TP.IX.A FACTORISATION DES POLYNOMES

Vous avez étudié au sein des TR VIII.A et VIII.B des critères permettant de vérifier l'irréductibilité de polynômes. Si ces derniers permettent de traiter des cas de degré arbitrairement grand, ils ne s'appliquent cependant pas à n'importe quel polynôme que l'on se donne explicitement. Par contre, MAPLE sait factoriser dans $\mathbb{Q}[x]$ (commande `factor` ou `factors`, selon l'affichage souhaité) tout polynôme, pourvu que le degré ne soit pas tel que l'on dépasse les capacités de la machine. Le but de ce TP est de comprendre et de réimplémenter l'algorithme qui se cache derrière la commande MAPLE (ou du moins un algorithme efficace qui réalise la factorisation).

Quitte à multiplier par un entier suffisamment grand, on peut toujours supposer que le polynôme P appartient à $\mathbb{Z}[x]$. On peut alors réduire P modulo un nombre premier p et se poser la question de la factorisation du polynôme $\overline{P}$ obtenu dans $\mathbb{F}_p[x]$ (où $\mathbb{F}_p$ désigne le corps fini $\mathbb{Z}/p\mathbb{Z}$). La commande MAPLE correspondante est `Factor(P) mod p` (ou `Factors(P) mod p`). Nous allons décrire un algorithme de factorisation sur un corps fini, dû à Berlekamp, qui utilise essentiellement de l'algèbre linéaire et le morphisme de Frobenius (*cf.* TR.IX.A). Pour simplifier, nous nous limiterons à $\mathbb{F}_p$. Signalons également qu'il existe d'autres algorithmes (Cantor-Zassenhaus, *etc...*) ; le lecteur trouvera dans [G-G] une description de ces derniers et une comparaison de leur efficacité en fonction des différents paramètres du problème.

L'algorithme de factorisation sur $\mathbb{Q}$ que nous décrirons est de nature « modulaire » : on factorise $\overline{P}$ sur $\mathbb{F}_p$ et reconstruit les facteurs de P dans $\mathbb{Z}[x]$ à partir des facteurs de $\overline{P}$. C'est possible grâce à une borne a priori M des coefficients des diviseurs de P (borne de Mignotte) ; on prend alors $p > 2M$. Nous nous limiterons au cas d'un seul grand nombre premier. Il existe d'autres variantes : par exemple, prendre un petit premier p et un entier n tel $p^n > 2M$. On relève alors la factorisation dans $\mathbb{F}_p$ en une décomposition dans $\mathbb{Z}/p^n\mathbb{Z}$ grâce au « lemme de Hensel ». Le lecteur intéressé trouvera dans [G-G] chapitre 15 une description de cette seconde méthode modulaire ainsi qu'une discussion de la pertinence des deux méthodes en fonction des paramètres du problème.

☞ *Quelques remarques concernant la manipulation des polynômes modulo p en* MAPLE : par rapport aux commandes relatives aux polynômes de $\mathbb{Z}[x]$ et $\mathbb{Q}[x]$, les noms sont en général conservés mais les commandes commencent par une majuscule et se terminent par `mod p`. On utilisera donc `Expand(P) mod p` pour développer, `Gcd(P,Q) mod p` pour le calcul du pgcd, `Quo(A,B,x) mod p` et `Rem(A,B,x) mod p` pour le quotient et le reste de la division euclidienne. Le degré s'obtient encore par `degree(P,x)`, le coefficient de degré i par `coeff(P,x,i)` et le coefficient dominant simplement via `lcoeff`.

Corps finis et irréductibles de $\mathbb{F}_p[x]$

Nous avons besoin, pour effectuer la factorisation dans $\mathbb{F}_p[x]$, d'un test d'irréductibilité. Nous allons donner un tel critère et en profiter pour indiquer comment construire de manière effective les corps finis $\mathbb{F}_{p^n}$ (ils seront étudiés en détail au chapitre XV, où on les définit à l'aide d'une clôture algébrique de $\mathbb{F}_p$, ce qui démontre l'existence et l'unicité de ces corps mais n'explique pas comment on calcule, en pratique, dans les corps finis). En effet, si P est un polynôme irréductible de degré n alors l'idéal (P) qu'il engendre est un idéal premier donc maximal de $\mathbb{F}_p[x]$ (en vertu de la principalité de $\mathbb{F}_p[x]$). Le quotient $\mathbb{F}_p[x]/(P)$ est donc un corps, et un $\mathbb{F}_p$-espace vectoriel de base $\overline{1}, \overline{x}, \ldots, \overline{x}^{n-1}$, où $n = \deg P$, c'est-à-dire un corps à p^n éléments.

Proposition 1. *Pour qu'un polynôme $P \in \mathbb{F}_p[x]$ de degré $n \geqslant 1$ soit irréductible, il faut et il suffit qu'il satisfasse aux deux conditions suivantes :*

(i) P divise $x^{p^n} - x$

(ii) pour tout diviseur strict d de n, P ne divise pas $x^{p^d} - x$.

Démonstration. Considérons les degrés des facteurs irréductibles de P. En vertu du lemme ci-dessous, la condition *(i)* signifie que ce sont tous des diviseurs de n et la condition *(ii)* qu'aucun d'entre eux n'est un diviseur strict de n. Il n'y a donc qu'un seul facteur irréductible et il est de degré n ; autrement dit, P est irréductible. □

Lemme 1. *Soit $n \geqslant 1$ un entier. Le polynôme $x^{p^n} - x \in \mathbb{F}_p[x]$ est exactement le produit de tous les polynômes irréductibles unitaires de $\mathbb{F}_p[x]$ de degré divisant n.*

Démonstration. Soit tout d'abord P un diviseur irréductible de $\mathbb{F}_p[x]$ de degré un diviseur d de n. Il s'agit de démontrer que P divise $x^{p^n} - x$. On a déjà vu que $\alpha^{p^d} = \alpha$ pour tout élément α d'un corps fini de cardinal p^d (TR.IX.A). Comme $K = \mathbb{F}_p[x]/(P)$ est un tel corps, on peut appliquer ce fait à la classe $\overline{x}$ de x dans K. Ensuite, sachant que d divise n, on en déduit que $\overline{x}^{p^n} = \overline{x}$ (on itère le Frobenius $\varphi_{p^d} : a \mapsto a^{p^d}$ qui est l'identité sur K), donc que P divise $x^{p^n} - x$.

Réciproquement, supposons que P soit un facteur irréductible de $x^{p^n} - x$ et démontrons que le degré d de P divise n. Considérons l'ensemble K' des éléments α du corps $K = \mathbb{F}_p[x]/(P)$ tels que $\alpha^{p^n} = \alpha$. Le fait que K' soit un corps découle directement du fait que φ_{p^n} est un morphisme de corps. De plus, il contient la classe de x modulo P, car P divise $x^{p^n} - x$; c'est donc K tout entier.

D'autre part, on a vu que le groupe des inversibles d'un corps est cyclique (TR.IX.A). Il existe donc un élément α de $K^\times$ d'ordre $p^d - 1$. Comme $\alpha^{p^n} = \alpha$, ou encore $\alpha^{p^n - 1} = 1$, on voit que $p^d - 1$ divise $p^n - 1$. Cela implique que d divise n : écrivons $n = dq + r$; alors $p^n - 1 = p^{dq}p^r - 1 = (p^{dq} - 1)p^r + p^r - 1$. Comme $p^d - 1$ divise $p^{dq} - 1$ et que $p^r - 1 < p^d - 1$, on voit que $p^r - 1$ est le reste de la division euclidienne de $p^n - 1$ par $p^d - 1$. Or ce reste est nul, donc $r = 0$.

Ainsi apparaissent dans la décomposition en irréductibles de $x^{p^n} - x$ tous les polynômes irréductibles unitaires de $\mathbb{F}_p[x]$ de degré divisant n et uniquement ceux-là. Il reste à prouver que ces facteurs sont tous de multiplicité un. On considère pour cela le polynôme dérivé $p^n x^{p^n - 1} - 1 = -1$; il est premier avec $x^{p^n} - x$, d'où le résultat. □

Cela démontre le critère. Existe-t-il pour autant de tels polynômes ?

Proposition 2. *Pour tout nombre premier p et tout entier $n \geqslant 1$ il existe des polynômes irréductibles de degré n dans $\mathbb{F}_p[x]$.*

On a besoin, afin de construire les corps finis, d'une preuve effective. La méthode utilisée en pratique est surprenante au premier abord : on tire au hasard un polynôme unitaire de degré n dans $\mathbb{F}_p[x]$, teste son irréductibilité, et recommence en cas d'échec.

En effet, notant $I(n,p)$ le nombre de polynômes irréductibles unitaires de $\mathbb{F}_p[x]$ de degré $n \geqslant 1$, il résulte du lemme précédent que $\sum_{d|n} dI(d,p) = p^n$. On en déduit la majoration $I(n,p) \leqslant p^n/n$ que l'on applique également aux $I(d,p)$ pour $d < n$ divisant n. Ainsi

$$p^n - nI(n,p) \leqslant \sum_{d|n, d<n} p^d \leqslant \sum_{d=1}^{E(n/2)} p^d = p(p^{E(n/2)} - 1)/(p-1) < p^{E(n/2)+1},$$

d'où une minoration de $I(n,p)$. Finalement :

$$\frac{p^n - p^{E(n/2)+1}}{n} \leqslant I(n,p) \leqslant \frac{p^n}{n}.$$

Cela montre que $I(n,p) > 0$. Mieux encore, on en déduit qu'un polynôme irréductible unitaire de grand degré n choisi au hasard a en gros une chance sur n d'être irréductible.

Enfin, expliquons comment vérifier le critère d'irréductibilité de manière efficace : on se place dans l'anneau quotient $\mathbb{F}_p[x]/(P)$ et calcule les puissances x^{p^i} de x modulo P. Puisque $x^{p^{i+1}} = (x^{p^i})^p$, on procède par récurrence et calcule successivement les restes R_i de la division euclidienne de R_{i-1}^p par P, à partir de $R_0 = x$. La condition *(i)* s'écrit $R_n = x$ et *(ii)* est équivalente à $R_i \neq x$ pour $i < n$ divisant n.

1. Ecrire une procédure `irreductible?:=proc(P,p)` testant l'irréductible de P sur $\mathbb{F}_p$ (où P est entré comme un polynôme à coefficients entiers). On utilisera la stratégie exposée ci-dessus.

La fonction suivante permet de tirer au hasard un polynôme unitaire de degré $n \geqslant 1$ dans $\mathbb{F}_p[x]$:

```
randpol:=(n,p)->sort(x^n+RandomTools[Generate](polynom(integer(range=0..p-1),
        x,degree=n-1))):
```

Vérifier que la probabilité d'obtenir un polynôme irréductible de degré n par un tel tirage au hasard est de l'ordre de $1/n$. On pourra écrire une procédure `test:=proc(N,n,p)` renvoyant la proportion de cas favorables pour N tirages.

Enfin, écrire une procédure `polirreductible:=proc(n,p)` renvoyant un polynôme de $\mathbb{F}_p[x]$ unitaire irréductible de degré n.

Factorisation sur $\mathbb{F}_p$

L'algorithme procède en plusieurs étapes.

La première étape consiste à éliminer les facteurs multiples à l'aide de la dérivation. Ecrivant $f = \sum a_i x^i \in \mathbb{F}_p[x]$, le polynôme dérivé est par définition $f' = \sum i a_i x^{i-1}$. Il est nul si et seulement si $f \in \mathbb{F}_p[x^p]$, ou encore, puisque $\sum a_{ip} x^{ip} = (\sum a_{ip} x^i)^p$, si et seulement si $f = g^p$, $g \in \mathbb{F}_p[x]$. En particulier, la dérivée d'un polynôme irréductible est non nulle.

Il s'agit d'écrire la « factorisation sans facteur carré » de f, c'est-à-dire la décomposition $f = \lambda h_1^1 h_2^2 \dots h_s^s$ où λ est le coefficients dominant de f et les h_i sont unitaires sans facteur carré et premiers deux à deux. Si $f = \lambda \prod_{i=1}^r f_i^{e_i}$ est la décomposition de f en facteurs irréductibles (unitaires) dans $\mathbb{F}_p[x]$, alors $h_i = \prod_{e_j=i} f_j$, d'où l'existence et l'unicité de la factorisation sans facteur carré.

Expliquons comment l'obtenir (sans factoriser !). Quitte à diviser par λ, on suppose f unitaire. Partant de $f' = \sum_i i h_i' h_i^{i-1} \prod_{j \neq i} h_j^j$, le lecteur vérifiera que

$$u = \operatorname{pgcd}(f, f') = \prod_{p \nmid i} h_i^{i-1} \prod_{p \mid i} h_i^i.$$

On définit alors deux suites u_k et v_k par récurrence comme suit : $u_1 = u$ et $v_1 = f/u = \prod_{p \nmid i} h_i$. Pour $k \geqslant 1$, on pose $v_{k+1} = \operatorname{pgcd}(u_k, v_k)$ si $p \nmid k$ et $v_{k+1} = v_k$ si $p \mid k$, puis $u_{k+1} = u_k / v_{k+1}$.

On vérifie facilement par récurrence que

$$u_k = \prod_{i>k, p\nmid i} h_i^{i-k} \prod_{p|i} h_i^i \text{ et } v_k = \prod_{i\geqslant k, p\nmid i} h_i.$$

Il en résulte que $h_k = v_k/v_{k+1}$ si $p \nmid k$. On obtient ainsi des h_k jusqu'à ce que v_k soit un polynôme constant, auquel cas $u_{k-1} = \prod_{p|i} h_i^i = g^p$. On remplace alors f par g et recommence.

2. Ecrire une procédure `sans2fact:=proc(f,p)` renvoyant la factorisation sans facteur carré de f, formatée comme une liste $[\lambda, [h_1, e_1], \ldots, [h_s, e_s]]$. Tester avec $f(x) = x^{15} + 2x^{14} + 2x^{12} + x^{11} + 2x^{10} + 2x^8 + x^7 + 2x^6 + 2x^4$ et $p = 3$; comparer avec le résultat de la commande Maple `Sqrfree(f) mod 3`.

La deuxième étape consiste à factoriser $P = h$ (sans facteur carré) en un produit d'irréductibles distincts : $P = \prod_{i=1}^r P_i$. D'après le lemme chinois, l'algèbre $A = \mathbb{F}_p[X]/(P)$ est isomorphe au produit $\prod_{i=1}^r \mathbb{F}_p[x]/(P_i)$. Comme les P_i sont irréductibles, chaque $\mathbb{F}_p[X]/(P_i)$ est un corps (à $p^{\deg(P_i)}$ éléments). Le Frobenius $\varphi_p : A \to A$, donné par $a \mapsto a^p$, est un morphisme d'algèbre. Sa matrice, dans la base $\overline{1}, \overline{x}, \ldots, \overline{x}^{n-1}$, où $n = \deg P$, s'appelle la matrice de Berlekamp.

☞ *Quelques remarques concernant l'algèbre linéaire sur $\mathbb{F}_p$ en* Maple : on utilise la librairie dédiée : faire `with(LinearAlgebra:-Modular)`. La matrice identité I_n de $\mathrm{M}_n(\mathbb{F}_p)$ se définit alors par la commande `Create(p,n,n,identity,integer)`. Déclarant une variable `M:=Mod(p,Matrix(n,n),integer)`, on remplit ensuite la matrice M par des affectations `M[i,j]:=...` Le noyau de M s'obtient via `Nullspace(M) mod p` ; l'algorithme sous-jacent est l'algorithme de Gauss-Jordan (appliqué à la transposée de M, *cf.* TP.VI.A).

3. Ecrire une procédure `Bmatrice:=proc(P,p)` renvoyant la matrice de Berlekamp B. Tester avec $P = x^4 + 1$ et $p = 3$, par exemple, et calculer le noyau de $B - I_4$. Comparer la dimension de ce noyau aux nombres de facteurs irréductibles dans la décomposition sur $\mathbb{F}_3$. Tester la conjecture que cela suscite à l'aide d'une procédure `test:=proc(P,p)` et de polynômes tirés au hasard par `randpol`. Enfin, démontrer au papier-crayon pour tout $P = \prod_{i=1}^r P_i$ que la sous-algèbre de Berlekamp N de A, noyau de $\varphi_p - \mathrm{Id}_n$, est isomorphe à $\mathbb{F}_p^r$, via le morphisme $a \mapsto (a \mod P_1, \ldots, a \mod P_r)$ du théorème Chinois.

4. Soit S une $\mathbb{F}_p$-base de N. Ecrire une procédure `Vect2Pol:=proc(v)` convertissant un vecteur $v = (y_1, \ldots, y_n) \in \mathbb{F}_p^r$ en le polynôme $\sum_{i=1}^n y_i x^{i-1}$. En déduire S sur l'exemple $P = x^4 + 1$ et $p = 3$.

On note $S = \{\overline{1}, \overline{v_1}, \ldots, \overline{v_{r-1}}\}$. Si $r \geqslant 2$, démontrer qu'il existe, pour tout $1 \leqslant i, j \leqslant r$, $i \neq j$, un élément $\alpha \in \mathbb{F}_p$ et un indice $1 \leqslant k \leqslant r-1$ tels que $v_k \equiv \alpha \mod P_i$ et $v_k \not\equiv \alpha \mod P_j$ (raisonner par l'absurde : si on avait $v_k \equiv \alpha_k \mod P_i$ et $v_k \equiv \alpha_k \mod P_j$ pour tout $1 \leqslant k \leqslant r-1$, exhiber une contradiction en regardant dans la base S un élément $\overline{a}$ tel que $a \equiv 1 \mod P_i$ et $a \equiv 0 \mod P_j$). En déduire que si Q est un diviseur de P non irréductible alors il existe un élément $\alpha \in \mathbb{F}_p$ et un indice $1 \leqslant k \leqslant r-1$ tels que $\mathrm{pgcd}(v_k - \alpha, Q)$ soit un diviseur strict de Q.

Finalement, démontrer que l'algorithme suivant factorise P :

```
on pose i := 1 ; L := [P] ;      # liste de polynomes dont le produit est P
tant que longueur(L) < r
  on prend Q := L[i] ;
```

```
    pour tout k ⩽ r − 1, α ∈ F_p
      on pose D := pgcd(v_k − α, Q) ;
      si 0 < degré(D) < degré(Q),
        remplacer Q par D dans L et rajouter Q/D a la fin
        recommencer au début de la boucle extérieure
    poser i := i+1 ;    # Q est irréductible, on n'y touche plus
  renvoyer L
```

L'implémenter (on écrira une procédure `Berlekamp1:=proc(P,p)` renvoyant la liste formatée $[\lambda, [P_1, 1], \ldots, [P_r, 1]]$ des facteurs irréductibles unitaires de multiplicité 1, précédés du coefficient dominant) et le tester avec $P = x^4 + 1$ et $p = 3, 17$. Comparer avec le résultat de la commande `Factors`.

5. On va maintenant introduire une variante probabiliste de l'algorithme précédent qui améliore le temps de calcul. Pour simplifier, on suppose $p \neq 2$ (l'algorithme est différent dans ce cas particulier ; voir [G-G]).

L'idée est la suivante : on choisit au hasard une combinaison linéaire $\overline{a}$ des éléments de la base S (les coefficients étant choisis par des tirages indépendants). Les $a \mod P_i$ sont donc des éléments aléatoirement uniformément distribués sur $\mathbb{F}_p$, indépendemment pour tout i. Alors, si cette combinaison est non nulle, soit $\mathrm{pgcd}(a, P)$ est un facteur non trivial de P et l'on a gagné, soit $a^{\frac{p-1}{2}} \equiv \pm 1 \mod P_i$ pour tout i et chaque cas se produit avec la probabilité $1/2$, indépendemment pour chaque indice i (résultat classique sur les carrés dans le corps $\mathbb{F}_p$, *cf.* TR.IX.A). Il y a beaucoup de chances pour que $\mathrm{pgcd}(a^{\frac{p-1}{2}} - 1, P)$ soit un facteur non trivial de P : il faut et suffit pour cela qu'il existe deux indices distincts i et j tels que $a^{\frac{p-1}{2}} - 1 \equiv 0 \mod P_i$ et $a^{\frac{p-1}{2}} - 1 \not\equiv 0 \mod P_j$.

Ecrire une procédure `test:=proc(P,p,S,N)` renvoyant, pour N tirages, la proportion q_1 de cas où $\mathrm{pgcd}(a, P)$ est un facteur non trivial de P et la proportion q_2 de cas où $\mathrm{pgcd}(a^{\frac{p-1}{2}} - 1, P)$ est un facteur non trivial de P parmi les cas où $\mathrm{pgcd}(a, P) = 1$. Tester avec $P = x^4 + 1$ et $p = 17$. Enfin, calculer les probabilités théoriques correspondantes et comparer sur l'exemple avec les proportions obtenues.

6. Même si la probabilité d'obtenir un facteur irréductible est élevée, il est nécessaire de vérifier qu'il en est bien ainsi : c'est là qu'intervient la procédure `irreductible?` de la première partie. Ecrire une procédure `Berlekamp2` renvoyant la factorisation obtenue par cette variante probabiliste. On modifiera `Berlekamp1`, les facteurs D de la liste L étant cette fois de la forme $\mathrm{pgcd}(a, P) = 1$ ou $\mathrm{pgcd}(a^{\frac{p-1}{2}} - 1, P)$.

Remarque. Il est difficile de mettre en évidence avec MAPLE que la variante probabiliste est meilleure, étant donnée la façon dont l'arithmétique élémentaire est implémentée (calculer avec des petits nombres prend le même temps qu'avec des nombres plus grands : MAPLE effectue les opérations en multiprécision). De plus, il faudrait optimiser l'exponentiation.

Factorisation sur $\mathbb{Q}$

On suppose P à coefficients entiers. Comme pour $\mathbb{F}_p$, la première étape consiste à écrire la décomposition sans facteur carré de P, *i.e.* $P = \lambda h_1^1 h_2^2 \ldots h_s^s$ où λ est le coefficient dominant de P et les $h_i \in \mathbb{Q}[x]$ sont unitaires sans facteur carré et premiers deux à deux.

7. La situation est plus simple qu'en caractéristique p : sur l'exemple $f = x^{12} + x^{11} - x^9 - 2x^8 + x^5 + x^4$, calculer $u = f/\operatorname{pgcd}(f, f')$, factoriser en irréductibles f/u, puis recommencer en remplaçant f par u, *etc...* Observer les facteurs des quotients f/u successifs et en déduire un algorithme donnant la décomposition sans facteur carré. L'implémenter au sein d'une procédure `Sans2Fact0:=proc(f)`, tester et comparer avec la commande `sqrfree` de MAPLE.

Remarque. En fait, la commande `sqrfree` renvoie la décomposition sans facteur carré de P dans $\mathbb{Z}[x]$, *i.e.* l'écriture $P = \lambda h_1^1 h_2^2 \dots h_s^s$ où $\lambda \in \mathbb{Q}$ et les $h_i \in \mathbb{Z}[x]$ sont primitifs sans facteur carré et premiers deux à deux. La décomposition en irréductibles dans $\mathbb{Z}[x]$ (*cf.* chapitre VIII) assure l'existence et l'unicité de cette décomposition.

8. Nous allons réduire P modulo un nombre premier p. Pour appliquer l'algorithme de Berlekamp, il faut s'assurer que la réduction $\overline{P}$ est sans facteur carré. Le but de cette question est d'expliquer quels nombres p conviennent, c'est-à-dire comment choisir p sans avoir à calculer $\operatorname{pgcd}(\overline{P}, \overline{P}')$ et recommencer avec un nouveau p si l'on ne trouve pas un polynôme constant.

Calculer `gcd(2*x,2); gcd(-2*x,2); gcd(x/2,1/2); Gcd(2*x,2) mod 3;` Quelle normalisation du pgcd MAPLE utilise-t-il ? Calculer `gcd(f,g) mod 3; Gcd(f,g) mod 3;` pour $f = 18x^3 - 42x^2 + 30x - 6$ et $g = -12x^2 + 10x - 2$. Calculer également les résultants suivants : `resultant(f,g,x) mod 2; Resultant(f,g,x) mod 2;` pour $f = 4x^3 - x$ et $g = 2x + 1$ (voir TR.VIII.C pour une définition du résultant, ou la partie du TP.XI qui y est consacrée).

Le pgcd et le résultant de deux polynômes ne se sont comportent donc pas bien a priori vis à vis de la réduction modulo p. Cependant, on voit facilement que si p ne divise pas le coefficient dominant des deux polynômes, alors le résultant réduit modulo p coïncide avec le résultant des réductions modulo p. On voit également que si p ne divise pas le coefficient dominant de l'un des polynômes, alors le résultant réduit modulo p n'est pas nul si et seulement si le résultant n'est pas divisible par p.

D'autre part, on a vu que le résultant de f et g (non tous les deux nuls), calculé sur un corps ($\mathbb{Q}$ ou $\mathbb{F}_p$), est nul si et seulement si $\operatorname{pgcd}(f, g)$ est non constant (TR.VIII.C). Ainsi, si p ne divise pas le coefficient dominant de l'un des polynômes f et g, alors $\operatorname{pgcd}(f, g)$ est non constant si et seulement si $\operatorname{pgcd}(\overline{f}, \overline{g})$ est non constant. En prenant $f = P$ et $g = P'$, on voit que, si p ne divise pas le coefficient dominant de P alors $\overline{P}$ est sans facteur carré si et seulement p ne divise pas le résultant de P et P'. En particulier, il n'y a qu'un nombre fini de mauvais p. Par définition, le *discriminant* de f est $D(f) = \frac{(-1)^{\frac{n-1}{2}} Res(f,f')}{a}$, où a désigne le coefficient dominant de f. On l'obtient avec la commande MAPLE `discrim(f,x)`. La définition du résultant montre que a^{2n-2} divise $D(f)$, donc a fortiori a. En défintive, si p ne divise pas $D(P)$ alors $\overline{P}$ est sans facteur carré. Tester en prenant $P = x^9 + x^6 + x^5 - 2x^4 - 2x - 2$.

Remarque. Si p ne divise pas le coefficient dominant de f et f, on peut montrer que $\operatorname{pgcd}(\overline{f}, \overline{g}) = \overline{c}\overline{\operatorname{pgcd}(f, g)}$, où c est le coefficient dominant de $\operatorname{pgcd}(f, g)$ calculé dans $\mathbb{Z}[x]$ (voir [G-G] chapitre 6.4).

9. Avant de poursuivre avec la description de l'algorithme à proprement parlé, faisons une petite disgression au sujet des tests modulaires d'irréductibilité : il s'agit d'exploiter au

maximum les factorisations de P modulo différents nombres premiers (puisque nous savons déjà tester l'irréductibilité et factoriser sur $\mathbb{F}_p$).

On se donne la liste $L = (x^7 + 2x^5 + 1,\ x^8 + 2x^5 + 1,\ x^9 + x^4 + x^3 + 5x^2 + 11,\ x^4 + 3x^2 + 7x + 4,\ x^6 + 2x^3 + 4x^2 + 15,\ x^7 + x + 1)$.

- Appliquer le critère par réduction du TR.VIII.B : pour quels polynôme de la liste L peut-on conclure à l'aide des premiers p inférieur à 20 (obtenus par exemple via `select(isprime([$1..20]))`? On écrira une procédure `test1:=proc(f)` que l'on appliquera aux éléments de la liste.
- Ecrire une procédure `test2:=proc(f)` renvoyant la liste des degrés des facteurs dans la décomposition en irréductibles sur $\mathbb{F}_p$, pour les différents p premiers inférieurs à 20 tels que cette décomposition soit sans facteur carré (et que p ne divise pas le coefficient dominant de P). Peut-on conclure, à l'aide de ces renseignements, pour tous les cas non tranchés par le test précédent ?
- Proposer un argument pour le cas restant.

La factorisation des polynômes sur $\mathbb{Q}[x]$ est possible par des méthodes modulaires grâce au théorème suivant (consulter [M] pour une preuve) :

Théorème 1. *Soit $P = QR$ avec $P = \sum_i a_i x^i$, $Q = \sum_i b_i x^i$ et R des polynômes de $\mathbb{Z}[x]$. On note d le degré de Q et $\|P\|$ la norme euclidienne de P, c'est-à-dire $\|P\| = (\sum_i |a_i|^2)^{1/2}$. Alors $|b_i| \leqslant \binom{d}{i}\|P\|$.*

Soit alors $M = \|P\| \sup_{1\leqslant d\leqslant \deg(P)/2} \sup_{1\leqslant i\leqslant d} \binom{d}{i}$, appelée borne de Mignotte (ou toute autre constante dont l'on sache que si Q est un diviseur non trivial de P alors les coefficients de l'un parmi Q et P/Q sont majorés en valeur absolue par M). Choisissons un nombre premier $p > 2M$ ne divisant pas le coefficient dominant de P et tel que la réduction $\overline{P}$ modulo p soit sans facteur carré. On écrit la décomposition $\overline{P} = \overline{\lambda}\prod_{i=1}^r \overline{P_i}$ en irréductibles dans $\mathbb{F}_p[x]$ (où λ désigne le coefficient dominant de P).

Si S est un sous-ensemble de $\{1, \ldots, r\}$, on note P_S le polynôme congru à $\prod_{i\in S} P_i$ modulo p dont tous les coefficients sont compris entre $-p/2$ et $p/2$ (choisir les représentants de $\mathbb{Z}/p\mathbb{Z}$ symétriques par rapport à 0, que l'on obtient en Maple avec l'opérateur `mod` en définissant au préalable `mod:='mods'`). Si P n'est pas irréductible, il s'écrit $P = \lambda QR$ et on a donc $QR \equiv \prod_{i=1}^r P_i \mod p$. Il existe donc une partition de $\{1, \ldots, r\}$ en deux sous-ensembles I et J tels que $Q \equiv P_I \mod p$ et $R \equiv P_J \mod p$. L'un des deux, par exemple Q, est de degré $\deg(Q) \leqslant \deg(P)/2$. En vertu du théorème précédent et du choix de p, Q est égal à P_I dans $\mathbb{Z}[x]$.

☞ *Autres commandes* Maple *utiles* : `floor` (partie entière), `binomial`, `norm(f,2)` (pour calculer $\|f\|$), `convert(S,'*')` (pour multiplier entre eux tous les polynômes de la liste S) ; enfin, si S est une liste de polynômes, `combinat[chose](S,i)` renvoie la liste des parties de S à i éléments.

10. Ecrire une procédure `trouve_p:=proc(f)` renvoyant un nombre premier (de préférence le plus petit) supérieur strictement à 2 fois la borne de Mignotte, ne divisant pas le coefficient dominant de f et tel que $\overline{P}$ soit sans facteur carré.

Traiter les exemples suivants : $P = x^6 + 2x^3 + 4x^2 + 15$, $P = x^9 + x^6 + x^5 - 2x^4 - 2x - 2$. On déterminera p puis testera la divisibilité par des P_S avec S de cardinal 1, puis 2, 3, *etc...* jusqu'à $|S|/2$. Lorsqu'un facteur non trivial $Q = P_S$ est obtenu, ne pas oublier

d'éliminer les indices correspondants de S avant de recommencer avec P/Q. En déduire la factorisation en irréductibles dans $\mathbb{Q}[x]$ de ces polynômes.

11. Ecrire une procédure `FactQ:=proc(P)` renvoyant la décomposition en produit d'irréductibles dans $\mathbb{Q}[x]$. On automatisera les calculs de la question précédente, la décomposition modulo p étant obtenue via `Factors(P) mod p`. On éliminera d'emblée les cas triviaux où P est de degré inférieur ou égal à un, cas où la borne de Mignotte n'est pas définie.

Références

[G-G] **J. von zur GATHEN, J. GERHARD**, Modern Computer Algebra. Second edition. Cambridge, 2003.

[M] **M. MIGNOTTE**, Mathématiques pour le calcul formel. PUF, 1989.