Université LYON 1
L1 Mathématiques
Automne 2009

UE Math I Algèbre. Seq. 1
Corrigé du CC1

Question 1 (4 pts)

(1) Enoncer le *principe de récurrence (simple)* sur $\mathbf{N}$.

(2) Enoncer le *théorème de division euclidienne* dans $\mathbf{Z}$.

(3) Enoncer le *théorème de factorisation en premiers* dans $\mathbf{N}$. Dresser la liste des diviseurs d'un entier $n \in \mathbf{N}$.

(4) Dans $\mathbf{Z}$, définir la notion de *congruence modulo un entier* $n \in \mathbf{N}$. Enoncer ses propriétés par rapport à l'addition $+$ et la multiplication $\times$ des entiers relatifs.

Enoncés:
(1) soit $P(n)$ une assertion portant sur l' entier naturel $n \in \mathbf{N}$. Pour que $P(n)$ soit vraie pour tout $n \geq n_0$ il faut et il suffit que
- $P(n_0)$ soit vraie
- $P(n) \Rightarrow P(n+1)$ soit vraie pour tout $n \geq n_0$.

(2) Pour tout $a \in \mathbf{Z}$ et $b \in \mathbf{N} \setminus \{0\}$, il existe un unique couple $(q, r) \in \mathbf{Z} \times \mathbf{N}$ tel que

$$a = bq + r, \quad 0 \leq r < b.$$

(3) Voici une manière d'écrire ce théorème (qui diffère quelque peu de celle du cours):
pour tout entier $n \in \mathbf{N} \setminus \{0, 1\}$ il existe d'uniques nombres premiers $p_1 < p_2 < \cdots < p_s$ et d'uniques entiers $r_1, r_2, \ldots, r_s \in \mathbf{N} \setminus \{0\}$ tels que

$$n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}.$$

L'ensemble des diviseurs positifs de n est

$$Div_+(n) = \{p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}, \quad 0 \leq m_i \leq r_i \text{ pour tout } i \in \{1, \ldots, s\}\}.$$

(4) Deux entiers relatifs a et b sont dits congrus modulo $n \in \mathbf{N} \setminus \{0\}$ si n divise $b - a$. On écrit alors $a \equiv b[n]$.
Si $a \equiv a'[n]$ et $b \equiv b'[n]$ alors $(a + b) \equiv (a' + b')[n]$ et $ab \equiv a'b'[n]$.

Question 2 (6 pts)

Répondre par *vrai* ou *faux* aux assertions suivantes en justifiant votre choix par un bref argument ou un contre-exemple.

(1) Il y a une infinité de nombres premiers $p \in \mathbf{N}$:

C'est *vrai*. Voici une preuve par l'absurde: on sait que tout entier $n \geq 2$ admet un facteur premier. S'il n'existait qu'un nombre fini de nombres premiers, disons $p_1, \ldots, p_l$, l'entier $p_1 p_2 \cdots p_l + 1$, n'étant divisible par aucun des $p_1, \ldots, p_l$, n'admettrait aucun facteur premier.

(2) si 33 et 77 divisent l'entier $n \in \mathbf{N}$ alors 231 divise aussi n:

C'est *vrai*. On a $33 = 3 \cdot 11$ et $77 = 7 \cdot 11$, dès lors $3, 7, 11$ divisent n. Comme ils sont deux à deux étrangers, le lemme de Gauss implique que $3 \cdot 7 \cdot 11 = 231$ divise aussi n.

(3) 2^{1111} a 1112 diviseurs positifs:

C'est *vrai*. Par l'énoncé (3) de la question 1, les diviseurs de 2^{1111} sont les entiers 2^m pour $0 \leq m \leq 1111$. Il y en a $1 + 1111 = 1112$.

(4) 444444444 est un multiple de 6:

C'est *vrai*. C'est clairement un multiple de 2. C'est aussi un multiple de 3 car l'entier n dont l'écriture décimale est $a_N a_{N-1} \cdots a_1 a_0$, $0 \leq a_i \leq 9$, $a_N \neq 0$, est un multiple de 3 ssi la somme $\sum_{i=0}^{N} a_i$ est un multiple de 3 (dans notre cas, cette somme vaut 36). Par Gauss, c'est donc un multiple de $2 \cdot 3 = 6$.

(5) quelquesoit l'entier strictement positif $n \leq 10$, 11 divise $n^{10} - 1$ et 13 divise $n^6 - 1$ ou $n^6 + 1$:

C'est *vrai*. Par Fermat, pour tout nombre premier p et tout entier $n \neq 0$ non multiple de p, on a $n^{p-1} \equiv 1[p]$ i.e. p divise $n^{p-1} - 1$. En particulier 11 divise $n^{10} - 1$ et 13 divise $n^{12} - 1 = (n^6 - 1)(n^6 + 1)$ ce qui implique (parcequ'il est premier) que 13 divise l'un des facteurs $(n^6 - 1)$, $(n^6 + 1)$.

(6) Il y a une infinité d'entiers $n \in \mathbf{Z}$ pour lesquels le reste de la division par 2 est égal au reste de la division par 3:

C'est *vrai*. Par restes chinois, on sait que pour p et q étrangers le système de congruences $x \equiv a[p]$ et $x \equiv b[q]$ admet une infinité de solutions $x \in \mathbf{Z}$. Dans notre cas $a = b \in \{0, 1\}$ et $p = 2, q = 3$.

Il se fait qu'il s'agit d'un cas particulièrement simple de restes chinois que l'on peut résoudre immédiatement par Gauss: $2 \mid x - r$ et $3 \mid x - r$ équivaut à $6 \mid x - r$ i.e. $x = r + 6k$, $k \in \mathbf{Z}$.

Question 3 (5 pts)

(1) Déterminer tous les entiers $u, v \in \mathbf{Z}$ tels que $11\,u + 7\,v = 1$.

(2) Déterminer le reste de la division euclidienne de 2^{3333} par 7 et par 11.

(3) En déduire le reste de la division euclidienne de 2^{3333} par 77.

Solution:
(1) Par l'algorithme d' Euclide ou par simple observation, on voit que $(u, v) = (2, -3)$ est solution. Supposons que (u', v') soit une autre solution i.e. que $11u' + 7v' = 1$. Par soustraction, il vient

$$11\,(u' - u) + 7\,(v' - v) = 0 \qquad (E)$$

dès lors $7 \mid 11(u' - u)$ et par Gauss $7 \mid (u' - u)$. Il existe donc $m \in \mathbf{Z}$ tel que $(u' - u) = 7m$ et (E) devient $11 \cdot 7m = -7 \cdot (v' - v)$ i.e. $(v' - v) = -11m$.
Conclusion: les solutions sont de la forme $(2 + 7m, -3 - 11m)$ pour $m \in \mathbf{Z}$. On vérifie ensuite que tout m convient.

(2) Par Fermat $2^6 \equiv 1[7]$. En écrivant $3333 = 6 \cdot 555 + 3$, on voit que

$$2^{3333} = \left(2^6\right)^{555} 2^3 \equiv 8[7] = 1[7].$$

On aurait pu observer directement $2^3 \equiv 1[7]$ et utiliser $3333 = 3 \cdot 1111$.
A nouveau par Fermat, $2^{10} \equiv 1[11]$. En écrivant $3333 = 10 \cdot 333 + 3$, on trouve

$$2^{3333} \equiv 2^3[11] = 8[11].$$

(3) L'entier $N = 2^{3333}$ satisfait le système de congruences $N \equiv 1[7]$, $N \equiv 8[11]$ dont on sait (cf cours) que les solutions sont de la forme $r + 77m, m \in \mathbf{Z}$. Reste à trouver r. Pour ce faire, on peut soit résoudre explicitement le système comme fait en tds, soit observer directement que $r = 8$ convient: en effet, $7 \mid N - 8$ et $11 \mid N - 8$ équivaut à $77 \mid N - 8$.