CORRIGÉ DU PARTIEL DU 3 AVRIL 2008

Problème 1. Les trois nombres entiers 7, 8 et 9 étant deux à deux premiers entre eux, l'application

$$\pi : \mathbb{Z} \to \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z},\ n \mapsto (n \pmod 7,\ n \pmod 8,\ n \pmod 9)$$

induit un isomorphisme de groupes abéliens

$$\mathbb{Z}/504\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$

en vertu du théorème chinois des restes.

Puisque $8.9 \equiv 2 \pmod 7$, $7.9 \equiv -1 \pmod 8$ et $7.8 \equiv 2 \pmod 9$,

$$\mathrm{N}_1 = 288 = 4.8.9 \equiv 1 \pmod 7,\ \ \mathrm{N}_2 = 441 = 7.7.9 \equiv 1 \pmod 8 \quad \text{et} \quad \mathrm{N}_3 = -224 = -4.7.8 \equiv 1 \pmod 9.$$

Par construction, $\pi(\mathrm{N}_1) = (1,0,0)$, $\pi(\mathrm{N}_2) = (0,1,0)$ et $\pi(\mathrm{N}_3) = (0,0,1)$. Comme π est un homomorphisme de groupes,

$$\pi(\mathrm{N}_1 + 2\mathrm{N}_2 + 3\mathrm{N}_3) = \pi(\mathrm{N}_1) + 2\pi(\mathrm{N}_2) + 3\pi(\mathrm{N}_3) = (1,2,3)$$

et par conséquent

$$\mathrm{N} = \mathrm{N}_1 + 2\mathrm{N}_2 + 3\mathrm{N}_3 = 288 + 2.441 - 3.224 = 1170 - 672 = 498$$

est une solution du système de congruences

$$\begin{cases} x \equiv & 1 \pmod 7 \\ x \equiv & 2 \pmod 8 \\ x \equiv & 3 \pmod 9 \end{cases};$$

en outre, puisque $0 \leq \mathrm{N} < 504$, N est le plus petit entier naturel satisfaisant à ces conditions.

Problème 2. 1. En vertu de l'identité

$$(4k+1)(4k'+1) = 16kk' + 8(k+k') + 1 = 4(4kk' + 2k + 2k') + 1,$$

le produit de deux nombres entiers de la forme $4\mathrm{K}+1$ avec $\mathrm{K} \in \mathbb{Z}$ est encore de cette forme.

2. Nous allons démontrer que l'ensemble S des nombres premiers de la forme $4k+3$ avec $k \in \mathbb{N} - \{0\}$ est infini. Raisonnons par l'absurde en supposant que S soit *fini*.

Le nombre entier

$$p(\mathrm{S}) = 3 + 4\prod_{p \in \mathrm{S}} p$$

étant supérieur à 3, il se décompose en un produit de nombres premiers en vertu du théorème fondamental de l'arithmétique. Puisque $p(\mathrm{S}) \equiv 3 \pmod 4$, il découle de la question précédente que l'un au moins des facteurs premiers de $p(\mathrm{S})$ n'est pas congru à 1 modulo 4 ; comme $p(\mathrm{S})$ est impair, nous en déduisons que $p(\mathrm{S})$ possède un facteur premier q tel que $q \equiv 3 \pmod 4$.

On a nécessairement $q > 3$: en effet, si 3 divisait $p(\mathrm{S})$, alors 3 diviserait $p(\mathrm{S}) - 3 = \prod_{p \in \mathrm{S}} p$ et donc 3 appartiendrait à S, ce qui exclu. D'autre part, q ne peut appartenir à S : sinon, q diviserait $p(\mathrm{S}) - \prod_{p \in \mathrm{S}} p$ et donc q diviserait 3, ce qui est impossible. Nous obtenons ainsi un nombre premier q de la forme $4k+3$ avec $k \in \mathbb{N} - \{0\}$ n'appartenant pas à S, en contradiction avec la définition même de l'ensemble S.

Nous avons par conséquent démontré qu'il existe une infinité de nombres premiers de la forme $4k+3$, $k \in \mathbb{N}$.

Problème 3. Soit p un nombre premier. L'ensemble $\mathbb{Q}_p$ des nombres rationnels dont le dénominateur est une puissance de p est un sous-groupe (commutatif) de $(\mathbb{Q}, +)$. Dans ce qui suit, H désigne un sous-groupe de $\mathbb{Q}_p$.

1. Soit x un élément de H tel que $\frac{x}{p} \notin \mathrm{H}$. Nous allons montrer que les classes $\frac{x}{p^i} + \mathrm{H},\ i \in \mathbb{N}$, sont toutes distinctes.

(a) Soient i et j deux entiers naturels tels que $i > j$. Si $\frac{x}{p^i} - \frac{x}{p^j} \in \mathrm{H}$, alors

$$\frac{x}{p^{i-j}} - x = p^j \left(\frac{x}{p^i} - \frac{x}{p^j} \right) = \left(\frac{x}{p^i} - \frac{x}{p^j} \right) + \ldots + \left(\frac{x}{p^i} - \frac{x}{p^j} \right) \in \mathrm{H} ;$$

comme x appartient à H, il en est donc de même de $\frac{x}{p^{i-j}}$.

(b) Supposons qu'il existe deux entiers naturels distincts $i > j$ tels que $\frac{x}{p^i} + \mathrm{H} = \frac{x}{p^j} + \mathrm{H}$. Comme cette identité équivaut à

$$\frac{x}{p^i} - \frac{x}{p^j} \in \mathrm{H},$$

$\frac{x}{p^{i-j}}$ appartient alors à H en vertu de la question précédente. Puisque $i - j > 0$, $i - j - 1 \geq 0$ et donc

$$\frac{x}{p} = p^{i-j-1} \frac{x}{p^{i-j}} = \frac{x}{p^{i-j}} + \ldots + \frac{x}{p^{i-j}} \in \mathrm{H},$$

ce qui contredit l'hypothèse initialement faite sur x. Nous venons de prouver que les classes modulo H $\frac{x}{p^i} + \mathrm{H},\ i \in \mathbb{N}$, sont toutes distinctes.

En particulier, l'indice de H dans $\mathbb{Q}_p$ est *infini* dès qu'il existe un élément x de $\mathbb{Q}_p$ tel que $x \in \mathrm{H}$ et $\frac{x}{p} \notin \mathrm{H}$.

2. Supposons maintenant que le sous-groupe H de $\mathbb{Q}_p$ soit d'indice *fini*.

(a) Comme H et $\mathbb{Z}$ sont deux sous-groupes de $\mathbb{Q}_p$, $\mathrm{H} \cap \mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ et, vu la structure des sous-groupes de $\mathbb{Z}$, il existe donc un unique entier naturel m tel que $\mathrm{H} \cap \mathbb{Z} = m\mathbb{Z}$.

Deux éléments distincts de $\mathbb{Q}_p$ appartiennent évidement à des classes distinctes modulo le sous-groupe $\{0\}$; comme le groupe $\mathbb{Q}_p$ est infini, il en découle que le sous-groupe $\{0\}$ n'est pas d'indice fini. Étant d'indice fini, le sous-groupe H n'est par suite pas réduit à $\{0\}$ et il contient donc un élément non nul $x = \frac{n}{p^r}$, $n \in \mathbb{Z} - \{0\}$, $r \geq 0$. Le sous-groupe $\mathrm{H} \cap \mathbb{Z} = m\mathbb{Z}$ contient alors l'entier non nul $n = p^r x$, ce qui prouve que l'entier naturel m est strictement positif.

(b) Si p divisait l'entier naturel non nul m de la question précédente, $\frac{m}{p}$ serait un entier naturel strictement compris entre 0 et m. Comme m est le plus petit entier naturel non nul appartenant à H, $\frac{m}{p}$ n'appartiendrait pas à H. Dans ces conditions, les classes $\frac{m}{p^i} + \mathrm{H},\ i \in \mathbb{N}$, seraient alors toutes distinctes en vertu de la question 1 et l'indice de H dans $\mathbb{Q}_p$ serait donc infini. Puisque cette conclusion contredit l'hypothèse faite sur H, nous en déduisons que p ne divise pas m.

(c) Puisque H est un sous-groupe de $\mathbb{Q}_p$ d'indice fini, il n'y a qu'un nombre fini de classes modulo H. Vu la question 1, cela entraîne

$$\forall x \in \mathbb{Q}_p, \quad x \in \mathrm{H} \implies \frac{x}{p} \in \mathrm{H}$$

et, en raisonnant par récurrence sur r, $\frac{x}{p^r} \in \mathrm{H}$ pour tout élément x de H et tout entier naturel r.

D'autre part, H étant un sous-groupe de $\mathbb{Q}_p$, alors $\frac{x}{p^{-s}} = p^s x \in \mathrm{H}$ pour tout $x \in \mathrm{H}$ et tout $s \in \mathbb{N}$. Nous avons ainsi prouvé :

$$\forall x \in \mathbb{Q}_p, \forall r \in \mathbb{Z}, \ \ x \in \mathrm{H} \implies \frac{x}{p^r} \in \mathrm{H}.$$

L'inclusion $m\mathbb{Q}_p \subset \mathrm{H}$ est une conséquence immédiate de cette observation : quels que soient en effet $n \in \mathbb{Z}$ et $r \in \mathbb{Z}$, $mn \in m\mathbb{Z} \subset \mathrm{H}$ et donc $m\frac{n}{p^r} = \frac{mn}{p^r} \in \mathrm{H}$.

(d) Nous venons de démontrer l'inclusion $m\mathbb{Q}_p \subset \mathrm{H}$. Soit réciproquement x un élément de H, que l'on écrit sous la forme $x = \frac{n}{p^r}$ avec $n \in \mathbb{Z}$ et $r \in \mathbb{N}$; alors $n = p^r x$ appartient à $\mathbb{Z} \cap \mathrm{H} = m\mathbb{Z}$ et donc $x = \frac{n}{p^r} = \frac{mn'}{p^r}$ appartient bien à $m\mathbb{Q}_p$. Conclusion : $\mathrm{H} = m\mathbb{Q}_p$.

(e) Soient $n \in \mathbb{Z}$ et $k \in \mathbb{N}$. Puisque p ne divise pas m, les nombres entiers m et p^k sont premiers entre eux et donc $\mathbb{Z} = p^k\mathbb{Z} + m\mathbb{Z}$ par application du théorème de Bézout. Il existe par conséquent des entiers u et v

tels que

$$n = p^k u + mv\,;$$

de plus, si $s \in \{0,\dots,m-1\}$ (resp. q) est le reste (resp. le quotient) de la division euclidienne de u par m, alors

$$n = p^k s + mv'$$

avec $v' = v+q$. Comme $\mathrm{H} = m\mathbb{Q}_p$, nous en déduisons

$$\frac{n}{p^k} + \mathrm{H} = s + m\frac{v'}{p^k} + \mathrm{H} = s + \mathrm{H}.$$

Étant donnés $s, s' \in \{0,\dots,m-1\}$, $s+\mathrm{H} = s'+\mathrm{H}$ si et seulement si $s = s'$. En effet, si $s+\mathrm{H} = s'+\mathrm{H}$, alors $s-s'$ appartient à H, donc à $\mathrm{H}\cap\mathbb{Z} = m\mathbb{Z}$, et par conséquent $s-s' = 0$ puisque $|s-s'| < m$.

Nous venons de prouver que toute classe modulo H s'écrit sous la forme $s+\mathrm{H}$ pour un unique entier naturel s de $\{0,\dots,m-1\}$, de sorte que $(\mathbb{Q}_p : \mathrm{H}) = m$.

(a) D'après la question 2 (d), tout sous-groupe d'indice fini de $\mathbb{Q}_p$ est de la forme $m\mathbb{Q}_p$ pour un certain entier naturel m, non nul et premier à p.

Si m et m' sont deux entier naturels non nuls et premiers à p tels que $\mathrm{H}_m = \mathrm{H}'_m$, alors

$$m\mathbb{Z} = \mathrm{H}_m \cap \mathbb{Z} = \mathrm{H}_{m'} \cap \mathbb{Z} = m'\mathbb{Z}$$

en vertu de la question 2 (a) et donc $m = m'$.

(b) Quels que soient $m, m' \in \mathscr{N}_p$, $\mathrm{H}_{m'} \subset \mathrm{H}_m$ si et seulement si $m' \in \mathrm{H}_m$, donc si et seulement s'il existe $n \in \mathbb{Z}$ et $r \in \mathbb{N}$ tels que $m' = m\frac{n}{p^r}$, c'est-à-dire tels que $m'p^r = mn$. Cette condition revient à dire qu'il existe $r \in \mathbb{N}$ tel que m divise $m'p^r$; puisque m et p^r sont premiers entre eux, cela est le cas si et seulement si m divise m'. On a donc

$$\mathrm{H}_{m'} \subset \mathrm{H}_m \iff m | m'.$$

Soient $m, m' \in \mathscr{N}_p$ tels que $m|m'$. Puisque $\mathrm{H}_{m'} \subset \mathrm{H}_m$, $\mathrm{H}_{m'}$ est contenu dans le noyau de la projection canonique $\pi : \mathbb{Q}_p \to \mathbb{Q}_p/\mathrm{H}_{m'}$ et celle-ci induit donc un homomorphisme surjectif de groupes finis

$$\mathbb{Q}_p/\mathrm{H}_{m'} \to \mathbb{Q}_p/\mathrm{H}_m$$

dont le noyau est le sous-groupe $\mathrm{H}_m/\mathrm{H}_{m'}$ de $\mathbb{Q}_p/\mathrm{H}_{m'}$. On a donc

$$|\mathbb{Q}_p/\mathrm{H}_{m'}| = |\mathbb{Q}_p/\mathrm{H}_m||\mathrm{H}_m/\mathrm{H}_{m'}|,$$

d'où

$$(\mathrm{H}_m : \mathrm{H}_{m'}) = |\mathrm{H}_m/\mathrm{H}_{m'}| = \frac{|\mathbb{Q}_p/\mathrm{H}_{m'}|}{|\mathbb{Q}_p/\mathrm{H}_m|} = \frac{(\mathbb{Q}_p : \mathrm{H}_{m'})}{(\mathbb{Q}_p : \mathrm{H}_m)} = \frac{m'}{m}.$$

(c) Soient m et m' deux éléments de $\mathscr{N}_p$. Vu la question précédente, $\mathrm{H}_{mm'} \subset \mathrm{H}_m \cap \mathrm{H}_{m'}$ et donc $\mathrm{H}_m \cap \mathrm{H}_{m'}$ est un sous-groupe d'indice fini de $\mathbb{Q}_p$. En vertu des questions 3 (a), 2 (a) et 2(d), $\mathrm{H}_m \cap \mathrm{H}_{m'} = \mathrm{H}_k$, où k est l'unique entier naturel non nul tel que $(\mathrm{H}_m \cap \mathrm{H}_{m'}) \cap \mathbb{Z} = k\mathbb{Z}$. Comme $\mathrm{H}_m \cap \mathrm{H}_{m'} \cap \mathbb{Z} = (\mathrm{H}_m \cap \mathbb{Z}) \cap (\mathrm{H}_{m'} \cap \mathbb{Z})$, k est l'unique entier naturel tel que $m\mathbb{Z} \cap m'\mathbb{Z} = k\mathbb{Z}$. Le sous-groupe $m\mathbb{Z} \cap m'\mathbb{Z}$ de $\mathbb{Z}$ étant précisément l'ensemble des multiples communs de m et m', k est le plus commun multiple de m et m'.

Nous avons ainsi démontré : $\mathrm{H}_m \cap \mathrm{H}_{m'} = \mathrm{H}_{\mathrm{ppcm}(m,m')}$.

4. Soit $\pi : \mathbb{Q}_p \to \overline{\mathbb{Q}}_p = \mathbb{Q}_p/\mathbb{Z}$ la projection canonique et soit K un sous-groupe d'indice fini de $\overline{\mathbb{Q}}_p$. L'application π étant un homomorphisme de groupes, l'image réciproque $\widetilde{\mathrm{K}} = \pi^{-1}(\mathrm{K})$ de K est un sous-groupe de $\mathbb{Q}_p$ contenant $\mathbb{Z} = \pi^{-1}(\overline{0})$ et la projection π induit un isomorphisme du groupe quotient $\mathbb{Q}_p/\widetilde{\mathrm{K}}$ sur le groupe quotient $\overline{\mathbb{Q}}_p/\mathrm{K}$; par suite, $\widetilde{\mathrm{K}}$ est d'indice fini dans $\mathbb{Q}_p$.

Comme $\widetilde{\mathrm{K}} \cap \mathbb{Z} = \mathbb{Z}$, $\widetilde{\mathrm{K}} = \mathbb{Q}_p$ en vertu des questions 2 (a) et 2 (d) et donc $\mathrm{K} = \pi(\widetilde{\mathrm{K}}) = \overline{\mathbb{Q}}_p$. Nous venons ainsi de démontrer que $\overline{\mathbb{Q}}_p$ est l'unique sous-groupe d'indice fini de $\overline{\mathbb{Q}}_p$.