Mathématiques - DS n°4

Partie CUPGE

Documents et calculettes interdits

Exercice 1 : (Arithmétique)

1. Résoudre dans $\mathbb{Z}$ le système de conguences suivant :

$$x \equiv 4 \mod 6 \quad \text{et} \quad x \equiv 7 \mod 9.$$

2. (a) Montrer que tout entier naturel congru à 3 modulo 4 possède au moins un diviseur premier congru à 3 modulo 4.
   (b) Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.
3. On pose $F_n = 2^{2^n} + 1$, le n^e nombre de Fermat.
   (a) Montrer que $F_n = 2 + \prod_{k=0}^{n-1} F_k$.
   (b) Montrer que $F_m \wedge F_n = 1$ pour $m \neq n$ entiers.
   (c) Montrer que tout entier naturel n qui n'est pas de la forme 2^m possède un diviseur impair autre que 1. En déduire que, si $2^n + 1$ est premier, alors soit c'est un nombre de Fermat, soit $n = 0$.

Solution

1. $x \equiv 4 \mod 6$ et $x \equiv 7 \mod 9$ ss'il y a $y, z \in \mathbb{Z}$ avec $6y + 4 = x = 9z + 7$, soit $6y - 9z = 7 - 4 = 3$, ou encore $2y - 3z = 1$. Il y a une solution évidente $(y_0, z_0) = (-1, -1)$. Si (y, z) est une autre solution, alors $2(y - y_0) = 3(z - z_0)$. Ainsi $2 \mid 3(z - z_0)$; puisque $2 \wedge 3 = 1$, le lemme de Gauss donne $2 \mid z - z_0$ et il y a $k \in Z$ avec $z = z_0 + 2k = 2k - 1$. Ceci nous fait $2y = 3z + 1 = 3(2k - 1) + 1 = 6k - 2$, soit $y = 3k - 1$, et finalement $x = 6y + 4 = 6(3k - 1) + 4 = 18k - 2$, avec $k \in Z$. On vérifie aisément que tout entier de cette forme satisfait le système.
2. (a) Soit $n \equiv 3 \mod 4$, et $n = \prod_i p_i$ la décomposition de n en facteurs premiers. Puisque n est impair, aucun p_i vaut 2. Les autres nombres premiers sont impairs, et congrus à soit 1 soit 3 modulo 4. Si tous les $p_i \equiv 1 \mod 4$, alors $n = \prod_i p_i \equiv \prod_i 1 = 1 \mod 4$, une contradiction. Donc au moins un des $p_i \equiv 3 \mod 4$.
   (b) Par l'absurde, on suppose qu'il n'y ait qu'un nombre fini de nombres premiers congrus à 3 modulo 4, disons $p_1, \dots, p_n$. Soit $k = \prod_{i=1}^n p_i$. Alors k est impair, et congru à 1 ou à 3 modulo 4. Dans le premier cas on pose $m = k + 2$, dans le deuxième cas $m = k + 4$. Alors $m \equiv 3 \mod 4$; d'après la partie (a) il y a un diviseur premier p de m avec $p \equiv 3 \mod 4$. Donc p est parmi les p_i, et $p \mid k$. Mais $p \mid m$, d'où $p \mid m - k \in \{2, 4\}$. Or, p est impair, une contradiction. Ainsi il y a une infinité de nombres premiers congrus à 3 modulo 4.
3. (a) Par récurrence sur n. Pour $n = 0$ le produit est vide et vaut 1. On a donc $F_0 = 2^{2^0} + 1 = 2^1 + 1 = 2 + 1 = 3$. Pour $n = 1$ on a $F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5 = 2 + 3 = 2 + F_0 = 2 + \prod_{k=0}^{1-1} F_k$.
   Supposons donc que $F_n = 2 + \prod_{k=0}^{n-1} F_k$, et calculons.

$$\begin{aligned} 2 + \prod_{k=0}^{n} F_k &= 2 + F_n(-2 + 2 + \prod_{k=0}^{n-1} F_k) = 2 + F_n(-2 + F_n) = 2 + (2^{2^n} + 1)(-2 + 2^{2^n} + 1) \\ &= 2 + (2^{2^n} + 1)(2^{2^n} - 1) = 2 + (2^{2^n})^2 - 1 = 2^{2^{n+1}} + 1 = F_{n+1}, \end{aligned}$$

   ce qui montre l'énoncé.
   (b) On peut suppose $m < n$. Alors $F_m \mid \prod_{k=0}^{n-1} F_k = F_n - 2$; d'après le théorème d'Euclide $F_n \wedge F_m = F_m \wedge 2$. Mais F_m est impair, d'où $F_m \wedge 2 = 1$.
   (c) Soit $n = \prod_i p_i$ la décomposition de n en facteurs premiers. Si aucun des p_i n'était impair, alors tous les $p_i = 2$ et n est une puissance de 2, ce qui démontre le premier énoncé par contraposition. Si $2^n + 1$ n'est pas un nombre de Fermat, n possède un facteur premier, et $n = pq$ avec p impair. Alors

$$2^n + 1 = 2^{pq} + 1 = (2^q)^p + 1 = (2^q + 1) \sum_{k=0}^{p-1} (-2^q)^k.$$

   Or $2 \leq 2^q + 1 < 2^n + 1$; ainsi $2^n + 1$ n'est pas premier.

Exercice 2 : (Dérivabilité)

1. Soit $f : \mathbb{R} \to \mathbb{R}$ convexe. Montrer que si f est majorée, alors f est constante.
2. Soient $a < b$ des réels, et $g \in \mathcal{C}^2([a,b], \mathbb{R})$. On suppose que $g(a) = g(b) = 0$ et $c \in]a,b[$. Montrer qu'il existe $d \in]a,b[$ tel que
$$g(c) = -\frac{(c-a)(b-c)}{2} g''(d).$$
(Indication : Considérer $G : t \mapsto g(t) + \lambda(t-a)(b-t)$ où λ est choisi pour que $G(c) = 0$. Utiliser Rolle deux fois pour G puis pour G'.)
3. Soit $h : \mathbb{R} \to \mathbb{R}$ continue en 0 et $\ell \in \mathbb{R}$. Montrer que h est dérivable en 0 avec $h'(0) = \ell$ si et seulement si
$$\forall\, \epsilon > 0\, \exists\, \delta > 0\, \forall\, (x,y) \in]0,\delta[^2 \quad \Big|\frac{h(x)-h(-y)}{x+y} - \ell\Big| \le \epsilon.$$

Solution

1. Supposons f non-constante. Il y a donc $a \neq b$ avec $f(a) < f(b)$; en remplaçant éventuellement $f(x)$ par $f(-x)$ (qui est également convexe), on peut supposer $a < b$. Soit $x > b$ et $\lambda = \frac{b-a}{x-a} \in [0,1]$. Alors $b = \lambda x + (1-\lambda)a$, et par convexité $f(b) \le \lambda f(x) + (1-\lambda) f(a)$, soit
$$f(x) \ge f(a) + \frac{f(b)-f(a)}{\lambda} = f(a) + \frac{x-a}{b-a}(f(b)-f(a)) \xrightarrow{x\to\infty} \infty.$$
Ainsi f n'est pas bornée.
2. On a $G(a) = G(c) = G(b)$ avec $G \in \mathcal{C}^2([a,b],\mathbb{R})$ et $a < c < b$. D'après le théorème de Rolle il y a $c' \in]a,c[$ et $c'' \in]c,b[$ avec $G'(c') = G'(c'') = 0$. Or, G' est encore dérivable sur $[c',c'']$ et il y a $d \in]c',c''[$ avec $G''(d) = 0$. Alors $d \in]a,b[$ et $0 = G''(d) = g''(d) - 2\lambda$. Or, $G(c) = 0$ nous donne
$$g(c) = -\lambda(c-a)(b-c) = -\frac{(c-a)(b-c)}{2} g''(d).$$
3. Supposons d'abord que h est dérivable en 0 avec $h'(0) = \ell$. Soit $\epsilon > 0$. Alors il y a $\delta > 0$ tel que pour $0 < x < \delta$ on a $\big|\frac{h(x)-h(0)}{x} - \ell\big| \le \frac{\epsilon}{2}$. Alors pour $x, y \in]0,\delta[$,
$$\begin{aligned}
\Big|\frac{h(x)-h(-y)}{x+y} - \ell\Big| &= \Big|\frac{h(x)-h(0)+h(0)-h(-y)}{x+y} - \ell\Big| \\
&= \Big|\frac{x}{x+y}\Big(\frac{h(x)-h(0)}{x} - \ell\Big) + \frac{y}{x+y}\Big(\frac{h(-y)-h(0)}{-y} - \ell\Big)\Big| \\
&\le \frac{x}{x+y}\Big|\frac{h(x)-h(0)}{x} - \ell\Big| + \frac{y}{x+y}\Big|\frac{h(-y)-h(0)}{-y} - \ell\Big| \\
&\le \frac{x}{x+y}\frac{\epsilon}{2} + \frac{y}{x+y}\frac{\epsilon}{2} = \epsilon.
\end{aligned}$$
Réciproquement, supposons $\forall\, \epsilon > 0\, \exists\, \delta > 0\, \forall\, (x,y) \in]0,\delta[^2 \quad \Big|\frac{h(x)-h(-y)}{x+y} - \ell\Big| \le \epsilon$. Alors par continuité de f en 0 on a pour $x \in]0\delta[$ fixé que
$$\epsilon \ge \lim_{y\to 0}\Big|\frac{h(x)-h(-y)}{x+y} - \ell\Big| = \Big|\frac{h(x)-h(0)}{x} - \ell\Big|.$$
De même, pour $y \in]0,\delta[$ fixé on a
$$\epsilon \ge \lim_{x\to 0}\Big|\frac{h(x)-h(-y)}{x+y} - \ell\Big| = \Big|\frac{h(-y)-h(0)}{-y} - \ell\Big|.$$
Ainsi $h'(0) = \lim_{x\to 0}\big|\frac{h(x)-h(0)}{x} = \ell$.

Exercice 3 : (Polynômes)

1. Soient $a \neq b$ éléments d'un corps K et $P \in K[X]$. Exprimer le reste de la division euclidienne de P par $(X-a)(X-b)$ en fonction de $P(a)$ et $P(b)$.
2. Soit $P \in \mathbb{R}[X] \setminus \{0\}$ tel que $P(X^2) = P(X)P(X+1)$. Montrer que si z est une racine de P, alors z^2 et $(z-1)^2$ aussi. En déduire que toute racine $\neq 0$ est de module 1, puis que les seules racines possibles sont 0 et 1. En déduire tous les polynômes solution de cette équation.

Solution

1. D'après la division euclidienne il y a $Q \in K[X]$ et $\alpha, \beta \in K$ tels que
$$P(X) = (X-a)(X-b)Q(X) + \alpha X + \beta.$$
Alors $P(a) = \alpha a + \beta$ et $P(b) = \alpha b + \beta$. Ainsi $P(a) - P(b) = \alpha(a-b)$ et $\alpha = \frac{P(a)-P(b)}{a-b}$, ce qui donne
$$\beta = P(a) - \alpha a = P(a) - (P(a) - P(b))\frac{a}{a-b} = \frac{aP(b) - bP(a)}{a-b}.$$
Le reste est donc $\frac{P(a)-P(b)}{a-b} X + \frac{aP(b)-bP(a)}{a-b}$.
2. Soit z une racine de P. Alors $P(z^2) = P(z)P(z+1) = 0$ et $P((z-1)^2) = P(z-1)P(z) = 0$. Donc z^2 et $(z-1)^2$ sont également des solutions.
Comme P n'a qu'un nombre fini de racines, il y en a une de module maximal, disons z. Mais $|z| > 1$ alors $|z^2| = |z|^2 > |z|$, une contradiction puisque z^2 est aussi racine. De même, si z est une racine de P de module minimal avec $0 < |z| < 1$ alors $0 < |z^2| = |z|^2 < |z|$, une contradiction. Ainsi toutes les racines de P sont soit 0, soit de module 1.
Soit maintenant z une racine de module 1. Alors $P((z-1)^2) = P(z-1)P(z-1+1) = 0$ et $(z-1)^2$ est 0 ou de module 1, donc $z = 1$ ou $|z-1| = 1$. Mais les seuls nombres complexes z de module 1 tels que $|z-1| = 1$ sont $-j$ et $-j^2$. Ainsi les racines de P sont parmi $0, 1, -j, -j^2$. Mais si $-j$ est une racine, $(-j)^2 = j^2$ aussi, une contradiction. De même, si $-j^2$ est une racine, $(-j^2)^2 = j$ aussi, une contradiction. Ainsi les seules racines possibles sont 0 et 1.
Donc $P(X) = aX^n(X-1)^m$. Alors
$$aX^n(X-1)^m a(X+1)^m X^m = P(X)P(X+1) = P(X^2) = aX^{2n}(X^2-1)^m = aX^{2n}(X+1)^m(X-1)^m.$$
D'après la factorisation unique en facteurs irréductibles, $a^2 = a$ et $a = 1$, et $n = m$. Donc $P(X) = X^n(X-1)^n$ pour $n \in \mathbb{N}$. Le calcul ci-dessus montre que tout polynôme de cette forme est solution de l'équation.