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

Hugues Randriam & Gilles Zémor

Mercredi 15 décembre 2004

Documents, ordinateurs et téléphones portables interdits.
Calculatrices autorisées.
2 pages.

Exercice 1 *a) Montrer que* 2 *est primitif modulo* 37.

b) Donner la liste explicite des éléments primitifs modulo 37.

Exercice 2 *a) Soit* p *un nombre premier égal à* 3 *modulo* 4. *Soit* x *un élément de* $\mathbb{Z}/p\mathbb{Z}$ *qui est un carré. Montrer que* $x^{\frac{p+1}{4}}$ *est une racine carrée de* x.

b) L'entier 2 *est-il un carré modulo* 1457 *? Si non, le prouver, et si oui, expliciter toutes ses racines carrées. Au besoin on pourra utiliser la décomposition en facteurs premiers :* $1457 = 31 \times 47$.

Les solutions à base de recherche exhaustive ne seront pas acceptées.

Exercice 3 *Si* n *est un entier naturel non nul on note* $c_j(n)$ *le* j*-ième chiffre après la virgule du développement décimal de* $1/n$. *Par exemple,* $1/7 = 0,1428571...$ *donc* $c_1(7) = 1$, $c_2(7) = 4$, $c_3(7) = 2$, *etc.*

a) Posons $q_k(n) = \left\lfloor \frac{10^k}{n} \right\rfloor$ *(la partie entière de* $\frac{10^k}{n}$*). Exprimer* $q_k(n)$ *en fonction des* $c_j(n)$.

b) Soit $r_k(n)$ *le reste de la division euclidienne de* 10^k *par* n, *de sorte que*

$$10^k = n.q_k(n) + r_k(n).$$

Montrer qu'on a

$$c_{k+1}(n) = \left\lfloor 10\frac{r_k(n)}{n} \right\rfloor.$$

Dans les questions suivantes, on supposera que $n = p$ est un nombre premier différent de 2 ou 5.

c) *Montrer que la suite qui à k associe $c_k(p)$ est périodique, de période divisant $p-1$. Calculer $c_p(p)$.*

d) *Montrer que $c_{p-1}(p)$ vaut 1, 3, 7, ou 9, selon que le chiffre des unités de p (en base 10) vaut 9, 3, 7, ou 1, respectivement.*

e) *Supposons p premier supérieur ou égal à 11. Montrer que $c_{\frac{p+1}{2}}(p)$ vaut 0 ou 9, selon que 10 est ou non un carré modulo p.*

Exercice 4 a) *Montrer que $X^{2^k} + X$ se décompose dans $\mathbb{F}_2[X]$ en le produit de tous les polynômes irréductibles de degré divisant k.*

b) *Dans $\mathbb{F}_2[X]$, calculer le reste de $X^{2^{2n}}$ modulo $X^{2^n} + X + 1$.*

c) *Montrer que tous les facteurs irréductibles de $X^{2^n} + X + 1$ dans $\mathbb{F}_2[X]$ sont de degré divisant $2n$.*

d) *Montrer que tous les facteurs irréductibles de $X^{2^n+1} + X + 1$ dans $\mathbb{F}_2[X]$ sont de degré divisant $3n$.*

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