Contrôle Continu - Corrigé
21/10/25

Exercice 1.

(a) À l'aide de l'algorithme d'Euclide étendu, calculer le pgcd entre 161 et 133, et une identité de Bézout.

(b) Déterminer, s'ils existent, l'inverse de 161 modulo 133 et l'inverse de 133 modulo 161.

(c) Donner une condition nécessaire et suffisante sur $a \in \mathbb{Z}$ pour que la congruence

$$21x \equiv a \pmod{133}$$

admette une solution dans $\mathbb{Z}$. Puis résoudre cette congruence pour la plus petite valeur strictement positive de a satisfaisant cette condition.

Solution

(a) [2 points] *On applique l'algorithme d'Euclide étentu pour déterminer le pgcd de 161 et 133 et une idéntité de Bézout :*

$$\begin{aligned} 161 &= 133 \cdot 1 + 28 \\ 133 &= 28 \cdot 4 + 21 \\ 28 &= 21 \cdot 1 + 7. \\ 21 &= 7 \cdot 3 + 0. \end{aligned}$$

Donc $\mathrm{pgcd}(161, 133) = 7$*. En remontant les égalités on obtient :*

$$\begin{aligned} 7 &= 28 - 21 \\ &= 28 - (133 - 28 \cdot 4) \\ &= 28 \cdot 5 - 133 \\ &= (161 - 133) \cdot 5 - 133 \\ &= 161 \cdot 5 + 133 \cdot (-6). \end{aligned}$$

Donc une idéntité de Bézout est :

$$7 = 161 \cdot 5 + 133 \cdot (-6).$$

(b) [1 point] *L'inverse de 161 modulo 133 et l'inverse de 133 modulo 161 n'existent pas car* 161 *et* 133 *ne sont pas premiers entre eux (*$\mathrm{pgcd}(161, 133) = 7$*).*

(c) [2 points] *La congruence*

$$21x \equiv a \pmod{133}$$

admet une solution dans $\mathbb{Z}$ *si et seulement si* $\operatorname{pgcd}(21, 133) \mid a$, *c'est-à-dire si et seulement si* $a \equiv 0 \pmod 7$. *Pour* $a = 7$ *(la plus petite valeur strictement positive de a satisfaisant cette condition) on a la congruence*

$$21x \equiv 7 \pmod{133}.$$

En simplifiant on obtient :

$$\frac{21}{7}x \equiv \frac{7}{7}\left(\operatorname{mod} \frac{133}{7}\right)$$

c'est-à-dire :

$$3x \equiv 1 \pmod{19}.$$

Enfin, on multiplie les deux membres par 13, l'inverse de 3 modulo 19 :

$$\begin{gathered} 13 \cdot 3x \equiv 13 \pmod{19} \\ \Updownarrow \\ x \equiv 13 \pmod{19}. \end{gathered}$$

En conclusion les solutions de la congruence $21x \equiv 7 \pmod{133}$ *sont données par l'ensemble :*

$$S_1 = \{13 + 19k : k \in \mathbb{Z}\}$$

Exercice 2.

(a) Soient $a, b, m, n \in \mathbb{Z}$, avec $m, n > 0$ et $m \mid n$. Montrer que si $a \equiv b \pmod n$, alors $a \equiv b \pmod m$.

(b) Résoudre dans $\mathbb{Z}$ le système de congruences suivant :

$$\begin{cases} 2x \equiv 0 \pmod 3 \\ 4x \equiv -1 \pmod 5 \\ 7x \equiv 5 \pmod{11} \end{cases}$$

(c) Déterminer, s'il en existe, toutes les valeurs du paramètre t, avec $0 \leq t \leq 14$, pour lesquelles le système

$$\begin{cases} 2x \equiv 0 \pmod 3 \\ 4x \equiv -1 \pmod 5 \\ 7x \equiv 5 \pmod{11} \\ 8x \equiv t \pmod{15} \end{cases}$$

admet une solution. Pour chacune de ces valeurs de t, déterminer l'ensemble des solutions du système dans $\mathbb{Z}$.

Solution

(a) [1 points] *Soient* $a, b, m, n \in \mathbb{Z}$, *avec* $m, n > 0$ *et* $m \mid n$. *Alors, il existe* $k \in \mathbb{Z}$ *tel que* $n = km$. *Supposons que* $a \equiv b \pmod{n}$. *Il existe alors un entier* $h \in \mathbb{Z}$ *tel que* $a - b = hn = hkm$. *On en déduit que* $a \equiv b \pmod{m}$.

(b) [2,5 points]

$$\begin{cases} 2x \equiv 0 \pmod 3 \\ 4x \equiv -1 \pmod 5 \\ 7x \equiv 5 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 7 \pmod{11} \end{cases}$$

Puisque $3, 5$ *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 :*

- $n_1 = 3, n_2 = 5, n_3 = 11$.
- $N = 3 \cdot 5 \cdot 11 = 165$.
- $N_1 = 5 \cdot 11 = 55, N_2 = 3 \cdot 11 = 33, N_3 = 3 \cdot 5 = 15$.
- *On détermine* U_1, U_2, U_3 *tels que* $N_i \cdot U_i \equiv 1 \pmod{n_i}$. *On obtient* $U_1 = 1, U_2 = 2$ *and* $U_3 = 3$.

Donc $x \equiv 0 \cdot 55 \cdot 1 + 1 \cdot 33 \cdot 2 + 7 \cdot 15 \cdot 3 \pmod{165} \equiv 51 \pmod{165}$ *et l'ensemble des solutions est* $\{51 + 165k \mid k \in \mathbb{Z}\}$.

(c) [1,5 points] *Tout d'abord on a*

$$\begin{cases} 2x \equiv 0 \pmod 3 \\ 4x \equiv -1 \pmod 5 \\ 7x \equiv 5 \pmod{11} \\ 8x \equiv t \pmod{15} \end{cases} \Leftrightarrow \begin{cases} x \equiv 51 \pmod{165} \\ x \equiv 2t \pmod{15} \end{cases}$$

D'après (a), puisque $15 \mid 165$, *si* $x \equiv 51 \pmod{165}$, *alors* $x \equiv 51 \equiv 6 \pmod{15}$. *De plus on sait que* $x \equiv 2t \pmod{15}$, *donc on obtient* $2t \equiv 6 \pmod{15}$, *c'est à dire* $t \equiv 3 \pmod{15}$. *Viceversa, si* $t \equiv 3 \pmod{15}$, *alors le système et compatible, car il est équivalent à la congruence*

$$x \equiv 51 \pmod{165}$$

(la deuxième congruence étant impliquée par la première) qui a été resolu au point (b). Donc l'unique entier t, *avec* $0 \leq t \leq 14$, *est* $t = 3$ *et pour cette valeur les solutions du système sont* $\{51 + 165k \mid k \in \mathbb{Z}\}$.

Exercice 3. Soit $n \in \mathbb{Z}_{>0}$ et soit $a \in \mathbb{Z}$.

(a) Montrer que a est inversible modulo n si et seulement si $\text{pgcd}(a, n) = 1$.

(b) Définir la fonction indicatrice d'Euler φ.

(c) En s'inspirant de la démonstration du petit théorème de Fermat vue en TD, montrer que si $\mathrm{pgcd}(a, n) = 1$, alors $a^{\varphi(n)} \equiv 1 \pmod{n}$.

(d) Soit $d \in \mathbb{Z}$ inversible modulo $\varphi(n)$, et soit e son inverse. Montrer que si $m \in \mathbb{Z}$ est premier avec n, on a

$$m^{ed} \equiv m \pmod{n}.$$

Solution [4 points]

(a) [1,5 point] *Si a est inversible modulo n, alors il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \pmod{n}$. Donc il existe $k \in \mathbb{Z}$ tel que $ab - nk = 1$. Cela implique que $\mathrm{pgcd}(a, n) \mid 1$, donc $\mathrm{pgcd}(a, n) = 1$. Réciproquement, si $\mathrm{pgcd}(a, n) = 1$, alors il existe $u, v \in \mathbb{Z}$ tels que $au + nv = 1$ (identité de Bézout). Donc $au - 1 = nu$ et $au \equiv 1 \pmod{n}$. On obtient que a est inversible modulo n.*

(b) [0,5 point] *Pout tout $n \in \mathbb{Z}$, $n \geq 1$, on définit*

$$\varphi(n) = \sharp\{a \in \mathbb{Z} : 1 \leq a \leq n, \mathrm{pgcd}(a, n) = 1\}.$$

(c) [2 points] *Soit $a \in \mathbb{Z}$ tel que $\mathrm{pgcd}(a, n) = 1$. Considérons l'application*

$$\begin{array}{rccc} \tau_a\colon & \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times & \to & \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times \\ & x & \mapsto & ax. \end{array}$$

Tout d'abord τ_a est bien définie, car si a et x sont inversibles modulo n, d'inverses respectivement a^{-1} et x^{-1}, alors leur produit est inversible modulo n, car $ax \cdot (x^{-1}a^{-1}) \equiv 1 \pmod{n}$. Montrons que τ_a est bijective. Soient $x, y \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ tels que $\tau_a(x) = \tau_a(y)$, alors $ax = ay$ et, en multipliant par a^{-1} les deux membres, on obtient $x = y$. Donc τ_a est injective. De plus, si $y \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$, alors $y = \tau_a(a^{-1}y)$, avec $a^{-1}y \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$. Donc τ_a est surjective. Cela implique que les ensembles $\left\{x : x \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times\right\}$ et $\left\{ax : x \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times\right\}$ sont égaux. Donc

$$\prod_{x \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times} x = \prod_{x \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times} ax.$$

Or, d'après (a) et (b), $\sharp\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times = \varphi(n)$. Donc

$$\prod_{x \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times} x = a^{\varphi(n)} \prod_{x \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times} x$$

et, en multipliant les deux membres par l'inverse de $\prod_{x \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times} x$, on obtient

$$a^{\varphi(n)} = 1,$$

ou, ce qui est équivalent, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

(d) [1 point] *Soit $d \in \mathbb{Z}$ inversible modulo $\varphi(n)$ et soit e son inverse. Alors $ed \equiv 1 \pmod{\varphi(n)}$, c'est-à-dire il existe $k \in \mathbb{Z}$ tel que $ed = 1 + k\varphi(n)$. En utilisant ce qu'on a montré en (c), on a :*

$$m^{ed} = m^{1+k\varphi(n)} = m \cdot (m^{\varphi(n)})^k \equiv m \cdot 1 \equiv m \pmod{n}.$$

Remarque : Maintenant que vous connaissez un peu de théorie des groupes, le résultat est évident. On sait que $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ est un groupe d'ordre $\varphi(n)$. D'après le théorème de Lagrange, on en déduit donc que $\forall a \in (\mathbb{Z}/n\mathbb{Z})^\times, a^{\varphi(n)} = a^{\sharp(\mathbb{Z}/n\mathbb{Z})^\times} = 1$.

Exercice 4. Soit $p > 2$ un nombre premier et soit $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ le groupe des éléments inversibles modulo p. Soit

$$A_p := \left\{ \gamma^2 : \gamma \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \right\}.$$

(a) Lister les éléments de A_{13}.

(b) Soit $\alpha \in \frac{\mathbb{Z}}{p\mathbb{Z}}$. Montrer que $\alpha^2 = 1$ si et seulement si $\alpha = \pm 1$.

(c) Soient $\alpha, \beta \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$. Montrer que $\alpha^2 = \beta^2$ si et seulement si $\alpha = \pm\beta$.

(d) En considérant l'application

$$\begin{array}{rccc} \sigma : & \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times & \to & \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \\ & \alpha & \mapsto & \alpha^2, \end{array}$$

montrer que $|A_p| = \frac{p-1}{2}$.

(e) Soit $\alpha \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$. Montrer que $\alpha^{\frac{p-1}{2}} = \pm 1$ et que si $\alpha \in A_p$ alors $\alpha^{\frac{p-1}{2}} = 1$.

Solution

(a) [1 point] $A_{13} = \{[1]_{13}, [2^2]_{13}, [3^2]_{13}, [4^2]_{13}, [5^2]_{13}, [6^2]_{13}, [7^2]_{13}, [8^2]_{13}, [9^2]_{13}, [10^2]_{13}, [11^2]_{13}, [12^2]_{13}\}$={1,4,9,3,12,10}

(b) [1 point] *Soit $\alpha = [a]_p$, avec $a \in \mathbb{Z}$. Alors $\alpha^2 = 1 \Leftrightarrow [a^2]_p = [1]_p \Leftrightarrow a^2 \equiv 1 \mod p \Leftrightarrow p \mid (a^2 - 1) \Leftrightarrow p \mid (a-1)$ ou $p \mid (a+1) \Leftrightarrow a \equiv 1 \mod p$ ou $a \equiv -1 \mod p \Leftrightarrow \alpha = \pm 1$.*

(c) [1 point] *Soient $\alpha, \beta \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$. Clairement, si $\alpha = \pm\beta$, alors $\alpha^2 = \beta^2$. Supposons maintenant que $\alpha^2 = \beta^2$. Alors $\left(\alpha\beta^{-1}\right)^2 = 1$, ce qui implique, d'après (b), que $\alpha\beta^{-1} = \pm 1$, ce qui équivaut à $\alpha = \pm\beta$.*

(d) [1 point] *Notons d'abord que* $\mathrm{Im}(\sigma) = A_p$. *Soit* $x \in A_p$. *Alors il existe* $\alpha \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ *tel que* $\sigma(\alpha) = x$, *et si* $\beta \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ *est aussi tel que* $\sigma(\beta) = x$, *alors, d'après (d),* $\alpha = \pm\beta$. *Cela implique que chaque élément en* $\mathrm{Im}(\sigma) = A_p$ *a exactement deux pré-images à travers* σ *(on remarque que, puisque* $p > 2$, *pour tout* $\alpha \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$, $\alpha \neq -\alpha$*). Donc* $|A_p| = \frac{p-1}{2}$.

(e) [1 point] *Soit* $\alpha \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$. *Alors, d'après le petit théorème de Fermat,* $(\alpha^{\frac{p-1}{2}})^2 = \alpha^{p-1} = 1$. *Donc, en utilisant (b), on obtient* $\alpha^{\frac{p-1}{2}} = \pm 1$. *De plus, si* $\alpha \in A_p$, *alors il existe* $\beta \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ *tel que* $\alpha = \beta^2$. *Donc, encore en appliquant le petit théorème de Fermat, on obtient*

$$\alpha^{\frac{p-1}{2}} = (\beta^2)^{\frac{p-1}{2}} = \beta^{p-1} = 1.$$

Remarque : On a même ici une équivalence. En effet, on rappelle que comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps. On sait alors que le polynôme $P(X) = X^{\frac{p-1}{2}} - 1$ (vu comme un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$) admet au plus $\deg(P) = \frac{p-1}{2}$ racines. Or, cet exercice nous a montré que les éléments de A_p étaient racines de P. Comme $\sharp A_p = \frac{p-1}{2}$, on en déduit que P n'admet pas d'autre racine. On a donc l'équivalence :

$$\alpha^{\frac{p-1}{2}} = 1 \iff \alpha \in A_p.$$