Séance 3 : Théorie des Nombres pour la Cryptographie

Hervé Talé Kalachi

Résumé

Ce cours introduit les concepts fondamentaux de la théorie des nombres avec une perspective cryptographique. Nous explorerons les propriétés algébriques des entiers, les algorithmes classiques et leurs applications modernes en sécurité informatique.

1 Divisibilité et Nombres Premiers

1.1 Définitions Fondamentales

Définition 1.1 (Divisibilité)**.** Un entier a est dit **divisible** par un entier $b \neq 0$ s'il existe $k \in \mathbb{Z}$ tel que :

$$a = b \cdot k$$

On note $b \mid a$.

Définition 1.2 (Nombre Premier)**.** Un entier $p > 1$ est dit **premier** si ses seuls diviseurs positifs sont 1 et lui-même. Dans le cas contraire, il est dit **composé**.

1.2 Théorème Fondamental de l'Arithmétique

Théorème 1.1 (Théorème de Factorisation Unique)**.** Tout entier $n > 1$ s'écrit de manière unique sous la forme :

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

où les p_i sont des nombres premiers distincts et $\alpha_i \in \mathbb{N}^*$.

1.3 Méthodes de Factorisation

Exemple 1.1 (Factorisation par Division Successive)**.** Factorisons 420 :

$$\begin{aligned} 420 \div 2 &= 210 \\ 210 \div 2 &= 105 \\ 105 \div 3 &= 35 \\ 35 \div 5 &= 7 \\ 7 \div 7 &= 1 \end{aligned}$$

Donc $420 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1$

Application Cryptographique

La difficulté de factoriser de grands nombres entiers (≥ 300 chiffres) est à la base de la sécurité du cryptosystème RSA.

2 PGCD et Algorithme d'Euclide

2.1 Définitions et Propriétés

Définition 2.1 (PGCD)**.** Le Plus Grand Commun Diviseur de deux entiers a et b, noté $PGCD(a, b)$, est le plus grand entier d tel que $d \mid a$ et $d \mid b$.

Théorème 2.1 (Bézout)**.** Si $d = PGCD(a, b)$, alors il existe $x, y \in \mathbb{Z}$ tels que :

$$ax + by = d$$

2.2 Algorithme d'Euclide Étendu

Étape	**Description**
Initialisation	Maintenir des coefficients de Bézout : $x_0 = 1$, $x_1 = 0$, $y_0 = 0$, $y_1 = 1$
Itération	À chaque division euclidienne $a = bq + r$, mettre à jour : $x_{n+1} = x_{n-1} - qx_n$ $y_{n+1} = y_{n-1} - qy_n$
Terminaison	Lorsque $b = 0$, retourner (a, x_0, y_0)

Exemple 2.1 (Calcul avec l'Algorithme Étendu)**.** Calculons $PGCD(99, 78)$ et les coefficients de Bézout :

a	b	r	q	x	y
99	78	21	1	1	-1
78	21	15	3	-3	4
21	15	6	1	4	-5
15	6	3	2	-11	14
6	3	0	2	26	-33

Solution : $PGCD(99, 78) = 3 = 99 \times (-11) + 78 \times 14$

3 Applications Cryptographiques

3.1 Primalité et Cryptosystèmes

— Génération de nombres premiers aléatoires (tests de primalité probabilistes)
— Cryptosystème RSA : $n = pq$ où p et q sont premiers
— Échange de clés Diffie-Hellman basé sur la difficulté du logarithme discret

3.2 Implémentation Algorithmique

Listing 1 – Algorithme d'Euclide en Python

```python
def euclide_etendu(a, b):
    x0, x1 = 1, 0
    y0, y1 = 0, 1
    while b != 0:
        q = a // b
        a, b = b, a % b
        x0, x1 = x1, x0 - q * x1
        y0, y1 = y1, y0 - q * y1
    return a, x0, y0
```

4 Exercices Avancés

1. Montrer que pour tout $n \geq 1$, $PGCD(F_n, F_{n+1}) = 1$ où F_n est le n-ième nombre de Fibonacci.
2. Soit p un nombre premier. Montrer que si $p \mid ab$ alors $p \mid a$ ou $p \mid b$ (Lemme d'Euclide).
3. Calculer $7^{-1} \mod 19$ en utilisant l'algorithme d'Euclide étendu.
4. **Défi** : Factoriser 3599 en utilisant seulement 3 divisions.

Références

[1] Katz, Jonathan. *Introduction à la Cryptographie Moderne*. CRC Press, 2ème édition, 2014.

[2] Cohen, Henri. *A Course in Computational Algebraic Number Theory*. Springer, 1993.

[3] Stallings, William. *Cryptographie et Sécurité des Réseaux*. Pearson, 4ème édition, 2017.