Arithmétique des polynômes, factorisation dans $\mathbb{Z}[X]$

N'oubliez pas de sauvegarder vos sessions (format .xws) sur la plate-forme, ainsi que les programmes (format .cxx).

Le but de ce TP est de factoriser des polynômes dans $\mathbb{Z}[X]$, en supposant que nous savons factoriser tout polynôme de $\mathbb{F}_p[X]$, où p est un nombre premier.

Remarque : La factorisation dans $\mathbb{F}_p[X]$ pourrait se trouver grâce à l'algorithme de Berlekamp, mais nous n'allons pas l'implémenter pour ce TP. Nous utiliserons simplement la commande `factor` de Xcas.

Factorisation d'un polynôme quelconque

$\mathbb{Z}[X]$ étant un anneau factoriel, la factorisation d'un polynôme P de $\mathbb{Z}[X]$ en facteurs irréductibles est de la forme $P = \epsilon\, c_1^{\alpha_1} \cdots c_s^{\alpha_s} P_1^{\beta_1} \cdots P_r^{\beta_r}$, où $\epsilon = \pm 1$, $c_i \in \mathbb{N}$ est un nombre premier, $P_j \in \mathbb{Z}[X]$ est un polynôme de degré au moins 1 et irréductible, et α_i et β_j des entiers naturels non nuls.
D'autre part, le lemme de Gauss pour les polynômes stipule :
$Q \in \mathbb{Z}[X]$, non constant, est irréductible dans $\mathbb{Z}[X]$ si et seulement s'il est primitif et irréductible dans $\mathbb{Q}[X]$.

Ainsi, en notant $co(P)$ le contenu de P et $pp(P)$ sa partie primitive, nous avons : $co(P) = \epsilon\, c_1^{\alpha_1} \cdots c_s^{\alpha_s}$ et $pp(P) = P_1^{\beta_1} \cdots P_r^{\beta_r}$.

Nous supposerons pour la suite que nous savons factoriser les entiers relatifs (par exemple par la commande `ifactor` de Xcas), donc que nous savons factoriser $co(P)$, et nous ne nous intéresserons plus qu'à la factorisation de $pp(P)$.

Si nous savons que P_j est un facteur irréductible de $pp(P)$, il est assez facile de déterminer la valeur de l'exposant β_j. Un moyen simple est par exemple de calculer les restes des divisions euclidiennes de $pp(P)$ par P_j^2, P_j^3,...,P_j^n jusqu'à ce que le reste soit non nul. β_j est alors l'exposant le plus grand pour lequel le reste est nul.

On voit donc que nous sommes ramenés à la détermination de la **factorisation de la partie sans facteurs carrés du polynôme primitif associé à** P, c'est-à-dire $\tilde{P} = P_1 \cdots P_r$.

Si P est un polynôme, comment trouver sa partie sans facteurs carrés $\tilde{P}$? C'est simple, en utilisant le PGCD. En effet, on a la relation : $\tilde{P} = P/PGCD(P, P')$.
A noter qu'avec Xcas, le polynôme dérivé de P s'obtient par la commande `deriver`.

Exercice 1. *Factorisation d'un polynôme, connaissant celle de sa partie primitive sans facteurs carrés*

Sachant que la factorisation du polynôme primitif $Q = 2X^7 + X^6 + 2X^5 + X^4 - 2X^2 - 3X - 1$ est $Q = (X-1)(2X+1)(X^2+X+1)(X^3+X+1)$, en déduire la factorisation dans $\mathbb{Z}[X]$:

1) de $P_1 = 56X^{17} + 56X^{16} + 238X^{15} + 392X^{14} + 560X^{13} + 826X^{12} + 868X^{11} + 784X^{10} + 476X^9 + 28X^8 - 434X^7 - 868X^6 - 980X^5 - 854X^4 - 658X^3 - 364X^2 - 112X - 14$.
2) de $P_2 = 24X^{11} - 84X^{10} + 120X^9 - 108X^8 + 72X^7 - 36X^6 + 36X^5 - 72X^3 + 48X^2 + 12X - 12$.

Factorisation d'un polynôme primitif sans facteurs carrés

Nous allons maintenant nous intéresser au cas d'un polynôme primitif sans facteurs carrés, pouvant donc se factoriser en $P = P_1 \cdots P_r$.

Soit p un nombre premier, et φ_p le morphisme de réduction modulo p.
Nous ferons deux hypothèses pour toute la suite, à savoir $p \nmid lc(P)$, où $lc(P)$ est le coefficient dominant de P, et $p \nmid res(P, P')$, où res est le résultant.
On peut alors en déduire que la factorisation de $\varphi_p(P)$ en éléments irréductibles dans $\mathbb{F}_p[X]$ est sans facteurs carrés et sous la forme $\varphi_p(P) = \varphi_p(lc(P))f_1 \cdots f_n$, avec $n \geqslant r$, et les f_i sont distincts, unitaires, de degré au moins 1 et irréductibles dans $\mathbb{F}_p[X]$.
Cette décomposition peut être obtenue par exemple par la commande `factor` de Xcas, ou bien la commande `factors` qui permet de récupérer la liste des facteurs.
On a alors les relations suivantes :
pour tout $i \in \{1, ..., r\}$, il existe $S \subset \{1, ..., n\}$, tel que $\dfrac{lc(P)}{lc(P_i)} P_i \equiv lc(P) \prod_{j \in S} f_j \mod p$.
De plus, si $n = 1$, alors $r = 1$ et P est irréductible.

Exercice 2. *Essais empiriques, réduction modulo plusieurs nombres premiers*

1) Soit $P(X) = X^5 + 3X^4 + 2X^3 - 6X^2 + 5$. Factoriser $\varphi_p(P)$ pour $p = 2$ puis pour $p = 7$. Que peut-on en déduire ?

2) Soit $Q(X) = 6X^5 + 5X^4 + 4X^3 + 3X^2 + 2X + 1$. Factoriser $\varphi_p(Q)$ pour des petits nombres premiers. Quel(s) nombre(s) premier(s) nous permet(tent) d'en déduire la factorisation de Q dans $\mathbb{Z}[X]$?

Il s'agit maintenant d'avoir des méthodes générales et systématiques permettant de déduire la factorisation de P connaissant celle de $\varphi_p(P)$. L'idée générale est la suivante :
1) nous déterminons une borne M, telle que les coefficients de tout facteur de P soient inférieurs à M. Cela sera obtenu grâce à la borne de Mignotte.
2) choisissons $p > 2lc(P)M$ (version "grand nombre premier"), ou bien $m = p^n > 2lc(P)M$ (version "petit nombre premier"), avec p premier, et factorisons $\varphi_p(P)$ dans $\mathbb{F}_p[X]$. Les coefficients des polynômes modulo p seront représentés par des entiers compris entre $-p/2$ et $p/2$, ou $-m/2$ et $m/2$ (ce que fait Xcas par défaut).
3) nous testons les différentes combinaisons possibles des facteurs f_j obtenus modulo p ou m, que l'on "relève" dans $\mathbb{Z}[X]$, pour trouver ceux qui sont bien des facteurs de P.

Nous aurons ainsi besoin du résultat suivant :
Borne de Mignotte : Soit $P \in \mathbb{Z}[X]$ de degré n, et $Q \in \mathbb{Z}[X]$ tel que Q divise P. Alors :

$$\|Q\|_\infty \leqslant (n+1)^{1/2} 2^n \|P\|_\infty.$$

Nous noterons donc pour la suite $M = (n+1)^{1/2} 2^n \|P\|_\infty$, la borne de Mignotte de P.

Exercice 3. *Méthode modulaire, version "grand nombre premier"*

A. Etude détaillée d'un exemple

1) Soit $P = 6X^4 + 5X^3 + 15X^2 + 5X + 4$. Vérifiez que P est primitif et sans facteurs carrés (cf partie factorisation d'un polynôme quelconque). Calculez M la borne de Mignotte de P, ainsi que $\Delta = res(P, P')$.
Remarques : pour avoir une valeur approchée de M, utiliser `evalf`.
2) Soit $p = 6473$. Vérifiez que p est un nombre premier, que $p > 2lc(P)M$ et $p \nmid \Delta$. Vérifiez que la factorisation de $P \mod p$ s'écrit sous la forme $P \equiv 6f_1f_2f_3f_4 \mod p$, où les f_i sont unitaires, de degré 1.
Pensez à utiliser `factors` pour pouvoir récupérer les valeurs des f_i pour la suite.
3) Test des facteurs de degré 1 : nous voulons savoir si P possède des facteurs irréductibles de degré 1, nécessairement obtenus par les f_i. Pour tout $1 \leqslant i \leqslant 4$, on calcule $Q_i \equiv 6f_i \mod p$, le relèvement

"naturel" de $6f_i$ dans $\mathbb{Z}[X]$. On pourra utiliser la commande `f mod 0` de Xcas. On teste alors si le polynôme primitif $pp(Q_i)$ divise P. Si oui, on a trouvé un facteur irréductible de P.
4) Test des facteurs de degré 2 : nous voulons savoir si P possède des facteurs irréductibles de degré 2, nécessairement obtenus par un produit de deux polynômes f_i. Nous allons cette fois tester les polynômes $pp(R_{i,j})$ définis par $R_{i,j} \equiv 6f_if_j \mod p$. Conclure.
5) Reprendre la méthode avec $p = 6451$ et $p = 6547$. Quel est le cas le plus facile à traiter ?

B. Application de la méthode à d'autres polynômes

Pour trouver un nombre premier $p > 2lc(P)M$, on pourra utiliser la commande `nextprime(floor(.))`.

1) Déterminez la factorisation du polynôme $30X^5 + 39X^4 + 35X^3 + 25X^2 + 9X + 2$.
2) Déterminez la factorisation du polynôme $X^8 + X^4 + 1$.
Pour ce dernier polynôme, en particulier, on remarquera que si l'on a trouvé un facteur irréductible Q de P, grâce au produit $lc(P)f_{i_1} \cdots f_{i_s}$, on continue les tests avec les f_i restants, où $i \in \{1, ...n\}\backslash\{i_1, ..., i_s\}$.

Exercice 4. *Méthode modulaire, version "petit nombre premier" via le lemme de Hensel*

La méthode sera analogue à celle de l'exercice 3, mais cette fois-ci, nous factoriserons P dans $\mathbb{F}_p[X]$ avec p premier petit, et nous en déduirons grâce au lemme de Hensel une factorisation dans $\mathbb{Z}/p^l\mathbb{Z}[X]$, où $m = p^l$ est suffisamment grand.

Nous utiliserons donc le théorème suivant :
Théorème de Hensel : Soit p un nombre premier, soient $P, Q_1, R_1 \in \mathbb{Z}[X]$, de degrés respectifs n, r, s tels que $n = r + s$, $p \nmid lc(P)$, Q_1 unitaire, $P \equiv Q_1R_1 \mod p$, et Q_1 et R_1 premiers entre eux modulo p.
Alors, pour tout $l \geqslant 2$, il existe des polynômes $Q_l, R_l \in \mathbb{Z}[X]$, uniques modulo p^l, tels que
$P \equiv P_lQ_l \mod p^l$, $Q_l \equiv Q_{l-1} \mod p^{l-1}$ et $R_l \equiv R_{l-1} \mod p^{l-1}$.

A. Etude détaillée d'un exemple

1) Soit $P = X^4 + X^3 + 2X^2 + X + 1$. Vérifiez que P est primitif et sans facteurs carrés. Calculez M la borne de Mignotte de P, ainsi que $\Delta = res(P, P')$.
2) Soit $p = 11$. Vérifiez que $p \nmid \Delta$, et que la factorisation de P dans $\mathbb{F}_p[X]$ s'écrit sous la forme $P = f_1f_2$ mod 5 avec $f_1 = X^2 + 1$ et $f_2 = X^2 + X + 1$.
Vérifiez que $p^3 > 2M$. On prendra donc $l = 3$. On admet que l'algorithme du relèvement de Hensel, nous permet d'obtenir : $f_1 \equiv X^2 + 1 \mod 11^3$, $f_2 \equiv X^2 + X + 1 \mod 11^3$.
Vérifiez alors que $P_1 = X^2 + 1$ et $P_2 = X^2 + X + 1$ sont bien les facteurs de P dans $\mathbb{Z}[X]$.
4) Prenons maintenant $p = 5$. Vérifiez que c'est un nombre premier acceptable et que l'on devra prendre $l = 4$. La factorisation modulo p fait apparaître deux facteurs du premier degré, $f_1 = X + 2$ et $f_2 = X - 2$, et un facteur du second degré, $f_3 = X^2 + X + 1$.
a) Etude des facteurs du premier degré.
Nous allons tout d'abord relever la factorisation $f_1 \cdot (f_2f_3)$ modulo 5^4. On obtient $f_1 \equiv X + 182 \mod 5^4$ et $f_2f_3 \equiv X^3 - 181X^2 - 181X - 182 \mod 5^4$. Montrer que ces deux polynômes ne sont pas des facteurs de P.
Nous allons ensuite relever la factorisation $f_2 \cdot (f_1f_3)$ modulo 5^4. On obtient $f_2 \equiv X - 182 \mod 5^4$ et $f_1f_3 \equiv X^3 + 183X^2 + 183X + 182 \mod 5^4$. Montrer que ces deux polynômes ne sont pas des facteurs de P.
b) Etude des facteurs du second degré.
Nous allons relever la factorisation $(f_1f_2) \cdot f_3$ modulo 5^4. On obtient $f_1f_2 \equiv X^2 + 1 \mod 5^4$ et $f_3 \equiv X^2 + X + 1 \mod 5^4$. Montrer que ces deux polynômes sont les facteurs de P.

B. Algorithme de relèvement de Hensel

Connaissant une démonstration effective du théorème de Hensel cité ci-dessus, nous pouvons proposer un algorithme permettant de construire les polynômes Q_l, R_l (nous reprenons les notations du théorème). Voici comment sont construits ces polynômes :
a) tout d'abord, en utilisant l'algorithme d'Euclide étendu (ou aussi la fonction `abcuv` de Xcas), il faut déterminer deux polynômes U et V de $\mathbb{Z}[X]$ tels que : $UQ_1 + VR_1 \equiv 1 \mod p$ avec $\deg(U) < \deg(R_1)$ et $\deg(V) < \deg(Q_1)$.

b) ensuite, pour passer de Q_j, R_j à Q_{j+1}, R_{j+1} :

- on calcule $C_j = (P - Q_j R_j)/p^j$,
- on effectue la division euclidienne, dans $\mathbb{F}_p[X]$, de VC_j par Q_j : $VC_j \equiv Q_j H + S \mod p$ avec $\deg(S) < \deg(Q_j)$, on relève S dans $\mathbb{Z}[X]$ avec le même degré,
- on calcule $T \equiv UC_j + R_j H \mod p$, et on relève T dans $\mathbb{Z}[X]$ avec le même degré,
- on a alors : $Q_{j+1} = Q_j + p^j S$, et $R_{j+1} = R_j + p^j T$.

Implémentez cet algorithme dans Xcas.

C. Application de la méthode à d'autres polynômes

1) Etudiez la factorisation du polynôme $P = X^6 + 1$.
2) Etudiez la factorisation du polynôme $P = X^9 + 4X^8 + X^7 + X^6 + X^5 + 2X^4 + 4X^3 + 3X^2 + 2$.