POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

LOG1810

STRUCTURES DISCRÈTES

TD 7 : THÉORIE DES NOMBRES ET CRYPTOGRAPHIE

Solutionnaire

Exercice 1 :

Résolvez dans $\mathbb{Z}$ l'équation :

$$720a + 27b = 36$$

Solution :

$\text{PGCD}(720{,}27) = 9$.
Comme 9 divise 36, l'équation $720a + 27b = 36$ possède des solutions.
Si on divise tout par 9, on obtient :

$$80a + 3b = 4.$$

Il suffit donc de résoudre $80x + 3y = 1$, puis de multiplier les résultats obtenus par 4 pour trouver a et b.

Utilisons l'algorithme étendu d'Euclide pour trouver x et y.
[80, 1, 0] [3, 0, 1]
[2, 1, -26] [3, 0, 1]
[2, 1, -26] [1, -1, 27]
[1, 2, -53] [1, -1, 27]
Nous pouvons prendre $x = -1$ et $y = 27$ comme une des solutions de $80x + 3y = 1$.
On en déduit que $a = -4$ et $b = 108$ constituent une solution particulière de l'équation $80a + 3b = 4$ et, par conséquent, une solution particulière de l'équation $720a + 27b = 36$.
Les solutions recherchées sont donc de la forme :

$$a = -4 - 3k \quad \text{et} \quad b = 108 + 80k, \quad \text{avec } k \in \mathbb{Z}.$$

Exercice 2 :

Dans le cadre d'un chiffrement RSA, on considère les valeurs $p = 41$, $q = 73$.

a) Calculez la base modulaire n.

Solution :
La base modulaire est $n = p \times q = 41 \times 73 = 2\,993$.

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

Solution :

$$i = \text{ppcm}(40{,}72)$$

Calculons le plus grand commun diviseur (PGCD) :

$$i = \frac{40 \times 72}{\text{pgcd}(40{,}72)}$$

$$\text{pgcd}(40{,}72) = 8$$

$$i = \frac{2880}{8}$$

$$i = 360$$

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

Solution :
Nous devons résoudre $e \cdot d \equiv 1 \pmod{i}$, soit :

$$163 \cdot d \equiv 1 \pmod{360}$$

Comme 163 et 360 sont relativement premiers, nous pouvons utiliser l'algorithme d'Euclide étendu pour trouver d.

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

$$[360{,}0{,}1] \quad [163{,}0{,}1]$$

$$[34{,}1,-2] \quad [163{,}0{,}1]$$

$$[7{,}5,-11] \quad [34{,}1,-2]$$

$$[5,-11{,}16] \quad [7{,}5,-11]$$

$$[1{,}16,-19] \quad [5,-11{,}16]$$

Nous avons trouvé que $d = 307$.

Ainsi, $163 \times 307 \equiv 1 \pmod{360}$.
On peut donc prendre $d = 307$ comme clé privée.

Exercice 3 :

En utilisant vos connaissances en théorie des nombres, montrez que 7 divise $2222^{5555} + 5555^{2222}$. Vous devez présenter toutes les étapes de votre réponse.

Solution :

En appliquant le petit théorème de Fermat, $2222^6 \equiv 1 \pmod 7$.

Or $5555 = 6 \times 925 + 5$, donc $2222^{5555} \equiv 1^{925} \times 2222^5 \pmod 7$.

$$2222^{5555} \equiv 2222^5 \pmod 7.$$

Or $2222 = 7 \times 317 + 3$, donc $2222 \equiv 3 \pmod 7$.

Ainsi, $2222^5 \equiv 3^5 \pmod 7$, soit $2222^5 \equiv 5 \pmod 7$.

D'où $2222^{5555} \equiv 5 \pmod 7$.

En appliquant le petit théorème de Fermat, $5555^6 \equiv 1 \pmod 7$.

Or $2222 = 6 \times 370 + 2$, donc $5555^{2222} \equiv 1^{370} \times 5555^2 \pmod 7$.

$$5555^{2222} \equiv 5555^2 \pmod 7.$$

Or $5555 = 7 \times 793 + 4$, donc $5555 \equiv 4 \pmod 7$.

Ainsi, $5555^2 \equiv 4^2 \pmod 7$, soit $5555^2 \equiv 2 \pmod 7$.

D'où $5555^{2222} \equiv 2 \pmod 7$.

Conclusion

$2222^{5555} \equiv 5 \pmod 7$ et $5555^{2222} \equiv 2 \pmod 7$.
Alors, $2222^{5555} + 5555^{2222} \equiv (5 + 2) \equiv 0 \pmod 7$.
Soit $2222^{5555} + 5555^{2222} \equiv 0 \pmod 7$. CQFD.
Note : Ici, les exposants ont été simplifiés en premier, puis les bases. On aurait pu simplifier aussi les bases en premier avant de simplifier les exposants.

Exercice 4 :

Soit a un entier. Prouvez que $2a + 1$ et $4a^2 + 1$ sont premiers entre eux, c'est-à-dire qu'ils n'ont aucun diviseur commun autre que 1.

Solution :
Soit d un diviseur commun de $2a + 1$ et $4a^2 + 1$.
Cela signifie que d divise $2a + 1$ et d divise $4a^2 + 1$.
Comme d divise $2a + 1$, nous pouvons multiplier cette expression par $2a$ pour obtenir une nouvelle relation :

$$d \mid 2a(2a + 1) = 4a^2 + 2a.$$

Cela signifie que d divise aussi $4a^2 + 2a$.

Nous savons que d divise également $4a^2 + 1$ (par l'hypothèse de départ). En utilisant ces deux informations, nous pouvons soustraire les deux expressions :

$$d \mid (4a^2 + 2a) - (4a^2 + 1) = 2a - 1.$$

Note: Si un nombre d divise deux nombres, il divise également leur différence.

Ainsi, d divise également $2a - 1$.

Nous avons maintenant deux relations : $d \mid 2a + 1$ et $d \mid 2a - 1$.
Nous pouvons à nouveau utiliser ces deux relations pour soustraire les expressions :

$$d \mid (2a + 1) - (2a - 1) = 2.$$

Cela signifie que d divise 2. Donc, d peut être soit 1, soit 2.

$2a + 1$ est un nombre impair car il s'agit de la somme d'un multiple de 2 et de 1.
Or, un nombre impair ne peut pas être divisible par 2. Cela signifie que d ne peut pas être égal à 2.
Comme d ne peut pas être égal à 2, il en découle que d doit être égal à 1.
Par conséquent, $2a + 1$ et $4a^2 + 1$ n'ont aucun diviseur commun autre que 1. Ils sont donc premiers entre eux. CQFD

Exercice 5 :

Soient a et b des entiers positifs. Prouvez que 2^a et $2^b - 1$ sont premiers entre eux en considérant leurs factorisations en nombres premiers.

On rappelle le théorème fondamental de l'arithmétique : Soit n un entier positif. Alors, n se factorise en un produit de nombres premiers.

Solution :

Considérons la factorisation en nombres premiers de $2^b - 1$, qui est $p_1, p_2, \ldots, p_k$. Remarquez que $p_i \neq 2$ pour tout $i \in \{1,2, \ldots, k\}$ car $2^b - 1$ est impair (puisque 2^b est pair et qu'un nombre impair n'est pas divisible par 2, ce qui implique que 2 ne peut pas figurer dans sa factorisation en nombres premiers).
Cependant, la factorisation en nombres premiers de 2^a est :

$$2 \cdot 2 \cdot \ldots \cdot 2 \quad \text{(a fois)}$$

Nous remarquons alors que la factorisation en nombres premiers de 2^a et $2^b - 1$ n'ont aucun facteur commun, ce qui implique qu'il n'existe aucun nombre premier p tel que $p \mid 2^a$ et $p \mid 2^b - 1$.

Nous savons aussi que a et b sont premiers entre eux si et seulement s'il n'existe aucun nombre premier p tel que $p \mid a$ et $p \mid b$. Cependant, ici il n'existe aucun nombre premier p tel que $p \mid 2^a$ et $p \mid 2^b - 1$, ce qui implique que 2^a et $2^b - 1$ sont premiers entre eux. CQFD

Exercice supplémentaire :

Mathieu, un brillant mathématicien, reçoit une lettre mystérieuse lui indiquant qu'il peut hériter d'un trésor s'il parvient à déchiffrer un code secret N. Ce code est protégé par plusieurs niveaux de cryptographie mathématique complexe. Les indices laissés par le mathématicien sont les suivants :

Premier Indice :
- Le nombre N est congru à 2 modulo 4.

Deuxième Indice :
- Le nombre N est congru à 4 modulo 5.

Troisième Indice :
- Le nombre N est congru à 4 modulo 7.

Quatrième Indice :
Pour confirmer que vous avez trouvé le bon N, il doit satisfaire $N^{\phi(13)} \equiv 1 \pmod{13}$, où ϕ est la fonction indicatrice d'Euler.
Note : $\phi(13) = 12$ car 13 est un nombre premier.

Aidez Mathieu à trouver le plus petit N qui satisfait toutes ces conditions et prouver sa validité en utilisant le théorème de Fermat.

Solution :

Les 3 premiers indices, nous permettent d'obtenir le système suivant ;
- $N \equiv 2 \pmod{4} \rightarrow \exists\, k \in Z,\ N = 4k + 2 \quad (L_1)$
- $N \equiv 4 \pmod{5} \rightarrow \exists\, k' \in Z,\ N = 5k' + 4 \quad (L_2)$
- $N \equiv 4 \pmod{7} \rightarrow \exists\, k'' \in Z,\ N = 7k'' + 4 \quad (L_3)$

$(L_1) = (L_2) \rightarrow 4k + 2 = 5k' + 4$
$\rightarrow 4k - 5k' = 2\ (*)$
$\text{PGCD}(4, 5) = 1 \rightarrow \exists\, a, b \in Z,\ 4a - 5b = 1$
$\rightarrow 4(2a) - 5(2b) = 2$
$\rightarrow (k, k') = (2a, 2b)$

Résolvons l'équation $4a - 5b = 1$
[4, 1, 0] [5, 0, 1]

[4, 1, 0] [1, –1, 1]
[1, 4, –3] [1, –1, 1]

Ainsi, on obtient la solution triviale (a, b) = (–1, –1) → (k, k') = (–2, –2) (**)
(*) et (**) → 4k – 5k' = 4(–2) – 5(–2)
→ 4k – 4(–2) = 5k' – 5(–2)
→ 4(k + 2) = 5(k' + 2)
→ ∃ s ∈ Z, k + 2 = 5s
→ k = 5s – 2 (***)
(***) dans (L_1) → N = 4(5s – 2) + 2
→ $N_{1,2}$ = 20s – 6 (L_4) ($N_{1,2}$ signifie que cette valeur de N vérifie uniquement les deux premières équations).

(L_3) = (L_4) → 20s – 6 = 7k'' + 4
→ 20s – 7k'' = 10 (α)
PGCD(20, 7) = 1 → ∃ a, b ∈ Z, 20a – 7b = 1
→ 20(10a) – 7(10b) = 10
→ (s, k'') = (10a, 10b)

Résolvons l'équation 20a – 7b = 1
[20, 1, 0] [7, 0, 1]
[6, 1, –2] [7, 0, 1]
[6, 1, –2] [1, –1, 3]
[1, 6, –17] [1, –1, 3]

Ainsi, on obtient une solution qui est (a, b) = (–1, –3) → (s, k'') = (–10, –30) (β)
(α) et (β) → 20s – 7k'' = 20(–10) – 7(–30)
→ 20s – 20(–10) = 7k''– 7(–30)
→ 20(s + 10) = 7(k''+ 30)
→ ∃ s' ∈ Z, s + 10 = 7s'
→ s = 7s' – 10 (****)
(****) dans (L_4) → N = 20(7s' – 10) – 6
→ $N_{1,2,3}$ = 140s' –206

La plus petite valeur de $N_{1,2,3}$ est obtenu pour s = 2 donc $N_{1,2,3}$ = 74

Vérification par utilisation du théorème de fermât :

74 ≡ 9 (mod 13) → $(74)^2$ ≡ 81 (mod 13) or 81 ≡ 3 (mod 13)
→ $(74)^2$ ≡ 3 (mod 13)

→ $(74)^{12} \equiv (3)^6 \pmod{13}$

→ $(74)^{12} \equiv 729 \pmod{13}$ or $729 \equiv 1 \pmod{13}$

→ $(74)^{12} \equiv 1 \pmod{13}$

On prouve ainsi que N = 74 satisfait à toutes les conditions; par conséquent le code secret qui ouvre le coffre est N = 74.