UNIVERSITÉ BORDEAUX I
UE: MHT 531

Algorithmique Algébrique

Examen

le 17 décembre 2012

Durée 3h. Documents non autorisés

Exercice 1. Système de congruences linéaires. Trouvez toutes les solutions du système

$$\begin{cases} 15x \equiv 6 \pmod{63}, \\ 4x \equiv -11 \pmod{135}. \end{cases}$$

Exercice 2. Soit $p > 2$ un nombre premier et $n \geqslant 1$ un entier. Dans cet exercice on étudie les congruences

$$X^n \equiv a \pmod{p}, \tag{1}$$

où a est un entier fixé tel que $PGCD(a, p) = 1$. Pour tout entier c on note $\bar{c}$ la classe de c modulo p. Soit g une racine primitive modulo p.

1) Rappeler pourquoi on peut écrire toute classe non nulle $\bar{c} \in (\mathbb{Z}/p\mathbb{Z})^*$ sous la forme $\bar{c} = \bar{g}^k$, $k \in \mathbb{Z}$. Montrer que k est unique modulo $p - 1$.

2) En utilisant la question 1) on écrit $\bar{X}$ et $\bar{a}$ sous la forme

$$\bar{X} = \bar{g}^y, \qquad \bar{a} = \bar{g}^m.$$

Montrer que la congruence (1) est équivalente à la congruence

$$ny \equiv m \pmod{(p-1)}.$$

3) Soit $d = PGCD(n, p - 1)$. Montrer que la congruence (1) est résoluble si et seulement si d divise m et que dans ce cas il existe exactement d classes de solutions de (1) modulo p.

4) Montrer que d divise m si et seulement si $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$.

5) Conclure.

Exercice 3. Soit p un nombre premier. On note $\mathbb{F}_p$ le corps fini à p éléments $\mathbb{Z}/p\mathbb{Z}$ et $\overline{\mathbb{F}}_p$ sa clôture algébrique.

1) En utilisant le théorème de Fermat trouver toutes les racines du polynôme $X^p - X$ dans $\mathbb{F}_p$. Décomposer $X^p - X$ en produit de facteurs de degré 1.

2) Soit $\alpha \in \overline{\mathbb{F}}_p$. Montrer que $\alpha^p = \alpha$ si et seulement si $\alpha \in \mathbb{F}_p$.

3) En utilisant la formule de binôme prouver que

$$(x + y)^p = x^p + y^p$$

pour tous $x, y \in \overline{\mathbb{F}}_p$.

4) Soit $f(X)$ un polynôme à coefficients dans $\mathbb{F}_p$ et soit $\alpha \in \overline{\mathbb{F}}_p$ une racine de $f(X)$. Montrer que α^p est une racine de $f(X)$.

5) Soit $f(X)$ un polynôme quadratique à coefficients dans $\mathbb{F}_p$. Supposons que $f(X)$ est irréductible sur $\mathbb{F}_p$. En utilisant la question 2) montrer que si α est une racine de $f(X)$, alors l'autre racine est α^p. En déduire que $\alpha^{p^2} = \alpha$.

6) En utilisant la question précédente montrer que si α et β sont deux racines d'un polynôme irréductible $f(X) \in \mathbb{F}_p[X]$ de degré 2, alors $\alpha^{p+1} = \beta^{p+1}$.

Exercice 4. Méthode $p+1$ de Williams. Le but de cet exercice est de prouver un théorème qui est à la base de la méthode de factorisation proposée en 1982 par Williams.

Soient X et Y deux variables. On note $u = X + Y$ et $v = XY$ les fonctions symétriques élémentaires. Pour tout $n \geqslant 1$ on pose

$$F_n = \frac{X^n - Y^n}{X - Y}.$$

1) Prouver que F_n est un polynôme symétrique en X et Y. En déduire qu'il existe un polynôme G_n en deux variables et à coefficients entiers tel que $F_n(X, Y) = G_n(u, v)$.

2) Calculer G_1, G_2 et G_3.

3) Supposons que m divise n. Prouver que $X^m - Y^m$ divise $X^n - Y^n$ dans $\mathbb{Z}[X, Y]$. En déduire que $G_m(u, v)$ divise $G_n(u, v)$.

4) Soit p un nombre premier et soit $f(X) = X^2 - aX + b \in \mathbb{Z}[X]$. En utilisant la question 6) de l'exercice 3 prouver que si $\bar{f}(X) = f(X) \pmod{p}$ est irréductible sur $\mathbb{F}_p[X]$, alors p divise $G_{p+1}(a, b)$.

5) Soit $N > 1$ un entier et soit p un diviseur premier de N. Supposons que $p+1$ est B-friable, c'est-à-dire que dans la factorisation

$$p + 1 = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s}, \qquad q_i \text{ premiers deux à deux distincts}$$

on a $q_i^{\alpha_i} \leqslant B$ pour tous $i = 1, 2, \ldots, s$. Posons $M = B!$. Prouver que si $\bar{f}(X)$ est irréductible sur $\mathbb{F}_p$, alors

$$PGCD(N, G_M(a, b)) > 1.$$

Exercice 5. On veut résoudre le système

$$\begin{cases} Y^2 + X^2 - Y - 3X = 0 \\ Y^2 - 6XY - X^2 + 11Y + 7X - 12 = 0 \end{cases} \tag{2}$$

dans $\mathbb{C}$.

1) Calculer le résultant $h(X) = Res(F(X, Y), G(X, Y))$ des polynômes

$$F(X, Y) = Y^2 + X^2 - Y - 3X \qquad \text{et } G(X, Y) = Y^2 - 6XY - X^2 + 11Y + 7X - 12$$

par rapport à la variable Y.

2) Résoudre l'équation $h(X) = 0$.

3) Trouver les solutions du système (2).

4) Quelles sont les courbes représentées par les équations $F(X, Y) = 0$ et $G(X, Y) = 0$?

FIN