Licence de Mathématiques.
Université d'Artois.

ARITHMÉTIQUE

Examen session 2 (28 février 2011)- Éléments de correction

Cours-Application. cf cours. Enfin, l'inverse de $\bar{x}^s$ dans $\mathbb{Z}/p\mathbb{Z}$ est $\bar{x}^{p-1-s}$: en effet, $p-1-s \in \mathbb{N}$ et $\bar{x}^{p-1-s}.\bar{x}^s = \bar{x}^{p-1} = \bar{1}$, d'après Fermat.

Exercice 1.1. Cf T.D.

2. (Cf T.D.) On constate que $\frac{1}{2} + i\frac{\sqrt{3}}{2} = \mathrm{e}^{i\pi/3} = \mathrm{e}^{2i\pi/6}$.

Posons $N = 2011000000000000000000000000002012$: ce qui nous intéresse est donc le comportement de N modulo 6. Comme $\rho(N) = 9 \equiv 0 \quad [3]$, on voit immédiatement que N est divisible par 3, il l'est aussi clairement par 2, donc (2 et 3 premiers entre eux): N est divisible par 6 et s'écrit donc $6q$ où $q \in \mathbb{N}$. Ainsi, on a

$$\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)^{2011000000000000000000000000002012} = \mathrm{e}^{2i\pi N/6} = \mathrm{e}^{2i\pi q} = 1.$$

Exercice 3.

1) Clairement le lecture de l'énoncé donne $N \equiv 6\,[17]$; $N \equiv 10\,[11]$; $N \equiv 3\,[4]$.

2) On a $N \equiv 10 \equiv -1 \quad [11]$ et $N \equiv 3 \equiv -1 \quad [4]$. Ainsi, 11 divise $N-(-1) = N+1$. De même, 4 divise $N+1$. Comme 4 et 11 sont premiers entre eux, on a 4×11 divise $N+1$.

3) On sait d'avance que des solutions existent: 44 et 17 sont premiers entre eux. Comme d'habitude, on applique par exemple l'algorithme d'Euclide: $\alpha = -5$ et $\beta = 13$ conviennent.

4) $6-(-1) = 7 = 7\times(-5\times 44+13\times 17)$ donc $n_0 = 6-91\times 17 = -1-35\times 44 = -1541$ convient.

5) Soit $n \in \mathbb{Z}$ tel que $n \equiv 6 \quad [17]$ et $n \equiv -1 \quad [44]$. On a donc $n \equiv n_0 \quad [17]$ et $n \equiv n_0 \quad [44]$. Ainsi 44 et 17 divisent $n - n_0$ donc par mutuelle primalité, 44×17 divise $n - n_0$: on en déduit que

$$n = n_0 + 748k \qquad \text{avec} \quad k \in \mathbb{Z}.$$

Réciproquement, il est clair que toutes ces valeurs de n conviennent.

6) Il n'y a qu'un élément de $\{-1541 + 748k |\ k \in \mathbb{Z}\}$ dans $\{0, \ldots, 1000\}$. Il s'agit de $N = 703$.