DM 8 : ordinaux et suites de Goodstein.

Il s'agit d'un sujet supplémentaire pour votre travail personnel.
Il n'est pas à rendre.
Un corrigé sera fourni le dimanche 6 novembre.

1 Suites de Goodstein

Décomposition d'un entier en base b : On rappelle que, si $b \in \mathbb{N}$ avec $b \geq 2$, tout entier naturel n non nul se décompose de manière unique sous la forme

$$n = a_h b^h + a_{h-1} b^{h-1} + \cdots + a_0 = \sum_{i=0}^{h} a_i b^i,$$

où $h \in \mathbb{N}$ et $a_h \neq 0$ et où, pour tout $i \in \{0, \ldots, h\}$, $a_i \in \{0, \ldots, b-1\}$.

Pour $h = -1$, la somme vide $\sum_{i=0}^{h} a_i b^i$ est nulle. Elle constitue la décomposition de 0 en base b.

1°) Décomposer 144 en base 3.

La **décomposition héréditaire** de l'entier n en base b consiste à n'écrire n qu'à l'aide des entiers $0, \ldots, b$: on écrit d'abord la décomposition de l'entier n en base b : $n = \sum_{i=0}^{h} a_i b^i$, puis, si $h > b$, pour tout $i > b$, on remplace dans cette égalité i par sa décomposition en base b et on itère le procédé.

Par exemple, 35 s'écrit en base 2 : $35 = 2^5 + 2 + 1$, or $5 = 2^2 + 1$, donc la décomposition héréditaire de 35 en base 2 est $35 = 2^{(2^2+1)} + 2^1 + 1$.

La décomposition héréditaire de $2^{35} + 35$ en base 2 vaut $2^{[2^{(2^2+1)}+2^1+1]} + 2^{(2^2+1)} + 2^1 + 1$.

Formellement, si l'on note $\mathrm{d}_b(n)$ la décomposition de l'entier n en base b, on définit la décomposition héréditaire $\mathrm{dh}_b(n)$ en convenant que :

— pour tout $n < b^{b+1}$, $\mathrm{dh}_b(n) = \mathrm{d}_b(n)$;

— lorsque $n \geq b^{b+1}$, si $\mathrm{d}_b(n)$ est l'écriture de n sous la forme « $\sum_{i=0}^{h} a_i b^i$ », alors $\mathrm{dh}_b(n)$ est l'écriture de n sous la forme « $\sum_{i=0}^{h} a_i b^{dh_b(i)}$ ».

2°) Donner la décomposition héréditaire en base 3 de $3^{144} + 144$.

3°) Montrer que, pour tout $h \in \mathbb{N}$, $2^h > h$.

4°) Montrer que $\mathrm{dh}_b(n)$ est correctement défini pour tout $b, n \in \mathbb{N}$ avec $b \geq 2$.

Soit $q, r \in \mathbb{N}$ tels que $2 \leq q < r$.
On note $f_{q,r}$ l'application de $\mathbb{N}$ dans $\mathbb{N}$ telle que, pour tout $n \in \mathbb{N}$, $f_{q,r}(n)$ est l'entier obtenu à partir de n en remplaçant formellement q par r dans la décomposition héréditaire de n en base q, sans changer les autres nombres.
Par exemple, $f_{2,3}(35) = 3^{(3^3+1)} + 3^1 + 1$ et $f_{2,3}(2^{35} + 35) = 3^{[3^{(3^3+1)}+3^1+1]} + 3^{(3^3+1)} + 3^1 + 1$.

5°) Montrer qu'on peut définir $f_{q,r}$ en convenant que :

— pour tout $i \in \{0, \ldots, q-1\}$, $f_{q,r}(i) = i$;

— pour tout $n \in \mathbb{N}^*$, si $\mathrm{d}_q(n)$ est l'écriture de n sous la forme $\displaystyle\sum_{i=0}^{k} a_i\, q^i$, avec $k \in \mathbb{N}$, $a_k \neq 0$ et pour tout $i \in \{0, \ldots, k\}$, $a_i \in \{0, \ldots, q-1\}$, alors $f_{q,r}(n) = \displaystyle\sum_{i=0}^{k} a_i\, r^{f_{q,r}(i)}$.

Soit $p \in \mathbb{N}$ et $q \in \mathbb{N}$ avec $q \geq 2$.
On définit la suite de Goodstein $(g_n^{p,q})_{n \in \mathbb{N}}$ de la manière suivante :

— $g_0^{p,q} = p$;
— $g_{n+1}^{p,q} = 0$ si $g_n^{p,q} = 0$;
— si $g_n^{p,q} \neq 0$, alors $g_{n+1}^{p,q} = f_{q+n,q+n+1}(g_n^{p,q}) - 1$.

Lorqu'il n'y aura pas d'ambiguïté sur les valeurs de p et q, on écrira g_n au lieu de $g_n^{p,q}$.

6°) Calculer la suite $(g_n^{p,q})_{n \in \mathbb{N}}$ lorsque $q = 2$ et $p = 3$.

7°) Soit $b \in \mathbb{N}$ avec $b \geq 2$ et $h \in \mathbb{N}$. Montrer que $\displaystyle\sum_{i=0}^{h} (b-1) b^i = b^{h+1} - 1$.

Jusqu'à la fin de cette partie, on choisit $q = 2$ et $p = 4$. On notera g_n au lieu de $g_n^{4,2}$.

8°) Déterminer les plus petits entiers h et k tels que $g_h = 2.(11)^2 + 11$ et $g_k = 2 \times 23^2$.

9°) Calculer g_n lorsque $n = 3.2^{27} - 3$.

10°) Déterminer le plus petit entier k tel que $g_k = 0$.

L'objectif de la suite de ce problème est de montrer le
Théorème de Goodstein (1944) :
pour tout $p, q \in \mathbb{N}$ avec $q \geq 2$, la suite $(g_n^{p,q})_{n \in \mathbb{N}}$ est nulle à partir d'un certain rang.

2 Ensembles bien ordonnés

11°) Soit E un ensemble et R une relation binaire sur E.
On dit que R est un ordre strict sur E si et seulement si :
- R est antiréflexive, c'est-à-dire que, pour tout $x \in E$, $\neg(x\ R\ x)$;
- R est transitive.

On note r la relation binaire sur E définie par : $\forall x, y \in E,\ \ [x\ r\ y \Longleftrightarrow (x\ R\ y) \vee (x = y)]$.
Si R est un ordre strict, montrer que r est une relation d'ordre. On dit que r est la relation d'ordre associée à l'ordre strict R.

12°) Réciproquement, si r est une relation d'ordre quelconque sur E, montrer qu'il existe un unique ordre strict auquel elle est associée.

13°) Soit "$<$" une relation binaire sur un ensemble E.
On dit que $(E, <)$ est bien ordonné si et seulement si "$<$" est un ordre strict sur E et si, pour la relation d'ordre associée à $<$ (que l'on notera $\leq$), toute partie non vide de E possède un minimum.
Montrer que dans ce cas, l'ordre $\leq$ est total et qu'il n'existe pas de suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de E strictement décroissante pour $\leq$.

14°) Soit $(A, <)$ et $(B, <)$ deux ensembles bien ordonnés.
On pose $A + B = [A \times \{0\}] \cup [B \times \{1\}]$ et on convient que,
pour tout $(c, i), (d, j) \in A + B$, $(c, i) < (d, j) \Longleftrightarrow [i < j] \vee [(i = j) \wedge (c < d)]$.
Montrer que $(A + B, <)$ est bien ordonné.

15°) Soit $(A, <)$ et $(B, <)$ deux ensembles bien ordonnés.
Si $(a, b), (c, d) \in A \times B$, on convient que $(a, b) < (c, d) \Longleftrightarrow [b < d] \vee [(b = d) \wedge (a < c)]$.
Montrer que $A \times B$ est bien ordonné par "$<$".

16°) Soit $(A, <)$ et $(B, <)$ deux ensembles bien ordonnés. On suppose que A est non vide et on note 0_A son minimum. On note $A^{(B)}$ l'ensemble des familles $(a_b)_{b\in B}$ d'éléments de A indexées par B telles que $\{b \in B\ /\ a_b \neq 0_A\}$ est de cardinal fini.
On convient que, pour tout $(a_b)_{b\in B}, (a'_b)_{b\in B} \in A^{(B)}$,

$$(a_b)_{b\in B} < (a'_b)_{b\in B} \Longleftrightarrow \exists b_0 \in B,\ \ [a_{b_0} < a'_{b_0}] \wedge [\forall b \in B,\ \ b_0 < b \Longrightarrow a_b = a'_b].$$

Montrer qu'on définit ainsi un ordre strict "$<$" sur $A^{(B)}$.
On **admettra** que $A^{(B)}$ est bien ordonné par "$<$".

17°) On suppose que $(E, <)$ est bien ordonné.
On considère un prédicat $P(x)$ défini pour tout $x \in E$ et tel que :

$$\forall x \in E,\ \ \Big([\forall y \in E,\ \ y < x \Longrightarrow P(y)] \Longrightarrow P(x)\Big).$$

Montrer que $P(x)$ est vrai pour tout $x \in E$.

18°) On suppose que $(E, <)$ est bien ordonné.

Si S est une partie de E, on dit que S est un segment initial de E si et seulement si $\forall x \in S,\ \forall y \in E,\ [y < x \Longrightarrow y \in S]$.
Pour tout $x_0 \in E$, on note $S_{x_0} = \{x \in E \ / \ x < x_0\}$.
Montrer que les seuls segments initiaux de E sont E et les S_{x_0} avec $x_0 \in E$.

On rappelle qu'une application f d'un ensemble E dans un ensemble F est une bijection si et seulement si pour tout $y \in F$, il existe un unique $x_y \in E$ tel que $f(x_y) = y$ et que de plus, en posant $f^{-1}(y) = x_y$ pour tout $y \in F$, on définit une bijection f^{-1} de F dans E telle que, pour tout $x \in E$ et $y \in F$, $f \circ f^{-1}(y) = y$ et $f^{-1} \circ f(x) = x$.

19°) Soient $(E, <)$ et $(F, <)$ deux ensembles bien ordonnés. Montrer qu'il existe au plus une bijection de E dans F qui est strictement croissante, c'est-à-dire telle que, pour tout $x, y \in E$, $x < y \Longrightarrow f(x) < f(y)$.

3 Les ordinaux

On se place dans le cadre de la théorie des ensembles de Zermelo-Fraenkel. En particulier, on ne suppose pas l'axiome de fondation.
Soit E un ensemble. Alors la relation d'appartenance est une relation binaire sur E, car pour tout $x, y \in E$, l'assertion "$x \in y$" est vraie ou fausse.

On dira que
E est transitif si et seulement si pour tout $x \in E$ et pour tout $y \in x$, $y \in E$.

On dira que
E est un ordinal si et seulement si E est transitif et si $(E, \in)$ est bien ordonné.

Lorsque E est un ordinal, la relation d'appartenance entre deux éléments de E est notée indifféremment "$\in$" ou "$<$".

20°) Montrer que $\emptyset$ est un ordinal.

21°) Montrer que $\{\emptyset, \{\emptyset\}\}$ est un ordinal.

Pour les questions 22 à 27 incluse, on fixe un ordinal α.

22°) Si $\alpha \neq \emptyset$, en utilisant $\min(\alpha)$, montrer que $\emptyset \in \alpha$.

23°) Montrer que $\alpha \notin \alpha$.

24°) Si β est un élément de α, montrer que β est aussi un ordinal.

25°) Avec les notations de la question 18, montrer que pour tout $\beta \in \alpha$, $S_\beta = \beta$.

26°) Soit β un ordinal. Montrer que $\beta \subset \alpha \Longleftrightarrow (\beta = \alpha) \vee (\beta \in \alpha)$.

27°) On pose $\alpha^+ = \alpha \cup \{\alpha\}$. Montrer que α^+ est un ordinal.
Montrer que si β est un ordinal tel que $\alpha \in \beta$, alors $\alpha^+ \subset \beta$.

28°) Soit α et β deux ordinaux.
Montrer qu'on est dans l'un des trois cas suivants : $\alpha \in \beta$, $\beta \in \alpha$ ou bien $\alpha = \beta$.

29°) Si A est un ensemble d'ordinaux, montrer que $(A, \in)$ est bien ordonné.

30°) Si A est un ensemble d'ordinaux, montrer que $\bigcup_{\alpha \in A} \alpha$ est un ordinal.

4 Le théorème de Goodstein

En posant $\overline{0} = \emptyset$ et $\overline{n+1} = \overline{n}^+$, on définit par récurrence les ordinaux $\overline{n}$ pour tout $n \in \mathbb{N}$. On admettra que l'axiome de l'infini permet de construire rigoureusement l'ensemble suivant : $\omega = \bigcup_{n \in \mathbb{N}} \overline{n}$. ω est un ordinal.

On admet que si $(X, <)$ est bien ordonné, il existe un unique ordinal α et une unique bijection strictement croissante de $(X, <)$ dans $(\alpha, \in)$. On dira dans ce cas que X et α sont isomorphes.
Soit α et β deux ordinaux. La question 14 permet de construire un ordre $<$ tel que $(\alpha + \beta, <)$ est bien ordonné. Cet ensemble bien ordonné est isomorphe à un unique ordinal, que par abus de notation, on notera encore $\alpha + \beta$.
De même on note $\alpha\beta$ et α^β les uniques ordinaux isomorphes aux ensembles bien ordonnés $(\alpha \times \beta, <)$ et $(\alpha^{(\beta)}, <)$ construits aux questions 15 et 16.
Lorsque $\alpha = \overline{0}$, on convient que $\overline{0}^\beta = \overline{0}$ si $\beta \neq \overline{0}$ et que $\overline{0}^{\overline{0}} = \overline{1}$.

On admet que l'addition et la multiplication entre ordinaux sont associatives mais non commutatives.

Soit $q \in \mathbb{N}$ avec $q \geq 2$.
On définit la suite d'ordinaux $(f_{q,\omega}(n))_{n \in \mathbb{N}}$ en convenant que :

— pour tout $i \in \{0, \ldots, q-1\}$, $f_{q,\omega}(i) = \overline{i}$;

— pour tout $n \in \mathbb{N}^*$, si n s'écrit sous la forme $\sum_{i=0}^{k} a_i\, q^i$, avec $k \in \mathbb{N}$, $a_k \neq 0$ et pour tout $i \in \{0, \ldots, k\}$, $a_i \in \{0, \ldots, q-1\}$,
alors $f_{q,\omega}(n) = \omega^{f_{q,\omega}(k)}\overline{a_k} + \omega^{f_{q,\omega}(k-1)}\overline{a_{k-1}} + \cdots + \omega^{\overline{0}}\overline{a_0}$.

On fixe $p, q \in \mathbb{N}$ avec $q \geq 2$.
On considère à nouveau la suite $(g_n^{p,q})_{n \in \mathbb{N}}$ définie en question 5, et on écrira g_n au lieu de $g_n^{p,q}$. Pour tout $n \in \mathbb{N}$, on pose $\alpha_n = f_{q+n,\omega}(g_n)$.

31°) Si $g_n \neq 0$, montrer que $\alpha_n = f_{q+n+1,\omega}(g_{n+1} + 1)$.

On admet les propriétés suivantes, où la relation d'appartenance est notée "$<$" et où α, β, γ sont trois ordinaux.

1. $\alpha + \overline{1} = \alpha^+$;
2. $\beta < \gamma \Longrightarrow \alpha + \beta < \alpha + \gamma$;
3. si $\alpha \neq \overline{0}$, $\beta < \gamma \Longrightarrow \alpha\beta < \alpha\gamma$;
4. si $\alpha > \overline{1}$, $\beta < \gamma \Longrightarrow \alpha^\beta < \alpha^\gamma$;

5. $\alpha(\beta+\gamma) = (\alpha\beta) + (\alpha\gamma)$;
6. $\alpha^{\overline{0}} = \overline{1}$ et $\alpha^{\overline{1}} = \alpha$;
7. $\alpha^{\beta+\gamma} = \alpha^{\beta}\alpha^{\gamma}$.
8. $\overline{1} \times \alpha = \alpha \times \overline{1} = \alpha$.

32°) On fixe $n \in \mathbb{N}$ avec $n \geq 2$.
Montrer que la suite $(f_{n,\omega}(x))_{x\in\mathbb{N}}$ est une suite strictement croissante d'ordinaux.

33°) Démontrer le théorème de Goodstein.