UFR de Mathématiques et Informatique
Université Bordeaux I
Année 2001–2002

Licence de Mathématiques et Informatique

Module d'Algorithmique Arithmétique

Corrigé du devoir surveillé du 15 novembre 2001

Exercice I

Nous avons les trois congruences $x \equiv r_5 \pmod 5$, $x \equiv r_6 \pmod 6$ et $x \equiv r_7 \pmod 7$. Comme les nombres 5, 6 et 7 sont premiers entre eux deux à deux, le théorème Chinois dit que ceci est soluble, et que x est unique modulo $5 \cdot 6 \cdot 7 = 210$. Nous devons faire le calcul explicite des coefficients. Considérons tout d'abord les deux premières congruences. L'identité de Bezout évidente $-1 \cdot 5 + 1 \cdot 6 = 1 = (5, 6)$ nous dit que si on pose $e_5 = -5$ et $e_6 = 6$ on a $5 \mid e_5$, $6 \mid e_6$, $e_5 \equiv 1 \pmod 6$ et $e_6 \equiv 1 \pmod 5$, d'où $x \equiv r_{30} = r_5 e_6 + r_6 e_5 \pmod{30}$. Nous recommençons maintenant avec les nombres 30 et 7. Une identité de Bezout entre ces deux nombres est par exemple $-3 \cdot 30 + 13 \cdot 7 = 1 = (30, 7)$, ce qui conduit à poser comme ci-dessus $e_{30} = -90$, $e_7 = 91$ avec des propriétés analogues à celles de e_5 et e_6, mais cette fois pour 30 et 7. On en déduit que $x \equiv r_{210} = r_{30} e_7 + r_7 e_{30} \pmod{210}$.

Remplaçant par les valeurs numériques, on a donc $r_{30} = 6r_5 - 5r_6$, donc $r_{210} = (6r_5 - 5r_6)91 - 90r_7 = 546r_5 - 455r_6 - 90r_7$. Comme r_{210} n'est défini que modulo 210, on choisit plutôt

$$r_{210} = 126r_5 - 35r_5 + 120r_7\ ,$$

d'ø'u $a_5 = 126$, $a_6 = -35$ et $a_7 = 120$. Les a_i sont ne sont uniques que modulo 210, donc il serait tout à fait correct de choisir par exemple $a_6 = 175$ à la place de $a_6 = -35$.

Exercice II

1) a) Puisque $p \equiv 3 \pmod 4$ le nombre $(p-1)/2$ est impair donc $(-1)^{(p-1)/2} = -1$. Supposons par l'absurde qu'il existe $x \in \mathbb{F}_p$ tel que $x^2 = -1$. On a alors $(-1)^{(p-1)/2} = x^{p-1} = 1$ d'après le théorème de Fermat (tout élément du groupe multiplicatif $\mathbb{F}_p^*$ est d'ordre un diviseur de $p-1$), d'où une contradiction.

b) Si par exemple $b \neq 0$, de $a^2 + b^2 = 0$ on tire $(a/b)^2 = -1$, contredisant la question a). De même si $a \neq 0$. On doit donc avoir $a = b = 0$.

2) a) On a clairement $M(a_1, b_1) - M(a_2, b_2) = M(a_1 - b_1, a_2 - b_2)$, donc K est un groupe additif abélien. D'autre part un calcul immédiat montre que

$$M(a_1, b_1)M(a_2, b_2) = M(a_1a_2 - b_1b_2, a_1b_2 + a_2b_1) ,$$

et comme $I = M(1, 0)$ est la matrice identité, il en résulte que K est un anneau. Enfin, soit $M(a, b)$ un élément non nul de K, c'est à dire tel que $(a, b) \neq (0, 0)$. On voit sur la loi de multiplication ci-dessus que

$$M(a, b)M(a, -b) = M(a^2 + b^2, 0) = (a^2 + b^2)I .$$

D'après la question 1b) on sait que $a^2 + b^2 \neq 0$, donc $M(a, b)$ est bien inversible, et on a

$$M(a, b)^{-1} = M\left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2}\right) ,$$

ce qui démontre que K est un corps.

Enfin le cardinal de K est égal au nombre de couples $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p$, donc à p^2.

b) D'après la question 1a) le polynôme $X^2 + 1$ n'a pas de racine dans $\mathbb{F}_p$. Comme c'est un polynôme de degré 2, il en résulte qu'il est irréductible dans $\mathbb{F}_p[X]$, donc que le quotient K' de $\mathbb{F}_p[X]$ par l'idéal principal engendré par $X^2 + 1$ est un corps.

L'ensemble des classes de polynômes de degré inférieur ou égal à 1 forme évidemment un système de représentant des éléments de K'. De plus, puisque la classe de X^2 est égale à la classe de -1, on a l'identité évidente

$$(a_1 + b_1X)(a_2 + b_2X) \equiv a_1a_2 - b_1b_2 + (a_1b_2 + a_2b_1)X \pmod{X^2 + 1} .$$

Il est d'autre part évident que $(a_1 + b_1X) + (a_2 + b_2X) = (a_1 + a_2) + (b_1 + b_2)X$. On voit donc que ces deux lois sont les mêmes que celles entre matrices $M(a, b) \in K$. Il en résulte que si on définit $f(M(a, b))$ comme la classe de $a + bX$, alors f sera un homomorphisme d'anneaux. D'autre part dans K aussi bien que dans K' les couples (a, b) parcourent une fois et une seule l'ensemble $\mathbb{F}_p \times \mathbb{F}_p$, donc f est bijective, donc est un isomorphisme de corps.

3) a) Il est clair que le corps K est commutatif, et dans un corps commutatif une équation de degré n possède au plus n racines comptées avec multiplicité. L'équation $X^{p-1} - I = 0$ possède donc au plus $p - 1$ racines. Mais d'autre part si on prend $X = aI$ avec $a \in \mathbb{F}_p^*$, le théorème de Fermat nous dit que $a^{p-1} = 1$, donc X vérifie bien l'équation. Comme il y a $p - 1$ éléments dans $\mathbb{F}_p^*$, il en résulte que les solutions de $X^{p-1} - I = 0$ sont exactement $X = aI$ pour $a \in \mathbb{F}_p^*$.

b) Si $X = M(a, b)^{p+1}$, on a $X^{p-1} = M(a, b)^{p^2-1}$. Or d'après la question 2a), le cardinal du groupe multiplicatif K^* est égal à $p^2 - 1$. D'après le théorème sur l'ordre d'un élément dans un groupe (généralisant le théorème de Fermat), puisque $M(a, b) \in K^*$ on a donc $M(a, b)^{p^2-1} = I$, donc $X^{p-1} - I = 0$. D'après la question a) la matrice X doit donc être un multiple scalaire de la matrice I, en d'autres termes il existe $n(a, b) \in \mathbb{F}_p$ tel que $M(a, b)^{p+1} = n(a, b)I$.

Remarque : si on prend le déterminant de légalité $M(a,b)^{p+1} = n(a,b)I$, on obtient, puisque $a^2+b^2 \in \mathbb{F}_p$:

$$n(a,b)^2 = (a^2+b^2)^{p+1} = (a^2+b^2)^2 ,$$

d'où $n(a,b) = \pm(a^2+b^2)$. Le but de la question 4) est de montrer que l'on doit prendre le signe $+$.

4) a) D'après les propriétés des coefficients du binôme, nous savons qu'en caractéristique p on a $(x+y)^p = x^p + y^p$. Puisque $S^2 = -I$ et que $a^p = a$ et $b^p = b$, on a donc ici

$$M(a,b)^p = (aI+bS)^p = a^pI^p + b^pS^p = aI + (-1)^{(p-1)/2}bS = aI - bS$$

puisque $(p-1)/2$ est impair.

b) Il en résulte que

$$M(a,b)^{p+1} = (aI-bS)(aI+bS) = a^2I - b^2S^2 = (a^2+b^2)I ,$$

donc $n(a,b) = a^2+b^2$.

Exercice III

1) a) Elevant au carré l'égalité $q\sqrt{d} = p$, on obtient $dq^2 = p^2$, donc $q \mid p^2 = 1 \cdot q^2$, et puisque p et q sont premiers entre eux, le lemme de Gauss entraîne que $q \mid 1$ donc que $q = 1$.

b) Il en résulte que $d = p^2$, contredisant l'hypothèse que d n'est pas le carré d'un nombre entier.

2) Montrons tout d'abord que $\mathbb{Q}_d$ et $\mathbb{Z}_d$ sont des sous-anneaux de $\mathbb{C}$. En effet,

$$(a_1+b_1\sqrt{d}) - (a_2+b_2\sqrt{d}) = (a_1-a_2) + (b_1-b_2)\sqrt{d} ,$$

donc ce sont bien des sous-groupes additifs. D'autre part

$$(a_1+b_1\sqrt{d})(a_2+b_2\sqrt{d}) = (a_1a_2+db_1b_2) + (a_1b_2+a_2b_1)\sqrt{d} ,$$

donc ce sont bien des sous-anneaux (il est clair que $1 \in \mathbb{Z}_d \subset \mathbb{Q}_d$). Enfin, il faut montrer que $\mathbb{Q}_d$ est un corps. En effet, on a $(a+b\sqrt{d})(a-b\sqrt{d}) = a^2-b^2d$. D'après la première question, on ne peut avoir $a^2-b^2d = 0$ que si $a = b = 0$ (si $b = 0$ il st clair que $a = 0$, et si $b \neq 0$ alors $\sqrt{d} = \pm(a/b)$, contredisant le résultat de la première question). Il en résulte que si $(a,b) \neq (0,0)$ on a

$$\frac{1}{a+b\sqrt{d}} = \frac{a}{a^2-b^2d} - \frac{b}{a^2-b^2d}\sqrt{d} \in \mathbb{Q}_d ,$$

prouvant que $\mathbb{Q}_d$ est bien un corps.

3) a) Puisque

$$(x_1 f + y_1\sqrt{d}) - (x_2 f + y_2\sqrt{d}) = (x_1 - x_2)f + (y_1 - y_2)\sqrt{d}\ ,$$

il est clair que I est un sous-groupe additif de $\mathbb{Z}_d$. D'autre part, si $a + b\sqrt{d} \in \mathbb{Z}_d$ on a

$$(a + b\sqrt{d})(xf + y\sqrt{d}) = (ax + byd/f)f + (ay + bxf)\sqrt{d} \in I\ ,$$

puisque $f \mid d$ (on n'a pas besoin ici de toute la force de la condition $f^2 \mid d$). Il en résulte que I est un idéal de $\mathbb{Z}_d$.

b) Soit e un diviseur commun de u et v. On a $\alpha/e = (u/e)f + (v/e)\sqrt{d}$, donc $\alpha/e \in I$, et puisque $I = \alpha\mathbb{Z}_d$, il en résulte que $1/e \in \mathbb{Z}_d$. Comme $1/e = 1/e + 0\sqrt{d}$, on a donc $1/e \in \mathbb{Z}$, donc $e = \pm 1$, ce qui prouve que u et v n'ont que ± 1 comme diviseurs communs, en d'autres termes qu'ils sont premiers entre eux.

c) Puisque $f = 1 \cdot f + 0\sqrt{d} \in I$ et $\sqrt{d} = 0 \cdot f + 1\sqrt{d} \in I$ et que $I = \alpha\mathbb{Z}_d$, il en résulte que $f/\alpha \in \mathbb{Z}_d$ et $\sqrt{d}/\alpha \in \mathbb{Z}_d$. On a

$$\frac{f}{\alpha} = \frac{f(uf - v\sqrt{d})}{u^2 f^2 - v^2 d} = \frac{uf^2}{n} - \frac{fv}{n}\sqrt{d}\ ,$$

d'où il résulte en particulier que $fv/n \in \mathbb{Z}$, donc que $n \mid fv$. De même

$$\frac{\sqrt{d}}{\alpha} = \frac{-vd + uf\sqrt{d}}{u^2 f^2 - v^2 d} = \frac{-vd}{n} + \frac{fu}{n}\sqrt{d}\ ,$$

d'où $fu/n \in \mathbb{Z}$, donc $n \mid fu$.

d) D'après l'identité de Bezout et la question b), il existe s et t tels que $su + tv = 1$. Il en résulte que n diviser $sfu + tfv = f$, donc $n \mid f$. Comme $n = f^2(u^2 - v^2 d/f^2)$ et que $u^2 - v^2 d/f^2 \in \mathbb{Z}$, on a donc $f^2 \mid n$, donc $f^2 \mid f$, donc $f \mid 1$, donc $f = 1$, ce qui est une contradiction puisque on a supposé $f > 1$. Noter qu'on utilise ici la pleine force de l'hypothèse $f^2 \mid d$.

4) a) A nouveau l'égalité

$$(2x_1 + y_1(1 + \sqrt{d})) - (2x_2 + y_2(1 + \sqrt{d})) = 2(x_1 - x_2) + (y_1 - y_2)(1 + \sqrt{d})$$

montre que I est un sous-groupe additif de $\mathbb{Z}_d$. D'autre part, si $a + b\sqrt{d} \in \mathbb{Z}_d$ on a

$$\begin{aligned}(a + b\sqrt{d})(2x + y(1 + \sqrt{d})) &= a(2x + y) + byd + (ay + b(2x + y))\sqrt{d}\\ &= 2(ax - bx + by(d - 1)/2) + (ay + 2bx + by)(1 + \sqrt{d}) \in I\ ,\end{aligned}$$

où nous utilisons l'hypothèse que d est impair (mais pas encore la pleine force de l'hypothèse $d \equiv 1 \pmod 4$). Il en résulte que I est bien un idéal de $\mathbb{Z}_d$.

b) Soit e un diviseur commun à u et v. Comme dans la question 3), on a $\alpha/e \in I$, donc $1/e \in \mathbb{Z}_d$, donc $e = \pm 1$, donc u et v sont premiers entre eux. D'autre part $2 \in I$ et $1 + \sqrt{d} \in I$, donc $2/\alpha \in \mathbb{Z}_d$ et $(1 + \sqrt{d})/\alpha \in \mathbb{Z}_d$. On a

$$\frac{2}{\alpha} = \frac{2(2u + v - v\sqrt{d}))}{(2u + v)^2 - dv^2} = \frac{4u + 2v}{n} - \frac{2v}{n}\sqrt{d}\ ,$$

d'où en particulier $2v/n \in \mathbb{Z}$ donc $n \mid 2v$, et de même

$$\frac{1 + \sqrt{d}}{\alpha} = \frac{(1 + \sqrt{d})(2u + v - v\sqrt{d})}{(2u + v)^2 - dv^2} = \frac{2u + v - vd}{n} - \frac{2u}{n}\sqrt{d}\ ,$$

d'où en particulier $2u/n \in \mathbb{Z}$ donc $n \mid 2u$. Puisque $(u, v) = 1$, comme en 3) l'identité de Bezout montre que $n \mid 2$, et comme $n = 4(u^2 + uv + ((1 - d)/4)v^2)$ et que $d \equiv 1 \pmod 4$, on a donc $4 \mid n$, donc $4 \mid 2$, ce qui est une contradiction. C'est ici qu'on utilise toute la force de l'hypothèse $d \equiv 1 \pmod 4$.

5) a) Choisissons pour a l'entier le plus proche de x, et pour b l'entier le plus proche de y, de telle façon que $|x - a| \leq 1/2$ et $|y - b| \leq 1/2$. On a donc

$$|(x - a)^2 - d(y - b)^2| \leq (x - a)^2 + |d|(y - b)^2 \leq (1 + |d|)/4\ .$$

Lorsque $d = -2$, $d = -1$ ou $d = 2$, ceci est plus petit ou égal à $3/4$, $1/2$ et $3/4$ respectivement, donc strictement inférieur à 1. Lorsque $d = 3$ on obtient 1, donc il faut reprendre l'inégalité sans valeur absolue. On a

$$-3/4 \leq (x - a)^2 - 3(y - b)^2 \leq 1/4\ ,$$

donc on a $|(x - a)^2 - d(y - b)^2| \leq 3/4$.

b) Comme $a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d})$, on vérifie immédiatement que ϕ est multiplicatif, c'est à dire que $\phi(\gamma\delta) = \phi(\gamma)\phi(\delta)$. Puisque $\mathbb{Q}_d$ est un corps, on peut écrire $\alpha/\beta = x + y\sqrt{d}$ avec x et y rationnels. Si on pose $q = a + b\sqrt{d}$ avec a et b choisis comme dans la question a), on a $\phi(\alpha/\beta - q) = |(x - a)^2 - d(y - b)^2| < 1$, donc par multiplicativité $\phi(\alpha - \beta q) < \phi(\beta)$. Comme d'autre part d'après la question 1) on ne peut avoir $\phi(\gamma) = 0$ que si $\gamma = 0$, il en résulte bien que ϕ est un stathme euclidien, donc que $\mathbb{Z}_d$ est euclidien pour les quatre valeurs de d données en a).