4 Théorème chinois des restes

4.1 Soient a, b, k et m des entiers.

1) À l'aide de l'exercice 2.9 2), montrer que si $a \equiv b \mod m$, alors on a $k\,a \equiv k\,b \mod m$.
2) À l'aide de l'exercice 2.10, donner un exemple qui illustre la fausseté de la réciproque : si $k\,a \equiv k\,b \mod m$, alors en général $a \not\equiv b \mod m$.

4.2 Soient a, b, k et m des entiers avec $k \neq 0$.
Montrer, grâce au lemme de Gauss, que si $k\,a \equiv k\,b \mod m$ et si k et m sont premiers entre eux, alors on a $a \equiv b \mod m$.

4.3 Montrer que si $a \equiv b \mod m$ et si d divise m, alors $a \equiv b \mod d$.

4.4 Soient a, b, m et n des entiers.
Montrer que si $a \equiv b \mod m$, $a \equiv b \mod n$ et si m et n sont premiers entre eux, alors $a \equiv b \mod m\,n$.

4.5

1) Montrer que 2^{560} est solution du système $\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 1 \mod 11 \\ x \equiv 1 \mod 17 \end{cases}$.
2) Décomposer 561 en produit de facteurs premiers.
3) En déduire que $2^{560} \equiv 1 \mod 561$.

4.6 Montrer que $2^{1728} \equiv 1 \mod 1729$.

Proposition : *l'équation $a\,x \equiv 1 \mod m$ admet une solution si et seulement si a et m sont premiers entre eux.*

4.7 Le but de cet exercice est de prouver cette proposition.

1) Montrer que l'équation $a\,x \equiv 1 \mod m$ est satisfaite si et seulement s'il existe un entier y tel que $a\,x + m\,y = 1$.
2) Démontrer la proposition précédente à l'aide des théorèmes de Bézout et de Bachet de Mériziac.

4.8 Montrer, à l'aide de la proposition précédente, que si a et m sont premiers entre eux, alors l'équation $a\,x \equiv b \mod m$ admet une solution pour tout $b \in \mathbb{Z}$.

4.9 Résoudre les équations suivantes :

1) $12\,x \equiv 5 \mod 25$
2) $12\,x \equiv 5 \mod 36$
3) $12\,x \equiv 5 \mod 47$
4) $12\,x \equiv 5 \mod 58$
5) $313\,x \equiv 1 \mod 543$
6) $7\,x \equiv 1 \mod 215$
7) $7\,x \equiv 13 \mod 215$

Théorème chinois des restes

Soient $m_1, m_2, \ldots, m_n$ des entiers distincts, deux à deux premiers entre eux, et $b_1, b_2, \ldots, b_n$ des entiers quelconques. Alors le système de congruences

$$\begin{cases} x \equiv b_1 \mod m_1 \\ x \equiv b_2 \mod m_2 \\ \qquad \vdots \\ x \equiv b_n \mod m_n \end{cases}$$

admet une solution unique modulo $\mathrm{M} = m_1\, m_2\, \ldots\, m_n$.

4.10 Le but de cet exercice est de prouver le théorème chinois des restes.

1) Prouvons d'abord l'existence d'une solution.
Pour tout $1 \leqslant i \leqslant n$, on pose $\mathrm{M}_i = \frac{\mathrm{M}}{m_i}$.
   (a) Montrer, grâce à la proposition de la première page, que chacune des équations $\mathrm{M}_i\, x \equiv 1 \mod m_i$ admet une solution x_i .
   (b) On pose $x = b_1\, \mathrm{M}_1\, x_1 + b_2\, \mathrm{M}_2\, x_2 + \ldots + b_n\, \mathrm{M}_n\, x_n$.
   Montrer que x constitue une solution du système de congruences.
2) Prouvons ensuite l'unicité de la solution modulo M .
   Soient x et x' deux solutions du système de congruences. Montrer, à l'aide de l'exercice 4.4, que $x \equiv x' \mod \mathrm{M}$.

4.11 Le but de cet exercice est de résoudre le système $\begin{cases} x \equiv 3 \mod 11 \\ x \equiv 6 \mod 8 \\ x \equiv -1 \mod 15 \end{cases}$.

1) En reprenant les notations de l'exercice 4.10, calculer M, M_1, M_2 et M_3 .
2) (a) Calculer $120 \mod 11$. En déduire une solution évidente de l'équation $120\, x \equiv 1 \mod 11$.
   (b) L'équation $165\, x \equiv 1 \mod 8$ équivaut à $165\, x + 8\, y = 1$ pour un certain $y \in \mathbb{Z}$. Résoudre l'équation diophantienne $165\, x + 8\, y = 1$ et en déduire une solution de l'équation $165\, x \equiv 1 \mod 8$.
   (c) Déterminer une solution de l'équation $88\, x \equiv 1 \mod 15$.
3) Résoudre le système de congruences $\begin{cases} x \equiv 3 \mod 11 \\ x \equiv 6 \mod 8 \\ x \equiv -1 \mod 15 \end{cases}$.

4.12 Résoudre le système $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 2 \mod 5 \\ x \equiv 0 \mod 4 \end{cases}$.

4.13 Trouver les nombres dont la division par 3 donne le reste 1, celle par 5 le reste 2 et celle par 7 le reste 3.

4.14 Un premier phare émet un signal toutes les 15 minutes et un second phare un signal toutes les 28 minutes. On a aperçu le signal du premier à 0 h 02 et celui du second à 0 h 08. À quelle heure au plus tôt les deux signaux coïncideront-ils ?

Cet exercice permet de mieux comprendre pourquoi les astronomes chinois se sont intéressés aux systèmes de congruence. Le théorème chinois des restes permet en effet de calculer — donc de prévoir — l'apparition simultanée de phénomènes cycliques différents. C'est précisément ce genre de prévisions liées à des événements astronomiques comme des conjonctions de planètes ou des éclipses qui étaient la tâche des astronomes chinois.

4.15 Dans combien de jours la pleine lune tombera-t-elle au solstice d'hiver, si la question se pose alors qu'il reste 6 jours avant le solstice d'hiver et 3 jours avant la pleine lune ?

Remarque : on admet que le solstice d'hiver et la pleine lune se produisent respectivement tous les 365 jours et tous les 28 jours.

4.16 Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

4.17

1) Pourquoi ne peut-on pas appliquer le théorème chinois des restes pour résoudre le système $\begin{cases} x \equiv 1 \mod 6 \\ x \equiv 4 \mod 15 \end{cases}$?

2) (a) À l'aide des exercices 4.3 et 4.4, montrer l'équivalence
$$x \equiv 1 \mod 6 \iff \begin{cases} x \equiv 1 \mod 2 \\ x \equiv 1 \mod 3 \end{cases}$$

   (b) Montrer l'équivalence $x \equiv 4 \mod 15 \iff \begin{cases} x \equiv 1 \mod 3 \\ x \equiv 4 \mod 5 \end{cases}$.

3) En déduire l'équivalence $\begin{cases} x \equiv 1 \mod 6 \\ x \equiv 4 \mod 15 \end{cases} \iff \begin{cases} x \equiv 1 \mod 2 \\ x \equiv 1 \mod 3 \\ x \equiv 4 \mod 5 \end{cases}$

   et résoudre ce système.

4.18 Résoudre le système $\begin{cases} x \equiv 8 \mod 12 \\ x \equiv 10 \mod 14 \\ x \equiv 3 \mod 7 \end{cases}$

4.19 L'adjudant-chef a un problème. S'il fait défiler ses hommes par rangs de quatre, il n'a que trois hommes sur le dernier rang. S'il les fait défiler par rangs de cinq, il lui manque trois hommes sur ce dernier rang et par rangs de six, il lui manque un homme.

Sachant que la compagnie comporte entre 100 et 150 hommes, combien d'hommes l'adjudant-chef doit-il faire défiler ?

4.20 Résoudre le système $\begin{cases} 5\,x \equiv 2 \mod 24 \\ 3\,x \equiv -26 \mod 88 \\ x \equiv 28 \mod 99 \end{cases}$.

4.21 Une vieille femme se rend à un marché pour y vendre ses œufs. Un cheval piétine sa corbeille et casse tous ses œufs. Le propriétaire du cheval offre de payer les dommages et lui demande combien d'œufs elle avait apportés. Elle ne se souvient pas du nombre exact, mais si elle les avait groupés par paquets de $2, 3, 4, 5$ ou 6, il en serait resté chaque fois 1, alors qu'en les groupant par paquets de 7, il n'en serait resté aucun. Quel nombre minimum d'œufs pouvait-elle avoir ?

Réponses

4.9 1) $x \equiv 15 \mod 25$ 2) impossible
3) $x \equiv 20 \mod 47$ 4) impossible
5) $x \equiv 229 \mod 543$ 6) $x \equiv 123 \mod 215$
7) $x \equiv 94 \mod 215$

4.11 1) $\mathrm{M} = 1320$, $\mathrm{M}_1 = 120$, $\mathrm{M}_2 = 165$ et $\mathrm{M}_3 = 88$.
2) (a) $120 \equiv -1 \mod 11$ $x_1 = -1$ (b) $x_2 = -3$ (c) $x_3 = 7$
3) $x \equiv 14 \mod 1320$

4.12 $x \equiv 32 \mod 60$

4.13 $52 + 105\,k$ où $k \in \mathbb{Z}$

4.14 1 h 32

4.15 9131 jours = 25 ans et 6 jours

4.16 785 pièces d'or

4.17 1) $\mathrm{pgcd}(6, 15) \neq 1$ 3) $x \equiv 19 \mod 30$

4.18 $x = 80 + 84\,k$ où $k \in \mathbb{Z}$

4.19 107

4.20 $x = 226 + 792\,k$ où $k \in \mathbb{Z}$

4.21 301