

Exercices - Chapitre IV

Exercice 1

Les sept questions sont indépendantes.

- 1) Montrer que 13 divise $2^{70} + 3^{70}$.
- 2) Soit n un entier naturel impair. Montrer que 7 divise $3^n + 4^n$.
- 3) Montrer que 17 divise $2^{32} - 1$.
- 4) Montrer que si n est un entier naturel impair, 7 divise $2^{2^n} + 3$. Montrer que si n est congru à 2 modulo 6, alors 19 divise $2^{2^n} + 3$.
- 5) Déterminer la congruence de 1823^{242} modulo 18.
- 6) Montrer que l'écriture décimale de 3^{1000} se termine par 01.
- 7) Déterminer l'ordre du groupe des éléments inversibles de l'anneau $\mathbb{Z}/1800\mathbb{Z}$.

Exercice 2

- 1) Décrire les groupes des éléments inversibles des anneaux $\mathbb{Z}/10\mathbb{Z}$ et $\mathbb{Z}/15\mathbb{Z}$.
- 2) Ces groupes sont-ils cycliques ?
- 3) Dans le groupe $(\mathbb{Z}/15\mathbb{Z})^*$, on constate que l'ordre de $\overline{14}$ n'est pas le plus petit commun multiple des ordres de $\overline{2}$ et $\overline{7}$. Comment peut-on l'expliquer ?

Indication : voir le bas de la page 37 du polycopié du cours.

Exercice 3 (Nombres de Fermat)

Pour tout $n \in \mathbb{N}$, posons $F_n = 2^{2^n} + 1$. Ces entiers s'appellent les nombres de Fermat.

- 1) Soient m et n des entiers naturels distincts. Montrer que F_m et F_n sont premiers entre eux.
- 2) En déduire qu'il existe une infinité de nombres premiers.
- 3) Supposons $n \geq 2$. Montrer que l'on a $2^{\frac{F_n-1}{2}} \equiv 1 \pmod{F_n}$.
- 4) Soit p un diviseur premier de F_n . Montrer que p est congru à 1 modulo 2^{n+1} .

Indication : considérer l'ordre de $\overline{2}$ dans $(\mathbb{Z}/p\mathbb{Z})^*$.

(On peut démontrer que pour tout $n \geq 2$, on a $p \equiv 1 \pmod{2^{n+2}}$, mais c'est plus difficile.)

Exercice 4 (Cipolla, 1904)

Soit a un entier ≥ 2 . Soit p un nombre premier impair qui ne divise pas $a^2 - 1$. Posons

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

- 1) Montrer que n est un entier qui n'est pas premier.
- 2) Montrer que l'on a $a^{n-1} \equiv 1 \pmod{n}$.

Remarque. Jusqu'au début du XIX^e siècle, on est resté avec l'idée que la congruence $2^{n-1} \equiv 1 \pmod{n}$ devait caractériser les entiers premiers impairs. Avec $a = 2$ et $p = 5$, on obtient ci-dessus $n = 341$, qui est le plus petit entier $n \geq 2$ non premier tel que $2^{n-1} \equiv 1 \pmod{n}$. Il a été trouvé par Sarrus en 1819.

Exercice 5

Soit φ la fonction indicatrice d'Euler. Soient a et n des entiers naturels ≥ 2 .

- 1) Montrer que n est l'ordre de a modulo $a^n - 1$.
- 2) En déduire que n divise $\varphi(a^n - 1)$.

Exercice 6

Montrer que $\overline{429}$ est inversible dans l'anneau $\mathbb{Z}/700\mathbb{Z}$ et déterminer son inverse.

Exercice 7

Déterminer l'ensemble des entiers relatifs congrus à 1 modulo 31 et à 2 modulo 53.

Exercice 8

Déterminer le plus petit entier naturel multiple de 7 et congru à 1 modulo 2, 3, 4, 5 et 6.

Exercice 9

Montrer que l'écriture décimale de 2^{1000} se termine par 76.

Indication : utiliser le théorème chinois.

Exercice 10

Soit m un entier naturel non nul. Montrer qu'il existe $x \in \mathbb{Z}$ tel que

$$(2x + 1)(3x + 1) \equiv 0 \pmod{m}.$$

Indication : posons $m = 2^t d$ où d est impair. Exprimer le fait que 3 est inversible modulo 2^t , que 2 est inversible modulo d , et utiliser le théorème chinois.

Exercice 11

Soit p un nombre premier. Soit q un diviseur premier, distinct de 3, de $2^p + 1$. Montrer que l'on a $q \equiv 1 \pmod{2p}$.

Indication : considérer l'ordre de $\bar{2}$ dans $(\mathbb{Z}/q\mathbb{Z})^*$.

Exercice 12

Montrer qu'il n'existe pas d'entiers $n \geq 2$ tels que n divise $2^n - 1$.

Indication : on suppose qu'il existe un tel entier n et on considère le plus petit diviseur premier p de n . Trouver une contradiction en examinant l'ordre de $\bar{2}$ dans $(\mathbb{Z}/p\mathbb{Z})^*$.

Exercice 13

Soit n un entier naturel impair. Montrer que n divise $2^{n!} - 1$.

Indication : utiliser le théorème d'Euler et remarquer que l'on a $\varphi(n) \leq n$.

Exercice 14

Soit n un entier naturel non nul. On s'intéresse ici à la description de l'ensemble S des solutions de l'équation $x^2 = 1$ dans l'anneau $\mathbb{Z}/n\mathbb{Z}$. On notera $|S|$ son cardinal.

- 1) Supposons n impair. Soit r le nombre de diviseurs premiers de n . Notons

$$n = p_1^{n_1} \cdots p_r^{n_r} \quad \text{avec} \quad n_i \geq 1,$$

la décomposition de n en produit de nombres premiers p_i . Soit A l'ensemble des entiers $a \in \mathbb{Z}$ tels que $a^2 \equiv 1 \pmod{n}$. Soit B l'ensemble des entiers $a \in \mathbb{Z}$ possédant la propriété suivante : pour tout $i = 1, \dots, r$, il existe $\varepsilon_i = \pm 1$ tel que

$$a \equiv \varepsilon_i \pmod{p_i^{n_i}}.$$

1.1) Montrer que $A = B$.

1.2) En déduire que $|S| = 2^r$.

- 2) Supposons que n soit une puissance de 2. Posons $n = 2^t$ avec $t \geq 1$.

2.1) Expliciter S si $t = 1$ et $t = 2$.

2.2) Supposons $t \geq 3$. Montrer que l'on a

$$S = \left\{ \pm 1 + 2^t\mathbb{Z}, \pm 1 + 2^{t-1} + 2^t\mathbb{Z} \right\}.$$

En particulier, on a dans ce cas $|S| = 4$.

- 3) En déduire $|S|$.

- 4) Expliciter S si $n = 128$ et $n = 735$.

Remarque. La résolution de l'équation $x^2 = 1$ dans $\mathbb{Z}/n\mathbb{Z}$ nécessite, a priori, la connaissance de la factorisation de n en produit de nombres premiers. Si l'on savait résoudre cette équation sans utiliser cette factorisation, il serait alors facile de trouver la factorisation de n . En effet, si a est un entier tel que $a^2 \equiv 1 \pmod{n}$ et $a \not\equiv \pm 1 \pmod{n}$, le calcul du pgcd de $a + 1$ (ou $a - 1$) avec n fournit un diviseur non trivial de n . Le problème de la factorisation des entiers serait ainsi résolu, et la sécurité de nombreux cryptosystèmes serait complètement remise en cause.

Exercice 15 (Système RSA)

Soit n un entier ≥ 1 . Alice utilise le cryptosystème RSA afin de se faire envoyer des messages codés par des éléments de $\mathbb{Z}/n\mathbb{Z}$. Soit (e, n) sa clé publique.

- 1) Déterminer sa clé secrète dans chacun des cas suivants :

$$(e, n) \in \{(5, 35), (139, 265), (31, 3599)\}.$$

Soient p et q des nombres premiers distincts congrus à 2 modulo 3. Posons

$$n = pq \quad \text{et} \quad e = \frac{2(p-1)(q-1)+1}{3} \quad (e \text{ est un entier}).$$

- 2) Montrer que e est premier avec $\varphi(n)$ et calculer son inverse modulo $\varphi(n)$.
3) Alice choisit comme clé publique le couple

$$(e, n) = (107, 187).$$

Bob lui envoie le cryptogramme $9 + n\mathbb{Z}$. Quel est le message secret que Bob souhaite transmettre à Alice ?
