Devoir surveillé n°07

- La présentation, la lisibilité, l'orthographe, la qualité de la rédaction et la précision des raisonnements entreront pour une part importante dans l'appréciation des copies.
- On prendra le temps de vérifier les résultats dans la mesure du possible.
- Les calculatrices sont interdites.

Exercice 1 ★★ **Algorithme RSA**

Soient p et q deux nombres premiers distincts. On pose $\mathrm{N} = pq$ et $\mathrm{M} = (p-1)(q-1)$.

1. Soit $(a,b,c) \in \mathbb{Z}^3$. Montrer que si a et b divisent c et si a et b sont premiers entre eux, alors ab divise c.

2. Montrer que p et q sont premiers entre eux.

3. Soit $e \in \mathbb{N}$ premier avec M. Justifier qu'il existe $d \in \mathbb{N}$ tel que $ed \equiv 1[\mathrm{M}]$.

4. Justifier que $ed \geq 1$.

5. Soit $x \in \mathbb{Z}$.

a. On suppose que p divise x. Montrer que $x^{ed} \equiv x[p]$.

b. On suppose que p ne divise pas x. Montrer à nouveau que $x^{ed} \equiv x[p]$.

6. Montrer que $x^{ed} \equiv x[\mathrm{N}]$.

Exercice 2 ★★ **Equation de Pell-Fermat**

On admet l'irrationalité de $\sqrt{2}$ et on introduit l'ensemble

$$\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2},\ (a,b) \in \mathbb{Z}^2\right\}$$

1. Montrer que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

$(\mathbb{Z}[\sqrt{2}], +, \times)$ est donc un anneau.

2. **a.** Montrer que pour tout $x \in \mathbb{Z}[\sqrt{2}]$, il existe un *unique* couple $(a,b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$.

On peut alors définir le *conjugué* de x par $\overline{x} = a - b\sqrt{2}$.

b. Montrer que pour $(x,y) \in \mathbb{Z}[\sqrt{2}]^2$, $\overline{x \times y} = \overline{x} \times \overline{y}$.

3. Pour $x \in \mathbb{Z}[\sqrt{2}]$, on pose $\mathrm{N}(x) = x\overline{x}$.

a. Justifier que pour tout $x \in \mathbb{Z}[\sqrt{2}]$, $\mathrm{N}(x) \in \mathbb{Z}$.

b. Montrer que pour tout $(x,y) \in \left(\mathbb{Z}[\sqrt{2}]\right)^2$, $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$.

c. Montrer que $x \in \mathbb{Z}[\sqrt{2}]$ est inversible dans l'anneau $(\mathbb{Z}[\sqrt{2}], +, \times)$ si et seulement si $|\mathrm{N}(x)| = 1$.

On note H l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}[\sqrt{2}]$. On rappelle qu'alors $(\mathrm{H}, \times)$ est un groupe. H est notamment stable par produit et par inversion. De plus, d'après la question précédente,

$$\mathrm{H} = \left\{x \in \mathbb{Z}[\sqrt{2}], |\mathrm{N}(x)| = 1\right\}$$

4. Soient $x \in \mathrm{H}$ et $(a,b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$.

a. Montrer que si $a \geqslant 0$ et $b \geqslant 0$, alors $x \geqslant 1$.

b. Montrer que si $a \leqslant 0$ et $b \leqslant 0$, alors $x \leqslant -1$.

c. Montrer que si $ab \leqslant 0$, alors $|x| \leqslant 1$.

5. On note $\mathrm{H}^+ = \mathrm{H} \cap]1, +\infty[$.

a. Soient $x \in \mathrm{H}^+$ et $(a,b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$. Montrer que $a > 0$ et $b > 0$.

b. En déduire que $u = 1 + \sqrt{2}$ est le minimum de H^+.

6. Soit $x \in \mathrm{H}^+$.

a. Montrer qu'il existe $n \in \mathbb{Z}$ tel que $u^n \leqslant x < u^{n+1}$.

b. Montrer que $x = u^n$.

7. En déduire que $\mathrm{H} = \{u^n, n \in \mathbb{Z}\} \cup \{-u^n, n \in \mathbb{Z}\}$.

Exercice 3 ★★ **Développement décimal**

Vocabulaire et notations

- Pour un réel t, on notera $\lfloor t \rfloor$ la partie entière de t.
- La notation $[\![0, 9]\!]$ désigne l'ensemble $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
- On dit qu'une suite (u_n) est périodique à partir d'un certain rang s'il existe $\mathrm{N} \in \mathbb{N}$ et $\mathrm{T} \in \mathbb{N}^*$ tel que $u_{n+\mathrm{T}} = u_n$ pour tout $n \geq \mathrm{N}$. On dit alors que (u_n) est T-périodique à partir du rang N.

Soit x un nombre réel. On définit deux suites (d_n) et (ε_n) de la manière suivante :

- On pose $d_0 = \lfloor x \rfloor$ et $\varepsilon_0 = x - \lfloor x \rfloor$.
- Pour tout $n \in \mathbb{N}$, on pose $d_{n+1} = \lfloor 10\varepsilon_n \rfloor$ et $\varepsilon_{n+1} = 10\varepsilon_n - \lfloor 10\varepsilon_n \rfloor$.

1. *Dans cette question uniquement*, on suppose $x = 123,456$. Calculer d_0, d_1, d_2, d_3 et $\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3$. Que valent d_n et ε_n pour $n \geq 4$?

2. On revient au cas général.

a. Montrer que pour tout $n \in \mathbb{N}$, $\varepsilon_n \in [0, 1[$.

b. En déduire que pour tout $n \in \mathbb{N}^*$, $d_n \in [\![0, 9]\!]$.

c. On pose $\mathrm{S}_n = \displaystyle\sum_{k=0}^{n} \frac{d_k}{10^k}$ pour tout $n \in \mathbb{N}$. Montrer que $x = \mathrm{S}_n + \dfrac{\varepsilon_n}{10^n}$ pour tout $n \in \mathbb{N}$.

d. En déduire que (S_n) converge vers x.

3. Soient $\mathrm{T} \in \mathbb{N}^*$ et $\mathrm{N} \in \mathbb{N}$. On suppose que la suite (d_n) est T-périodique à partir du rang N.

a. Pour $n \in \mathbb{N}$, on pose $u_n = 10^{\mathrm{N}+\mathrm{T}}\mathrm{S}_{n+\mathrm{N}+\mathrm{T}} - 10^{\mathrm{N}}\mathrm{S}_{n+\mathrm{N}}$. Montrer que la suite (u_n) est constante.

b. En déduire qu'il existe $p \in \mathbb{Z}$ tel que pour tout $n \in \mathbb{N}$

$$10^{\mathrm{N}+\mathrm{T}}\mathrm{S}_{n+\mathrm{N}+\mathrm{T}} - 10^{\mathrm{N}}\mathrm{S}_{n+\mathrm{N}} = p$$

c. En déduire que x est rationnel.

4. Soit α le nombre dont l'écriture décimale est $0,123\,456\,456\,456\,456...$. Montrer que α est rationnel et l'écrire sous la forme d'une fraction de deux entiers.

On suppose désormais que x est rationnel. Il existe donc $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ tel que $x = \dfrac{a}{b}$. On définit deux suites (q_n) et (r_n) de la manière suivante.

- q_0 et r_0 sont respectivement le quotient et le reste de la division euclidienne de a par b.
- Pour tout $n \in \mathbb{N}$, q_{n+1} et r_{n+1} sont respectivement le quotient et le reste de la division euclidienne de $10r_n$ par b.

5. **a.** Justifier qu'il existe deux entiers naturels N et M distincts tels que $r_{\mathrm{N}} = r_{\mathrm{M}}$.

b. En déduire que (r_n) est périodique à partir d'un certain rang.

c. En déduire que (q_n) est également périodique à partir d'un certain rang.

d. Montrer que pour tout $n \in \mathbb{N}$, $r_n = b\varepsilon_n$ et $q_n = d_n$.
On a donc prouvé que la suite (d_n) était périodique à partir d'un certain rang.

6. On suppose que $x = \dfrac{13}{35}$. Déterminer $\mathrm{N} \in \mathbb{N}$ et $\mathrm{T} \in \mathbb{N}^*$ tels que la suite (d_n) soit T-périodique à partir du rang N.