UFR de Mathématiques et Informatique
Université Bordeaux I

Année 2001–2002

Licence de Mathématiques et Informatique

Module d'Algorithmique Arithmétique

Devoir surveillé de novembre 2001

Durée 3 heures

Documents interdits. Le barème (donné sur 20 points) n'est qu'indicatif.

Exercice I (3 points)

On considère le jeu mathématique suivant. Vous demandez à un ami de penser à un nombre entier x positif ou nul et inférieur ou égal à 209, et de vous donner les restes r_5, r_6 et r_7 de la division de x par 5, 6 et 7 respectivement (par exemple, s'il choisit $x = 113$, il vous donnera 3, 5 et 1). Presque immédiatement, vous lui restituez son nombre x. Pour cela, il vous faut dans cet exercice calculer trois entiers a_5, a_6 et a_7 (petits si possibles), tels que x soit le reste de la division par 210 de $a_5r_5 + a_6r_6 + a_7r_7$. Il faudra tout d'abord montrer l'existence de ces entiers, puis les calculer par des algorithmes de Bezout. Attention: le simple fait de donner les valeurs de ces entiers sans justification ne sera pas accepté.

Exercice II (6 points)

Soit p un nombre premier tel que $p \equiv 3 \pmod 4$, et soit comme d'habitude $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments.

1) a) Montrer que -1 n'est pas un carré dans $\mathbb{F}_p$, c'est à dire qu'il ne peut pas exister $x \in \mathbb{F}_p$ tel que $x^2 = -1$ dans $\mathbb{F}_p$ (pour cela, on pourra calculer $(-1)^{(p-1)/2}$ de deux manières différentes).

b) En déduire que si a, b sont des éléments de $\mathbb{F}_p$ tels que $a^2+b^2 = 0$, alors $a = b = 0$.

2) On définit

$$K = \left\{ M(a,b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix},\ a,\ b \in \mathbb{F}_p \right\}\ .$$

a) Montrer que K est un corps. Quel est le cardinal de K ? On notera I la matrice identité d'ordre 2, qui est donc l'élément neutre de K pour la multiplication.

b) On définit

$$K' = \frac{\mathbb{F}_p[X]}{(X^2+1)\mathbb{F}_p[X]} \ .$$

Montrer que K' est également un corps, puis que K' est isomorphe à K (on explicitera l'isomorphisme).

3) a) Rappeler brièvement pourquoi l'équation $X^{p-1} - I = 0$ possède au plus $p-1$ solutions dans K, et donner ces solutions en utilisant le petit théorème de Fermat.

b) On suppose désormais que $(a,b) \neq (0,0)$ dans $\mathbb{F}_p$. Montrer que $X = M(a,b)^{p+1}$ est solution de l'équation $X^{p-1} - I = 0$ ci-dessus. En déduire qu'il existe $n(a,b) \in \mathbb{F}_p$ tel que $M(a,b)^{p+1} = n(a,b)I$.

4) On pose $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, ce qui fait que $M(a,b) = aI + bS$. Il est clair que $S^2 = -I$ (inutile de le vérifier).

a) En utilisant le fait que $\mathbb{F}_p$ est de caractéristique p et le petit théorème de Fermat, calculer des éléments c et d de $\mathbb{F}_p$ tels que $M(a,b)^p = cI + dS$.

b) En déduire $M(a,b)^{p+1}$, donc la valeur de $n(a,b)$ dans la question 3).

Exercice III (11 points)

Soir d un entier (positif ou négatif) qui n'est pas le carré d'un nombre entier.

1) On se propose tout d'abord de montrer que $\sqrt{d} \notin \mathbb{Q}$. On suppose donc par l'absurde que $\sqrt{d} = p/q$ avec $(p,q) = 1$.

a) Montrer que q divise p^2, puis que $q = 1$.

b) En déduire la contradiction souhaitée.

On pose

$$\mathbb{Q}_d = \{a + b\sqrt{d} \,/\ a,\ b \in \mathbb{Q}\}$$

et

$$\mathbb{Z}_d = \{a + b\sqrt{d} \,/\ a,\ b \in \mathbb{Z}\} \ .$$

2) En utilisant la première question, montrer le plus brièvement possible (mais rigoureusement) que $\mathbb{Q}_d$ est un corps et que $\mathbb{Z}_d$ est un sous-anneau de $\mathbb{Q}_d$.

3) On suppose qu'il existe un entier $f > 1$ tel que $f^2 \mid d$. On pose

$$I = \{xf + y\sqrt{d} \,/\ x,\ y \in \mathbb{Z}\} \ .$$

a) Montrer que I est un idéal de $\mathbb{Z}_d$.

On se propose de montrer par l'absurde que I n'est pas un idéal principal. Soit donc $\alpha = uf + v\sqrt{d} \in I$ un générateur de I, donc tel que $I = \alpha\mathbb{Z}_d$.

b) Montrer que u et v sont premiers entre eux.

c) On pose $n = u^2f^2 - v^2d = f^2(u^2 - v^2d/f^2)$. En utilisant le fait (qu'on justifiera) que $f/\alpha \in \mathbb{Z}_d$ et $\sqrt{d}/\alpha \in \mathbb{Z}_d$, montrer que $n \mid fu$ et $n \mid fv$.

d) Déduire de b) et c) que $n \mid f$, puis que $f^2 \mid f$, donc que $f = 1$, d'où une contradiction.

4) On suppose maintenant que $d \equiv 1 \pmod 4$, et on ne fait pas d'hypothèse particulière sur l'existence de f. On pose

$$I = \{2x + y(1 + \sqrt{d}) \;/\; x,\ y \in \mathbb{Z}\}\ .$$

a) Montrer que I est un idéal de $\mathbb{Z}_d$.

On se propose de montrer par l'absurde que I n'est pas un idéal principal. Soit donc $\alpha = 2u + v(1 + \sqrt{d}) \in I$ un générateur de I, donc tel que $I = \alpha\mathbb{Z}_d$.

b) En imitant très exactement le raisonnement de la question précédente, montrer successivement que u et v sont premiers entre eux, que si $n = (2u + v)^2 - dv^2 = 4(u^2 + uv + ((1 - d)/4)v^2)$ on a $n \mid 2v$, $n \mid 2u + 2v$, donc $n \mid 2$ donc $4 \mid 2$, absurde.

Il résulte des questions 3) et 4) que s'il existe $f > 1$ tel que $f^2 \mid d$, ou si $d \equiv 1 \pmod 4$, alors $\mathbb{Z}_d$ n'est pas principal. Désormais, on suppose donc que d est “sans facteur carré”, c'est à dire qu'il n'existe pas de $f > 1$ tel que $f^2 \mid d$, et que $d \not\equiv 1 \pmod 4$, donc que d est congru à 2 ou à 3 modulo 4. Il est alors possible que $\mathbb{Z}_d$ soit principal, mais ce n'est pas toujours vrai.

5) a) Soient x, y deux nombres rationnels. Montrer que si $d = -2$, $d = -1$, $d = 2$ ou $d = 3$ (qui sont bien sans facteur carré et congrus à 2 ou 3 modulo 4), il existe deux entiers a et b tels que $|(x - a)^2 - d(y - b)^2| < 1$ (dans le cas $d = 3$, bien faire attention à démontrer l'inégalité stricte).

b) Ecrivant une division euclidienne $\alpha = \beta q + r$ dans $\mathbb{Z}_d$ sous la forme $\alpha/be - q = r/q$, montrer en utilisant la question précédente que pour les quatre valeurs de d données ci-dessus l'anneau $\mathbb{Z}_d$ est euclidien pour le stathme $\phi(a + b\sqrt{d}) = |a^2 - db^2|$.