

Exercices sur le chapitre II

Exercice 1

- 1) Quel est le reste de la division euclidienne de 1823^{242} par 18 ?
- 2) Quel est le reste de la division euclidienne de 2222^{321} par 20 ?
- 3) Soit n un entier naturel.
 - 3.1) Montrer que l'on a $10^{6n+4} + 3 \equiv 0 \pmod{7}$.
 - 3.2) Montrer que l'on a $2^{2^{6n+2}} + 3 \equiv 0 \pmod{19}$.
- 4) Pour tout $n \geq 2$, posons $u_n = 2^n - 3$.
 - 4.1) Si n est congru à 3 modulo 4, montrer que 5 divise u_n .
 - 4.2) Si n est congru à 4 modulo 12, montrer que 13 divise u_n .
 - 4.3) Montrer que l'on a $u_{n+12} \equiv u_n \pmod{65}$.
 - 4.4) En déduire que 65 ne divise pas u_n .

Exercice 2

Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

Indication : on suppose le contraire. Soit $\{p_1, \dots, p_k\}$ l'ensemble des nombres premiers congrus à 1 modulo 4. En considérant l'entier

$$4(p_1 \cdots p_k)^2 + 1,$$

et en utilisant l'alinéa 6 des exemples 2.1 du cours, en déduire une contradiction.

Exercice 3

Soit p un nombre premier impair distinct de 5. Pour tout $n \geq 1$, posons

$$R_n = 1 \cdots 1$$

l'entier constitué de n chiffres 1. Montrer qu'il existe une infinité d'entiers n tels que R_n soit divisible par p .

Indication : remarquer que l'on a $R_n = \frac{10^n - 1}{9}$ et $10^{p-1} \equiv 1 \pmod{p}$.

Exercice 4

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 multiplicatif de 2 modulo q .

Exercice 5

Soit p un nombre premier tel que $2^{p-1} \equiv 1 \pmod{p^2}$. Soit m un entier naturel tel que $2^m \equiv 1 \pmod{p}$. Montrer que l'on a

$$2^m \equiv 1 \pmod{p^2}.$$

Indication : considérer l'ordre multiplicatif de 2 modulo p .

Exercice 6

Soient p et q des nombres premiers distincts. Posons $n = pq$.

- 1) Soit t un entier naturel congru à 1 modulo $\varphi(n)$, où $\varphi(n)$ est l'indicateur d'Euler de n . Montrer que pour tout $a \in \mathbb{Z}$, on a

$$a^t \equiv a \pmod{n}.$$

- 2) Montrer que connaître n et $\varphi(n)$ est équivalent à connaître p et q .

Exercice 7

Soit $n \geq 1$ un entier. Notons $d(n)$ le nombre de diviseurs positifs de n .

- 1) Déterminer $d(n)$ en fonction de la décomposition en facteurs premiers de n .
- 2) Montrer que n est un carré si et seulement si $d(n)$ est impair.
- 3) Trouver tous les entiers $n \leq 30$ tels que $d(n) = \varphi(n)$, où φ est la fonction indicatrice d'Euler.

Exercice 8

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 9

Soient p et q des nombres premiers impairs distincts. Posons

$$n = pq \quad \text{et} \quad d = \text{pgcd}(p-1, q-1).$$

Montrer que l'on a

$$2^{n-1} \equiv 1 \pmod{n} \iff 2^d \equiv 1 \pmod{n}.$$

Indication : utiliser l'égalité $n - 1 = (p - 1)q + (q - 1)$ et la démonstration du lemme 2.9.

Exercice 10

Soit p un nombre premier. Posons $p - 1 = 2^s t$ avec t impair. Soit a un entier non divisible par p . Montrer que l'on est dans l'un des cas suivants :

- 1) on a $a^t \equiv 1 \pmod{p}$.
- 2) Il existe un entier i tel que $0 \leq i \leq s - 1$ et $a^{2^i t} \equiv -1 \pmod{p}$.

Exercice 11 (Pocklington, 1914)

Soit n un entier > 1 . Supposons qu'il existe un nombre premier q divisant $n - 1$ vérifiant l'inégalité $q > \sqrt{n} - 1$, et qu'il existe un entier $a \geq 1$ tels que l'on ait

$$a^{n-1} \equiv 1 \pmod{n} \quad \text{et} \quad \text{pgcd}\left(a^{\frac{n-1}{q}} - 1, n\right) = 1.$$

Montrer que n est premier.

Indication : on suppose que n n'est pas premier. Il existe alors un diviseur premier p de n plus petit que \sqrt{n} . Montrer que p divise $a^{\frac{n-1}{q}} - 1$ et en déduire une contradiction.

Exercice 12

Soit p un nombre premier. Posons

$$N_p = \frac{p^p - 1}{p - 1}.$$

- 1) Montrer que N_p est un entier naturel.
- 2) Pour tout $k \geq 1$, montrer que l'on a

$$p^k \equiv p \pmod{(p^2 - p)}.$$

- 3) En déduire que l'on a

$$N_p \equiv 1 \pmod{(p^2 - p)}.$$

- 4) Soit ℓ un diviseur premier de N_p .
 - 4.1) Montrer que ℓ ne divise pas $p^2 - p$.
 - 4.2) En déduire que l'on a

$$\ell \equiv 1 \pmod{p}.$$