/

Systèmes de congruence

Leçons : 120, 142.

Enoncés : • Th 1 (reste chinois) : A principal, $m_1, \dots, m_s \in A$ 2à2 premiers entre eux, $m = \prod_{i=1}^{s} m_i$.

$\begin{cases} A/mA \to \prod_{i=1}^{s} (A/m_iA) \\ \overline{x}^m \mapsto (\overline{x}^{m_1}, \dots, \overline{x}^{m_s}) \end{cases}$ est un isomorphisme d'anneaux. Si pour $1 \le i \le s$ on a la relation de Bézout $u_i m_i + v_i \prod_{j \neq i} m_j = 1$, l'antécédent de $(\overline{y_i}^{m_i})_{1 \le i \le s}$ est la classe modulo m de $\sum_{i=1}^{s} y_i v_i \prod_{j \neq i} m_j$.

• Lemme : A pricipal, $m_1, \dots, m_s \in A$. Il existe $n_1 | m_1, \dots, n_s | m_s$ 2à2 premiers entre eux et de produit $m_1 \vee \dots \vee m_s$.

• Th 2 : A principal, $m_1, \dots, m_s, a_1, \dots, a_s \in A$. Le système $\begin{cases} x \equiv a_1 \ [m_1] \\ \vdots \\ x \equiv a_s \ [m_s] \end{cases}$ a des solutions ssi $\forall i,j$, $a_i \equiv a_j \ [m_i \wedge m_j]$. Si c'est le cas, il équivaut au système $\begin{cases} x \equiv a_1 \ [n_1] \\ \vdots \\ x \equiv a_s \ [n_s] \end{cases}$, où les n_i sont pris comme dans le lemme.

⊛ Th 1.

On définit le morphisme d'anneaux $\psi : \begin{cases} A \to \prod_{i=1}^{s} (A/n_iA) \\ x \mapsto (\overline{x}^{n_1}, \dots, \overline{x}^{n_s}) \end{cases}$. Par th d'isomorphisme il suffit de mq $\ker \psi = mA$ et la surjectivité avec la formule.

D'abord pour $x \in A$: $\psi(x) = 0 \Leftrightarrow \forall i,\ n_i | x \Leftrightarrow m | x$ puisque $m = n_1 \cdots n_s = n_1 \vee \dots \vee n_s$.

Ensuite avec les relations de l'énoncé (qui sont bien def car $\forall i$, $n_i \wedge \left(\prod_{j \neq i} n_j\right) = 1$), soit $1 \le k \le s$. $v_k \prod_{j \neq k} n_j = 1 - u_k n_k \equiv 1 \ [n_k]$; et pour $i \neq k$, $v_i \prod_{j \neq i} n_j \equiv 0 \ [n_k]$ car n_k apparaît. On a donc bien $\sum_{i=1}^{s} y_i v_i \prod_{j \neq i} n_j \equiv y_k \ [n_k]$. D'où la surjectivité. □

⊛ Lemme.

• Soit P un système de représentants des irréductibles de A (qui est factoriel). On note $m = m_1 \vee \dots \vee m_s$ et pour $\gamma | m$ on choisit un $1 \le i \le s$ tq $v_\gamma(m_i) = v_\gamma(m)$, et on le note $i(\gamma)$. On note aussi $\alpha(\gamma) = v_\gamma(m_{i(\gamma)}) = v_\gamma(m)$ la valuation associée. Alors pour $1 \le i \le s$ on pose $n_i = \prod_{\substack{\gamma | m \\ i(\gamma) = i}} \gamma^{\alpha(\gamma)}$. Mq cela convient.

• Si $i(\gamma) = i$, par def de $\alpha(\gamma)$, $\gamma^{\alpha(\gamma)} | m_i$: $n_i | m_i$.

Soient $i \neq j$. Si on a un $\gamma \in P$ qui divise n_i et n_j, alors $i = i(\gamma) = j$: c'est absurde, et $n_i \wedge n_j = 1$.

Enfin $\prod_{i=1}^{s} n_i = \prod_{i=1}^{s} \prod_{\substack{\gamma | m \\ i(\gamma) = i}} \gamma^{\alpha(\gamma)} = \prod_{\gamma | m} \gamma^{\alpha(\gamma)} = m$. □

⊛ Th 2.

- Supposons que l'on a une solution du système $\mathcal{S} : \begin{cases} x \equiv a_1 [m_1] \\ \vdots \\ x \equiv a_s [m_s] \end{cases}$. D'abord $m_i \wedge m_j$ divise à la fois m_i et m_j donc $a_i \equiv x \equiv a_j [m_i \wedge m_j]$. Ensuite si $1 \leq i \leq s$, $n_i | m_i$ donc $x \equiv a_i [n_i]$ et x est solution du système $\mathcal{S}' : \begin{cases} x \equiv a_1 [n_1] \\ \vdots \\ x \equiv a_s [n_s] \end{cases}$.

- Réciproquement supposons que les a_i vérifient la condition et que l'on a une solution x de $\mathcal{S}'$. Fixons $1 \leq i \leq s$. Soit $p | m_i$: on pose $\alpha = v_p(m_i)$ et $1 \leq j \leq s$ tq $p | n_j$. Puisque les n_k sont deux à deux premiers entre eux et que p^α divise leur produit, on a $p^\alpha | n_j | m_j$. On a donc aussi $p^\alpha | m_i \wedge m_j$. Comme par hypothèse $x \equiv a_j [n_j]$, on a $x \equiv a_j \equiv a_i [p^\alpha]$. Ceci est vrai pour chaque $p | m_i$, donc le th des restes chinois lui-même donne $x \equiv a_i [m_i]$.

□

Complément 1 : Cryptosystème RSA.

- Système de cryptographie asymétrique. Principe : Alice veut que l'on puisse lui envoyer des messages chiffrés qu'elle seule pourra déchiffrer. Repose sur le principe que l'application "chiffrage" soit facilement faisable par n'importe qui (clé publique) mais que sa réciproque ne soit facilement faisable que par Alice (clé privée).
Dans le cadre de RSA, Alice choisit deux grands nombres premiers $p \neq q$ et pose $n = pq$. Elle choisit encore $1 < e < \varphi(n)$ premier avec $\varphi(n) = (p-1)(q-1)$ et calcule son inverse modulo $\varphi(n)$, d. La clé publique est alors (n, e) et la clé privée (n, d).
Un message est représenté par un $M \in \mathbb{Z}/n\mathbb{Z}$. Le chiffrage se fait par $M \mapsto M^e$, le déchiffrage par $N \mapsto N^d$.
- Vérifions que l'on a bien $M^{ed} \equiv M [n]$. D'après le th des restes chinois il suffit de mq $M^{ed} \equiv M [p]$ (de même pour q ; c'est symétrique). Si $M \equiv 0 [p]$ c'est trivial. Sinon, $ed \equiv 1 [p-1]$ car $p-1 | \varphi(n)$, donc on écrit $ed = 1 + k(p-1)$. Or que $M^{p-1} \equiv 1 [p]$, $M^{ed} = M \cdot (M^{p-1})^k \equiv M [p]$.

□

Complément 2 : Interpolation de Lagrange-Sylvester.

Soient $\mathbb{K}$ un corps de caractéristique nulle, $x_0, \dots, x_n \in \mathbb{K}$ 2 à 2 $\neq$. $y_0^{(0)}, \dots, y_0^{(m_0)}, \dots, y_n^{(0)}, \dots, y_n^{(m_n)} \in \mathbb{K}$.
Il existe un unique $P \in \mathbb{K}[X]$ de degré $< \sum_{i=0}^{n} (m_i + 1)$ tq $\begin{cases} \left(P^{(k)}(x_0) = y_0^{(k)}\right)_{0 \leq k \leq m_0} \\ \vdots \\ \left(P^{(k)}(x_n) = y_n^{(k)}\right)_{0 \leq k \leq m_n} \end{cases}$.

Preuve. On mq pour chaque $0 \leq i \leq n$, $\left(P^{(k)}(x_i) = y_i^{(k)}\right)_{0 \leq k \leq m_i}$ équivaut à $P \equiv \sum_{k=0}^{m_i} \frac{y_i^{(k)}}{k!} (X - x_i)^k \left[(X - x_i)^{m_i + 1}\right]$.
En effet le th des restes chinois s'applique alors, avec pour module $\prod_{i=0}^{n} (X - x_i)^{m_i + 1}$, dont le degré est $\sum_{i=0}^{n} (m_i + 1)$.
Pour d assez grand, la formule de Taylor en x_i donne $P = \sum_{k=0}^{d} \frac{P^{(k)}(x_i)}{k!} (X - x_i)^k$. Si on a les valeurs dérivées on a la congruence. Si on a la congruence, on l'a encore en remplaçant m_i par $0 \leq l \leq m_i$; cela donne successivement, par récurrence, $P^{(0)}(x_i) = y_i^{(0)}, \dots, P^{(m_i)}(x_i) = y_i^{(m_i)}$.

□

Réf :
- Objectif agrégation : p 241 (th 1, compléments 1).
- Carnet de voyage en algèbre : p 167 (th 1, compléments 1).
- Tattersall – Elementary number theory : p 186 (th 2).

↳ Dans le th 1 on note $\dot{-}^n$ la proj canonique modulo $n \in A$. Dans la formule de l'antécédent, $x_i \in A$ est un relèvement quelconque de $\overline{x_i}^{n_i}$.

↳ Pour leçon 120 : remplacer par $\mathbb{Z}$! Par cardinalité on n'a alors pas besoin de montrer la surjectivité, mais on le fait quand même pour la formule.

↳ Tout est effectif.

↳ Dans le lemme il n'y a pas unicité. Par exemple (6, 10) peut donner (3, 10) ou (6, 5).

↳ Un peu court a priori ; terminer en disant un mot sur un compléments (le premier pour 120, le second pour 142). Dans les deux cas c'est une application du th de base (th 1).

↳ Commentaires sur RSA. Le base sur le fait que si p, q grands, il n'est pas possible en temps raisonnable de retrouver, à partir de la clé publique (n, e), d ou a fortiori p, q ou $\varphi(n)$. Pour choisir p, q Alice tire des entiers de 99 milliers de bits au hasard et teste leur primalité ; pour e elle tire de $\hat{m}$ au hasard et vérifie que $e \wedge \varphi(n) = 1$. Par ailleurs l'exponentiation doit se faire dans $\mathbb{Z}/n\mathbb{Z}$ et pas dans $\mathbb{Z}$.

↳ Complément 2 : généralisation d'interpolation Lagrange, qui est le cas $m_0 = \dots = m_n = 0$. Utile en analyse numérique. Pas de réf.

↳ Dans Carnet de voyage : cas $s = 2$ du th 2. Était en utilisant plus explicitement des isomorphismes.

↳ Dans Tattersall (qui n'est pas dans la BA officielle) le lemme et le th 2 sont énoncés mais pas démontrés.