Contrôle Continu

23/10/24

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 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 $x, y \in \mathbb{Z}$.

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 et 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.

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 ?

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