

Théorème des restes chinois + Application

Lemme: Soit A principal, $(a_i)_{i=1}^n \in A^n$ 2 à 2 premiers, $b_i := \prod_{j \neq i} a_j$. Alors $(b_i)_{i=1}^n$ premières entre eux.

Supposons que $\exists d \in A^* / A^*$ tel que $d | b_i, \forall i \in \{1, n\}$. Puisque A est factoriel car principal, $\exists p \in A$ facteur premier de d . Donc $p | b_i$ et $\exists j \in \{2, n\}$ tel que $p | a_j$. Or $p | b_j$, donc $\exists i \neq j$ tel que $p | a_i$. C'est absurde car $\text{pgcd}(a_i, a_j) = 1$, donc les $(b_i)_{i=1}^n$ sont premières entre eux.

Théorème: Soit $a := \prod_{i=1}^n a_i$, alors $\phi: \pi(n) \in A / \langle a \rangle \mapsto (\pi_1(n), \dots, \pi_n(n)) \in \prod_{i=1}^n A / \langle a_i \rangle$ isomorphisme

① Construction $\phi: A \rightarrow \prod_{i=1}^n A / \langle a_i \rangle$ ② Calcul $\text{Ker } \phi$ ③ Calcul $\text{Im } \phi$ ④ Conclusion

① On pose $\phi: A \rightarrow \prod_{i=1}^n A / \langle a_i \rangle$. C'est un morphisme d'anneau, puisque les π_i sont des $x \mapsto (\pi_1(x), \dots, \pi_n(x))$ morphisme d'anneau.

② On calcule

$$x \in \text{Ker } \phi \Leftrightarrow \forall i \in \{1, n\} \pi_i(x) = 0 \Leftrightarrow \forall i \in \{1, n\} x \in \langle a_i \rangle = \text{Ker } \pi_i \Leftrightarrow \forall i \in \{1, n\} \exists \alpha_i, x = \alpha_i a_i$$

Or les $(a_i)_{i=1}^n$ sont 2 à 2 premiers, donc $\text{ppcm}(a_1, \dots, a_n) = a$ et $\text{Ker } \phi = \langle a \rangle$.

③ Puisque A est principal, d'après Bezout et le lemme, $\exists (u_i)_{i=1}^n \in A^n$ tel que $\sum_{i=1}^n u_i b_i = 1$.

Soit $y \in \prod_{i=1}^n A / \langle a_i \rangle$, par surjectivité des π_i , $\exists (x_i)_{i=1}^n \in A^n$ tel que $y = (\pi_1(x_1), \dots, \pi_n(x_n))$

On pose $x := \sum_{i=1}^n x_i u_i b_i$, puisque $\forall i, j \in \{1, n\} \pi_j(b_i) = 0$ si $i \neq j$, on a

$$\pi_j(x) = \sum_{i=1}^n \pi_j(x_i) \pi_j(u_i) \pi_j(b_i) = \pi_j(x_j) \pi_j(u_j) \pi_j(b_j) = \pi_j(x_j) \sum_{i=1}^n \pi_j(u_i) \pi_j(b_i) = \pi_j(x_j) \pi_j(1) = \pi_j(x_j)$$

Alors, on a $\phi(x) = y$ et ϕ est surjective.

④ Par théorème d'isomorphisme, ϕ se factorise en un isomorphisme Φ , d'inverse Φ^{-1} .

$$\Phi^{-1}: (\pi_1(x_1), \dots, \pi_n(x_n)) \in \prod_{i=1}^n A / \langle a_i \rangle \mapsto \pi \left(\sum_{i=1}^n x_i u_i b_i \right) \in A / \langle a \rangle$$

Application: le système d'équation diophantienne (S): $\begin{cases} k \equiv 2 \pmod{4} \\ k \equiv 3 \pmod{5} \\ k \equiv 1 \pmod{9} \end{cases}$ donne $k \in 119 + 180\mathbb{Z}$

Avec $\begin{cases} a_1 = 4 \\ a_2 = 5 \\ a_3 = 9 \end{cases}$ 2 à 2 premiers et $\begin{cases} b_1 = 45 \\ b_2 = 36 \\ b_3 = 20 \end{cases}$, on cherche dans $\mathbb{Z}_{180\mathbb{Z}}$ $\Phi^{-1}([2]_4, [3]_5, [1]_9)$

On calcule u_1, u_2, u_3 :

$$45 = 36(1) + 9, 36 = 9(4) + 0 \text{ donc } 45 \vee 36 = 9 = 45(1) + 36(-1)$$

$$20 = 9(2) + 2, 9 = 2(4) + 1 \text{ donc } 20 \vee 9 = 9(1) + 2(-4) = 9(1) + (-4)(20(1) - 9(2))$$

Alors $45 \vee 36 \vee 20 = 9(9) + 20(-4) = 45(9) + 36(-9) + 20(-4)$. (a solution dans $\mathbb{Z}_{180\mathbb{Z}}$ est

$$k = 2(45)(9) + 3(36)(-9) + 1(20)(-4) = x_1 b_1 u_1 + x_2 b_2 u_2 + x_3 b_3 u_3$$

Lemme (Bezout): $(b_i)_{i=1}^n \in A^n$ premiers entre eux $\Leftrightarrow \exists (u_i)_{i=1}^n \in A^n$ tq $\sum_{i=1}^n u_i b_i = 1$

Rq: Comme A principal, $I = \langle (b_i)_{i=1}^n \rangle \in \text{Id}(A)$ et $\exists d \in A$ tq $I = \langle d \rangle$. Donc $\forall i \in \{1, n\} \langle b_i \rangle \subset \langle d \rangle$ et $d \mid b_i$. Si $d \in A$ tel que $d \nmid b_i \forall i \in \{1, n\}$. Puisque $d \in I$, $\exists (u_i)_{i=1}^n \in A^n$ tel que $\sum_{i=1}^n u_i b_i = d$. Donc $d \mid d$, et $d = \text{pgcd}((b_i)_{i=1}^n)$.

$(\Rightarrow)$ Puisque $\text{pgcd}((a_i)_{i=1}^n) = 1$, on a $I = \langle (b_i)_{i=1}^n \rangle = A$ et $\exists (u_i)_{i=1}^n \in A^n$ tq $\sum_{i=1}^n u_i b_i = 1$

$(\Leftarrow)$ Soit $d = \text{pgcd}((b_i)_{i=1}^n)$, on a $d \mid b_i \forall i \in \{1, n\}$ donc $d \mid \sum_{i=1}^n b_i u_i$ et $d \mid 1$. Alors $d \in A^\times$.

Lemme: $(a_i)_{i=1}^n \in A^n$ 2 à 2 premiers entre eux, alors $\text{ppcm}((a_i)_{i=1}^n) = \prod_{i=1}^n a_i$

Rq: Si $d = a \cdot b$, $\exists \alpha, \beta \in A^\times$ tq $1 = \alpha \cdot \beta$ et $d\alpha = a$, $d\beta = b$. Soit $p := a \cdot b = a\beta = \alpha\beta d$, donc

$a \mid p$ et $b \mid p$. Soit $p' \in A$, $a \mid p'$ et $b \mid p'$, donc $\exists u, v \in A^\times$ tq $au = bv = p'$. Alors on a

$p' = d\alpha u = d\beta v$, et $\alpha u = \beta v$. Comme $\alpha \cdot \beta = 1$ et $a \mid \beta v$ on a $\alpha \mid v$ et $\exists \tilde{v} \in A$, $\alpha \tilde{v} = v$.

Alors $p' = d\beta \alpha \tilde{v} = p \tilde{v}$ et $p \mid p'$, et $p = a \cdot b$. Finalement $ab = d\alpha d\beta = dp$. $\square$ Par récurrence.

① $n=2$, on pose $p = a_1 a_2$. On a $a_1 a_2 = (a_1 | a_2) (a_1 v a_2) = p \cdot 1 = p \cdot n$

Rq: $a_1 \mid p$ et $a_2 \mid p \Rightarrow p \in \langle a_1 \rangle \cap \langle a_2 \rangle$. Si $p \in \langle a_1 \rangle \cap \langle a_2 \rangle$, $a_1 \mid p$ et $a_2 \mid p \Rightarrow p \mid p$ et $p \in \langle p \rangle$. $\langle p \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle$

② Si $p = \text{ppcm}((a_i)_{i=1}^n)$ on a aussi $\langle p \rangle = \bigcap_{i=1}^n \langle a_i \rangle$. Or $\langle p \rangle = \langle a_1 \rangle \cap (\bigcap_{i=2}^n \langle a_i \rangle)$

ie $p = \text{ppcm}(a_1, \text{ppcm}((a_i)_{i=2}^n)) = \text{ppcm}(a_1, \prod_{i=2}^n a_i) = \prod_{i=1}^n a_i$ car $\text{pgcd}(a_1, \prod_{i=2}^n a_i) = 1$

$\Rightarrow \text{ppcm}((a_i)_{i=1}^n) = \text{ppcm}(\text{ppcm}((a_i)_{i=1}^{n-1}), a_n) = \text{ppcm}(\prod_{i=1}^{n-1} a_i, a_n) = \prod_{i=1}^n a_i$

Application: Soit $n = \prod_{i=1}^r p_i^{\alpha_i}$, Alors $\varphi(n) = \prod_{i=1}^r p_i^{\alpha_i - 1} (p_i - 1)$

Si $n = p \in \mathbb{P} \cap \mathbb{N}$, $\varphi(p) = |\{x \in \{1, n\} \mid \text{pgcd}(x, n) = 1\}| = |\mathbb{Z}/p\mathbb{Z}^\times| = p-1$

Si $n = p^\alpha$, $p \in \mathbb{P} \cap \mathbb{N}$, $\alpha \in \mathbb{N}^*$, on a $\forall x \in \{1, p^\alpha\}$, $\text{pgcd}(x, p^\alpha) = 1 \Leftrightarrow p \nmid x \Leftrightarrow \exists u \in \{1, p^{\alpha-1}\}$, $pu = x$

$\varphi(p^\alpha) = |\{1, p^\alpha\} \setminus \{x \in \{1, p^\alpha\} \mid p \mid x\}| = p^\alpha - |\{1, p^{\alpha-1}\}| = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$

Si $n = \prod_{i=1}^r p_i^{\alpha_i}$, on a $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^r \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ d'anneaux donc $\mathbb{Z}/n\mathbb{Z}^\times \simeq \prod_{i=1}^r \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}^\times$ et $\varphi(n) = \prod_{i=1}^r \varphi(p_i^{\alpha_i}) = \prod_{i=1}^r p_i^{\alpha_i - 1} (p_i - 1)$