Petit mémo d'arithmétique

Division euclidienne et congruences

Théorème. *Soient a et k deux entiers. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que*

$$a = kq + r \qquad 0 \leq r < k$$

On nomme q le quotient de la division euclidienne de a par k, *et r le* reste.

Définition. Soient a, b et k trois entiers.

- On dit que a et b sont *congrus mod k* lorsqu'ils admettent le même reste dans la division euclidienne par k. On note alors $a \equiv b \pmod{k}$.
- On dit que *k divise a* lorsque $a \equiv 0 \pmod{k}$. On note alors $k \mid a$.

Notation. Soit n un entier. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble $\{0, \dots, n-1\}$ des restes modulo n.

Théorème. *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un anneau.*

En d'autres termes, on peut effectuer des additions, soustractions et multiplications dans $\mathbb{Z}/n\mathbb{Z}$.

PGCD, PPCM et nombres premiers

Théorème. *Soient m et n deux entiers.*

- *Il existe un plus grand entier qui divise à la fois m et n. On le nomme le* plus grand diviseur commun *de m et n, et on le note* $\text{pgcd}(m, n)$[1].
- *Il existe un plus petit entier divisible à la fois par m et n. On le nomme le* plus petit multiple commun *de m et n, et on le note* $\text{ppcm}(m, n)$[1].

Théorème. *Soient a et b deux entiers. Soit $a = bq + r$ la division euclidienne de a par b. Soit d un diviseur commun de a et b. Alors d divise r.*

Remarque. On obtient donc une méthode de calcul du pgcd de deux entiers: l'algorithme d'Euclide.

Définition. Soient m, n et p trois entiers.

- On dit que m et n sont *premiers entre eux* lorsque $\text{pgcd}(m, n) = 1$.
- On dit que p est *premier* lorsque, pour $q \in \{1, \dots, p-1\}$, $\text{pgcd}(p, q) = 1$.

On note $\mathcal{P}$ l'ensemble (infini) des nombres premiers[2].

Exemple. Les entiers 2, 3, 5, 7, 11, 13, ... sont premiers.

Théorème (Théorème Fondamental de l'Arithmétique)**.** *Soit m un entier. Il existe une unique famille d'entiers $(m_p)_{p \in \mathcal{P}}$ telle que*

$$m = \pm 2^{m_2} \times 3^{m_3} \times \dots$$

Les m_p sont appelés valuation p-adique de m, *notés $v_p(m)$.*

Théorème. *Soient m et n deux entiers. Soit p un nombre premier. Alors*

$$v_p(\text{pgcd}(m, n)) = \min(v_p(m), v_p(n))$$

$$v_p(\text{ppcm}(m, n)) = \max(v_p(m), v_p(n))$$

En particulier, $\text{pgcd}(m, n) \times \text{ppcm}(m, n) = m \times n$.

Remarque. On obtient donc une seconde méthode de calcul du pgcd de deux entiers: la décomposition en facteurs premiers.

[1] On rencontre parfois également les notations $m \wedge n$ et $m \vee n$.
[2] Cette notation n'est pas standard.

Définition. Soient m et n deux entiers. On dit que m est *inversible* modulo n lorsqu'il existe un entier u tel que

$$mu \equiv 1 \pmod{n}$$

Théorème (Identité de Bachet-Bézout)**.** *Soient a et b deux entiers. Soit $d = \text{pgcd}(m, n)$. Il existe un unique couple $(u, v) \in \mathbb{Z}^2$ tel que*

$$au + bv = d$$

Les entiers u et v sont appelés coefficients de Bézout *associés à a et b.*
De plus, pour tous entiers m et n,

$$d \mid am + bn$$

Corollaire. *Soient m et n deux entiers. Alors m est inversible modulo n si et seulement si*

$$\text{pgcd}(m, n) = 1$$

Dans ce cas, le coefficient de Bézout associé à m est son inverse modulo n.[3]

Équations

Théorème. *Soient a, b et n trois entiers. L'équation*

$$ax \equiv b \pmod{n}$$

admet une solution entière si et seulement si $\text{pgcd}(a, n) \mid b$.

Théorème. *Soient a, b et c trois entiers. L'équation*

$$ax + by = x$$

admet une solution entière si et seulement si $\text{pgcd}(a, b) \mid c$.
De plus, si (x_0, y_0) est une solution particulière de l'équation, alors l'ensemble des solution est

$$\{(x_0 + kb, y_0 - ka) \mid k \in \mathbb{Z}\}$$

Théorème. *Soient $m_1, \ldots, m_n$ des entiers premiers entre eux deux à deux.*
En notant $M = m_1 \times m_2 \times \cdots \times m_n$, $M_i = \frac{M}{m_i}$ et y_i un inverse de M_i modulo m_i. Le système d'équations

$$(E) : \begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_1} \\ \vdots \\ x \equiv b_n \pmod{m_n} \end{cases}$$

admet une unique solution modulo M:

$$x \equiv b_1 \times M_1 \times y_1 + b_2 \times M_2 \times y_2 + \cdots + b_n \times M_n \times y_n \pmod{M}$$

[3] Symétriquement, n est inversible modulo m et le coefficient de Bézout associé est son inverse modulo m.

Méthodes de résolution

Une équation, une inconnue

Considérons l'équation (E) : $ax \equiv b \pmod{n}$.

- On commence par vérifier que $\text{pgcd}(a, n) \mid b$. Si ce n'est pas le cas, l'équation n'admet aucune solution.
- Soit $d = \text{pgcd}(a, n)$. On pose $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ et $n' = \frac{n}{d}$. On se ramène à l'équation (E') : $a'x \equiv b' \pmod{n'}$.
- Comme a' et n' sont premiers entre eux, a' admet un inverse c modulo n'. Ainsi,

$$ca'x \equiv cb' \pmod{n'}$$

  Donc

$$x \equiv cb' \pmod{n'}$$

- L'ensemble des solutions de (E) est alors $\{cb + kn' \mid k \in \mathbb{Z}\}$.

Exemple. Considérons l'équation (E) : $6x \equiv 3 \pmod{9}$:

- On remarque que $\text{pgcd}(6, 9) = 3$ et que $3 \mid 3$, donc l'équation admet une solution.
- En divisant par 3, on se ramène à un cas plus simple:

$$6x \equiv 3 \pmod{9} \iff 2x \equiv 1 \pmod{3}$$

- On cherche maintenant un inverse de 2 modulo 3. On sait[4] que $2 \times 2 - 3 = 1$, donc 2 est un inverse de 2 modulo 3.
- On peut donc résoudre

$$2x \equiv 1 \pmod{3} \iff 2 \times 2x \equiv 2 \times 1 \pmod{3} \iff x \equiv 2 \pmod{3}$$

- Ainsi, l'ensemble des solutions dans $\mathbb{Z}$ de l'équation initiale est $\{2 + 3k \mid k \in \mathbb{Z}\}$.

Une équation, deux inconnues

Considérons l'équation (E) : $ax + by = c$. Soit $d = \text{pgcd}(a, b)$.

- On commence par vérifier que $d \mid c$. Si ce n'est pas le cas, l'équation n'a *aucune* solution.
- On pose $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ et $c' = \frac{c}{d}$. On se ramène donc à l'équation (E') : $a'x + b'y = c'$, avec $\text{pgcd}(a', b') = 1$.
- On calcule des coefficients de Bézout u et v de a' et b', $a'u + b'v = 1$. Alors $(c'u, c'v)$ est une solution particulière de l'équation (E'), donc également de l'équation (E).
- L'ensemble des solutions de l'équation (E) est donc $\{(c'u + kb', c'v - ka') \mid k \in \mathbb{Z}\}$.

Exemple. Considérons l'équation (E) : $32x - 24y = 16$.

- On remarque que $\text{pgcd}(32, 24) = 8$ et que $8 \mid 16$. Donc l'équation admet une solution.
- En divisant par 8, on se ramène à un cas plus simple:

$$(E') : 4x - 3y = 2$$

- On calcule des coefficients de Bézout[4] de 4 et -3: $4 \times 1 - 3 \times 1 = 1$. Donc $(2, 2)$ est une solution particulière de l'équation.
- L'ensemble des solutions dans $\mathbb{Z}$ de l'équation initiale est donc $\{(2 + 3k, 2 + 4k) \mid k \in \mathbb{Z}\}$.

[4] Par un algorithme d'Euclide étendu par exemple.

Plusieurs équations, une inconnue

On considère pour cette section un système d'équations à une inconnue.

$$(E): \begin{cases} a_1 x & \equiv & b_1 & \pmod{m_1} \\ a_2 x & \equiv & b_2 & \pmod{m_1} \\ & \vdots & & \\ a_n x & \equiv & b_n & \pmod{m_n} \end{cases}$$

- On commence par se ramener à un système plus simple à étudier:

$$(E'): \begin{cases} x & \equiv & b'_1 & \pmod{m_1} \\ x & \equiv & b'_2 & \pmod{m_1} \\ & \vdots & & \\ x & \equiv & b'_n & \pmod{m_n} \end{cases}$$

  On obtient ce système en calculant, pour chaque ligne i, un inverse de a_i modulo m_i.

- Lorsque les m_i ne sont pas premiers entre eux, on est amenés à "casser" les équations en plusieurs sous-équations:
  - On calcule la décomposition en produit de facteurs premiers de chaque m_i:

$$m_i = p_{i,1} \times p_{i,2} \times \cdots \times p_{i,n}$$

  - On réduit chaque équation i modulo $p_{i,j}$ pour chaque j.
  - On élimine les équations redondantes.

  Exemple. Le système

$$(E): \begin{cases} x & \equiv & 0 & \pmod{2} \\ 5x & \equiv & 4 & \pmod{6} \end{cases}$$

  est équivalent au système

$$(E'): \begin{cases} x & \equiv & 0 & \pmod{2} \\ x & \equiv & 0 & \pmod{2} \\ 2x & \equiv & 1 & \pmod{3} \end{cases} \iff \begin{cases} x & \equiv & 0 & \pmod{2} \\ 2x & \equiv & 1 & \pmod{3} \end{cases}$$

- On applique enfin le théorème de résolution vu plus haut.

Considérons le système d'équations

$$(E): \begin{cases} 5x \equiv 2 \pmod 7 \\ x \equiv 3 \pmod 6 \\ 4x \equiv 6 \pmod 9 \\ x \equiv 1 \pmod 5 \end{cases}$$

- On calcule un inverse de 5 modulo 7 et de 4 modulo 9 pour simplifier le système, 3 et 7 conviennent. Ainsi

$$(E) \iff \begin{cases} x \equiv 6 \pmod 7 \\ x \equiv 3 \pmod 6 \\ x \equiv 6 \pmod 9 \\ x \equiv 1 \pmod 5 \end{cases}$$

- On remarque que 6 et 9 ne sont pas premiers entre eux, donc on doit casser ces équations, on commence par la deuxième ligne:

$$(E) \iff \begin{cases} x \equiv 6 \pmod 7 \\ x \equiv 1 \pmod 2 \\ x \equiv 0 \pmod 3 \\ x \equiv 6 \pmod 9 \\ x \equiv 1 \pmod 5 \end{cases}$$

- Comme $x \equiv 6 \pmod 9 \implies x \equiv 0 \pmod 3$, on peut éliminer la troisième équation, on obtient alors

$$(E) \iff \begin{cases} x \equiv 6 \pmod 7 \\ x \equiv 1 \pmod 2 \\ x \equiv 6 \pmod 9 \\ x \equiv 1 \pmod 5 \end{cases}$$

2, 5, 7 et 9 sont premiers entre eux deux à deux, on peut passer à la résolution.

- On note $M = 7 \times 2 \times 9 \times 5 = 630$, et on calcule

$$M_1 = \frac{M}{7} = 90$$

$$M_2 = \frac{M}{2} = 315$$

$$M_3 = \frac{M}{9} = 70$$

$$M_4 = \frac{M}{5} = 126$$

- On calcule des inverses des M_i modulo m_i:

$$6 \times 90 \equiv 1 \pmod 7$$

$$1 \times 315 \equiv 1 \pmod 2$$

$$4 \times 70 \equiv 1 \pmod 9$$

$$1 \times 126 \equiv 1 \pmod 5$$

- Ainsi, l'unique solution du système d'équations (E) est (modulo M)

$$x = 6 \times 90 \times 6 + 1 \times 315 \times 1 + 6 \times 70 \times 4 + 1 \times 126 \times 1 \equiv 321 \pmod{630}$$

- L'ensemble des solutions dans $\mathbb{Z}$ du système (E) est $\{321 + 630k \mid k \in \mathbb{Z}\}$.