Feuille d'exercices n° 3

Théorème Chinois

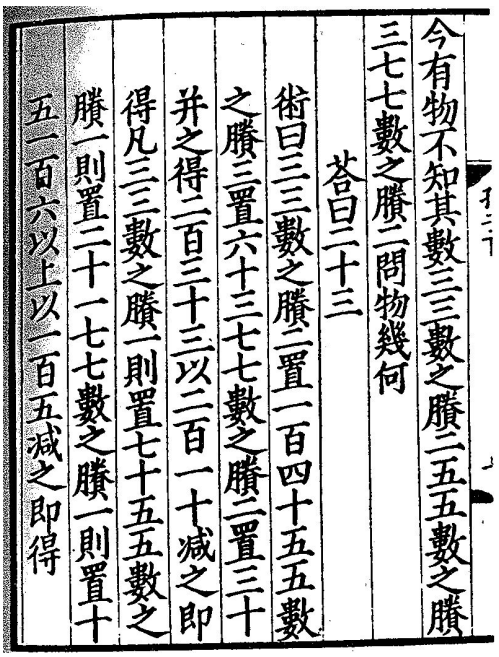
今有物不知其數三三數之賸二五五數之賸二七七數之賸二問物幾何
答曰二十三
術曰三三數之賸二置一百四十五五數之賸三置六十三七七數之賸二置三十并之得二百三十三以二百一十減之即得凡三三數之賸一則置七十五五數之賸一則置二十一七七數之賸一則置十五一百六以上以一百五減之即得

FIG. 1 – Le célèbre problème de Sunzi, le plus ancien exemple du théorème chinois.

Exercice 1 . Résoudre les systèmes :

$$\begin{cases} x \equiv 17 \mod 19 \\ x \equiv 4 \mod 11\,, \end{cases}$$

$$\begin{cases} 7x \equiv 5 \mod 19 \\ 3x \equiv 1 \mod 11 \end{cases}$$

Exercice 2 . (Sun-Zi, IVème siècle après J.-C.) Trouver le plus petit entier positif x tel que

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7. \end{cases}$$

Exercice 3 . Résoudre les systèmes :

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 4 \\ x \equiv 4 \mod 5 \end{cases}, \quad \begin{cases} x \equiv 3 \mod 10 \\ x \equiv 11 \mod 13 \\ x \equiv 15 \mod 17 \end{cases}, \quad \begin{cases} x \equiv 8 \mod 12 \\ x \equiv 11 \mod 15. \end{cases}$$

Exercice 4 . La comète A passe tous les 5 ans et a été observée l'année dernière. La comète B passe tous les 8 ans et a été observée il y a 2 ans. La comète C passe tous les 11 ans et a été observée il y a 8 ans. Quelle est la prochaine fois où on pourra observer ces 3 comètes la même année ?

Exercice 5 . Quel est le plus petit multiple positif de 7 congru à 1 modulo $2, 3, 4, 5$ et 6 ?

Fonction d'Euler

Exercice 6 . On appelle indicatrice, ou fonction d'Euler le nombre :

$$\varphi(n) = \#\{a : 1 \leq a \leq n-1 \text{ et } \mathrm{pgcd}(a,n) = 1\}.$$

1) Rappelez le lien entre $\varphi(n)$ et $\mathbb{Z}/n\mathbb{Z}$.
2) Montrer que, si p est un nombre premier, $\varphi(p) = p-1$.
3) Montrer que, si p est un nombre premier, pour tout entier $k \geq 1$, $\varphi(p^k) = p^{k-1}(p-1)$.
4) Montrer que, si m et n sont premiers entre eux alors $\varphi(mn) = \varphi(m)\varphi(n)$.
5) En déduire une méthode générale pour calculer $\varphi(n)$ en fonction de n.
6) Calculer $\varphi(12)$, $\varphi(100)$, $\varphi(108)$ et $\varphi(pq)$ (avec p et q premiers).

Exercice 7 . (Gauss) Soit φ la fonction d'Euler. Montrer que

$$\sum_{d|n, d>0} \varphi(d) = n$$

(*Indication* : Considérer la partition de $\{1, \ldots, n\}$ en $\bigsqcup_{d|n}\{x : \mathrm{pgcd}(x,n) = d\}$.)

Exercice 8 . Démontrer les propositions suivantes :
(a) Si n est impair, alors $\varphi(n) = \varphi(2n)$.
(b) Si n est pair, alors $\varphi(2n) = 2\varphi(n)$
(c) $\varphi(3n) = 3\varphi(n)$ si et seulement si $n \equiv 0 \mod 3$.
(d) $\varphi(3n) = 2\varphi(n)$ si et seulement si $n \not\equiv 0 \mod 3$.
(e) $\varphi(n) = n/2$ si et seulement si $n = 2^k$ avec $k \geq 1$.

Exercice 9 . Montrer que si $m, n \in \mathbb{Z}$ sont tels que chaque premier qui divise n divise aussi m alors $\varphi(nm) = n\varphi(m)$.

Exercice 10 . Démontrer que si $d|n$, alors $\varphi(d)|\varphi(n)$.

Compléments

Exercice 11 . Un bateau de pirates s'empare d'un butin en pièces d'or. Les 17 pirates décident de se répartir également les pièces et de donner le reste au cuisinier : celui-ci reçoit 6 pièces. Une bagarre éclate à l'issue de laquelle 6 pirates sont tués, les survivants refont la répartition et le cuisinier se retrouve avec 10 pièces. Une tempête tue ensuite 7 autre pirates, le cuisinier voit sa part réduite 3 pièces. Il décide alors d'empoisonner les survivants et de s'emparer du trésor. Combien de pièces d'or possèdera-t-il au minimum ?

Exercice 12 . Soient m, n dans $\mathbb{N} \setminus \{0\}$. Soit $\psi : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ le morphisme qui a $x \in \mathbb{Z}$ associe $(x + m\mathbb{Z}, x + n\mathbb{Z})$.
(1) Montrer que $\mathrm{Ker}(\psi) = \mathrm{ppcm}(m,n)\mathbb{Z}$.
(2) Montrer que $\mathrm{Im}(\psi) = \{(a + m\mathbb{Z}, b + n\mathbb{Z}) : \mathrm{pgcd}(m,n)|b-a\}$.

Exercice 13 . Montrer par récurrence l'existence d'une suite d'entiers $x_0, x_1, x_2, \ldots$ vérifiant :
(1) $x_{n+1} \equiv x_n \mod 7^{n+1}$ pour tout $n \in \mathbb{N}$.
(2) $x_n^2 \equiv 2 \mod 7^{n+1}$.

Exercice 14 . (1) Calculer le reste de la division euclidienne de 3^{774} par 385.
(2) Calculer le reste de la division euclidienne de 3^{164} par 88.
b. Calculer l'ordre de 3 dans $(\mathbb{Z}/88\mathbb{Z})^*$.
c. Quel est l'ordre de 7 dans $(\mathbb{Z}/88\mathbb{Z})^*$?

Exercice 15 . Déterminer tous les entiers n tels que $4n^2 + 1$ soit divisible par 5 et $n^2 - 3$ par 13.

Exercice 16 . Montrer que $2^{70} + 3^{70}$ est divisible par 13.

Exercice 17 . Montrer que pour tout entier naturel n, $2^{2^{6n+2}} + 3$ est divisible par 19.

Exercice 18 . Montrer que $20^{15} - 1$ est divisible par 20801.

Exercice 19 . (a) Montrer que $a^{13} \equiv a \mod 2730$. (Indication : $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$.) (b) Si a est impair, alors $a^{33} \equiv a \mod 4080$. (Indication : $4080 = 15 \cdot 16 \cdot 17$.)