POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

LOG2810
STRUCTURES DISCRÈTES

TD 7 : **THÉORIE DES NOMBRES**

É2022

SOLUTIONNAIRE

Exercice 1. Utilisez l'algorithme d'Euclide étendu pour trouver le pgcd de **99999** et **1110**.

Réponse :
On utilise les vecteurs de l'algorithme étendu d'Euclide, soit :
[99999, 1, 0] [1110, 0, 1]
[99, 1, -90] [1110, 0, 1]
[99, 1, -90] [21, -11, 991]
[15, 45, -4054] [21, -11, 991]
[15, 45, -4054] [6, -56, 5045]
[3, 157, -14144] [6, -56, 5045]
[3, 157, -14144] [3, -213, 19189]
Le pgcd de 99999 et 1110 est donc **3**.

Exercice 2. Soit a un entier et n un entier naturel. En utilisant vos notions en théorie des nombres, montrez que **$a(a^{2n} – 1)$ est divisible par 3**.

Réponse :
$a(a^{2n} – 1) = a((a^2)^n – 1)$

- Si a est divisible par 3, alors c'est trivial.
- Si a n'est pas divisible par 3.
  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 :
  $(a^2)^n – 1 \equiv 0 \pmod 3$
  $(a^{2n} – 1) \equiv 0 \pmod 3$
  $a(a^{2n} – 1) \equiv 0 \pmod 3$
  D'où $(a+1)^n - a^n - 1$ est divisible par n.

Des deux cas, on déduit que $a(a^{2n} – 1)$ est divisible par 3.

Exercice 3. Calculez 101^{1001} mod 13

Réponse :
$101 \equiv 10 \pmod{13}$, alors $101^{1001} \equiv 10^{1001} \pmod{13}$
13 est un nombre premier. D'après le petit théorème de Fermat $10^{12} \equiv 1 \pmod{13}$.
On sait que $1001 = (83 \times 12) + 5$ donc $10^{1001} = 10^{12 x 83.}\ 10^5$.
$10^{1001} \equiv (10^{12})^{83}\ 10^5 \pmod{13}$
$10^{1001} \equiv 1^{83}\ 10^5 \pmod{13}$
$10^{1001} \equiv 10^5 \pmod{13}$
$10^5 = 10.(10^2)^2 = 10.(100)^2$
$100 \equiv 9 \pmod{13}$
$10^5 \equiv (10 \times 9^2) \pmod{13}$
$9^2 \equiv 3 \pmod{13}$
$10^5 \equiv (10 \times 3) \pmod{13}$
$10^5 \equiv 30 \pmod{13}$
$10^5 \equiv 4 \pmod{13}$
D'où $101^{1001} \equiv 4 \pmod{13}$.

Exercice 4. Quel est le plus petit un entier naturel qui divisé par 8, 15, 18 et 24 donne pour reste 7, 14, 17 et 23, respectivement ?

Réponse :
Soit n cet entier naturel.
Soit les entiers a, b, c, d. On a :
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 = 0, soit n = 719.

Exercice 5. Dans le cadre d'un chiffrement RSA, on considère les valeurs p=79, q=67

a) Calculez la base modulaire n.

Réponse :
La base modulaire est n = p.q = 79.67= 5293

b) Calculez l'indicatrice de Carmichael i = ppcm(p - 1, q - 1)

Réponse :
i = ppcm(78, 66)
i = 858

c) En considérant que la clé de chiffrement est e=251, Calculez la valeur de la clé privée d

Réponse :
e.d ≡ 1 (mod i)
e.d ≡ 1 (mod 858)
251d ≡ 1 (mod 858)
Nous avons donc l'équation 251d +858a = 1
251et 858 sont relativement premiers.
Résolvons l'équation avec l'algorithme d'Euclide étendu.
[251, 1, 0] [858, 0, 1]
[251, 1, 0] [105, -3, 1]
[41, 7, -2] [105, -3, 1]
[41, 7, -2] [23, -17, 5]
[18, 24, -7][23, -17, 5]
[18, 24, -7][5, -41, 12]
[3, 147, -43][5, -41, 12]
[3, 147, -43][2, -188, 55]
[1, 335, -98][2, -188, 55]
[1, 335, -98][2, -523, 153]

On peut prendre d=335 comme clé privée.
On vérifiera aisément que 251.335 ≡ 1 (mod 858)

d) **(Facultatif)** Le message à crypter est découpé en 3 blocs comme ci-dessous. Quel est le résultat du chiffrement.

0090 0086 0067

Réponse :

Chiffrement bloc 1 : 0090^{251} mod 5293 = 5259
Chiffrement bloc 2 : 0086^{251} mod 5293 = 2684
Chiffrement bloc 3 : 0067^{251} mod 5293 = 0670

Le résultat du chiffrement est : 5259 2684 0670

e) **(Facultatif)** Vérifiez le résultat précédent en appliquant la clé privée pour le déchiffrer.

Réponse :

Il faut déchiffrer 052 080 551 en calculant les 3 blocs
5259^{335} mod 5293
2684^{335} mod 5293
0670^{335} mod 5293