Licence de Math-Info: L2MI. Université d'Artois.
04/01/10. Durée 3h

# Examen - session 1
# ARITHMÉTIQUE

Éléments de correction

**Cours et application.**

3) On fait comme cela a été vu en cours et en TD. Ici, en appliquant l'algorithme d'Euclide, on trouve une relation de Bézout: $(-39) \times 441 + 43 \times 400 = 1$. On en déduit que $(-117, 129)$ est une solution particulière. Puis, on montre que l'ensemble des solutions est

$$\Big\{(-117 + 400k, 129 - 441k) |\ k \in \mathbb{Z}\Big\}$$

**Exercice 1 et 2.**

Voir T.D.

**Exercice 3.**

1)a) On remarque que $p$ n'est pas pair donc ne peut être congru à 0 ou 2 modulo 4. D'autre part, si $p \equiv 1\ [4]$ alors $p$ est un des $q_j$ par hypothèse. Mais alors $p$ divise $A$ donc $A^2$. Comme $p$ divise aussi $B$, on aurait $p$ divise $B - A^2 = 1$ ce qui est impossible. Ainsi, la seule possibilité est $p \equiv 3\ [4]$.

b) i) On a $A^4 - 1 = (A^2 - 1)(A^2 + 1) = B(A^2 - 1)$. Comme $p$ divise $B$, on a la conclusion.

ii) On a $4m + 2 = p - 1$ et $p$ ne divise pas $A$ (cf justification du 1.). Donc, d'après le petit théorème de Fermat, $p$ divise $A^{p-1} - 1 = A^{4m+2} - 1$.

c) On remarque que $A^{4m+2} - 1 = A^{4m+2} - A^2 + A^2 - 1 = A^2(A^{4m} - 1) + (A^2 - 1)$. Mais $A^{4m} - 1 = (A^4 - 1)\Big(A^{4(m-1)} + \ldots + 1\Big)$ que l'on écrit $(A^4 - 1)q$. Donc $A^{4m+2} - 1 = (A^4 - 1)Q + (A^2 - 1)$ où $Q = qA^2$. Ainsi pour conclure, il suffit de remarquer que $0 \leq A^2 - 1 < A^4 - 1$ car $A > 1$ (car par exemple $q_1 = 5$).

d) Comme $p$ divise $A^{4m+2} - 1$ et $p$ divise $A^4 - 1$ (cf 1.b.), on en déduit que $p$ divise aussi $A^{4m+2} - 1 - Q(A^4 - 1) = A^2 - 1$.

D'autre part, on a $p$ divise $B = A^2 + 1$ donc $p$ divise la différence $(A^2 + 1) - (A^2 - 1) = 2$.

e) La conclusion du d est impossible puisque $p \geq 3$. L'hypothèse du début sur l'existence d'un tel $p$ est donc fausse et le seul diviseur premier de $B$ est donc 2.

2) On utilise la propriété du produit dans $\mathbb{Z}/4\mathbb{Z}$: pour chaque $j$, on a $\overline{q_j} = \bar{1}$ donc on a $\bar{A} = \overline{q_1} \ldots \overline{q_n} = \bar{1} \ldots \bar{1} = \bar{1}$ puis $\overline{A^2} = \overline{A}^2 = \bar{1}^2 = \bar{1}$. Enfin $\bar{B} = \bar{A}^2 + \bar{1} = \bar{2}$ donc $B$ est congru à 2 modulo 4.

3) On déduit du 1. que $B = 2^s$ pour un entier $s \geq 1$ mais la question 2. impose que $s = 1$ (sinon $B$ divisible par 4 donc congru à 0 modulo 4). On aurait que $A = 1$ ce qui est faux.

Ainsi l'hypothèse de finitude du début est fausse. C'est ce que l'on voulait montrer.