Contrôle Continu - Corrigé

23/10/24

Exercice 1 de rechauffement.

(a) Définir quand un entier a divise un entier b.

(b) Soient $a, b, n \in \mathbb{Z}$. Montrer que si n divise a et n divise b, alors n divise $ax + by$, pour tout $x, y \in \mathbb{Z}$.

Solution

(a) [1 point] *Soient $a, b \in \mathbb{Z}$. Un entier a divise un entier b s'il existe $k \in \mathbb{Z}$ tel que $b = ka$.*

(b) [2 points] *Soient $a, b, n \in \mathbb{Z}$. Si n divise a et n divise b, alors il existe $h, k \in \mathbb{Z}$ tels que $a = kn$ et $b = hn$. Donc on a*

$$ax + by = knx + hny = n(kx + hy),$$

ce qui implique que n divise $ax + by$.

Exercice 2.

(a) Définir le plus grand commun diviseur (pgcd) de deux entiers a et b.

(b) À l'aide de l'algorithme d'Euclide étendu, calculer le pgcd entre 13 et 23, et une identité de Bézout.

(c) Déterminer, s'ils existent, l'inverse de 13 modulo 23 e l'inverse de 23 modulo 13.

(d) Déterminer toutes les solutions dans $\mathbb{Z}$ de la congruence

$$91x \equiv 14 \pmod{161}.$$

(e) Dans cet ensemble de solutions, déterminer celles qui sont congruentes à 2 modulo 5.

Solution

(a) [1 point] *Un entier $d \in \mathbb{Z}_{\geq 0}$ est dit le plus grand commun diviseurs de $a, b \in \mathbb{Z}$ si :*

- *$d \mid a$ et $d \mid b$;*
- *si $d' \in \mathbb{Z}$ est tel que $d' \mid a$ et $d' \mid b$, alors $d' \mid d$.*

(b) [2 points] *On applique l'algorithme d'Euclide étentu pour déterminer le pgcd de 13 et 23 et une idéntité de Bézout :*

$$\begin{aligned} 23 &= 13 \cdot 1 + 10 \\ 13 &= 10 \cdot 1 + 3 \\ 10 &= 3 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

Donc $\text{pgcd}(23, 13) = 1$. *En remontant les égalités on obtient :*

$$\begin{aligned} 1 &= 10 - 3 \cdot 3 = \\ &= 10 - (13 - 10 \cdot 1) \cdot 3 = \\ &= 13 \cdot (-3) + 10 \cdot 4 = \\ &= 13 \cdot (-3) + (23 - 13 \cdot 1) \cdot 4 = \\ &= 13 \cdot (-7) + 23 \cdot 4. \end{aligned}$$

Donc une idéntité de Bézout est :

$$1 = 13 \cdot (-7) + 23 \cdot 4.$$

(c) [1 point] *Tout d'abord l'inverse de 13 modulo 23 et l'inverse de 23 modulo 13 existent, car pgcd(13,23)=1. Pour les déterminer, on réduit l'idéntité de Bézout trouvée modulo 23 et modulo 13 :*

$$\textit{Modulo 23 :} \qquad 1 \equiv 13 \cdot (-7) \pmod{23}.$$

Donc -7 ($\equiv 16 \pmod{23}$*) est l'inverse de 13 modulo 23.*

$$\textit{Modulo 13 :} \qquad 1 \equiv 23 \cdot 4 \pmod{13}.$$

Donc 4 est l'inverse de 23 modulo 13.

(d) [1 point] *On rappelle que la congruence*

$$91x \equiv 14 \pmod{161}$$

a une solution si et seulement si $\text{pgcd}(91, 161) \mid 14$. *Avec l'algorithme d'Euclide on trouve que :*

$$\begin{aligned} 161 &= 91 \cdot 1 + 70 \\ 91 &= 70 \cdot 1 + 21 \\ 70 &= 21 \cdot 3 + 7 \\ 21 &= 7 \cdot 3 + 0, \end{aligned}$$

donc $\text{pgcd}(91, 161) = 7$ *et* $7 \mid 14$. *En semplifiant la congruence on obtient :*

$$\frac{91}{7}x \equiv \frac{14}{7} \left(\text{mod } \frac{161}{7} \right)$$

c'est-à-dire :

$$13x \equiv 2 \pmod{23}.$$

En multipliant les deux membres par 16, l'inverse de 13 modulo 23, on a :

$$\begin{aligned} 16 \cdot 13x &\equiv 16 \cdot 2 \pmod{23} \\ x &\equiv 9 \pmod{23}. \end{aligned}$$

En conclusion les solutions de la congruence $91x \equiv 14 \pmod{161}$ *sont données par l'ensemble :*

$$S_1 = \{9 + 23k : k \in \mathbb{Z}\}$$

(e) [1 point] *Déterminons* $k \in \mathbb{Z}$ *tel que* $9 + 23k \equiv 2 \pmod{5}$. *On a :*

$$\begin{aligned} 9 + 23k &\equiv 2 \pmod{5} \\ 3k &\equiv 3 \pmod{5} \\ k &\equiv 1 \pmod{5}. \end{aligned}$$

Donc $k = 1 + 5h$, $h \in \mathbb{Z}$. *On obtient que le sous-ensemble de* S_1 *dont les éléments sont congru à 2 modulo 5 est :*

$$S_2 = \{9 + 23(1 + 5h) : h \in \mathbb{Z}\} = \{32 + 115h : h \in \mathbb{Z}\}.$$

Exercice 3. Le théorème chinois des restes est ainsi nommé parce que sa première formulation remonte à un texte du III ou IV siècle après J.-C. du mathématicien et astronome chinois Sun Zi. La première preuve générale et constructive de ce théorème est apparu beaucoup plus tard, dans l'ouvrage *Shùshū Jiŭzhāng* (« Traité mathématique en neuf chapitres ») du mathématicien chinois Qin Jiushao. On sait que ce livre a été publié dans le XIIIe siècle et que l'année de publication n satisfait les conditions suivantes :

- n est impair.
- le reste de la division de n par 9 est 5 ;
- $11 \mid (2n + 3)$;

Dans quelle année le livre *Shùshū Jiŭzhāng* a-t-il été publié ?

Solution [4 points]

L'année de publication du livre Shùshū Jiŭzhāng *est un entier* $a \in [1200, 1299]$ *qui est solution du système de congruences suivant :*

$$\begin{cases} n \equiv 1 \pmod{2} \\ n \equiv 5 \pmod{9} \\ 2n + 3 \equiv 0 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} n \equiv 1 \pmod{2} \\ n \equiv 5 \pmod{9} \\ n \equiv 4 \pmod{11} \end{cases}$$

Puisque $2, 9$ *et* 11 *sont premiers entre eux deux à deux, on peut utiliser le théorème des restes chinois pour calculer les solutions du système. On a :*

- $n_1 = 1, n_2 = 9, n_3 = 11$.
- $N = 2 \cdot 9 \cdot 11 = 198$.
- $N_1 = 9 \cdot 11 = 99, N_2 = 2 \cdot 11 = 22, N_3 = 2 \cdot 9 = 18$.
- *On détermine* U_1, U_2, U_3 *tels que* $N_i \cdot U_i \equiv 1 \pmod{n_i}$. *On obtient* $U_1 = 1, U_2 = 7$ *and* $U_3 = 8$.

Donc $n \equiv 1 \cdot 99 \cdot 1 + 5 \cdot 22 \cdot 7 + 4 \cdot 18 \cdot 8 \pmod{198} \equiv 59 \pmod{198}$.

Il est simple de voir qu'il y a un unique entier congru à 59 modulo 198 dans l'intervalle $[1200, 1299]$ *: c'est 1247 (*$= 59+198\cdot 6$*), qui est donc l'année de pubblication du livre.*

Exercice 4. On rappelle que si p est un nombre premier et $p \mid ab$, avec $a, b \in \mathbb{Z}$, alors $p \mid a$ ou $p \mid b$. De plus, on utilise la notation standard pour la factorielle $n! := n(n-1)(n-2)\cdots 1$.

(a) Pour chaque élément de $(\mathbb{Z}/11\mathbb{Z})^\times$, déterminer son inverse. Une fois tous les inverses déterminés, expliquez pourquoi, il est possible de calculer 10! modulo 11 sans effectuer aucun produit supplémentaire.

(b) Soit $a \in \mathbb{Z}$ et soit p un nombre premier. Montrer que $a^2 \equiv 1 \pmod{p}$ si et seulement si $a \equiv 1 \pmod{p}$ ou $a \equiv p-1 \pmod{p}$.

(c) En déduire que $(p-2)! \equiv 1 \pmod{p}$ et conclure que $(p-1)! \equiv -1 \pmod{p}$.

Vous venez alors de démontrer le *Théorème de Wilson* :

Si p *est un nombre premier, alors* $(p-1)! \equiv -1 \pmod{p}$.

Solution

(a) [1,5 points] *On a :*

$$(\mathbb{Z}/11\mathbb{Z})^\times = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

et $1^{-1} = 1$, $2^{-1} = 6$, $3^{-1} = 4$, $4^{-1} = 3$, $5^{-1} = 9$, $6^{-1} = 2$, $7^{-1} = 8$, $8^{-1} = 7$, $9^{-1} = 5$, $10^{-1} = 10$.
En utilisant la commutativité et l'associativité du produit, on peut réécrire 10! *de la façon suivante.*

$$\begin{aligned} 10! &= 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = \\ &= 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 \equiv \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 10 \pmod{11} \equiv \\ &\equiv 10 \pmod{11} \equiv -1 \pmod{11} \end{aligned}$$

On a donc calculé 10! *sans effectuer aucun produit supplémentaire.*

(b) [2 points] *Il est clair que si* $a \equiv 1 \pmod{p}$ *ou* $a \equiv p-1 \pmod{p}$ *alors* $a^2 \equiv 1 \pmod{p}$ *(*$(p-1)^2 = p^2 - 2p + 1 \equiv 1 \pmod{p}$*.).*
Pour l'implication inverse, si $a^2 \equiv 1 \pmod{p}$*, alors* $p \mid a^2 - 1 = (a-1)(a+1)$*. Mais, puisque* p *est premier, cela implique que* $p \mid a-1$ *ou* $p \mid a+1$*, ou, équivalemment,* $a \equiv 1 \pmod{p}$ *ou* $a \equiv -1 \equiv p-1 \pmod{p}$.

(c) [1,5 points] *La congruence est trivialement vérifiée pour* $p = 2, 3$*. Soit donc* $p > 3$*. D'après (b), chaque élément de l'ensemble* $\{2, 3, \ldots, p-2\}$ *possède un unique inverse distinct dans cet ensemble. Par conséquent, les* $p-3$ *éléments de* $\{2, 3, \ldots, p-2\}$ *peuvent être appariés deux à deux en couples d'inverses. Ainsi, nous obtenons :*

$$(p-2)! = (p-2)(p-3)\cdots 3 \cdot 2 \equiv 1 \cdots 1 \equiv 1 \pmod{p}.$$

En multipliant les deux membres par $p-1$*, on a :*

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}.$$