Université Lyon 1 | Automne 2008/2009
Math I Algèbre | Seq 2 (J. Melleray)

Contrôle Continu n° 1 - Correction

Exercice 1. (*2 pts*)
Sachant que $96842 = 256 \times 375 + 842$, déterminer le reste de la division euclidienne de 96842 par 256.
Correction.
On a $842 = 256 \times 3 + 74$; avec l'égalité fournie par l'énoncé on obtient $96842 = 256 \times 378 + 74$, et comme $0 \leq 74 \leq 255$ on voit que le reste de la division euclidienne de 96842 par 256 est égal à 74.

Exercice 2. (*4 pts*).
Calculer le reste de la division de 100^{100} par 17.
Correction. On utilise la compatibilité de la congruence avec l'addition et la multiplication.
On a $6 \times 17 = 102$, ce dont on déduit $100 \equiv -2\,[17]$. Par suite on voit successivement que

$$100^2 \equiv 4\ [17], \qquad 100^3 \equiv -8\ [17], \qquad 100^4 \equiv 16\,[17]\ .$$

Autrement dit, $100^4 \equiv -1\,[17]$ et comme $100 = 25 \times 4$ on obtient

$$100^{100} \equiv (100^4)^{25} \equiv (-1)^{25} \equiv -1\,[17]\ .$$

Comme le reste de la division euclidienne de 100^{100} par 17 est le seul nombre r entre 0 et 16 tel que $r \equiv 100^{100}\ [17]$, on en déduit que ce reste est égal à 16.

Exercice 3. (*5 pts*)
(a) Lors d'un calcul, un étudiant a divisé un nombre n par 8 et a obtenu un reste égal à 4 ; il a aussi divisé n par 12 et a obtenu un reste égal à 3. Qu'en pensez-vous ?
(b) Pendant le même examen, un étudiant qui avait fini en avance, a divisé le millésime de l'année par 17 et a obtenu 16 pour reste ; il a aussi divisé le millésime par 12 et a obtenu un reste égal à 1. Sachant qu'après l'examen l'étudiant en question a pris un tramway à énergie électrique, en quelle année cela se passait-il ?
Correction. (a) Comme n est congru à 4 modulo 8, n doit être pair ; mais comme n est congru à 3 modulo 12 on voit aussi que n doit être impair. Il y a donc un problème : aussi impensable que cela puisse paraître, l'étudiant a dû faire une erreur de calcul.
(b) Appelons m le millésime de l'année où se déroule l'examen. D'après l'énoncé, on doit avoir $m \equiv 16\,[17]$ et $m \equiv 1\,[12]$. Comme 12 et 17 sont premiers entre eux, on sait grâce au théorème des restes chinois que ce système a des solutions, et que si m_0 est une solution alors l'ensemble des solutions est exactement l'ensemble des entiers congrus à m_0 modulo $12 \times 17 = 204$.
Pour trouver une solution particulière, on commence par appliquer l'algorithme d'Euclide :

$$17 = 12 + 5; \qquad 12 = 2 \times 5 + 2; \qquad 5 = 2 \times 2 + 1\ .$$

On en déduit une relation de Bezout entre 17 et 12 :

$$1 = 5 - 2 \times 2 = 5 - 2(12 - 2 \times 5) = 5 \times 5 - 2 \times 12 = 5(17 - 12) - 2 \times 12 = 5 \times 17 - 7 \times 12\ = 85 - 84.$$

En particulier, 85 vaut 0 modulo 17 et 1 modulo 12, tandis que 84 vaut -1 modulo 17 et 0 modulo 12.
On cherche un entier qui vaut 16 modulo 17 et 1 modulo 12, ou encore -1 modulo 17 et 1 modulo 12.

Grâce à notre relation de Bezout, on voit donc que $m_0 = 85 + 84 = 169$ est solution. Maintenant, on sait que le millésime m qui nous intéresse s'écrit $169 + 204k$ pour un entier k, et que $1900 \leq m \leq 2009$. Il y a au plus un m congru à m_0 modulo 204 et appartenant à cet intervalle.
En tâtonnant un peu, on voit que $m = 169 + 204 \times 9 = 2005$ est solution. Par conséquent, l'examen se tenait en 2005.

Exercice 4. (*5pts*).
(a) Montrer par récurrence que, pour tout $n \in \mathbb{N}$ et tout entier $k \geq 1$ on a

$$2^{2^{n+k}} - 1 = (2^{2^n} - 1). \prod_{i=0}^{k-1} (2^{2^{n+i}} + 1) \ .$$

(b) Montrer que, pour tous $n, m \in \mathbb{N}$ tels que $n \neq m$, les entiers $2^{2^n} + 1$ et $2^{2^m} + 1$ sont premiers entre eux.
Indication : on pourra utiliser (a) pour montrer que leur pgcd divise 2*, puis conclure.*
(c) En déduire une nouvelle preuve du fait qu'il existe une infinité de nombres premiers.
Correction. (a) Fixons n, et raisonnons par récurrence sur k.
On a $(2^{2^n} - 1)(2^{2^n} + 1) = (2^{2^n})^2 - 1 = 2^{2^{n+1}} - 1$, et on voit donc que l'égalité qu'on souhaite établir est vraie pour $k = 1$.
Supposons maintenant que notre égalité est vraie au rang k, et essayons d'établir qu'elle est vraie au rang $k + 1$. On a

$$2^{2^{n+k+1}} - 1 = (2^{2^{n+k}})^2 - 1 = (2^{2^{n+k}} - 1)(2^{2^{n+k}} + 1) \ .$$

En utlisant l'hypothèse de récurrence, on en déduit que

$$2^{2^{n+k+1}} - 1 = \big((2^{2^n} - 1). \prod_{i=0}^{k-1} (2^{2^{n+i}} + 1)\big).(2^{2^{n+k}} + 1) = (2^{2^n} - 1). \prod_{i=0}^{k} (2^{2^{n+i}} + 1) \ .$$

Par conséquent l'égalité est vraie au rang $k + 1$; par récurrence, on en déduit donc que cette égalité est vraie pour tout entier $k \geq 1$.
(b) Pour nous simplifier la vie, notons, pour $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$. Supposons par exemple que $n < m$, et posons $m = n + k$. Alors on a, d'après la question (a) :

$$F_m - 2 = (F_n - 2). \prod_{i=0}^{k-1} F_{n+i}$$

Appellons d le pgcd de F_m et F_n. Comme d divise F_n, d divise $\prod_{i=0}^{k-1} F_{n+i}$; et puisque d divise F_m on en déduit que d divise $F_m - (F_n - 2). \prod_{i=0}^{k-1} F_{n+i} = 2$. Par conséquent, si $m \neq n$ alors $d = \text{pgcd}(F_n, F_m)$ divise 2, c'est-à-dire que $d = 1$ ou $d = 2$. Comme tous les F_n sont impairs, on en déduit que $d = 1$.
(c) Pour tout $n \in \mathbb{N}$, $F_n \geq 2$ et donc F_n a au moins un diviseur premier ; choisissons un tel diviseur premier et appelons-le p_n. Comme F_n et F_m sont premiers entre eux si $n \neq m$, que p_n divise F_n et p_m divise F_m, on doit avoir $p_n \neq p_m$ dès que $n \neq m$. Donc $\{p_n : n \in \mathbb{N}\}$ est un ensemble infini de nombres premiers.