UFR de Mathématiques et Informatique
Université Bordeaux I

Année 1999–2000

Licence de Mathématiques et Informatique

Module d'Algorithmique Arithmétique

Corrigé du devoir surveillé du 16 novembre 2000

Exercice I

1) On a $A_3(X) = X^2 - 3X + 2$, donc $\overline{A_3}(X) = X^2 - \overline{1}$. D'autre part $A_5(X) = X^4 - 10X^3 + 35X^2 - 50X + 24$, donc $\overline{A_5}(X) = X^4 - \overline{1}$.

2) a) Comme $\mathbb{F}_p$ est un corps, $\mathbb{F}_p^*$ est un groupe multiplicatif ayant $p-1$ élements. Par un théorème du cours, tout élément d'un groupe fini élevé à l'ordre du groupe égal l'élément neutre du groupe. Donc, pour tout élément $\overline{a}$ de $\mathbb{F}_p^*$ on a $\overline{a}^{p-1} = \overline{1}$ dans $\mathbb{F}_p$. Bien sûr, ceci n'est rien d'autre que la démonstration du théorème de Fermat.

Il en résulte donc que les $p-1$ éléments non nuls de $\mathbb{F}_p$ sont racines de $\overline{B_p}(X)$. Comme $\overline{B_p}$ est un polynôme de degré $p-1$, il a au plus $p-1$ racines comptées avec multiplicité, donc il ne peut pas y avoir d'autres racines que les éléments non nuls de $\mathbb{F}_p$, et celles-ci sont simples.

b) Les polynomes $\overline{A_p}(X)$ et $\overline{B_p}(X)$ ont donc les mêmes racines avec le même ordre de multiplicité, donc ils ne diffèrent que par une constante multiplicative. Comme ils sont tous deux unitaires, ils sont donc égaux. Ce raisonnement est essentiellement correct, mais il faut prendre garde que lorsqu'on parle de racines, il s'agit de racines *dans une clôture algébrique*. Ici, il n'y a pas de problème puisque toutes les racines sont dans $\mathbb{F}_p$. Mais par exemple, dans $\mathbb{R}[X]$, les polynômes X^3+X et X^3+2X ont tous deux les mêmes racines dans $\mathbb{R}$ (à savoir 0, racine simple), sont unitaires et de même degré, mais bien sûr ne sont pas égaux. En effet, nous ne prenons pas en compte les racines complexes de ces polynômes, c'est à dire les racines appartenant à $\mathbb{C}$, clôture algébrique de $\mathbb{R}$.

Revenant à notre exercice, on a donc la congruence coefficient par coefficient

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

c) Les termes constants donnent la congruence

$$\prod_{1\leq a\leq p-1} (-a) \equiv -1 \pmod{p} ,$$

soit
$$(-1)^{p-1}(p-1)! \equiv -1 \pmod p \ .$$
Or on a $(-1)^{p-1} \equiv 1 \pmod p$: en effet, c'est clair si p est impair, et aussi si $p = 2$ puisque $-1 \equiv 1 \pmod 2$. On en déduit donc bien le théorème de Wilson $(p-1)! \equiv -1 \pmod p$.

3) a) Il est bon de connaître sans hésitation les formules

$$\sum_{1 \leq a \leq n} a = \frac{n(n+1)}{2}$$
$$\sum_{1 \leq a \leq n} a^2 = \frac{n(n+1)(2n+1)}{6}$$
$$\sum_{1 \leq a \leq n} a^3 = \frac{n^2(n+1)^2}{4}$$

(nous n'aurons besoin que des deux premières).

On a donc en particulier

$$S_1 = \sum_{1 \leq a \leq p-1} a = \frac{p(p-1)}{2} \ .$$

Si $p \geq 3$, p est premier à 2. Comme p divise $2S_1$, d'après le lemme de Gauss, p divise S_1. De même
$$S_2 = \sum_{1 \leq a \leq p-1} a^2 = \frac{p(p-1)(2p-1)}{6} \ .$$
Si $p \geq 5$, p est premier à $6 = 2 \cdot 3$. Comme p divise $6S_2$, d'après le lemme de Gauss, p divise S_2.

b) D'après la question 2b) nous savons que

$$A_p(X) \equiv X^{p-1} - 1 \pmod p \ .$$

D'autre part, par définition

$$A_p(X) = \sum_{k=0}^{p-1} (-1)^k \sigma_k X^{p-1-k} \ .$$

Il en résulte que pour tout $k \neq p-1$ on a $\sigma_k \equiv 0 \pmod p$, et que $\sigma_{p-1} \equiv -1 \equiv -1 \pmod p$ (nous avons vu ci-dessus que $(-1)^{p-1} \equiv 1 \pmod p$).

D'après les formules de Newton rappelées dans l'énoncé, pour tout $k \geq 1$ on a

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

Comme $\sigma_i \equiv 0 \pmod p$ pour tout $i \neq p-1$, on en déduit que la seule expression peut-être non divisible par p dans la somme sur j est celle pour $k - j = p - 1$, c'est à dire

$j = k - p + 1$. Si $k \leq p - 1$, ce n'est pas une valeur possible de j, alors que pour $k \geq p$ c'en est une. On a donc

$$S_k \equiv \begin{cases} (-1)^{k-1} k\sigma_k \pmod p & \text{si} \quad k \leq p-1 \\ (-1)^{p-2}\sigma_{p-1} S_{k-p+1} \pmod p & \text{si} \quad k \geq p\ , \end{cases}$$

puisque par convention $\sigma_k = 0$ pour $k \geq p$. Comme $\sigma_{p-1} \equiv -1 \pmod p$ et que les autres sont divisibles par p, on en déduit les résultats suivants :

$$S_k \equiv \begin{cases} 0 \pmod p & \text{si} \quad k \leq p-2 \\ -1 \pmod p & \text{si} \quad k = p-1 \\ S_{k-p+1} & \text{si} \quad k > p-1\ . \end{cases}$$

Pour l'instant nous n'avons pas raisonné par récurrence. Mais maintenant il est très facile de le faire : tous les S_k sont divisibles par p pour $1 \leq k \leq p-2$, et $S_{p-1} \equiv -1 \pmod p$. La troisième congruence montre que les valeurs de S_k modulo p se répètent quand k augmente de $p-1$. Il en résulte par récurrence que $S_k \equiv 0 \pmod p$ pour tout k non divisible par $p-1$, et que $S_k \equiv -1 \pmod p$ pour k divisible par $p-1$ (ce qui n'était pas demandé).

4) a) Il est clair que

$$X^{p-1} A_p(1/X) = X^{p-1} \prod_{1 \leq a \leq p-1} (1/X - a) = \prod_{1 \leq a \leq p-1} (1 - aX) = R_p(X)\ ,$$

d'où la formule $R_p(X) = X^{p-1} A_p(1/X)$.

b) D'après a), on a

$$R_p(X) \equiv X^{p-1}((1/X)^{p-1} - 1) \equiv 1 - X^{p-1} \equiv -(X^{p-1} - 1) \pmod p\ .$$

Si on appelle τ_k les fonctions symétriques élémentaires du polynôme $R_p(X)$, on a donc comme ci-dessus $\overline{\tau_k} = \overline{0}$ dans le corps $\mathbb{F}_p$ pour $k \neq p-1$. Toutefois, on ne peut pas tout à fait légalement écrire ceci sous la forme $\tau_k \equiv 0 \pmod p$, car ceci sous-entend que τ_k est un entier, alors que c'est seulement un nombre rationnel. Toutefois, si on écrit $R_p(X) = \sum_{0 \leq i \leq p-1} a_i X^i$, on a par définition $\tau_k = (-1)^k a_{p-1-k}/a_{p-1}$. Or les a_i sont des nombres entiers, et $a_{p-1} = (-1)^{p-1}(p-1)!$. Il en résulte que $(p-1)!\tau_k$ est un entier. Comme p est premier, $(p-1)!$ est inversible modulo p (en fait est congru à -1 modulo p d'après le théorème de Wilson), donc l'égalité $\overline{\tau_k} = \overline{0}$ dans $\mathbb{F}_p$ est équivalente à $\overline{(p-1)!\tau_k} = \overline{0}$, qui elle peut légalement s'écrire $(p-1)!\tau_k \equiv 0 \pmod p$.

Le reste du raisonnement fait au 3b) peut alors se poursuivre identiquement, en multipliant la k-ième identité de Newton par $(p-1)!^k$ pour n'avoir affaire qu'à des entiers (il est clair en effet que $(p-1)!^i T_i$ est un entier). On en déduit comme ci-dessus que $(p-1)!^k T_k \equiv 0 \pmod p$ pour tout k non divisible par $p-1$, et que $(p-1)!^k T_k \equiv -1 \pmod p$ pour k divisible par $p-1$.

c) Les nombres rationnels de l'énoncé ne sont autres que les T_k. Si on pose $T_k = u/v$ avec u et v premiers entre eux, d'après la question précénte, si k n'est pas divisible par $p-1$ on a $(p-1)!^k u/v \equiv 0 \pmod p$, donc p divise en particulier $(p-1)!^k u$. D'après le lemme de Gauss, puisque p est premier à $(p-1)!$ on en déduit que p divise u.

Exercice II

1) a) On trouve $N = 5 \cdot 13 \cdot 17$.

b) D'après le théorème de Fermat, si $(a, N) = 1$ (donc en particulier $(a, p) = 1$ pour $p \mid N$), on a $a^4 \equiv 1 \pmod 5$ donc $a^{48} = (a^4)^{12} \equiv 1 \pmod 5$, puis $a^{12} \equiv 1 \pmod{13}$ donc $a^{48} = (a^{12})^4 \equiv 1 \pmod{13}$, et enfin $a^{16} \equiv 1 \pmod{17}$, donc $a^{48} = (a^{16})^3 \equiv 1 \pmod{17}$. Il en résulte que $a^{48} - 1$ est divisible par 5, 7 et 13, donc par leur produit puisqu'ils sont premiers entre eux. On a donc $a^{48} \equiv 1 \pmod N$, donc $a^{N-1} = a^{1104} = (a^{48})^{23} \equiv 1 \pmod N$. Le nombre N se comporte donc comme un nombre premier vis-à-vis du thèorème de Fermat, alors que ce n'en est pas un : c'est ce qu'on appelle un nombre de Carmichael.

c) D'après le théorème de Fermat, si a n'est pas divisible par p on a $a^{p-1} \equiv 1 \pmod p$, donc $a^{k(p-1)} \equiv 1 \pmod p$ pour tout k, donc $a^{k(p-1)+1} \equiv a \pmod p$ pour tout k. Mais, quand a est divisible par p, cette congruence est également trivialement vraie puisque les deux membres sont congrus à 0 modulo p. On en déduit donc que pour tout a et tout k on a

$$a^{k(p-1)+1} \equiv a \pmod p .$$

Ceci peut se reformuler en disant que si $(p-1)$ divise $(N-1)$ alors $a^N \equiv a \pmod p$. Or, on a effectivement $4 \mid 1104$, $12 \mid 1104$ et $16 \mid 1104$. On a donc $a^N \equiv a \pmod p$ pour $p = 5$, 13 et 17, et donc comme ci-dessus $a^N \equiv a \pmod N$.

2) a) Si $a + bj \in A$ et $c + dj \in A$, on a $(a + bj) - (c + dj) = (a - c) + (b - d)j \in A$, donc A est un sous-groupe additif de $\mathbb{C}$. De plus, on a

$$\begin{aligned}(a + bj)(c + dj) &= ac + (ad + bc)j + bdj^2 = ac + (ad + bc)j + bd(-1 - j)\\ &= (ac - bd) + (ad + bc - bd)j \in A ,\end{aligned}$$

donc la multiplication est stable, donc A est bien un sous-anneau de $\mathbb{C}$, et ce sous-anneau est unitaire puisque $1 = 1 + 0j \in A$. Noter que la raison essentielle pour laquelle ceci est vrai est qu'on a pu remplacer j^2 par une combinaison linéaire à coefficients entiers de 1 et j, c'est à dire parce que j satisfait à une équation du second degré à coefficients entiers, et unitaire. Le résultat ne serait pas vrai avec j remplacé par $\sqrt[3]{2}$ (équation de degré 3) ou par $j/2$ (équation non unitaire).

b) Soit $x = a + bj \in A$. D'après la formule du binôme de Newton, on a

$$x^p = a^p + b^p j^p + \sum_{1 \le k \le p-1} \binom{p}{k} a^k (bj)^{p-k} .$$

Puisque p est premier, les coefficients du binôme $\binom{p}{k}$ sont divisibles par p quand $1 \le k \le p-1$. De plus, d'après le théorème de Fermat, on a $a^p \equiv a \pmod p$ et $b^p \equiv b \pmod p$. On a donc $x^p \equiv a + bj^p \pmod{pA}$.

Si $p \equiv 1 \pmod 3$, on a $j^p = j \cdot (j^3)^{(p-1)/3} = j$, donc $x^p \equiv a + bj \equiv x \pmod{pA}$. D'autre part, si $p \equiv 2 \pmod 3$, on a $j^p = j^2 \cdot (j^3)^{(p-2)/3} = j^2$, donc $x^p \equiv a + bj^2 \equiv \overline{x} \pmod{pA}$.

3) Puisque $x = 1 + 2j = \sqrt{-3}$, on a

$$x^{N-1} = \sqrt{-3}^{1104} = (-3)^{552} = 3^{552} = 3^{(N-1)/2} \ .$$

a) Comme au début, comme $a = 3$ est premier à N, on en déduit que $3^4 \equiv 1 \pmod 5$ donc $3^{552} = (3^4)^{138} \equiv 1 \pmod 5$. De même, $3^{12} \equiv 1 \pmod{13}$ donc $3^{552} = (3^{12})^{46} \equiv 1 \pmod{13}$. Par contre, 552 n'est pas divisible par $16 = 17 - 1$, mais seulement par 8. Or $3^4 = 81 \equiv -4 \pmod{17}$, donc $3^8 \equiv 16 \equiv -1 \pmod{17}$. Il en résulte que $3^{552} = (3^8)^{69} \equiv (-1)^{69} \equiv -1 \pmod{17}$.

b) Il en résulte bien que $x^N \not\equiv x \pmod{17A}$, et à fortiori $x^N \not\equiv x \pmod{NA}$. D'après la question 2b), comme $N \equiv 1 \pmod 3$, si N était premier on aurait $x^N \equiv x \pmod{NA}$, ce qui n'est pas le cas, donc N n'est pas premier.

4) a) Comme à la question 2a), on vérifie immédiatement que K est un sous-anneau unitaire de $\mathbb{C}$. Il reste à montrer que tout élément non nul est inversible. Or si $x = a+bj \in K$, on a

$$\frac{1}{x} = \frac{a+bj^2}{(a+bj)(a+bj^2)} = \frac{a-b}{a^2-ab+b^2} - \frac{b}{a^2-ab+b^2} j \ ,$$

et ceci appartient bien à K puisque les coefficients de 1 et j sont rationnels.

b) Soit $x = x_1 + x_2 j \in K$, et posons $q = q_1 + q_2 j \in A$, où q_i est l'entier le plus proche de x_i. On a donc $|x_i - q_i| \leq 1/2$. Il en résulte que

$$|x-q|^2 = |(x_1-q_1)+(x_2-q_2)j|^2 = (x_1-q_1)^2-(x_1-q_1)(x_2-q_2)+(x_2-q_2)^2 \leq \frac{1}{4}+\frac{1}{4}+\frac{1}{4} = \frac{3}{4} \ ,$$

donc $|x - q| \leq \sqrt{3}/2 < 1$, comme il est demandé.

c) Soient a et b dans A avec $b \neq 0$. Si on pose $x = a/b$, puisque $A \subset K$ et que K est un corps, on en déduit que $x \in K$, et d'après la question précédente il existe donc $q \in A$ tel que $|x-q| < 1$. Ceci s'écrit $|a/b-q| < 1$, donc $|a-bq| < |b|$. Si on pose $r = a-bq \in A$, on a donc $a = bq + r$ avec $|r| < |b|$ donc $|r|^2 < |b|^2$, ce qui est donc bien une division euclidienne. De plus il est clair que $\phi(a) = |a|^2$ satisfait aux autres axiomes d'un stathme euclidien : c'est positif ou nul, nul seulement pour $a = 0$, et à valeurs entières. Notons que $\phi(a) = |a|$ n'est pas à valeurs entières, donc n'est pas un stathme euclidien au sens de la définition du cours. Il en résulte que A est un anneau euclidien, et donc principal.

d) Si $a = 1 + 10j$ et $b = 7 + 5j$, on calcule que $a/b = (4 + 5j)/3$, donc en prenant les entiers les plus proches, on trouve $q = 1+2j$. On a donc $a = bq+r$ avec $r = a-bq = 4+j$. De même, on effectue la division euclidienne de b par r, et on trouve que $b/r = 2 + j \in A$. On a donc $b = q_1 r + 0$ avec $q_1 = 2 + j$, donc r est le PGCD demandé, en d'autres termes un PGCD de a et de b est égal à $4 + j$. Noter que deux PGCD ne peuvent différer multiplicativement que par un élément inversible de A. Il est facile de montrer que ceux-ci sont ± 1, $\pm j$ et $\pm j^2 = \pm(-1 - j)$. Il en résulte que les 6 valeurs suivantes sont des PGCD de a et de b : $\pm(4 + j)$, $\pm(-1 + 3j)$ et $\pm(3 + 4j)$.