

Correction du partiel 23 novembre 2017

Exercice 1

- 1) En utilisant l'algorithme d'Euclide, on obtient le tableau suivant :

	1	7	2	1	2	
67	59	8	3	2	1	0
1	0	1	-7	15	-22	
0	1	-1	8	-17	25	

- 1.1) On en déduit que le plus grand diviseur commun de a et b vaut 1, autrement dit a et b sont premiers entre eux. On peut aussi remarquer que 59 et 67 sont des nombres premiers distincts, donc ils sont premiers entre eux.
- 1.2) On obtient de plus la relation de Bézout

$$(1) \quad 25 \times 59 - 22 \times 67 = 1.$$

Par suite, le couple $(u, v) = (-22, 25)$ convient.

- 1.3) On déduit de la démonstration du théorème chinois (th. 4.3 du cours) et de l'égalité (1), que l'entier

$$3 \times 25 \times 59 - 2 \times 22 \times 67 = 1477$$

satisfait les deux congruences de l'énoncé (*loc. cit.*, égalité (11)). Un tel entier est unique modulo $59 \times 67 = 3953$. C'est donc le plus petit entier naturel vérifiant la condition cherchée.

- 2.1) Pour tout $n \geq 1$, on a

$$2^{2^n} = (2^2)^{2^{n-1}} \equiv 1 \pmod{3}.$$

- 2.2) Soit $n \geq 1$ un entier. D'après la question précédente, t_n est divisible par 3. On $t_n > 3$, donc t_n n'est pas premier. Par ailleurs, on a $t_0 = 7$. Ainsi, $n = 0$ est le seul entier naturel pour lequel t_n soit un nombre premier.
- 3) Soit p un nombre premier divisant $3^p + 7$. D'après le petit théorème de Fermat, p divise $3^p - 3$ (cor. 4.3). Il en résulte que p divise $3^p + 7 - (3^p - 3) = 10$, d'où $p = 2$ ou $p = 5$. Inversement, 2 divise $3^2 + 7$ et 5 divise $3^5 + 7 = 250$. L'ensemble cherché est donc $\{2, 5\}$.

Exercice 2

- 1) Soit φ la fonction indicatrice d'Euler. L'ordre de G est $\varphi(27)$, qui est égal à 18 (cor. 4.1).
- 2) Cela résulte du fait que 2 est premier avec 27 (th. 4.1).
- 3) On peut remarquer que $2 \times 14 = 28$, qui est congru à 1 modulo 27. Par suite, on a $\overline{2}^{-1} = \overline{14}$.
- 4) D'après le théorème de Lagrange (th. 2.1), on a $\overline{2}^{18} = \overline{1}$. Par suite, l'ordre d cherché divise 18. On a donc $d \in \{1, 2, 3, 6, 9, 18\}$. On a $2^6 \equiv 10 \pmod{27}$ et $2^9 \equiv -1 \pmod{27}$. Il en résulte que l'on a $d = 18$ (prop. 2.9).
- 5) C'est une conséquence directe des questions 1 et 4.
- 6) L'ordre de $\overline{2}^{12}$ est donc $\frac{18}{\text{pgcd}(12, 18)}$, qui est égal à 3 (prop. 2.8). On peut aussi remarquer que l'on a $(\overline{2}^{12})^3 = \overline{2}^{36} = \overline{1}$ et $\overline{2}^{12} \neq \overline{1}$.
- 7) L'entier 18 possède six diviseurs positifs, donc G possède exactement six sous-groupes (th. 2.4, assertion 3).
- 8) Parce que G est cyclique d'ordre 18, son nombre de générateurs est $\varphi(18) = 6$ (th. 2.5).

Exercice 3

- 1.1) Vérifions que f est injective. Considérons pour cela des éléments x et y de A tels que $f(x) = f(y)$. On obtient $a(x - y) = 0$. Parce que A est intègre et que a est non nul, on en déduit que $x = y$, d'où l'assertion. L'ensemble A étant fini, f est donc aussi une surjection de A sur A , d'où le résultat.
 - 1.2) D'après la question précédente, il existe $x \in A$ tel que $f(x) = 1$. Ainsi, a est inversible.
 - 1.3) Tout élément non nul de A étant inversible, A est un corps.
(On obtient ainsi la proposition 3.2 du cours.)
 - 2) Il existe un élément non nul x dans I . Il est inversible car A est un corps. Par définition d'un idéal, $xx^{-1} = 1$ appartient donc à I , ce qui implique $I = A$.
 - 3) L'anneau $A \times A$ n'est pas intègre, car $(1, 0)(0, 1) = (0, 0)$ et A étant intègre, on a en particulier $1 \neq 0$, donc $(1, 0)$ et $(0, 1)$ sont non nuls (voir les exemples 3.7).
 - 4) Soit A^* le groupe des éléments inversibles de A . Le groupe des éléments inversibles de $A \times A$ est $A^* \times A^*$ (lemme 3.4). L'ordre de A^* étant $n - 1$, celui de $A^* \times A^*$ est donc $(n - 1)^2$.
-