Colle 13 • INDICATIONS
Arithmétique des entiers

Exercice 13.1

1. En raisonnant par l'absurde, montrer que le système

$$(\mathrm{S}) \quad \begin{cases} x \equiv 5 \ [6] \\ x \equiv 4 \ [8] \end{cases}$$

n'admet pas de solution $x \in \mathbb{Z}$.

2. **(a)** Énoncer le théorème de Bézout dans $\mathbb{Z}$.

(b) Soient a et b deux entiers naturels premiers entre eux. Soit $c \in \mathbb{Z}$. Montrer que :

$$\left[a \mid c \quad \text{et} \quad b \mid c\right] \quad \Longleftrightarrow \quad ab \mid c\,.$$

3. On considère le système (S) d'inconnue $x \in \mathbb{Z}$ suivant :

$$(\mathrm{S}) \quad \begin{cases} x \equiv 6 \ [17] \\ x \equiv 5 \ [16] \\ x \equiv 4 \ [15]\,. \end{cases}$$

(a) Déterminer une solution particulière $x_0 \in \mathbb{Z}$ de (S).

(b) Déduire des questions précédentes l'ensemble des solutions de (S) dans $\mathbb{Z}$.

indication

Il s'agit de l'exercice 94 de la banque CCINP (filières MP et MPI) : `https://www.concours-commun-inp.fr/fr/epreuves/les-epreuves-orales.html`.

Exercice 13.2

Déterminer tous les couples d'entiers naturels (a, b) tels que :

$$\begin{cases} a^2 - b^2 = 9792 \\ a \wedge b = 24. \end{cases}$$

indication

- Se donner $(x, y) \in \mathbb{N}^2$ tel que :

$$a = 24x, \quad b = 24y, \quad \text{et} \quad x \wedge y = 1.$$

- Réécrire le système sous la forme :

$$\begin{cases} (x+y)(x-y) = 17 \\ x \wedge y = 1. \end{cases}$$

Cet exercice est issu du cahier de calcul pour les prépas : `https://colasbd.github.io/cdc/`.

résultat

$$(a, b) = (216, 192).$$

Exercice 13.3

1. Donner une solution dans $\mathbb{Z}^2$ de l'équation diophantienne

$$5u + 13v = 1.$$

2. Résoudre dans $\mathbb{Z}$ l'équation de congruence :

$$5x + 4 \equiv 7 \ [13].$$

indication

1. Utiliser l'algorithme d'Euclide pour 13 et 5 et « remonter » les égalités.

2.
- ♦ Déterminer l'inverse de 5 modulo 13 : on a $8 \times 5 = 40 \equiv 1 \ [13]$.
- ♦ Multiplier l'équation par 8 (inverse de 5 modulo 13) de façon à trouver $x \equiv 11 \ [13]$.
- ♦ Vérifier que, réciproquement, les entiers congrus à 11 modulo 13 sont solutions.

Cet exercice est issu du cahier de calcul pour les prépas : `https://colasbd.github.io/cdc/`.

résultat

1. $(u, v) = (-5, 2)$.

2. $\{11 + 13k \ ; \ k \in \mathbb{Z}\}$.

Exercice 13.4

Soient $n, m \in \mathbb{N}^*$. Montrer que :

$$\mathbb{U}_n \cap \mathbb{U}_m = \{1\} \iff n \wedge m = 1.$$

indication

$\boxed{\Rightarrow}$ Raisonner par contraposée : si $n \wedge m = d > 1$, se donner $z_0 \in \mathbb{U}_d \setminus \{1\}$, et montrer que $z_0 \in \mathbb{U}_n \cap \mathbb{U}_m$.

$\boxed{\Leftarrow}$ Utiliser une relation de Bezout : il existe $(u, v) \in \mathbb{Z}^2$ tel que $nu+mv = 1$ donc, si $z \in \mathbb{U}_n \cap \mathbb{U}_m$, $z = z^{nu+mv}$.

Exercice 13.5

Soit $a \in \mathbb{N}$ tel que $a \geqslant 2$. Soient $n, m \in \mathbb{N}^*$.
Montrer que :

$$\mathrm{PGCD}(a^n - 1, a^m - 1) = a^{\mathrm{PGCD}(n,m)} - 1.$$

indication

On note $d := \mathrm{PGCD}(n, m)$ et $g := \mathrm{PGCD}(a^n - 1, a^m - 1)$.

- ♦ Montrer que $a^d - 1 \,\big|\, g$ en écrivant que $n = dp$ et $m = dq$, puis :

$$a^n - 1 = (a^d - 1)\sum_{k=0}^{p-1} a^{dk} \quad \text{et} \quad a^m - 1 = (a^d - 1)\sum_{\ell=0}^{q-1} a^{d\ell}.$$

- Remarquer que $a^n \equiv 1 \ [g]$ et $a^m \equiv 1 \ [g]$, puis, avec le théorème de Bezout, écrire $d = un + vm$ pour montrer que $a^d \equiv 1 \ [g]$.

Exercice 13.6

Soit $x \in \mathbb{Q}$. Soit $n \in \mathbb{N}^*$. Soient $a_0, \dots, a_{n-1} \in \mathbb{Z}$.
Montrer que :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad \Longrightarrow \quad x \in \mathbb{Z}.$$

indication

Écrire $x = \dfrac{p}{q}$ avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ et $p \wedge q = 1$, puis utiliser la relation donnée en isolant x^n pour montrer que $q \mid 1$.

Exercice 13.7

On note, pour $n \in \mathbb{Z}$, $\mathrm{Div}(n)$ l'ensemble des diviseurs positifs de n.
Soient $a, b \in \mathbb{Z}$ tels que a et b sont premiers entre eux.
Montrer que l'application

$$\varphi : \left| \begin{array}{rcl} \mathrm{Div}(a) \times \mathrm{Div}(b) & \longrightarrow & \mathrm{Div}(ab) \\ (k, \ell) & \longmapsto & k\ell \end{array} \right.$$

est correctement définie et bijective.

indication

On pourra utiliser l'existence et l'unicité de la décomposition d'un nombre en produit de facteurs premiers. En particulier, lorsque deux entiers sont premiers entre eux, les nombres premiers intervenant dans les décompositions sont nécessairement distincts.

Exercice 13.8

Soit $n \in \mathbb{N}$.

1. Montrer qu'il existe un unique couple $(a_n, b_n) \in \mathbb{N}^2$ tel que :

$$\left(1 + \sqrt{2}\right)^n = a_n + b_n\sqrt{2}.$$

2. **(a)** Calculer ${a_n}^2 - 2{b_n}^2$.

(b) En déduire que a_n et b_n sont premiers entre eux.

indication

1.
- <u>Existence.</u> Utiliser la formule du binôme de Newton et séparer les termes pairs et impairs de la somme.
- <u>Unicité.</u> En supposant l'existence de deux couples différents, aboutir à une contradiction en utilisant que $\sqrt{2}$ est irrationnel.

2. **(a)** Remarquer que $(1 - \sqrt{2})^n = a_n - b_n\sqrt{2}$ et utiliser l'identité remarquable $u^2 - v^2 = \cdots$.

(b) Utiliser une relation de Bézout.

résultat

1. $a_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} 2^k$ et $b_n = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2k+1} 2^k$.

2. **(a)** ${a_n}^2 - 2{b_n}^2 = (-1)^n$.

Exercice 13.9

Soit $\sigma : \mathbb{Z} \longrightarrow \mathbb{N}$ telle que, pour $n \in \mathbb{Z}$, $\sigma(n)$ est la somme des diviseurs positifs de n.

1. Soit p un nombre premier. Soit $\alpha \in \mathbb{N}^*$. Calculer $\sigma(p^\alpha)$.

2. Soient $a, b \in \mathbb{Z}$ deux entiers premiers entre eux.

(a) Soit d un diviseur positif de ab. Montrer que :

$$\exists!(d_1, d_2) \in \mathbb{N}^* : \quad \begin{cases} d_1 \mid a\,, \quad d_2 \mid b \\ d = d_1 d_2. \end{cases}$$

(b) En déduire que $\sigma(ab)$ en fonction de $\sigma(a)$ et $\sigma(b)$.

3. Soit $n \in \mathbb{N}$. Exprimer $\sigma(n)$ en fonction de la décomposition en produit de facteurs premiers de n.

indication

1. Les diviseurs positifs de p^α sont $1, p, p^2, \ldots, p^\alpha$.

2. **(a)**
- EXISTENCE. Poser $d_1 := d \wedge a$ et $d_2 := d \wedge b$.
  Montrer que $d_1 \wedge d_2 = 1$, puis $d_1 d_2 \mid d$.
  Pour montrer que $d \mid d_1 d_2$, écrire les relations de Bezout pour d_1 et d_2 et les multiplier.
- UNICITÉ. Se donner un couple $(\widetilde{d_1}, \widetilde{d_2})$ et montrer que $\widetilde{d_1} \mid d_1$ et $d_1 \mid \widetilde{d_1}$ et de même pour d_2 et $\widetilde{d_2}$.

(b) Utiliser ce qui précède.

3. Utiliser ce qui précède : les éléments intervenant dans la décomposition d'un entier en produits de facteurs premiers sont des puissances de nombres premiers premiers entre eux.

résultat

1. $\sigma(p^\alpha) = \dfrac{p^{\alpha+1} - 1}{p - 1}$.

2. **(b)** $\sigma(ab) = \sigma(a)\sigma(b)$.

3. Si $n = {p_1}^{\alpha_1} \cdots {p_N}^{\alpha_N}$, alors $\sigma(n) = \prod_{k=1}^{N} \dfrac{{p_k}^{\alpha_k+1} - 1}{p_k - 1}$.

Exercice 13.10

Soit p un nombre premier impair.
Montrer que :

$$\forall k \in \mathbb{N}, \quad (1+p)^{p^k} \equiv 1 + p^{k+1} \ \left[p^{k+2}\right].$$

indication

Procéder par récurrence sur k en écrivant, pour l'hérédité,

$$(1+p)^{p^{k+1}} = \left(1 + p^{k+1}(1+pq)\right)^p \quad \text{où } q \in \mathbb{Z},$$

puis utiliser le binôme de Newton en sortant les deux premiers termes.

Utiliser le fait que, si $\ell \in [\![2, p-1]\!]$, p divise $\binom{p}{\ell}$, donc :

$$\forall \ell \in [\![2, p-1]\!], \quad p^{k+3} \,\Big|\, \binom{p}{\ell} p^{\ell(k+1)}.$$

Exercice 13.11

Soit $n \in \mathbb{N}^*$ tel que $n \geqslant 2$.
Montrer que :

$$n \text{ est premier} \quad \Longleftrightarrow \quad (n-1)! \equiv -1 \ [n].$$

indication

- $\boxed{\Rightarrow}$ Le résultat est acquis pour $n = 2$. Pour $n \geqslant 3$, écrire $(n-2)! = 2 \times \cdots \times (n-2)$ et regrouper les éléments en produits $x \times y$ où $xy \equiv 1 \ [n]$ (en ayant justifié préalablement que les seuls éléments tels que $x^2 \equiv 1 \ [n]$ sont 1 et n). On peut ensuite multiplier par $n - 1 \equiv -1 \ [n]$.
- $\boxed{\Leftarrow}$ Raisonner par l'absurde. Se donner un diviseur $d \in [\![2, n-1]\!]$ de n et montrer que :

$$d \,|\, (n-1)! + 1 \quad \text{et} \quad d \,|\, (n-1)!\,,$$

pour en déduire que $d \,|\, 1$.