Contrôle de connaissances – Brique CQFD
Algèbre, arithmétique et corps finis

Hugues Randriam & Gilles Zémor

Vendredi 19 décembre 2003

Les documents et les calculatrices sont autorisés.[1]

Exercice 1 *On travaillera ici sur le corps $\mathbb{F}_2 = \{0, 1\}$ à deux éléments.*

a) *Écrire une relation de Bézout entre les polynômes $X^3 + X + 1$ et $X^4 + X + 1$.*

b) *Calculer le reste de la division euclidienne de X^{93} par $X^7 + X^5 + X^3 + X^2 + 1$.*

Exercice 2 *Calculer :* $2^{2^{2003}} \mod 11$.

Exercice 3 *Soit $P(X) \in \mathbb{F}_q[X]$ un polynôme de degré $n \geq 2$ à coefficients dans le corps fini $\mathbb{F}_q$, où q est une puissance d'un nombre premier.*

a) *Montrer que P est primitif si et seulement si les deux conditions suivantes sont vérifiées :*
   - *$P(X)$ divise $X^{q^n-1} - 1$*
   - *$P(X)$ est premier à $X^d - 1$ pour tout d diviseur strict de $q^n - 1$.*

b) *Montrer que P est irréductible si et seulement si les deux conditions suivantes sont vérifiées :*
   - *$P(X)$ divise $X^{q^n-1} - 1$*
   - *$P(X)$ est premier à $X^d - 1$ pour tout d diviseur strict de $q^n - 1$ pouvant s'écrire sous la forme $d = q^m - 1$, où m est un diviseur strict de n.*

c) *Dans les deux questions précédentes, que se passe-t-il si l'on remplace « $P(X)$ est premier à $X^d - 1$ » par « $P(X)$ ne divise pas $X^d - 1$ » ? Obtient-on encore un critère (nécessaire et suffisant) de primitivité (cas a)) ou d'irréductibilité (cas b)) ? Si oui, le prouver, et si non, donner un contre-exemple.*

C'est tout. Bon courage et joyeuses fêtes de fin d'année !

---

[1] mais avec un minimum de réflexion, on se rendra compte qu'il est possible de s'en passer complètement — et de toutes façons, calculatrice ou pas, tous les résultats devront être justifiés !