Théorème des Restes Chinois

A∼Z

June 2022

1 Décomposition en produit binaire

Étant donné un idéal bilatère I d'un anneau R, on a une projection naturelle $\pi : R \to R/I$. La question usuelle se pose: quand est-ce que $R \cong R/I \times R/J$? En considérant $R = \mathbb{Z}/4\mathbb{Z}$ et $I = (\bar{2})$, on peut voir que ce n'est pas toujours le cas.

Le lemme de séparation donne une condition nécessaire et suffisante dans le cas des modules: $M \cong A \oplus B$ si et seulement si la suite exacte courte

$$0 \longrightarrow A \xrightarrow{i} M \xrightarrow{\pi} B \longrightarrow 0$$

est séparée, ce qui revient à dire que M se projette naturellement sur A par une flèche ρ telle que $\rho i = 1_A$. On a alors $M = \ker\pi + \ker\rho$ et $\ker\pi \cap \ker\rho = 0$. En effet $(i\rho)^2 = i\rho i\rho = i\rho$, donc $p := i\rho$ est un projecteur. On en déduit que $M = \operatorname{Im} p \oplus \ker p$ (somme directe interne), soit $M = \ker\pi \oplus \ker\rho$.

Cette condition étant très naturelle, on peut penser qu'elle se vérifiera dans d'autres structures. En effet, c'est le cas pour les groupes:

Lemme 1.1. *Soit H et K sont des sous-groupes de G, l'un au moins distingué. Si $HK = G$ et $H \cap K = 1$, alors $G \cong H \times K$.*

Preuve. Soit $f : (h, k) \mapsto hk$. Comme $hkh^{-1}k^{-1}$ est dans H et dans K, il est dans leur intersection. Ainsi les éléments de H commutent avec ceux de K, et f est un morphisme. Il est surjectif car $HK = G$, et injectif car $hk = 1$ implique que $h = k^{-1}$ est dans l'intersection. □

Le résultat s'étend aux anneaux sans aucun problème.

Lemme 1.2. *Si I et J sont des idéaux bilatères de R tels que $I + J = R$ et $I \cap J = 0$, alors $R \cong R/I \times R/J$.*

Preuve. D'après le lemme précédent, on a

$$R \cong J \times I \cong R/I \times R/J$$

en tant que groupes, les isomorphismes $J \to R/I$ et $I \to R/J$ étant donnés par $j \mapsto j + I$ et $i \mapsto i + J$.
Ainsi, l'isomorphisme de groupe s'écrit

$$f : r = i + j \mapsto (j, i) \mapsto (j + I, i + J) = (i + j + I, i + j + J) = (r + I, r + J),$$

et est bien un morphisme d'anneaux. □

On aimerait bien que la réciproque soit vraie. Et ça tombe bien, parce qu'elle l'est.

Théorème 1.1. *Soit I et J deux idéaux bilatères d'un anneau R. Alors $R \cong R/I \times R/J$ si et seulement si $I + J = R$ et $I \cap J = 0$.*

Preuve. On a déjà montré un sens. Soit $f = \sigma \times \tau$ un isomorphisme, en considérant σ et τ des projections sur R/I et R/J respectivement.

- $\ker\sigma = I$ et $\ker\tau = J$, soit $I \cap J = \ker f = 0$.
- Soit $x \in R$. En posant $i = f^{-1}(0 + I, \tau(x))$, on a $i \in I$ et $\tau(x) = \tau(i)$, donc $x - i \in J$ soit $x \in I + J$. □

2 Cas particulier de $\mathbb{Z}/n\mathbb{Z}$

On s'intéresse particulièrement aux anneaux de la forme $\mathbb{Z}/n\mathbb{Z}$: les étudier permet de montrer de nombreux résultats d'arithmétique élémentaire, et leur compréhension est sans surprise importante en cryptographie.
Par exemple, que se passe-t-il si $d|n$?

Lemme 2.1. *Soit n et d des entiers tels que $d|n$. Alors d génère l'unique idéal de $\mathbb{Z}/n\mathbb{Z}$ d'ordre n/d, et quotienter par cet idéal donne $\mathbb{Z}/d\mathbb{Z}$.*

Preuve. D'après le théorème de correspondance $d\mathbb{Z}/n\mathbb{Z}$ est un idéal de $\mathbb{Z}/n\mathbb{Z}$, et le second théorème d'isomorphisme montre

$$\frac{\mathbb{Z}/n\mathbb{Z}}{d\mathbb{Z}/n\mathbb{Z}} \cong \frac{\mathbb{Z}}{d\mathbb{Z}}.$$

D'où $|d\mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}/n\mathbb{Z}|/|\mathbb{Z}/d\mathbb{Z}| = n/d$ en passant au cardinal. Le caractère cyclique de $\mathbb{Z}/n\mathbb{Z}$ considéré en tant que groupe donne l'unicité. □

On déduit de ce lemme une jolie expression de $\mathbb{Z}/mn\mathbb{Z}$ quand m et n sont premiers entre eux.

Théorème 2.1 (Théorème des Restes Chinois)**.** *Si m et n sont des entiers premiers entre eux, alors*

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Preuve. Soit (m) et (n) les idéaux générés par m et n, que l'on considérera indifféremment dans $\mathbb{Z}/mn\mathbb{Z}$ ou dans $\mathbb{Z}$ grâce au théorème de correspondance.

- Dans $\mathbb{Z}$, on a $(m) \cap (n) = (\operatorname{lcm}(m,n)) = (mn)$ et $(m) + (n) = (\gcd(m,n)) = (1)$.
- Dans $\mathbb{Z}/mn\mathbb{Z}$, on a $(mn) = 0$ et $(1) = \mathbb{Z}/mn\mathbb{Z}$.

Le lemme et le théorème précédents donnent alors

$$\mathbb{Z}/mn\mathbb{Z} \cong \frac{\mathbb{Z}/mn\mathbb{Z}}{(m)} \times \frac{\mathbb{Z}/mn\mathbb{Z}}{(n)} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}. \quad \square$$

Il existe une autre preuve bien plus élémentaire, mais moins conceptuelle. Elle présente cependant tout de même un intérêt puisqu'elle explicite l'isomorphisme réciproque.
Preuve. Soit a et b deux entiers, construisons $x \in \mathbb{Z}$ tel que $x \equiv a \pmod{n}$ et $x \equiv b \pmod{m}$.
m étant premier avec n, il existe un entier m' tel que $mm' \equiv 1 \pmod{n}$. De même pour n. Alors en posant $x = amm' + bnn'$, on a

$$\begin{aligned} x \equiv amm' + bnn' &\equiv bnn' \equiv b \pmod{m} \\ \text{et } x \equiv amm' + bnn' &\equiv amm' \equiv a \pmod{n}. \end{aligned}$$

La fonction $(a,b) \mapsto x$ est bien un morphisme, puisque c'est la réciproque de $x \mapsto (x \bmod m, x \bmod n)$ quand x est pris dans $\mathbb{Z}/mn\mathbb{Z}$. □

3 Applications

3.1 Une formule pour $\varphi(n)$

On appelle indicatrice d'Euler la fonction φ qui à tout n de $\mathbb{N}^*$ associe le nombre d'entiers premiers à n dans $[\![1,n]\!]$. Le théorème de bézout a pour conséquence que $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$, nous allons utiliser cela afin d'obtenir une formule pour $\varphi(n)$ dépendant de la factorisation de n.

Lemme 3.1 (Multiplicativité de φ)**.** *Si m et n sont des entiers premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$*

Preuve.

$$\varphi(mn) = |(\mathbb{Z}/mn\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*| = \varphi(m)\varphi(n). \quad \square$$

Cela permet déjà de réduire le problème à trouver une formule pour les puissances de premiers entiers, ce que nous allons faire par dénombrement. Si p est un premier entier, les seuls entiers ayant un facteur commun non trivial avec lui sont ses multiples. On trouve p^{k-1} multiples de p entre p et p^k, donc $\varphi(p^k) = p^k - p^{k-1}$.

Corollaire 3.1. *Si $\prod_i p_i^{k_i}$ est la factorisation en nombres premiers de $n \in \mathbb{N}^*$, alors*

$$\varphi(n) = \prod_i \varphi(p_i^{k_i}) = \prod_i p^{k-1}(p-1).$$

3.2 Attaques par Morphismes

En cryptographie, un problème important est celui du logarithme discret. Étant donné un groupe G, un élément $g \in G$, et un élément $h = g^k$, on veut retrouver k (modulo l'ordre de g).

C'est un problème considéré comme cryptographiquement difficile — on peut même montrer qu'il n'est pas résoluble en temps polynomial de manière générique [Sho97] — ce pourquoi il est utilisé à la base d'algorithmes tels que DHKE (Diffie-Hellman Key Exchange), DSA (Digital Signature Algorithm), ECDSA (Elliptic Curve Digital Signature Algorithm), etc...
Il peut cependant se révéler trivial dans certains cas, comme par exemple si G le groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Une classe d'attaques importante est celle des attaques par isomorphisme. Il s'agit de trouver un isomorphisme d'un groupe "compliqué", dans lequel résoudre le logarithme discret est difficile, vers un groupe "facile", dans lequel résoudre le logarithme discret est facile. Un exemple d'un tel procédé est l'attaque de Smart [Sma99], qui relève certaines courbes elliptiques $E(\mathbb{F}_p)$ vers un sous-groupe de $E(\mathbb{Q}_p)$ dans lequel le logarithme discret est calculable.

Grâce au théorème des restes chinois, on n'a pas nécessairement besoin d'un isomorphisme: un ou plusieurs morphismes suffisent.

Lemme 3.2. *Si $f : G \to H$ est un morphisme de groupe et $g \in G$, alors* $\operatorname{ord} f(g) \mid \operatorname{ord} g$

Preuve.

$$f(g)^{\operatorname{ord} g} = f(g^{\operatorname{ord} g}) = f(1) = 1. \quad \square$$

Lemme 3.3. *Si $f : G \to H$ est un morphisme de groupe, $g \in G$, et $h = g^k$ pour un certain entier k, alors*

$$\operatorname{dlog}_{f(g)} f(h) \equiv k \mod \operatorname{ord} f(g),$$

où $\operatorname{dlog}_x y$ est le plus petit entier naturel n tel que $x^n = y$.

Preuve. Un tel entier existe bien: $f(g)^k = f(g^k) = f(h)$. Si on appelle n le plus petit d'entre eux, alors $f(g)^n = f(g)^k$ d'où $f(g)^{n-k} = 1$ et $\operatorname{ord} f(g) \mid n - k$. $\square$

Étant donné plusieurs morphismes vers des groupes où le logarithme discret est calculable, on est dans le cadre du théorème des restes chinois: on a une valeur de k modulo des diviseurs de $\operatorname{ord} g$, et utiliser le théorème donne une valeur de k modulo un gros diviseur de $\operatorname{ord} g$, voir $\operatorname{ord} g$ lui-même. Le fait que ces diviseurs ne soient pas nécessairement premiers entre eux n'est en réalité pas un problème.

Lemme 3.4. *Soit m et n deux entiers. Le système d'équation $x \equiv a \mod m$ et $x \equiv b \mod n$ admet une solution modulo $\operatorname{lcm}(m, n)$ si et seulement si $a \equiv b \mod \gcd(m, n)$.*

Preuve. Posons $d = \gcd(m, n)$.

⇒) Si x est solution, alors $x \equiv a \mod d$ et $x \equiv b \mod d$.

⇐) On décompose n et m en facteurs premiers, ie

$$n = \prod_i p_i^{n_i} \text{ et } m = \prod_i q_i^{m_i}.$$

Le théorème des restes chinois garantit que le système d'équations $x \equiv a \mod p_i^{n_i}$ aura pour solution a modulo n, et que $x \equiv b \mod q_i^{m_i}$ aura pour solution b modulo m. La condition $a \equiv b \mod d$ permet alors de regrouper ces équations, en choisissant le modulus présentant la plus grande puissance si $p_i = q_j$. Le théorème des restes chinois donne alors une solution modulo $\operatorname{lcm}(m, n)$ à l'équation de base. $\square$

References

[Sho97] Victor Shoup. "Lower Bounds for Discrete Logarithms and Related Problems". In: *Advances in Cryptology — EUROCRYPT '97*. Ed. by Walter Fumy. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 256–266. ISBN: 978-3-540-69053-5.

[Sma99] N. P. Smart. "The discrete logarithm problem on elliptic curves of trace one". English. In: *J. Cryptology* 12.3 (1999), pp. 193–196. ISSN: 0933-2790. DOI: 10.1007/s001459900052.