Université de Versailles – Saint-Quentin-en-Yvelines
Université Paris Saclay

Septembre 2025
Groupe de TD 1

Master 1 Informatique – Compléments de maths
CC 2 – arithmétique

NOM: _____	Prénom: _____	Num. Étu.: 2☐☐☐☐☐☐☐☐

Exercice 1.

En utilisant le théorème de Bézout, montrer l'énoncé suivant.
Soit $a, b, c \in \mathbb{Z}$. On suppose que a divise bc et que a et b sont premiers entre eux. Alors a divise c.
Indice : $c = 1 \times c \ldots$

Réponse.

D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $au+bv = \mathrm{pgcd}(a, b)$. Or a et b sont premiers entre eux donc $\mathrm{pgcd}(a, b) = 1$. On a donc $1 = au + bv$ et on en déduit donc que $c = cau + cbv$.

Par hypothèse, a divise bc donc il existe $k \in \mathbb{Z}$ tel que $bc = ak$. Ainsi $c = cau + akv = a(cu + kv)$. Ainsi, a est un diviseur de c.

Exercice 2.

1. Calculer en justifiant $\varphi(99)$.
2. En déduire la valeur de $2^{243} \bmod 99$. La division euclidienne de 243 par $\varphi(99)$ pourra être utile.

Réponse.

1. On observe que $99 = 11 \times 3^2$. On en déduit donc que $\varphi(99) = \varphi(11 \times 3^2) = \varphi(11)\varphi(3^2) = (11-1)(3^2-3) = 10 = 60$. où l'on a utilisé successivement le fait que $\varphi(nm) = \varphi(n)\varphi(m)$ pour tout n, m premiers entre eux et le fait que $\varphi(p^k) = p^k - p^{k-1}$ pour tout puissance d'un nombre premier p.
2. On observe que 2 et 99 sont premiers entre eux (car 2 est premier et n'apparait pas dans la décomposition en facteurs premiers de 99). Le théorème d'Euler nous permet donc de dire que $2^{60} \equiv 1 \bmod 99$. Puisque $243 = 60 \times 4 + 3$, on en déduit que $2^{243} \equiv 2^3(2^{60})^4 \equiv 8 \cdot 1^4 \equiv 8 \bmod 99$.