Contrôle Continu

21/10/25

Consignes. *La durée du contrôle continu est 1h30. Il est constitué de quatre exercices indépendants. Toute question non résolue peut être admise dans la suite. Les réponses doivent être correctement rédigées. Aucun document ni calculatrice n'est autorisé.*

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.

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 $\mathbb{Z}$.

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 $\text{pgcd}(a, n) = 1$, 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

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

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