

Contrôle continu 2

Arithmétique

Semestre 3

L'épreuve dure 2h. Les 4 exercices sont indépendants. La notation tiendra compte de la clarté et de la rigueur de la rédaction. Toute affirmation doit être justifiée.

Exercice 1

Justifier les assertions suivantes ou donner un contre-exemple.

1. Soient $d, n \in \mathbb{Z}$. Si $d \mid n^2$, alors $d \mid n$.
2. L'équation

$$21x \equiv 6 \pmod{60}$$

admet 2 solutions modulo 60.

3. Soient $a, b \in \mathbb{Z}^*$. Alors $\text{pgcd}(a, b)$ est la plus petite valeur positive de l'ensemble

$$\{ax + by \mid x, y \in \mathbb{Z}\}.$$

4. $2^{33} - 1$ est divisible par $2^{11} - 1$.

Exercice 2 (Nombre de Frobenius)

L'objectif de l'exercice est de déterminer tous les entiers de l'ensemble

$$\mathbf{E} = \{3u + 4v \mid u, v \in \mathbb{N}\}.$$

1. Montrer que l'équation

$$3u + 4v = 5, \quad u, v \in \mathbb{N}$$

n'a pas de solution.

2. Soit $a \in \mathbb{N}^*$.

(a) Résoudre l'équation

$$3u + 4v = a, \quad u, v \in \mathbb{Z}.$$

(b) Montrer qu'il existe un unique couple d'entiers $u, v \in \mathbb{Z}$ tels que $3u + 4v = a$ et $0 \leq v \leq 2$.

(c) En déduire que si $a > 5$, alors $a \in \mathbf{E}$.

3. Déterminer \mathbf{E} .

Exercice 3 (Une fonction arithmétique)

On appelle σ la fonction qui, à un entier plus grand que 1, associe la somme de ses diviseurs positifs :

$$\sigma : \begin{cases} \mathbb{N}^* & \longrightarrow & \mathbb{N} \\ n & \longmapsto & \sum_{d \in \Delta(n)} d. \end{cases}$$

On a noté $\Delta(n)$ l'ensemble des diviseurs positifs de n :

$$\Delta(n) = \{d \in \llbracket 1; n \rrbracket, d \mid n\}.$$

1. Calculer $\sigma(11)$ et $\sigma(28)$.
2. Soient $p \in \mathbb{N}$ un nombre premier et $k \in \mathbb{N}$. Montrer que

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}.$$

3. Montrer que σ est une *fonction arithmétique*, c'est-à-dire que

$$\forall n, m \in \mathbb{N}^*, \quad \text{pgcd}(n, m) = 1 \implies \sigma(nm) = \sigma(n)\sigma(m).$$

Indication : Établir une bijection entre $\Delta(nm)$ et $\Delta(n) \times \Delta(m)$.

Soit $n \in \mathbb{N}^*$. On dit que n est **déficient** si $\sigma(n) < 2n$; **parfait** si $\sigma(n) = 2n$; **abondant** si $\sigma(n) > 2n$.

4. Déterminer la nature de 6, 9 et 12.

5. Soit $p \in \mathbb{N}$ un nombre premier. Quelle est la nature de p ?

6. Soit $n \in \mathbb{N}^*$ un entier parfait. On suppose qu'on peut l'écrire $n = 2^k m$, où $k \in \mathbb{N}^*$ et m est un entier impair.

(a) Montrer que

$$2^{k+1}m = (2^{k+1} - 1)\sigma(m).$$

(b) En déduire que $2^{k+1} - 1$ divise m . On note $d \in \mathbb{N}^*$ tel que

$$m = (2^{k+1} - 1)d.$$

(c) Vérifier que

$$\sigma(m) = 2^{k+1}d; \quad n = 2^k(2^{k+1} - 1)d; \quad \sigma(n) = 2^{k+1}(2^{k+1} - 1)d.$$

(d) On suppose que $d > 1$. Montrer que

$$\sigma(m) \geq 1 + d + (2^{k+1} - 1)d,$$

et en déduire que $d = 1$, puis que $\sigma(m) = m + 1$.

Exercice 4 (RSA)

1. Écrire $n := 65$ comme produit deux nombres premiers (positifs) p et q .

2. Rappeler la définition de l'indicatrice d'Euler ϕ et montrer que

$$\phi(n) = pq - p - q + 1.$$

3. Trouver l'inverse u de 7 modulo $\phi(n)$.

4. Résoudre alors

$$x^7 \equiv 2 \pmod{n}.$$