POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

LOG2810

STRUCTURES DISCRÈTES

TD 7 : THÉORIE DES NOMBRES

A2022

Directives pour la remise :

- Répondez directement sur ce document papier.
- La remise est individuelle, mais le travail en équipe est encouragé.
- La remise se fait à la fin de la séance de TD.
- **Aucun retard ne sera accepté.**
- **Le non-respect des consignes entraînera automatiquement la note 0 pour ce TD.**

Identification

Veuillez inscrire votre section, nom, prénom et matricule ainsi que les noms des collègues avec lesquels vous avez collaboré pour le TD

Section :

Nom :

Prénom :

Matricule :

Collègues :

Exercice 1 :
Utilisez l'algorithme d'Euclide Étendu pour trouver le pgcd de 4830 et 476.

Réponse :
On utilise les vecteurs de l'algorithme étendu d'Euclide, soit :
[4830, 1, 0] [476, 0, 1]
[70,1,-10] [476, 0, 1]
[70,1,-10] [56,-6,61]
[14,7,-71] [56,-6,61]
[14,7,-71][14,-27,274]

Vérification :
7. 4830 + (-71).476 = 14
(-27).4830 + 274.476 = 14

Le pgcd de 4830 et 476 est 14.

Exercice 2 :
Dans le cadre d'un chiffrement RSA, on considère les valeurs p=41, q=73

a) Calculez la base modulaire n.
Réponse :
La base modulaire est n = p.q = 41.73= 2 993

b) Calculez l'indicatrice de Carmichael i = ppcm(p - 1, q - 1)
Réponse :
i = ppcm(40, 72)
i = 40. 72 / pgcd(40,72)
i = 2880/8
i = 360

c) En considérant que la clé de chiffrement est e= 163, Calculez la valeur de la clé privée d

Réponse :

e.d ≡ 1 (mod i)

e.d ≡ 1 (mod 360)

163.d ≡ 1 (mod 360)

Nous avons donc l'équation 163d +360a = 1

163et 360 sont relativement premiers.

Résolvons l'équation avec l'algorithme d'Euclide étendu.

[360, 1, 0] [163,0,1]

[34, 1, -2] [163, 0, 1]

[34, 1, -2] [27, -4, 9]

[7, 5, -11] [27, -4, 9]

[7, 5, -11] [6, -19, 42]

[1, 24, -53] [6, -19, 42]

[1, 24, -53] [1, -139, 307]

On peut prendre d=307 comme clée privée :

163*307 ≡ 1 (mod 360)

Exercice 3 :

En utilisant vos notions en théorie des nombres, montrez que :

a) Soit n un entier naturel, 3^{6n}-1 est divisible par 7.

Réponse :

3 n'est pas divisible par 7 et 7 est premier, donc d'après le petit théorème de Fermat :

$3^6 \equiv 1 \bmod 7$

$(3^6)^n \equiv 1^n \bmod 7$

$3^{6n} \equiv 1 \bmod 7$

$3^{6n} - 1 \equiv 0 \bmod 7$

D'où 3^{6n} -1 est divisible par 7 .

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

Réponse :

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 :
$a^2 \equiv 1 \pmod 3$ donc $(a^2)^n \equiv 1^n \pmod 3$, soit $(a^2)^n \equiv 1 \pmod 3$
On obtient successivement :
$(a^2)^n – 1 \equiv 0 \pmod 3$
$(a^{2n} – 1) \equiv 0 \pmod 3$
$a(a^{2n} – 1) \equiv 0 \pmod 3$

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 :
Calculez $11^{5072} \bmod 131$.

Réponse :
$5072 = 130.39 + 2$
Donc $11^{5072} = 11^{130.39 + 2}$
11 n'est pas divisible par 131 et 131 est premier, donc d'après le petit théorème de Fermat : $11^{130} \equiv 1 \pmod{131}$
D'où :
$(11^{130})^{39} \equiv 1^{39} \pmod{131}$
$11^{130.39} \equiv 1 \pmod{131}$
$11^{130.39 + 2} = 11^{130.39}.11^2 \equiv 1.11^2 \pmod{131}$
$11^{5072} \equiv 121 \pmod{131}$

Exercice 5 :

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

Réponse :

Soit n cet entier naturel.

On a :

$n \equiv 7 \pmod 8$

$n \equiv 14 \pmod{15}$

$n \equiv 17 \pmod{18}$

$n \equiv 23 \pmod{24}$

MÉTHODE 1 :

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.

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

MÉTHODE 2 (hors-programme par rapport au cours) :

On peut réécrire les modulos :

$n+1 \equiv 0 \pmod 8$

$n+1 \equiv 0 \pmod{15}$

$n+1 \equiv 0 \pmod{18}$

$n+1 \equiv 0 \pmod{24}$

La plus petite valeur de n+1 sera donc ppcm(8,15,18,24).

On peut en déduire que la plus petite valeur possible de n sera ppcm(8,15,18,24) – 1.

Calcul du ppcm

Méthode A : en utilisant la décomposition en facteurs premiers :

$8 = 2^3.3^0.5^0$

$15 = 2^0.3^1.5^1$

$18 = 2^1.3^2.5^0$

$24 = 2^3.3^1.5^0$

Pour trouver le ppcm, il suffit de faire le produit de chaque facteur premier à l'exposant le plus élevé. On a donc :

$ppcm(8,15,18,24) = 2^3.3^2.5^1 = 360$

Méthode B : à la calculatrice

Ppcm(8,15,18,24) = ppcm(ppcm(8,15), ppcm(18,24))

Ppcm(8,15,18,24) =ppcm (120,72)

Ppcm(8,15,18,24) =360

d'où (n+1) = 360

et n = 359