869 \pmod{3149}$

Il faudra donc envoyer la séquence 2757 1177 2869.