

ARITHMÉTIQUE

Examen session 1 - Éléments de correction

Exercice 1. Un exercice isométrique a été traité en TD. La question est en fait de savoir à quoi est congru 1234^{28} modulo 10. Ce qui revient donc à la question : à quoi est congru 4^{28} modulo 10 ? Or on constate que $4^3 \equiv 4 \pmod{10}$ donc comme $28 = 3^3 + 1$, on a $4^{28} \equiv 4 \cdot ((4^3)^3)^3 \equiv 4 \cdot 4^3 \equiv 6 \pmod{10}$. La réponse est donc : 6.

Autre méthode : on remarque que $1234 \equiv -6 \pmod{10}$ et que $6^2 \equiv 6 \pmod{10}$. Dès lors, on retrouve immédiatement le résultat.

Exercice 2. Cet exercice a été traité en TD.

Exercice 3.

Les premières questions sont du cours...

2.a. Si $k \in \Omega_n(a) \neq \emptyset$, alors $l = k - 1 \in \mathbb{N}$ et un inverse de a est a^l .

Réciproquement, si $a \in (\mathbb{Z}/n\mathbb{Z})^*$, alors le théorème d'Euler nous donne justement que $\varphi(n) \in \Omega_n(a)$.

2.b. Soit $a \in (\mathbb{Z}/n\mathbb{Z})^*$. L'ensemble $\Omega_n(a)$ est alors une partie de $\mathbb{N}$ non vide d'après le 2.a. donc admet un plus petit élément : $\omega_n(a)$.

On pourrait aborder la question en remarquant que $\{k \in \mathbb{Z} \mid a^k = \bar{1}\}$ est un sous-groupe additif de $\mathbb{Z}$ qui n'est autre que $\omega_n(a)\mathbb{Z}$. Comme $\varphi(n) \in \Omega_n(a) \subset \omega_n(a)\mathbb{Z}$, le résultat vient. Suivons la méthode suggérée par l'énoncé (qui en fait redétaille simplement la preuve des faits précédents):

On effectue la division euclidienne de $\varphi(n)$ par $\omega_n(a)$: on a $\varphi(n) = Q\omega_n(a) + r$ avec $Q, r \in \mathbb{N}$ et $0 \leq r < \omega_n(a)$. On remarque que

$$\bar{1} = a^{\varphi(n)} = \left(a^{\omega_n(a)}\right)^Q \cdot a^r = \bar{1}^Q \cdot a^r = a^r$$

car $\omega_n(a) \in \Omega_n(a)$ donc $a^{\omega_n(a)} = \bar{1}$.

Ainsi, supposons que r soit non nul: on a alors $r \in \Omega_n(a)$ donc $r \geq \omega_n(a)$ (puisque $\omega_n(a)$ est le plus petit). Mais c'est contradictoire, donc $r = 0$.

3.a. 5 et 16 sont premiers entre eux donc d'après le cours $\bar{5} \in (\mathbb{Z}/16\mathbb{Z})^*$.

3.b. On a $5^2 \equiv 9 \equiv -7 \pmod{16}$ donc $5^4 \equiv 49 \equiv 1 \pmod{16}$ donc le reste est 1.

3.c. Clairement 1, 2, 3 ne sont pas dans $\Omega_{16}(\bar{5})$. Donc $\omega_{16}(\bar{5}) \geq 4$. D'après 3.b., c'est exactement 4.

3.d. Ainsi l'inverse est $\bar{5}^3 = \overline{-35} = \overline{13}$.

3.e. Le problème est: trouver tous les entiers x tels que $\bar{5} \cdot \bar{x} = \bar{5x} = \bar{2}$ dans $\mathbb{Z}/16\mathbb{Z}$. C'est donc équivalent à résoudre $\bar{x} = \overline{13} \cdot \bar{2} = \overline{10}$. Ainsi l'ensemble des solutions est $\{10 + 16K \mid K \in \mathbb{Z}\}$.