UFR de Mathématiques et Informatique
Université Bordeaux I — Année 1999–2000

Licence de Mathématiques et Informatique

Module d'Algorithmique Algébrique

Devoir surveillé du 16 novembre 2000

Durée 3 heures

Documents interdits. Le barême n'est qu'indicatif.

Exercice I (12 points)

Soit p un nombre premier fixé. On note comme d'habitude $\mathbb{F}_p$ le corps fini à p éléments, qu'on identifie à $\mathbb{Z}/p\mathbb{Z}$. On pose

$$A_p(X) = \prod_{1 \leq a \leq p-1} (X - a) \in \mathbb{Z}[X] \, ,$$

et on note $\overline{A_p}(X)$ le polynôme de $\mathbb{F}_p[X]$ obtenu en réduisant tous les coefficients de $A_p(X)$ modulo p.

1) Calculer $A_3(X)$ et $A_5(X)$, puis $\overline{A_3}(X)$ et $\overline{A_5}(X)$.

2) a) Soit $\overline{B_p}(X) = X^{p-1} - 1$ considéré comme polynôme de $\mathbb{F}_p[X]$. Montrer que tous les éléments non nuls de $\mathbb{F}_p$ sont racines de $\overline{B_p}(X)$, et que ces racines sont simples.

b) En déduire que $\overline{A_p}(X) = \overline{B_p}(X)$, et donc que l'on a la congruence coefficient par coefficient

$$A_p(X) = \prod_{1 \leq a \leq p-1} (X - a) \equiv X^{p-1} - 1 \pmod{p} \, .$$

c) En comparant les termes constants, en déduire le théorème de Wilson $(p-1)! \equiv -1 \pmod{p}$.

3) a) Montrer que

$$\sum_{1 \leq a \leq p-1} a \equiv 0 \pmod{p} \quad \text{et que}$$
$$\sum_{1 \leq a \leq p-1} a^2 \equiv 0 \pmod{p} \, ,$$

la première congruence étant valable uniquement pour $p \geq 3$ et la deuxième pour $p \geq 5$.

b) Plus généralement, on appelle σ_k la k-ième fonction symétrique élémentaire des racines de $A_p(X)$ (par convention égale à 0 si $k > p-1$) et $S_k = \sum_{1\leq a\leq p-1} a^k$ la somme des puissances k-ièmes de ces racines. En utilisant les formules de Newton (valables pour tout $k \geq 1$)

$$S_k = (-1)^{k-1} k\sigma_k + \sum_{1\leq j\leq k-1} (-1)^{k-1-j} \sigma_{k-j} S_j \ ,$$

montrer par récurrence que $S_k \equiv 0 \pmod{p}$ pour tout $k \geq 1$ tel que $p-1$ ne divise pas k.

4) On pose

$$R_p(X) = \prod_{1\leq a\leq p-1} (1 - aX) \ .$$

a) Calculer $R_p(X)$ en fonction du polynôme A_p.

b) On appelle T_k la somme des puissances k-ièmes des racines du polynôme $R_p(X)$. Comme ces racines sont les a^{-1} pour $1 \leq a \leq p-1$, il est raisonnable d'écrire $T_k = S_{-k}$. En utilisant le même raisonnement qu'en 3b) (qu'on ne reproduira que très brièvement), montrer que pour tout $k \geq 1$ tel que $p-1$ ne divise pas k on a $(p-1)!^k T_k \equiv 0 \pmod{p}$, ou en d'autres termes que $(p-1)!^k S_{-k} \equiv 0 \pmod{p}$.

c) En déduire que le numérateur des nombres rationnels

$$\sum_{1\leq a\leq p-1} \frac{1}{a^k}$$

est divisible par p pour tout $k \in \mathbb{Z}$ non divisible par $p-1$.

Remarque. On peut démontrer que quand k est impair, si $p \geq k+4$ le numérateur des nombres rationnels $\sum_{1\leq a\leq p-1} 1/a^k$ est en fait divisible par p^2, mais c'est plus difficile.

Exercice II (8 points)

On pose $N = 1105$.

1) a) Factoriser N à la main.

b) Montrer que si $(a, N) = 1$ on a $a^{48} \equiv 1 \pmod{N}$ (en utilisant le théorème de Fermat, on montrera que ceci est vrai modulo chaque diviseur premier de N). En déduire que pour un tel a on a $a^{N-1} \equiv 1 \pmod{N}$.

c) Montrer qu'en fait pour tout a (premier ou non avec N) on a $a^N \equiv a \pmod{N}$.

2) Soit $j = (-1+\sqrt{-3})/2$ la racine cubique de l'unité habituelle, satisfaisant $j^2+j+1 = 0$. On pose

$$A = \mathbb{Z}[j] = \{a + bj \in \mathbb{C} / \ a, \ b \in \mathbb{Z}\} \ .$$

a) Expliquer brièvement pourquoi A est un sous-anneau de $\mathbb{C}$.

b) Montrer que pour tout nombre premier $p \neq 3$ et tout $x \in A$ on a $x^p \equiv x \pmod{pA}$ si $p \equiv 1 \pmod{3}$ et $x^p \equiv \overline{x} \pmod{pA}$ si $p \equiv 2 \pmod{3}$, où $\overline{x}$ désigne le conjugué complexe de x.

3) On prend $x = 1 + 2j = \sqrt{-3}$, et on reprend $N = 1105$ comme dans la question 1). On a donc $x^{N-1} = 3^{(N-1)/2}$.

a) En utilisant le petit théorème de Fermat, montrer que $x^{N-1} \equiv 1 \pmod 5$ et que $x^{N-1} \equiv 1 \pmod{13}$, mais que $x^{N-1} \equiv -1 \pmod{17}$.

b) En déduire que $x^N \not\equiv x \pmod{NA}$, et donc que N n'est pas premier (bien sûr ici c'est évident car N est petit, mais ce test peut aussi être utilisé pour des N ayant plusieurs milliers de chiffres).

4) On pose

$$K = \mathbb{Q}(j) = \{a + bj \in \mathbb{C} / \ a,\ b \in \mathbb{Q}\} \ .$$

a) Montrer que K est un sous-corps de $\mathbb{C}$.

b) Montrer que pour tout $x \in K$ il existe $q \in A$ tel que $|x - q| \leq \sqrt{3}/2$, où $|y|$ est le module de y dans $\mathbb{C}$ (si $x = x_1 + x_2 j$, on prendra $q = q_1 + q_2 j$ avec q_i l'entier le plus proche de x_i).

c) En déduire que A est un anneau euclidien, et donc principal.

d) Question facultative : en utilisant la question 1b), calculer un PGCD de $a = 1 + 10j$ et de $b = 7 + 5j$.