UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Feuille n°3 : Anneaux et structure d'anneaux sur $\mathbf{Z}/n\mathbf{Z}$

Exercice 1

1 20606 appartient-il à $14443 + 3079\mathbf{Z}$?
2 Calculer l'élément 2169 dans $\mathbf{Z}/13\mathbf{Z}$. Le résultat doit être représenté par un nombre compris entre 0 et 12.
3 Considérons une application $f : \mathbf{Z}/8\mathbf{Z} \to \mathbf{Z}/8\mathbf{Z}$, qui envoie x sur x^3. Est-elle injective ?
4 $[2]_{26}$ est-il un diviseur de $[0]$ dans $\mathbf{Z}/26\mathbf{Z}$?
5 $187489 = 433^2$, où 433 est un nombre premier. Combien de diviseurs de zéro y a-t-il dans $\mathbf{Z}/187489\mathbf{Z}$?
6 Déterminer les puissances de 2 modulo 9. Que dire du groupe $(\mathbf{Z}/9\mathbf{Z})^\times$?

Exercice 2

1 Soit m et n deux entiers naturels non nuls premiers entre eux. On a vu comment trouver une relation de Bézout $um + vn = 1$. Montrer alors que l'application

$$\begin{array}{ccc} (\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z}) & \to & \mathbf{Z}/(mn)\mathbf{Z} \\ (x, y) & \mapsto & umy + vnx \end{array}$$

est bien définie, est un isomorphisme. Déterminer son isomorphisme réciproque.
2 Trouver l'entier entre 0 et 100 congru à 9 modulo 11 et à 3 modulo 13.

Exercice 3

Il est souvent important de calculer a^t modulo n avec a, t, n grands (calculer a^t dans $\mathbf{Z}$ n'est pas envisageable). Méthode : Ecrire t en binaire : $t = \Sigma t_i 2^i$ (où $t^i \in \{0, 1\}$). Les a^{2^i} se calculent facilement par élévations au carré successives modulo n, et a^t modulo n est le produit (modulo n) des a^{2^i} pour lesquels $t^i = 1$. Calculer 3^{2010} modulo 50.

Exercice 4

Voici la table d'un groupe fini. Déterminer l'ordre de a.

$*$	a	b	c	d
a	c	d	a	b
b	d	a	b	c
c	a	b	c	d
d	b	c	d	a

Exercice 5

Soit p un nombre premier impair.
1 Quels éléments de $(\mathbf{Z}/p\mathbf{Z})^\times$ sont leur propre inverse ?
2 Démontrer le théorème de Wilson,

Théorème de Wilson : Soit n un entier naturel supérieur à 3. Alors n est premier si, et seulement si, $(n-1)! = -1 \pmod n$.