Licence de Mathématiques.
Université d'Artois.
Pascal Lefèvre

ARITHMÉTIQUE
Examen - session 2
Éléments de correction.

Exercice 1.

1)a) On cherche les années $N \geq 2008$ telles $N = 1996 + \lambda 107$, où $\lambda \in \mathbb{N}$: à partir de 1996 puis tous 107 ans; autrement dit $N \equiv 1996\,[107]$. De même, on a aussi $N \equiv 2000\,[17]$.

Ainsi, le problème se formule de la façon annoncée avec $\alpha = 1996$, $a = 107$, $\beta = 2000$, $b = 17$.

b) Ce problème est équivalent à $N \geq 2008$ et $N = \alpha + na$, où $n \in \mathbb{Z}$, et $N = \beta + mb$, où $m \in \mathbb{Z}$. Ceci implique $\beta - \alpha = na - mb$, où $(n, m) \in \mathbb{Z}^2$ et, comme $N \geq 2008$, on doit avoir $m \geq 1$.

Réciproquement si on trouve $(n, m) \in \mathbb{Z}^2$ tels que $\beta - \alpha = na - mb$ avec $m \geq 1$. Alors $N = \beta + mb = \alpha + na$ est clairement solution du problème initial.

2) On remarque que a et b sont premiers entre eux. Plus précisément, l'algorithme d'Euclide donne $a = 6b + r$ avec $r = 5$. Puis $b = 3r + r'$ avec $r' = 2$. Enfin $r = 2r' + 1$. Ainsi, $1 = 7a - 44b$. Ce qui confirme le primalité entre a et b et donne une solution de l'équation de Bézout. Ainsi $(28, 176)$ est une solution particulière. Soient (n, m) une solution alors $28a - 176b = na - mb$ donc a divise $b(176 - m)$. Comme a et b sont premiers entre eux, a divise $176 - m$ donc $m = 176 + ka$ où $k \in \mathbb{Z}$. En remplaçant, on a $n = 28 + kb$. Réciproquement, ces couples (n, m) sont solutions. Finalement les solutions sont exactement les couples $(28 + kb, 176 + ka)$ où k décrit $\mathbb{Z}$.

3) Parmi les solutions trouvées dans 2., on cherche celles telles que $m \geq 1$, or c'est équivalent à $k \geq -1$. Ainsi, les solutions du problème initial sont les années $N = 2000 + (176 + k107)17$ où $k \geq -1$, ou encore $N = 2000 + (69 + p107)17$ où $p \in \mathbb{N}$. Autrement dit, les comètes A et B seront visibles de la terre toutes les deux en 3173 puis tous les 1819 ans.

Exercice 2. cf TD.

Exercice 3.

1) En appliquant Bézout, on obtient l'existence d'entiers p et q tels que $bq - cp = d$.

i) On peut toujours supposer p et q positifs, quitte à les remplacer respectivement par $p + kb$ et $q + kc$, avec k assez grand. Dans $\mathbb{Z}/n\mathbb{Z}$, on sait que $\bar{a}^b = \bar{a}^c = \bar{1}$ donc

$$\bar{a}^d = (\bar{a}^c)^p.\bar{a}^d = \bar{a}^{\,d+cp} = \bar{a}^{bq} = (\bar{1})^q = \bar{1}.$$

ii) On pouvait aussi utiliser une variante en prenant directement $\bar{1} = (\bar{a})^{bq-cp} = \bar{a}^d$, auquel cas l'usage des puissances négatives est justifié par le fait que $\bar{a}$ est nécessairement inversible dans $\mathbb{Z}/n\mathbb{Z}$, puisque $\bar{a}^c = \bar{1}$ (l'inverse de $\bar{a}$ est $\bar{a}^{c-1}$).

Autrement dit: n divise $a^d - 1$ donc $a^d \equiv 1\,[n]$.

2)a) $a^2 \equiv -1\,[p]$ i.e. $\bar{a}^2 = \overline{-1} = -\bar{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. Donc $\bar{a}^4 = (-\bar{1})^2 = \bar{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. Ainsi $a^4 \equiv 1\,[p]$. D'autre part, d'après Fermat, $a^{p-1} \equiv 1\,[p]$ car p est premier et $\bar{a} \neq \bar{0}$. Enfin, notons d le pgcd de $p-1$ et 4. Comme d divise 4, on a $d = 1$ ou 2 ou 4. Or $p-1$ est pair et n'est pas divisible par 4 par hypothèse : $p - 1 \equiv 2\,[4]$. Donc $d = 2$.

Ainsi, par 1., on a $a^2 \equiv 1\,[p]$.

b) Ainsi, si a était une solution, on aurait dans $\mathbb{Z}/p\mathbb{Z}$: $\bar{a}^2 = \overline{-1}$ et $\bar{a}^2 = \bar{1}$ donc $\overline{-1} = \bar{1}$ i.e. p divise 2. Faux. L'ensemble des solutions est donc vide.

3)a) Dans $\mathbb{Z}/p\mathbb{Z}$, on a alors $\bar{x}$ non nul donc inversible (pour le produit). Ainsi il existe $z \in \{1, \cdots, p-1\} \subset \mathbb{N}$ tel que $\bar{x}.\bar{z} = \bar{1}$.

Or, par hypothèse: $-(\bar{y})^2.(\bar{z})^2 = (\bar{x})^2.(\bar{z})^2$ puisque $(\bar{x})^2 + (\bar{y})^2 = \bar{0}$. On en déduit que $(\bar{y})^2.(\bar{z})^2 = -\bar{1}$.

b) Mais alors $a = -yz$ serait une solution dans 2.b.: il n'y en a pas ! Donc p divise x. Mais alors p divise x^2 et $x^2 + y^2$ donc y^2. Comme p est premier, p divise y lui-même.

4) Supposons que $N = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ où $s \geq 1$; les $p_1, \dots, p_s$ sont des nombres premiers distincts et les $\alpha_1, \dots, \alpha_s$ sont des entiers non nuls. Supposons que N est somme de deux carrés $N = X^2 + Y^2$ et que l'un des nombres premiers congrus à 3 modulo 4 intervenant dans la décomposition de N apparaisse avec un exposant pair. Notons le p et $\alpha = 2k + 1 \geq 1$ l'exposant associé. D'après ce qui précède p divise X et Y. Notons alors $j \geq 1$ le plus grand exposant tel que p^j divise à la fois X et Y. Donc p^{2j} divise N et ainsi $2j \leq \alpha$ donc $j \leq k$. On peut écrire $N = p^{2j}N'$ où $N' = x^2 + y^2$ (en fait $X = p^j x$ et $Y = p^j y$). Par définition de j, p ne divise pas x ou ne divise pas y. Mais comme p^α divise N et $2j < 2k + 1 = \alpha$, on a p divise N'. D'après 3., p divise x et y. Contradiction.

Remarque: on peut aussi rédiger autrement la seconde partie en faisant une récurrence, au lieu d'introduire j.