Jacky Spareau et le cuisinier chinois

A. Devys

Niveau : Terminale
Difficulté : ★★★
Durée : 4 heures
Rubrique(s) : Théorie des nombres

La petite histoire...
À bord de la *Perle noire*, une bande de 17 pirates menée par Jacky Spareau s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident 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 6 d'entre eux sont tués. Après partage, le cuisinier recevrait alors 4 pièces.
Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

Les exercices qui suivent vont donner une méthode pour répondre à cette question de deux manières, l'une plus pratique, l'autre plus théorique. Le premier exercice détaille des résultats d'arithmétique qui seront utiles dans la suite. Le deuxième exercice répond à la question. Le troisième démontre le "théorème chinois".

Exercice 1 (Divisibilité et algorithme d'Euclide).

Définition. Soient a et b des entiers. On dit que a *divise* b s'il existe un entier s avec $as = b$ on dit aussi que a est un *diviseur* de b et que b est un *multiple* de a. On note $a \mid b$.

1. Vrai ou faux ?
- **a.** $3 \mid 12$;
- **b.** $8 \mid 12$;
- **c.** $0 \mid 1$;
- **d.** $0 \mid 0$;
- **e.** $1 \mid 0$.

Définition. Soient a et b deux entiers. On appelle $\mathrm{PGCD}(a, b)$ le plus grand entier naturel qui divise à la fois a et b. On dit que deux entiers a et b sont *premiers entre eux*, (ou que a est premier avec b ou encore que b est premier avec a) si le seul entier naturel qui divise à la fois a et b est 1, c'est-à-dire si leur PGCD vaut 1. On note parfois $a \wedge b = 1$.

Division euclidienne. Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}$, $b \neq 0$. Il existe un unique couple d'entiers relatifs (q, r) tel que :

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b.$$

2.a. On effectue la division euclidienne de a par b : $a = bq + r$. Montrer que alors $\text{PGCD}(a, b) = \text{PGCD}(b, r)$.
2.b. Que vaut $\text{PGCD}(r, 0)$? En déduire une méthode pour calculer le PGCD de deux entiers.
2.c. Calculer le PGCD de 4 147 et 10 672.

Identité de Bézout. Si a et b sont deux entiers, alors il existe deux entiers relatifs u et v tels que $au + bv = \text{PGCD}(a, b)$. Ce type d'égalité s'appelle *identité de Bézout*. En particulier, les entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers relatifs u et v tels que $au + bv = 1$.

3.a. Montrer que 11 et 17 sont premiers entre eux. Trouver deux entiers u et v tels que $11u + 17v = 1$.
3.b. Si a et b sont deux entiers premiers entre eux, existe-t-il une méthode qui fonctionne à tous les coups pour déterminer des entiers u et v tels que $au + bv = 1$? Existe-t-il un seul couple (u, v) qui fonctionne ?
3.c. Vérifier que s'il existe deux entiers relatifs u et v tels que $au+bv = 1$ alors a et b sont premiers entre eux.

4.a. Montrer que si a et b sont premiers entre eux et que $a \mid bc$ alors $a \mid c$. Ce résultat est connu sous le nom de théorème de Gauss.
4.b. Montrer que si a et b sont premiers entre eux et que a et c sont premiers entre eux, alors a est premier avec le produit bc.

5. Déterminer tous les entiers u et v tels que $11u + 17v = 1$.

Exercice 2.
Revenons au problème des pirates.
Appelons N le nombres de pièces constituant le trésor. On peut alors écrire que $N = 17p + 3$ avec p la quantité de pièces qu'aurait reçue chacun des pirates avant la querelle et $N = 11q + 4$ d'après le second partage. On a écrit ici les divisions euclidiennes de N successivement par 17 et 11. On dit que N est *congru à 3 modulo 17* et que N est congru à 4 modulo 11 et on parle de *congruences*. On écrit :

$$N \equiv 3 \mod 17 \quad \text{et} \quad N \equiv 4 \mod 11.$$

Définition. Soient a et b deux entiers relatifs, et n un entier naturel. On dit que a est congru à b modulo n et on note $a \equiv b \mod n$ si, et seulement si, n divise $a - b$.
Cela revient à dire que a et b ont le même reste dans la division euclidienne par n.

1.a. Si $a \equiv b \mod n$ et $b \equiv c \mod n$, montrer que $a \equiv c \mod n$. Cette propriété s'appelle la *transitivité*.
1.b. Montrer que si $a \equiv a' \mod n$ et $b \equiv b' \mod n$ alors $a + a' \equiv b + b' \mod n$ et $aa' \equiv bb' \mod n$.
1.c. On suppose que d divise n. Montrer que si $a \equiv b \mod n$ alors $a \equiv b \mod d$.
Remarque. La propriété de transitivité ajoutée à celle de *réflexivité* $\left(a \equiv a \mod n\right)$ et de *symétrie* $\left(\text{si } a \equiv b \mod n \text{ alors } b \equiv a \mod n\right)$ font de la relation binaire R définie sur $\mathbb{N}^2$ par aRb si et seulement si $a \equiv b \mod n$, une relation d'*équivalence* (Voir la fiche "Relations binaires").

2.a. Montrer que le problème des pirates se ramène au problème suivant : il existe p et q des entiers tels que

$$\begin{cases} N &= 3 + 17p \\ N &= 4 + 11q \end{cases}$$

Ce système s'appelle un système de congruences.
2.b. Résoudre ce système.

3. Existe-t-il toujours une solution à un système de congruences ?
a. Le système suivant a-t-il une solution ? Pourquoi ?

$$\begin{cases} N &\equiv 13 \mod 24 \\ N &\equiv 9 \mod 15 \end{cases}.$$

b. À quelle condition un système :

$$(\mathcal{S}) \begin{cases} N &\equiv a \mod m \\ N &\equiv b \mod n \end{cases}$$

où a, b, m, n sont des entiers relatifs donnés et où N est l'inconnue, a-t-il une solution ?

4. Avant que le cuisinier n'ait eu le temps d'empoisonner tout le monde, survient un naufrage et seuls 6 des pirates, le cuisinier et le trésor sont sauvés. On prévoit à nouveau de partager et le cuisinier obtiendrait 5 pièces d'or. Dans ce cas, quelle est la fortune minimale que peut espérer maintenant le cuisinier chinois s'il empoisonne tout le monde ?

Exercice 3 (Le théorème chinois (difficile)).
Le théorème des restes chinois nous dit :
Soient k entiers naturels $m_1, m_2, \ldots, m_k$ premiers entre eux deux à deux[1] ($k \geq 1$) et k entiers $s_1, s_2, \ldots, s_k$. On pose $M = m_1 m_2 \ldots m_k$. Le système de congruences :

$$\begin{cases} x & \equiv & s_1 & \mod m_1 \\ x & \equiv & s_2 & \mod m_2 \\ & \ldots & & \\ x & \equiv & s_k & \mod m_k \end{cases}$$

admet au moins une solution notée x et toute autre solution est de la forme $x + nM$ avec n entier. On dit que le système admet une unique solution x modulo M, c'est-à-dire que toute solution est congrue à x modulo M.

1.a. Pour tout $i \in \{1, \ldots, k\}$, on pose $M_i = \frac{M}{m_i} = m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_k$. On a bien M_i entier.
Montrer que, pour tout i, il existe deux entiers u_i et v_i tels que $M_i u_i + m_i v_i = 1$. En déduire que $u_i M_i s_i \equiv s_i \mod m_i$ et que pour tout $j \neq i$, $u_j M_j s_j \equiv 0 \mod m_i$.

1.b. En déduire que $x = u_1 M_1 s_1 + u_2 M_2 s_2 + \cdots + u_k M_k s_k$ est une solution du système de congruences.

2. Montrer que si x et y sont deux solutions du système, alors M divise $x - y$.

3. Vérifier que l'on a démontré le théorème chinois.

4. Reprenons le problème des pirates complet (jusqu'au naufrage), le système de congruences est le suivant :

$$\begin{cases} N & \equiv & 3 & \mod 17 \\ N & \equiv & 4 & \mod 11 \\ N & \equiv & 5 & \mod 6 \end{cases}.$$

Pouvez-vous retrouver la solution précédente en utilisant le théorème chinois ? Aviez-vous trouvé ce résultat avec la méthode précédente ?

1. On dit que les k entiers naturels $m_1, m_2, \ldots, m_k$, ($k \geq 1$) sont premiers entre eux deux à deux, si quels que soient deux entiers distincts pris dans la liste, leur PGCD vaut 1. Attention il faut distinguer premiers entre eux dans leur ensemble, c'est-à-dire le seul diviseur commun à tous les m_i est 1, et premier entre eux deux à deux. Par exemple les entiers $6, 4, 9$ sont premiers dans leur ensemble mais pas premiers deux à deux puisque par exemple 6 et 9 sont tous les deux divisibles par 3.

Exercice 4 (difficile).
Un casse-tête pour les professeurs [Proposé par G.H. Hardy et E. M. Wright dans "An introduction to the theory of Numbers", 1938].

« Six professeurs commencent une série de cours respectivement un lundi, un mardi, un mercredi, un jeudi, un vendredi et un samedi, et annoncent leur intention de donner leurs cours tous les deux, trois, quatre, un, six et cinq jours, respectivement. Le règlement de l'université interdit le cours le dimanche (de sorte que les cours du dimanche sont supprimés). Quand, pour la première fois, les six professeurs seront-ils forcés simultanément de supprimer leur cours ? »

Indications

Indications sur l'Exercice 1

2.a. On peut montrer que si d divise a et b alors d divise b et r et réciproquement, puis en déduire que l'ensemble des diviseurs communs de a et b est exactement l'ensemble des diviseurs communs de b et r. Conclure.

4.a. Écrire une relation de Bézout entre a et b.

4.b. Encore une fois, penser que deux nombres premiers vérifient une identité de Bézout.

Indications sur l'Exercice 2

2.b. Commencer par montrer que p et q ainsi définis sont solutions d'une équation de type Bézout que l'on pourra commencer par résoudre. On pourra utiliser les résultats de l'exercice 1.

Indications sur l'Exercice 3

1.a. Que dire de m_i et M_i ? Déduire de la relation de Bézout, que $M_i u_i \equiv 1 \mod m_i$.

Indications sur l'Exercice 4

Écrire le système de congruences et montrer qu'on peut réduire le nombre d'équations à 4. Attention, ensuite, les diviseurs ne sont pas tous premiers entre eux deux à deux.

Corrections

Correction de l'Exercice 1

1.a. Vrai : $3 \times 4 = 12$.
1.b. Faux. En effet, si c'était vrai, il existerait un entier k tel que $12 = 8k$. D'où $k = \frac{12}{8} = \frac{3}{2}$ et $\frac{3}{2}$ serait un entier !
1.c. Faux. En effet, si c'était vrai, il existerait un entier k tel que $1 = 0.k$, d'où $1 = 0$. Ce qui est absurde.
1.d. Vrai. En effet, 1 est un entier qui vérifie $0 = 1.0$, ce qui signifie que 0 divise 0.
Attention : s'il est vrai que $0 \mid 0$, on ne peut pas écrire $\frac{0}{0}$.
1.e. Vrai. Tous les entiers divisent zéro car pour tout n entier $0 = n \times 0$.

2.a. Soit d un diviseur de a et b. Alors il existe deux entiers s et t tels que $a = ds$ et $b = dt$ et donc $r = a - bq = ds - dtq = d(s - tq)$. Comme $s - tq$ est un entier, on en déduit que d divise r. Ainsi, d divise r et b.
Réciproquement, si d divise r et b, alors il existe des entiers s' et t' tels que $r = ds'$ et $b = dt'$ donc $a = bq + r = dt'q + ds' = d(t'q + s')$. Comme $t'q + s'$ est un entier, on en déduit que d divise a. Ainsi, d divise a et b.
L'ensemble des diviseurs communs de a et b est donc exactement l'ensemble des diviseurs communs à b et r et donc en prenant le plus grand d'entre eux, on obtient : $\text{PGCD}(a, b) = \text{PGCD}(b, r)$.
2.b. Tous les entiers divisent 0. De plus le plus grand diviseur de r est r lui-même ($r \geq 0$), donc $\text{PGCD}(r, 0) = r$.
Remarque : si r est de signe quelconque, $\text{PGCD}(r, 0) = |r|$.
Pour calculer le PGCD de a et b, ($a > b$), si $b = 0$ on a immédiatement $\text{PGCD}(a, b) = a$ ($a \geq 0$). Sinon, on réalise la division euclidienne de a par b, et $\text{PGCD}(a, b) = \text{PGCD}(b, r_1)$, avec $0 \leq r_1 < b$. Si $r_1 = 0$, on a $\text{PGCD}(a, b) = \text{PGCD}(b, r_1) = b$, sinon, à nouveau, on réalise la division euclidienne de b par r_1, et $\text{PGCD}(b, r_1) = \text{PGCD}(r_1, r_2)$, avec $0 \leq r_2 < r_1$.
Puisqu'à chaque fois le reste est positif et strictement plus petit que le diviseur qui est positif, le processus finit par s'arrêter. À la fin, on arrive à $r_p = 0$ avec $r_{p-1} > 0$ et le PGCD de a et b veut r_{p-1}, le dernier reste non nul. Ce procédé s'appelle *l'algorithme d'Euclide*.
2.c. On trouve 29. En effet, appliquons l'algorithme d'Euclide, $a = 10672$, $b = 4147$

$$\begin{array}{rcrcll} 10672 & = & 2 \times 4147 & + & 2378 & r_1 = 2378 \\ 4147 & = & 1 \times 2378 & + & 1769 & r_2 = 1769 \\ 2378 & = & 1 \times 1769 & + & 609 & r_3 = 609 \\ 1769 & = & 2 \times 609 & + & 551 & r_4 = 551 \\ 609 & = & 1 \times 551 & + & 58 & r_5 = 58 \\ 551 & = & 9 \times 58 & + & \boxed{29} & r_6 = 29 \\ 58 & = & 2 \times 29 & + & 0 & r_7 = 0 \end{array}$$

3.a. Les entiers 17 et 11 sont deux nombres premiers distincts, ils sont donc premiers entre eux et après quelques essais on trouve par exemple :

$$2 \times 17 - 3 \times 11 = 1.$$

3.b. Les entiers 17 et 11 sont premiers entre eux et donc leur PGCD vaut 1. On sait qu'en appliquant l'algorithme d'Euclide le dernier reste non nul est 1.

Dans la division euclidienne de a par b, on peut exprimer le reste r en fonction de a et b. En "remontant" l'algorithme d'Euclide, en exprimant à chaque fois le reste en fonction du diviseur et du dividende, on va pouvoir exprimer 1, le dernier reste non nul, en fonction de a et b.
Appliquons cette méthode à l'exemple ($a = 17$, $b = 11$) :

$$\begin{array}{rcrcl} 17 & = & 1\times 11 & + & 6 \\ 11 & = & 1\times 6 & + & 5 \\ 6 & = & 1\times 5 & + & 1 \end{array} \qquad \begin{array}{rcrcll} a & = & 1\times b & + & r_1, & \text{où } r_1 = 6 \\ b & = & 1\times r_1 & + & r_2, & \text{où } r_2 = 5 \\ r_1 & = & 1\times r_2 & + & r_3, & \text{où } r_3 = 1 \end{array} \qquad \begin{array}{rcrcl} r_1 & = & a & - & 1\times b \\ r_2 & = & b & - & 1\times r_1 \\ r_3 & = & r_1 & - & 1\times r_2 \end{array}$$

Dans les deux colonnes de gauche, on a écrit la suite des divisions euclidiennes et à droite, à chaque fois, on a exprimé le reste. On "remonte" maintenant l'algorithme :

$$\begin{array}{rcll} 1 = r_3 & = & r_1 - 1\times r_2 & \text{on réécrit } r_3 \text{ en fonction de } r_2 \text{ et } r_1 \\ & = & r_1 - 1\times (b - 1\times r_1) & \text{on remplace } r_2 \text{ en fonction de } r_1 \text{ et } b \\ & = & 2\times r_1 - 1\times b & \text{on simplifie} \\ & = & 2\times (a - 1\times b) - 1\times b & \text{on remplace } r_1 \text{ en fonction de } b \text{ et } a \\ & = & 2\times a - 3\times b & \text{on simplifie} \end{array}$$

Il n'y a pas d'unicité, par exemple :

$$1 = 2\times 17 - 3\times 11 = 13\times 17 - 20\times 11.$$

Il n'y a pas unicité du couple de Bézout. Si (u, v) est solution alors $(u', v') = (u + bk, v - ak)$ avec k entier vérifie également $au' + bv' = 1$. En effet :

$$au' + bv' = a(u + bk) + b(v - ak) = au + bv + abk - abk = au + bv = 1.$$

3.c. Supposons qu'il existe u et v tels que $au+bv = 1$. Soit d un diviseur positif commun à a et b. Alors il existe des entiers n et m tels que $a = dn$ et $b = dm$. Donc $au+bv = d(nu+mv)$. Comme $nu + mv$ est un entier, on en déduit que $d\big|au + bv$, c'est-à-dire que $d\big|1$. Il s'ensuit que $d = 1$ puisque d est positif. Donc 1 est le seul diviseur positif commun à a et b, de sorte que a et b sont premiers entre eux.

4.a. Comme a et b sont premiers entre eux, il existe deux entiers relatifs u et v tels que $au + bv = 1$. En multipliant par c, on obtient : $acu + bcv = c$. Comme de plus $a\big|bc$, il existe un entier s tel que $bc = as$ et donc $c = acu + asv = a(cu + sv)$. Comme $cu + sv$ est un entier, on en déduit que $a\big|c$.

4.b. Comme a et b sont premiers entre eux, ainsi que a et c, il existe deux couples d'entiers (u, v) et (u', v') tels que

$$\begin{cases} au + bv = 1 \\ au' + cv' = 1. \end{cases}$$

Multiplions la deuxième ligne par bv. On obtient : $abu'v + bcv'v = bv$. Or $bv = 1 - au$ donc $abu'v + bcv'v = 1 - au$ qui se réécrit $a(bu'v + u) + bc(v'v) = 1$. Comme $bu'v + u$ et $v'v$ sont des entiers, on en déduit, d'après le théorème de Bézout, que a et bc sont premiers entre eux.

5. D'après la question 3.a., on a donc $p = 2$ et $q = 3$ solution possible. Cherchons toutes les solutions possibles. Soient p et q deux entiers naturels solution de $17p - 11q = 1$.
On a donc

$$\begin{array}{rcrcl} 17p & - & 11q & = & 1 \\ 17\times 2 & - & 11\times 3 & = & 1 \end{array}$$

En soustrayant, on obtient :

$$17(p-2) = 11(q-3) \qquad (*)$$

Puisque 17 et 11 sont premiers entre eux, le théorème de Gauss nous dit que 11 divise $p-2$ donc qu'il existe un entier relatif k tel que $p-2 = 11k$ En injectant dans $(*)$ on obtient $q-3 = 17k$. Ainsi tous les couples (p,q) solutions sont de la forme $(2+11k, 3+17k)$, où $k \in \mathbb{Z}$.

Il reste à montrer que tous les couples $(2+11k, 3+17k)$, où $k \in \mathbb{Z}$ sont effectivement solutions.

Or : $17(2+11k) - 11(3+17k) = 34 + 17 \times 11k - 33 - 11 \times 17k = 1$.

Il s'ensuit que les solutions de l'équation $17p - 11q = 1$ sont les couples $(2+11k, 3+17k)$, où $k \in \mathbb{Z}$. Finalement pour N on trouve $N = 3 + 17(2+11k) = 37 + 17 \times 11 \times k$.

□

Correction de l'Exercice 2

1.a. Si $a \equiv b \mod n$ alors il existe un entier q tel que $a = qn+b$. Or on a aussi $b \equiv c \mod n$ donc il existe un entier q' tel que $b = q'n + c$. On remplace b par cette expression dans celle donnant a et on obtient $a = qn + q'n + c = (q+q')n + c$ ce qui signifie, puisque $q+q'$ est un entier, que $a \equiv c \mod n$.

1.b. De même, si $a \equiv a' \mod n$ et $b \equiv b' \mod n$, alors il existe deux entiers p et q tels que $a = pn+a'$ et $b = qn+b'$. En additionnant ces deux égalités, on obtient $a+b = (p+q)n+a'+b'$ ce qui signifie, puisque $p+q$ est un entier, $a+b \equiv a'+b' \mod n$.

En multipliant ces inégalités, on obtient $ab = (pn+a')(qn+b') = n(pqn+pb'+qa') + a'b'$. Comme $pqn+pb'+qa'$ est un entier, on en déduit : $ab \equiv a'b' \mod n$.

1.c. Comme d divise n, il existe un entier q tel que $n = dq$. Comme de plus, $a \equiv b \mod n$, il existe un entier p tel que $a = pn + b$, d'où $a = dpq + b$. Comme pq est un entier, on en déduit : $a \equiv b \mod d$.

2.a. Revenons à nos pirates et à notre cuisinier chinois. On cherche donc le nombre de pièces d'or N solution du système de congruences :

$$\begin{cases} N \equiv 3 \mod 17 \\ N \equiv 4 \mod 11 \end{cases}$$

C'est-à-dire qu'il existe des entiers p et q tels que :

$$\begin{cases} N = 3 + 17p \\ N = 4 + 11q \end{cases}.$$

2.b. En soustrayant la première ligne à la deuxième, on obtient $17p - 11q = 1$. C'est une relation de Bézout entre les deux entiers premiers 17 et 11. On remarque que, comme $N = 3 + 17p = 4 + 11q$ est un entier naturel, p et q sont des entiers naturels. On a vu à l'exercice 1 que les solutions de l'équation $17p - 11q = 1$ sont les couples $(2+11k, 3+17k)$, où $k \in \mathbb{Z}$. Il ne faut retenir ici que les solutions positives, soit les couples $(2+11k, 3+17k)$, où $k \in \mathbb{N}$.

Finalement pour N on trouve $N = 3 + 17(2+11k) = 37 + 17 \times 11 \times k$. La plus petite solution possible est $N = 37$ $(k = 0)$.

3.a. Il n'y a pas de solution au système proposé. En effet, selon la seconde congruence, la solution devrait être un multiple de 3 mais la première ligne implique le contraire. Cet exemple de système est dû à Euler.

3.b. Pour trouver la condition sous laquelle $(\mathcal{S})$ a une solution, on remarque que dire qu'il existe une solution à $(\mathcal{S})$ est équivalent à dire :

$$\text{il existe } (p,q)\in\mathbb{Z}^2 \text{ tel que } \left\{\begin{array}{rcrcr} N & = & a & + & mp \\ N & = & b & + & nq \end{array}\right. .$$

On en déduit alors l'équation

$$mp - nq = b - a \qquad (E)$$

Réciproquement si p et q sont deux entiers relatifs solutions de (E) alors $a + mp = b + nq$ de sorte que si on a $N = a + mp(= b + nq)$ alors N est une solution de $(\mathcal{S})$.
L'existence d'une solution N de $(\mathcal{S})$ se ramène donc à l'existence d'un couple (p, q) d'entiers relatifs solution de (E).
L'équation (E) s'appelle une équation *diophantienne*. Elle n'admet de solution que si $b - a$ est un multiple du PGCD de m et n.
En effet, soit $d = \text{PGCD}(m, n)$. Alors, il existe des entiers m' et n' premiers entre eux tels que $m = dm'$ et $n = dn'$. Le théorème de Bézout assure qu'il existe deux entiers u et v tels que $m'u+n'v = 1$ puis en multipliant par d : $mu+nv = d$. Si $b-a$ est un multiple de d, il s'écrit $b - a = dk$ où k est un entier. Il reste à multiplier par k : $m(ku) - n(-kv) = dk = b - a$ donc $b - a$ est un multiple de d. Réciproquement, si (p, q) est une solution de (E) alors $mp - nq = b - a$ alors $d \mid mp$ et $d \mid nq$ donc $d \mid mp - nq$ et $d \mid b - a$.

4. Dans ce cas, le nouveau système s'écrit

$$\left\{\begin{array}{rcl} N & = & 3 + 17p \\ N & = & 4 + 11q \\ N & = & 5 + 6r \end{array}\right. .$$

On sait déjà que si N satisfait aux deux premières égalités, alors

$$N = 37 + 11 \times 17k = 37 + 187k.$$

$$\left\{\begin{array}{rcl} N & = & 37 + 187k \\ N & = & 5 + 6r \end{array}\right.$$

On applique la même méthode. Les entiers naturels k et r vérifient l'identité

$$32 = 6r - 187k.$$

On résout d'abord l'identité de Bézout $6r' - 187k' = 1$ car 6 et 187 sont premiers entre eux. On a $187 = 31 \times 6 + 1$ donc $k' = -1$ et $r' = -31$ conviennent.

$$1 = 187 \times 1 - 6 \times 31.$$

En multipliant par 32, on obtient $(r, k) = (-992, -32)$ solution de $32 = 6r - 187k$. Pour trouver toutes les solutions on écrit :

$$\begin{array}{rcrcl} 32 & = & -187 \times (-32) & - & 6 \times 992 \\ 32 & = & -187 \times k & + & 6 \times r \end{array}$$

ce qui donne $187(32+k) = 6(992+r)$. Comme précédemment, comme 6 et 187 sont premiers entre eux, le théorème de Gauss entraîne l'existence d'un entier relatif ℓ tel que $32 + k = 6\ell$ et donc $992 + r = 187\ell$, c'est-à-dire $(k, r) = (-32 + 6\ell, -992 + 187\ell)$. Ce que l'on peut

réécrire, pour travailler avec des entiers plus petits : $(k, r) = (4 + 6\ell', 130 + 187\ell')$, où on a posé $\ell' = \ell - 6$ (en fait, ℓ' est un entier naturel car k est un entier naturel). Il reste à montrer que les couples de la forme $(4 + 6\ell', 130 + 187\ell')$, où $\ell' \in \mathbb{N}$, sont effectivement solution : $6r - 187k = 6(130 + 187\ell') - 187(4 + 6\ell') = 6 \times 130 - 187 \times 4 = 780 - 748 = 32$.
On remplace dans la dernière ligne du système initial et on obtient :

$$N = 5 + 6(130 + 187\ell') = 785 + 1122\ell'.$$

Les solutions sont les entiers naturels $N \equiv 785 \mod 1122$. Le plus petit entier vérifiant cette condition est 785. C'est la fortune minimale que peut espérer le cuisinier.

□

Correction de l'Exercice 3

1.a. Comme pour tout $j \neq i$, m_i et m_j sont premiers entre eux, les entiers m_i et M_i sont alors aussi premiers entre eux. En effet, s'il existait un nombre premier d divisant à la fois m_i et M_i, alors d diviserait aussi au moins l'un des entiers m_j pour $j \neq i$, de sorte que m_i et m_j ne pourraient être premiers entre eux.
D'après le théorème de Bézout, il existe donc deux entiers u_i et v_i tels que $M_i u_i + m_i v_i = 1$, c'est-à-dire $M_i u_i \equiv 1 \mod m_i$. On en déduit $u_i M_i s_i \equiv s_i \mod m_i$. De plus pour $j \neq i$, $m_i \mid M_j$ car M_j est le produit des m_k sauf pour $k = j$ donc contient le facteur m_i. On en déduit que $M_j \equiv 0 \mod m_i$ et $u_j M_j s_j \equiv 0 \mod m_i$.
1.b. Posons $x = u_1 M_1 s_1 + u_2 M_2 s_2 + \cdots + u_k M_k s_k$. Alors $x \equiv s_i \mod m_i$.
Cela est vrai pour tous les i compris entre 1 et k donc x est solution du système. On a montré l'existence d'une solution au système de congruences.

2. Puisque x et y sont solutions du système de congruences, pour tout i entre 1 et k on a $x - y \equiv 0 \mod m_i$, c'est-à-dire que m_i divise $x - y$. Comme les m_i sont premiers entre eux deux à deux, on en déduit, par le théorème de Gauss, que leur produit M divise $x - y$.
On dit que le système admet une unique solution modulo M.

3. On a montré dans les deux questions précédentes, d'une part que le système de congruences admet une solution

$$x = u_1 M_1 s_1 + u_2 M_2 s_2 + \cdots + u_k M_k s_k,$$

et d'autre part que toute solution lui est égale à un multiple de M près.
En résumé, on a montré que les solutions du système sont les entiers $u_1 M_1 s_1 + \cdots + u_k M_k s_k + nM$ avec n entier. Et le théorème chinois est démontré.

4. On a donc ici : $s_1 = 3$, $s_2 = 4$, $s_3 = 5$, $m_1 = 17$, $m_2 = 11$, $m_3 = 6$. Et on pose :
$M = m_1\, m_2\, m_3 = 17 \times 11 \times 6 = 1122$,
$M_1 = 11 \times 6 = 66$, $M_2 = 17 \times 6 = 102$, $M_3 = 17 \times 11 = 187$.
Puisque 17, 11 et 6 sont premiers entre eux deux à deux, le théorème chinois nous dit que l'on peut chercher les solutions sous la forme :

$$\begin{aligned} N &= u_1 M_1 s_1 + u_2 M_2 s_2 + u_3 M_3 s_3 + nM \\ &= u_1 \times 11 \times 6 \times 3 + u_2 \times 17 \times 6 \times 4 + u_3 \times 17 \times 11 \times 5 + n \times 17 \times 11 \times 6. \end{aligned}$$

Reste à trouver les u_i. Pour u_1 on cherche une relation de Bézout entre M_1 et m_1 à l'aide de l'algorithme d'Euclide.

$$\begin{array}{rclcl} 66 &=& 3 \times 17 &+& 15 \\ 17 &=& 1 \times 15 &+& 2 \\ 15 &=& 7 \times 2 &+& 1 \end{array} \qquad \begin{array}{rclcll} M_1 &=& 3 \times m_1 &+& r_1 & \text{où } r_1 = 15 \\ m_1 &=& 1 \times r_1 &+& r_2 & \text{où } r_2 = 2 \\ r_1 &=& 7 \times r_2 &+& r_3 & \text{où } r_3 = 1. \end{array}$$

Puis en "remontant", on obtient :

$$\begin{array}{rcll} 1 = r_3 & = & r_1 - 7 \times r_2 & \text{on écrit } r_3 = 1 \text{ en fonction de } r_1 \text{ et } r_2 \\ & = & r_1 - 7 \times (m_1 - 1 \times r_1) & \text{on remplace } r_2 \text{ en fonction de } m_1 \text{ et } r_1 \\ & = & 8 \times r_1 - 7 \times m_1 & \text{on simplifie} \\ & = & 8 \times (M_1 - 3 \times m_1) - 7 \times m_1 & \text{on remplace } r_1 \text{ en fonction de } M_1 \text{ et } m_1 \\ & = & 8 \times M_1 - 31 \times m_1 & \text{on simplifie} \end{array}$$

et $u_1 = 8$ convient.
De la même façon, on trouve $u_2 = 4$ et $u_3 = 1$. Les solutions du système sont donc :

$$N = 8 \times 198 + 4 \times 408 + 1 \times 935 + n \times 1122 = 4151 + 1122\,n, \qquad n \in \mathbb{Z}.$$

Le nombre 4151 est donc une solution possible pour notre cuisinier mais ce n'est pas la plus petite. Il suffit maintenant d'effectuer la division euclidienne de 4151 par 1122. On trouve 785 comme reste, qui est le nombre minimal de pièces que peut espérer notre cuisinier. On peut aussi voir que $N \geq 0$ si et seulement si $n \geq -3$, et que, pour $n = -3$, on obtient la plus petite solution positive.

□

Correction de l'Exercice 4
En numérotant les jours de la semaine de 1 à 7 avec 1 pour lundi et 7 pour dimanche, le problème est équivalent au système de congruences suivant :

$$\begin{array}{rcll} x & \equiv & 1 \mod 2 & (L_1) \\ x & \equiv & 2 \mod 3 & (L_2) \\ x & \equiv & 3 \mod 4 & (L_3) \\ x & \equiv & 4 \mod 1 & (L_4) \\ x & \equiv & 5 \mod 6 & (L_5) \\ x & \equiv & 6 \mod 5 & (L_6) \\ x & \equiv & 0 \mod 7 & (L_7) \end{array}$$

On peut remarquer que si $x \equiv 3 \mod 4$ alors $x \equiv 1 \mod 2$. En effet, s'il existe un entier k tel que $x = 4k + 3$, alors $x = 2(2k + 1) + 1$. On peut donc retirer la première ligne du système. De plus, $x \equiv 4 \mod 1$ est toujours vrai. On peut alors retirer cette ligne également. Enfin, on remarque que si $x \equiv 5 \mod 6$ alors il existe un entier k tel que $x = 6k + 5$ de sorte que $x = 3(2k + 1) + 2$ et donc $x \equiv 2 \mod 3$. On peut donc aussi retirer la seconde ligne. Enfin, écrire $x \equiv 6 \mod 5$ signifie qu'il existe un entier k tel que $x = 5k + 6$, mais comme $6 = 1 \times 5 + 1$, cela s'écrit encore $x = 5(k + 1) + 1$, et l'avant dernière ligne équivaut à $x \equiv 1 \mod 5$.
Finalement, on est ramené au système :

$$(S) \begin{cases} x \equiv 3 \mod 4 \\ x \equiv 5 \mod 6 \\ x \equiv 1 \mod 5 \\ x \equiv 0 \mod 7 \end{cases}$$

On résout d'abord le sous-système (S') $\begin{cases} x \equiv 5 \mod 6 \\ x \equiv 1 \mod 5 \\ x \equiv 0 \mod 7 \end{cases}$.

Les nombres 6, 5 et 7 sont premiers entre eux deux à deux, on peut donc appliquer la méthode du théorème chinois. On a : $M = 6 \times 5 \times 7 = 210$.

$M_1 = \frac{M}{6} = 35$	$m_1 = 6$	$s_1 = -1$	$6 \times 6 - 35 = 1 = 3 \times m_1 - M_1$	$u_1 = -1$
$M_2 = \frac{M}{5} = 42$	$m_2 = 5$	$s_2 = 1$	$17 \times 5 - 2 \times 42 = 1 = 17 \times m_2 - M_2$	$u_2 = -2$
$M_3 = \frac{M}{7} = 30$	$m_3 = 7$	$s_3 = 0$	(*)	(*)

(*) : puisque s_3 est nul, inutile de calculer u_3, mais par application de l'algorithme d'Euclide (ou par une habitude des calculs) on trouverait $1 = 4 \times 30 - 17 \times 7 = 4 \times M_3 - 17 \times m_3$ et donc $u_3 = 4$.
Finalement, il existe un entier k tel que :

$$x = u_1 M_1 s_1 + u_2 M_2 s_2 + u_3 M_3 s_3 + k \times M = -1 \times 35 \times (-1) + (-1) \times 42 \times 1 + 210 \times k,$$

c'est-à-dire $x = -49 + 210 \times k$, soit $x \equiv -49 \mod 210$.
On remplace (S') par cette équation et on obtient le système :

$$\begin{cases} x & \equiv & 3 & \mod 4 \\ x & \equiv & -49 & \mod 210. \end{cases}$$

Les entiers 4 et 210 ne sont pas premiers entre eux, leur PGCD vaut 2. Mais $3 - (-49) = 52$ est un multiple de 2 donc comme on l'a vu à l'exercice 2, ce système a une solution.

$$(S) \Leftrightarrow \begin{cases} x & = & 4p + 3 \\ x & = & 210q - 49 \end{cases}$$

$$\begin{array}{rrcl} \Rightarrow & 210q - 4p & = & 52 \\ \Rightarrow & 105q - 2p & = & 1. \end{array}$$

Les entiers $p_0 = 92$ et $q_0 = 2$ conviennent : $105 \times 2 - 2 \times 92 = 26 = 105q - 2p$.
On obtient donc $105(q-2) = 2(p-92)$. Comme 105 et 2 sont premiers entre eux, d'après le théorème de Gauss, il existe un entier k tel que $q = 2 + 2k$ et $p = 92 + 105k$. Finalement x s'écrit $x = 210(2 + 2k) - 49 = 371 + 420k$.
Comme on a procédé a priori par implications successives et non par équivalences, il faut vérifier que les nombres de la forme $x = 371 + 420 \times k$ où $k \in \mathbb{Z}$ sont effectivement solutions du système (S). Or :

$$\begin{array}{lll} 371 + 420 \times k = 4\,(105k + 92) + 3 & \text{d'où } x \equiv 3 & \mod 4\ ; \\ 371 + 420 \times k = 6\,(70k + 61) + 5 & \text{d'où } x \equiv 5 & \mod 6\ ; \\ 371 + 420 \times k = 5\,(84k + 74) + 1 & \text{d'où } x \equiv 1 & \mod 5\ ; \\ 371 + 420 \times k = 7\,(60k + 53) & \text{d'où } x \equiv 0 & \mod 7. \end{array}$$

Les solutions du système (S) sont donc bien les nombres de la forme $371 + 420 \times k$ où $k \in \mathbb{Z}$.
La réponse au problème de départ est donc 371 jours. L'année scolaire sera terminée bien avant que cela n'arrive !

□

