Correction partielle de l'interrogation du 14/10/2008

Cette petite correction est surtout prétexte à vous rappeler les erreurs récurrentes qu'il faut à tout prix éviter, et à vous donner une idée de ce que j'appelle "bien rédiger une réponse" (ici, la rédaction est volontairement détaillée).

1. Soit E un ensemble. Donner la définition d'une relation d'équivalence sur E.
$\rightsquigarrow$ Une relation d'équivalence $\mathcal{R}$ sur E est une relation binaire vérifiant les trois propriétés suivantes :

- ***Réflexivité :*** $\forall a \in E$, $a\mathcal{R}a$
- ***Symétrie :*** $\forall a, b \in E$, $a\mathcal{R}b \Rightarrow b\mathcal{R}a$
- ***Transitivité :*** $\forall a, b, c \in E$, si $a\mathcal{R}b$ et $b\mathcal{R}c$, alors $a\mathcal{R}c$

2. Montrer que la relation définie par : "a est en relation avec b si et seulement si a divise b" est une relation d'ordre sur l'ensemble $\mathbb{N}^*$.
$\rightsquigarrow$ On vous demande ici de le montrer, il faut donc tout faire en détail (je sais que c'est du cours, mais le but d'un contrôle continu est de vérifier que vous le connaissez justement).
Notons $|$ cette relation : on veut montrer que c'est une relation d'ordre sur $\mathbb{N}^*$. Nous avons donc trois points à vérifier :

- ***Réflexivité :*** Soit $a \in \mathbb{N}^*$. On a $a = a \times 1$ donc $a|a$.
- ***Antisymétrie :*** Soient a, $b \in \mathbb{N}^*$ tels que $a|b$ et $b|a$. Nous devons prouver que $a = b$.
  Dire que $a|b$ signifie qu'il existe $k \in \mathbb{Z}$ tel que $b = ka$. Comme a et b sont > 0, k est lui aussi > 0.
  De même, dire que $b|a$ signifie qu'il existe $k' \in \mathbb{Z}$ tel que $a = bk'$. Là encore, comme a et b sont > 0, k' est lui aussi > 0.
  On a donc en particulier : $a = kk'a$, ce qui implique, *puisque a est non nul*, que $kk' = 1$, et donc, *puisque k et k' sont* > 0, que $k = k' = 1$, c'est-à-dire que $a = b$.
- ***Transitivité :*** Soient a, b, $c \in \mathbb{N}^*$ tels que $a|b$ et $b|c$. Nous devons montrer que $a|c$.

Dire que $a|b$ signifie qu'il existe $k \in \mathbb{Z}$ tel que $b = ka$. De même, dire que $b|c$ signifie qu'il existe $k' \in \mathbb{Z}$ tel que $c = k'a$. Ceci implique en particulier que l'on a $c = (k'k)a$ avec $k'k \in \mathbb{Z}$, donc que $a|c$.

Conclusion : $|$ est bien une relation d'ordre sur $\mathbb{N}^*$.

3. Énoncer le théorème d'existence et d'unicité de la décomposition en facteurs premiers d'un entier $n \geq 2$.
$\rightsquigarrow$ Pour tout entier $n \geq 2$, il existe $r \in \mathbb{N}^*$, des entiers premiers $p_1, \cdots, p_r$ deux à deux distincts, et des entiers naturels non nuls $\alpha_1, \cdots, \alpha_r$ tels que n puisse s'écrire sous la forme $p_1^{\alpha_1} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$.
De plus, les couples $(p_1, \alpha_1), \cdots, (p_r, \alpha_r)$ sont uniques à permutation près.

4. Donner le reste de la division euclidienne de 58473625 par 37.
On a fait une dizaine de calculs de ce type en TD, ce qui vous a donné une dizaine d'occasions de vous faire réexpliquer la méthode.. Visiblement, ce n'était pas suffisant pour une bonne partie d'entre vous, donc je corrige cet exemple, qui sera le dernier.
Chercher le reste de la division euclidienne de 58473625 par 37 signifie que l'on cherche à combien est congru 58473625 modulo 37. Pour cela, on remarque que l'on a :

$$58473625 = 5\times10^7+8\times10^6+4\times10^5+7\times10^4+3\times10^3+6\times10^2+2\times10^1+5\times10^0$$

avec $10^0 \equiv 1$ [37], $10^1 \equiv 10$ [37], $10^2 \equiv -11$ [37] et $10^3 \equiv 1$ [37], et donc $10^4 \equiv 10$ [37], $10^5 \equiv -11$ [37], $10^6 \equiv 1$ [37] et $10^7 \equiv 10$ [37]. Par compatibilité de $\equiv$ à l'addition et à la multiplication, on a donc :

$$58473625 \equiv 5\times10+8\times1+4\times(-11)+7\times10+3\times1+6\times(-11)+2\times10+5\times1 \text{ [37]}$$

ce qui donne :

$$58473625 \equiv 58 - 44 + 73 - 66 + 25 \text{ [37]}$$

ou encore, en calculant les termes par paquets de deux (dans l'ordre) :

$$58473625 \equiv 14 + 7 + 25 \text{ [37]}$$

Or $14 + 25 = 39$ est congru à 2 modulo 37 : on en déduit donc que :

$$58473625 \equiv 2 + 7 \text{ [37]}$$

soit donc que 58473625 est congru à 9 modulo 37. Comme $0 \leq 9 < 37$, on peut en conclure que le reste de la division euclidienne de 58473625 par 37

est égal à 9.

5. Parmi les sous-ensembles de $\mathbb{R}$ suivants, dire (en justifiant) ceux qui sont des groupes pour l'addition : $\mathbb{Q}$, l'ensemble des éléments pairs de $\mathbb{Z}$.
$\rightsquigarrow$ Rappelons tout d'abord que pour montrer qu'un ensemble est un groupe, il faut **AVANT TOUTE CHOSE** vérifier que la loi est une loi de composition **interne**, c'est-à-dire que si j'applique la loi à deux éléments de l'ensemble, je trouve encore un élément de l'ensemble !
Ensuite, il faut vérifier que la loi est **associative**, ce que beaucoup d'entre vous oublient encore de faire !!!

D'autre part, la méthode la plus souvent employée pour montrer que quelque chose est un groupe est de montrer que c'est un **sous-groupe** d'un groupe connu, ce qui évite justement d'avoir à vérifier l'associativité à la main. Pour cela, encore faut-il vérifier proprement que c'est un sous-groupe !!

Pour $(\mathbb{Q}, +)$: On sait que $(\mathbb{R}, +)$ est un groupe. Nous allons donc montrer que $(\mathbb{Q}, +)$ en est un sous-groupe :

1. *Inclusion* : $\mathbb{Q}$ est bien inclus dans $\mathbb{R}$.
2. *Stabilité* : Soient x, $y \in \mathbb{Q}$. Nous devons montrer que $x + y \in \mathbb{Q}$.
   On peut écrire $x = \dfrac{p}{q}$ et $y = \dfrac{a}{b}$ avec p, $a \in \mathbb{Z}$ et q, $b \in \mathbb{N}^*$. On a alors :
   $$x + y = \frac{p}{q} + \frac{a}{b} = \frac{pb + qa}{bq}$$
   avec $pb + qa \in \mathbb{Z}$ et $bq \in \mathbb{N}$, donc $x + y \in \mathbb{Q}$.
3. *Possession de l'élément neutre* : On **sait** que 0 est élément neutre pour $+$ dans $\mathbb{R}$. Il nous suffit donc de prouver que $0 \in \mathbb{Q}$, ce qui est le cas $(0 = \dfrac{0}{1})$.
4. *Stabilité pour le symétrique* : Là encore, on **sait** que si x est un réel, son symétrique pour $+$ est donné par $-x$. Il suffit donc de vérifier que, pour tout $x \in \mathbb{Q}$, $-x \in \mathbb{Q}$.
   Or, si $x = \dfrac{p}{q}$, alors $-x = \dfrac{-p}{q}$ est encore dans $\mathbb{Q}$.

Conclusion : $(\mathbb{Q}, +)$ est bien un groupe (car c'est un sous-groupe du groupe $(\mathbb{R}, +)$).

Pour $(2\mathbb{Z}, +)$: On sait que $(\mathbb{R}, +)$ est un groupe. Nous allons donc montrer que $(2\mathbb{Z}, +)$ en est un sous-groupe :

1. *Inclusion* : $2\mathbb{Z}$ est bien inclus dans $\mathbb{R}$.

2. *Stabilité* : Soient x, $y \in 2\mathbb{Z}$. Nous devons montrer que $x+y \in 2\mathbb{Z}$. Par définition, on peut écrire $x = 2a$ et $y = 2b$ avec a, $b \in \mathbb{Z}$. On a alors :

$$x + y = 2a + 2b = 2(a + b)$$

avec $a + b \in \mathbb{Z}$, donc $x + y \in 2\mathbb{Z}$.

3. *Possession de l'élément neutre* : On **sait** que 0 est élément neutre pour $+$ dans $\mathbb{R}$. Il nous suffit donc de prouver que $0 \in 2\mathbb{Z}$, ce qui est le cas $(0 = 20)$.
4. *Stabilité pour le symétrique* : Là encore, on **sait** que si x est un réel, son symétrique pour $+$ est donné par $-x$. Il suffit donc de vérifier que, pour tout $x \in 2\mathbb{Z}$, $-x \in 2\mathbb{Z}$.
   Or, si $x = 2b$ avec $b \in \mathbb{Z}$, alors $-x = 2(-b)$ est encore dans $2\mathbb{Z}$.

Conclusion : $(2\mathbb{Z}, +)$ est bien un groupe (car c'est un sous-groupe du groupe $(\mathbb{R}, +)$).

Je ne corrige pas ici les questions subsidiaires. Remarquons tout de même que lorsque l'on donne un contre-exemple, il faut justifier en quoi c'est un contre-exemple, et ne pas se contenter de vagues généralités (par exemple : $GL_2(\mathbb{R})$ n'est pas commutatif car $AB \neq BA$. Qui sont A et B ?).