Arithmétique

Exercice 3.4.(c) Existe-il des nombres entiers a et b tels que $7a^2 - 3b^3 = 6$?

Supposons qu'il existe un couple solution (a, b). Alors $3b^3 + 6$ est congru à 0 modulo 7. Or, lorsque $b = 0, 1, \ldots, 6$ on voit que les valeurs modulo 7 *prises par b^3 sont $0, 1, 1, 6, 1, 6, 6$. Donc les valeurs prises par $3b^3 + 6$ sont $6, 2, 2, 3, 2, 3, 3$ qui n'est jamais nul. Contradiction, donc il n'existe pas de tels entiers a et b.*

Exercice 3.5. Un nombre entier strictement positif $\overline{abc}$ à trois chiffres est un nombre premier. Montrer que $b^2 - 4ac$ n'est pas le carré d'un nombre entier.

Notons $p = \overline{abc}$, qui est un nombre premier par hypothèse. D'abord, on peut oberver que $a \geqslant 1$ (car sinon p serait un nombre à au plus 2 chiffres) et $c \geqslant 1$ (car sinon p serait divisible par 10). Supposons que $b^2 - 4ac = d^2$ pour un certain entier $d \geqslant 0$. Nous allons montrer qu'alors le polynôme $F(X) = aX^2 + bX + c$ est produit de deux polynômes de degré 1 à coefficients entiers positifs ; comme $p = F(10)$, cela mènera à une contradiction avec l'hypothèse que c'est un nombre premier. Tout d'abord, comme $b^2 - 4ac = d^2$ alors en regardant modulo 2 on voit que b et d ont la même parité, donc leur somme et leur différence sont paires i.e. il existe des entiers $r \geqslant 1$ et $s \geqslant 1$ tels que $b - d = 2r$ et $b + d = 2s$. En faisant le produit de ces nombres, on trouve $ac = rs$. Ensuite, posons $e = \mathrm{pgcd}(a, r) \geqslant 1$ donc par définition il existe $f \geqslant 1$ et $r' \geqslant 1$ premiers entre eux tels que $a = ef$ et $r = er'$. Comme $er's = rs = ac = efc$, on trouve $r's = fc$ donc d'après le lemme de Gauss f divise s, c'est-à-dire, il existe $s' \geqslant 1$ tels que $s = fs'$. Enfin, en utilisant tout ce qui précède on trouve :

- $ef = a$,
- $er' + fs' = r + s = b$,
- $r's'a = r's'ef = rs = ac$, *donc* $r's' = c$,

ce qui mène à $(eX + s')(fX + r') = efX^2 + (er' + fs')X + r's' = aX^2 + bX + c$. Alors $p = 100a + 10b + c = F(10) = (10e + s')(10f + r')$ n'est pas premier.

Polynômes

On note k un corps et $k[X]$ l'anneau des polynômes à coefficients dans k.

Exercice 1 Soient a, b deux entiers. Dans $k[X]$, effectuez la division euclidienne de $X^a - 1$ par $X^b - 1$.

Soit $a = bq + r$ avec $r < b$ la division euclidienne de a par b. On a :

$$\begin{aligned} X^a - 1 = X^{bq}X^r - 1 =& (X^b - 1 + 1)^q X^r - 1 \\ =& \left(\sum_{i=0}^{q} \binom{q}{i} (X^b - 1)^i \right) X^r - 1 \\ =& \left(\sum_{i=1}^{q} \binom{q}{i} (X^b - 1)^{i-1} \right) X^r (X^b - 1) + (X^r - 1). \end{aligned}$$

Comme $\deg(X^r - 1) r < b = \deg(X^b - 1)$, on a trouvé la division euclidienne : le quotient est $Q = \sum_{i=1}^{q} \binom{q}{i} (X^b - 1)^{i-1} X^r$ et le reste est $R = X^r - 1$.

Exercice 2 Prouvez les faits suivants.

(1) Un polynôme irréductible possède une racine dans k si et seulement s'il est de degré 1.

(2) Un polynôme de degré 2 ou 3 est irréductible si et seulement s'il n'a pas de racine.

(3) Il existe un corps k, et un polynôme de degré $n \geqslant 4$ qui n'a pas de racine mais n'est pas irréductible.

(1) Soit P un polynôme irréductible. S'il possède une racine $\lambda \in k$ alors la division euclidienne de P par $X - \lambda$ a un reste nul, donc $P = (X - \lambda)Q$. Mais comme P est irréductible, Q est constant et $\deg(P) = 1$. Réciproquement si $\deg(P) = 1$ alors $P = aX + b$ avec $a \neq 0$, et $\lambda = -b/a$ est une racine.
(2) Soit P un polynôme de degré $n = 2$ ou $n = 3$. Alors P n'est pas irréductible si et seulement s'il est produit de deux facteurs de degrés > 1. Lorsque $n = 2$ les degrés des facteurs sont 1 et 1 et lorsque $n = 3$ les degrés sont 1 et 2. Dans les deux cas il existe un facteur de degré 1, donc une racine.
(3) Sur $k = \mathbb{R}$, le polynôme $P = (X^2 + 1)^2$ est de degré 4, non irréductible, sans racine. Ceci montre que le résultat de la question précédente ne peut pas être étendu au degré 4.

Exercice 3 On considère le corps k à deux éléments, noté $\mathbb{F}_2$.

(1) Rappelez la table d'addition et la table de multiplication de k.

(2) Trouvez tous les polynômes irréductibles de degré 2 de $k[X]$ et donnez leur nombre.

(3) Trouvez tous les polynômes irréductibles de degré 3 de $k[X]$ et donnez leur nombre.

(4) Trouvez tous les polynômes irréductibles de degré 4 de $k[X]$ et donnez leur nombre.

(2) On commence par trois petites remarques liées au fait que k ne contient que 0 et 1 : tous les polynômes non nuls sont unitaires ; un élément $\lambda \in k$ n'est pas racine de P ssi $P(\lambda) = 1$; un polynôme P est sans racine ssi $P(0) = P(1) = 1$. Venons à la question proprement dite. En utilisant l'exercice précédent, on cherche les polynômes $P = X^2 + aX + b$ sans racine i.e.

tels que $P(0) = P(1) = 1$. Ceci donne $b = 1$ puis $a = 1$. On tombe sur $P = X^2 + X + 1$ qui est le seul polynôme irréductible de degré 2.

(3) Encore d'après l'exercice précédent, on cherche les polynômes $P = X^3 + aX^2 + bX + c$ tels que $P(0) = P(1) = 1$ c'est-à-dire $c = 1$ et $a + b = 1$. Ainsi $P = X^3 + aX^2 + (a + 1)X + 1$ ce qui fait, selon que $a = 0$ ou $a = 1$, deux polynômes irréductibles de degré 3.

(4) Même s'il n'est plus vrai en degré $\geqslant 4$ que les polynômes irréductibles sont les polynômes sans racine, nous allons voir qu'on peut encore s'appuyer sur les polynômes sans racine. On sait qu'un polynôme irréductible de degré 4 est sans racine (cf exercice précédent). À quoi ressemble un polynôme de degré 4 sans racine et non irréductible ? Un tel polynôme se décompose en produit de deux facteurs qui sont chacun de degré 2 (car s'il y a un facteur de degré 1, il y a une racine) et irréductibles (car sinon, même chose, il y a une racine !). On a vu qu'il n'y a qu'un polynôme de degré 2 irréductible, c'est $X^2 + X + 1$. Donc il n'y a qu'un polynôme de degré 4 sans racine non irréductible, c'est $(X^2 + X + 1)^2$. Finalement, dans l'ensemble des polynômes de degré 4, on a l'égalité entre les deux sous-ensembles suivants :

$$\{ \text{ polynômes sans racine } \} = \{ \text{ polynômes irréductibles } \} \cup \{(X^2 + X + 1)^2\}.$$

Or il n'est pas trop difficile d'énumérer les polynômes $P = X^4 + aX^3 + bX^2 + cX + d$ sans racine. En effet, il faut et il suffit de demander que $P(0) = P(1) = 1$ i.e. $d = 1$ et $a+b+c = 1$. On trouve donc les polynômes $P = X^4+aX^3+bX^2+(a+b+1)X+1$. Comme a et b parcourent $k = \{0, 1\}$, ceci fait une liste de 4 polynômes de laquelle il faut enlever celui correspondant à $a = 0$ et $b = 1$ qui est le polynôme $(X^2+X+1)^2$. Finalement on obtient 3 polynômes de degré 4 irréductibles qui sont :

- *pour $a = b = 0$, $X^4 + X + 1$,*
- *pour $a = b = 1$, $X^4 + X^3 + X^2 + X + 1$,*
- *pour $a = 1$ et $b = 0$, $X^4 + X^3 + 1$.*