Factorisation de polynômes (sur $\mathbb{Z}$)

B. Parisse
Institut Fourier
UMR 5582 du CNRS
Université de Grenoble I

1er octobre 2002

On présente ici quelques algorithmes utilisés pour factoriser un polynôme à coefficients entiers. Pour un polynôme en une variable, cele se fait en plusieurs étapes : on commence par se ramener à un polynôme P dont tous les facteurs sont de multiplicité un, ensuite on factorise P dans $\mathbb{Z}/p\mathbb{Z}$ (par la méthode de Berlekamp ou Cantor-Zassenhauss), puis on remonte à $\mathbb{Z}/p^k Z$ pour k suffisamment grand (en fonction de la borne de Landau sur les facteurs de P), et on recombine enfin les facteurs modulaires pour trouver les facteurs de P. Lorsque P à plusieurs variables, on utilise une méthode analogue à celle permettant de trouver le pgcd de polynômes à plusieurs variables.

Rappel
Le pgcd des coefficients d'un polynôme est appelé contenu de ce polynôme. Un polynôme est dit primitif si son contenu est égal à 1.

1 Les facteurs multiples

Étant donné un polynôme P à coefficients entiers, on cherche à écrire :

$$P = \Pi_{k=1}^n P_k^k$$

où les P_k n'ont pas de facteurs multiples et sont premiers entre eux deux à deux. Comme on est en caractéristique 0, cela revient à dire que $\text{pgcd}(P_k, P_k') = 1$ et $\text{pgcd}(P_k, P_j) = 1$. Bien entendu on va utiliser la dérivée de P dans l'algorithme de recherche des P_k :

$$P' = \sum_{k=1}^n k P_k' P_k^{k-1} \Pi_{j\neq k} P_j^j$$

Soit G le pgcd de P et de P'. On a :

$$G = \Pi_{k=1}^n P_k^{k-1},$$

en effet G divise P et P' :

$$W_1 = \frac{P}{G} = \Pi_{k=1}^n P_k, \quad Z_1 = \frac{P'}{G} = \sum_{k=1}^n k P_k' \Pi_{j\neq k} P_j$$

il s'agit de vérifier que W_1 et Z_1 sont premiers entre eux. Soit F un facteur irréductible du pgcd de W_1 et Z_1, alors F divise l'un des P_k, appelons P_l ce facteur. Comme F divise $\Pi_{j\neq k}P_j$ si $k \neq l$, on en déduit que F divise le dernier terme de la somme de Z_1, c'est-à-dire que F divise $lP_l'\Pi_{j\neq l}P_j$ donc F divise P_l' puisque les P_k sont premiers entre eux. Donc P_l et P_l' ont un facteur en commun, ce qui est contraire aux hypothèses.

On pose alors :

$$Y_1 = Z_1 - W_1' = \sum_{k>1}(k-1)P_k'\Pi_{j\neq k}P_j$$

On définit alors par récurrence des suites de polynômes W_n, Y_n et G_m par :
- $G_m = \text{pgcd}(W_m, Y_m)$
- $W_{m+1} = W_m/G_m$ et $Y_{m+1} = Y_m/G_m - W_m'$

On va montrer que $P_m = G_m$. Commençons au rang $n = 1$, on voit que P_1 divise Y_1 (puisqu'il est commun à tous les $\Pi_{j\neq k}P_j$ car $k > 1$) et divise W_1. Et c'est le seul facteur commun, car tout autre facteur irréductible serait un diviseur d'un P_l pour $l > 1$, donc diviserait $(l-1)P_l'\Pi_{j\neq l,j>1}P_j$, donc diviserait P_l'. Le raisonnement en un rang quelconque est identique, les polynômes sont donnés par :

$$G_m = P_m,\ W_m = \Pi_{k>=m}P_k,\ Y_m = \sum k > m(k-m)P_k'\Pi_{j\geq m,j\neq k}P_j$$

Lorsqu'on programme cet algorithme, le test d'arrêt est $G_m = 1$.

Square-free factorisation (Algorithme de Yun)

Argument : un polynôme primitif P à coefficients entiers (ou dans $\mathbb{Z}[i]$ ou dans un corps de caractéristique nulle).

Valeur renvoyée : une liste de polynômes P_m telle que $P = \Pi_{k=1}^n P_k^k$.

1. Initialiser la liste résultat à liste vide.
2. Initialiser W à P et Y à P'. Calculer le pgcd G de W et Y et simplifier W et Y par leur pgcd puis poser $Y = Y - W'$.
3. Boucle infinie.
4. Calculer le pgcd G de W et Y. Si $G = 1$, on renvoie la liste résultat sinon ajouter G à la liste résultat.
5. Simplifier W et Y par G, puis poser $Y = Y - W'$ et passer à l'itération suivante.

Remarque : lorsqu'on veut factoriser un polynôme à coefficients modulaires, il faut aussi se ramener à un polynôme sans facteurs multiples mais on ne peut pas utiliser cet algorithme tel quel car la caractéristique du corps n'est pas nulle.

Exemple : factorisation sans facteurs multiples de $P(X) = (X^3-1)(X+2)^2(X^2+3)^3$. En mode interactif avec un logiciel de calcul formel, effectuons l'étape d'initialisation :

```
W:=normal((x^3-1)*(x+2)^2*(x^2+3)^3);
Y:=diff(W,x);
```

```
G:=gcd(W,Y);
        x^5+2*x^4+6*x^3+12*x^2+9*x+18
W:=normal(W/G);
        x^6+2*x^5+3*x^4+5*x^3+-2*x^2+-3*x-6
Y:=normal(Y/G);
Y:=normal(Y-diff(W,x));
        5*x^5+8*x^4+3*x^3+-5*x^2+-8*x-3
```

On vérifie bien que $W = (x+2) * (x^3 - 1) * (x^2 + 3)$ est le produit des facteurs P_i. On entame maintenant la boucle :

```
G:=gcd(W,Y);
        x^3-1   -> P1
Y:=normal(Y/G);
W:=normal(W/G);
Y:=normal(Y-diff(W,x));
        2*x^2+4*x
G:=gcd(W,Y);
        x+2     -> P2
Y:=normal(Y/G);
W:=normal(W/G);
Y:=normal(Y-diff(W,x));
        0
G:=gcd(W,Y);
        x^2+3   ->  P3
```

puis $W = 1$ et $Y = 0$ et le prochain G vaut 1, on a bien trouvé tous les facteurs P_i.

2 Factorisation en une variable

On suppose maintenant qu'on veut factoriser un polynôme P sans facteur multiple (et primitif). En général on commence par simplifier P par ses facteurs linéaires (détectés avec l'algorithme présenté dans le premier article de cette série). On commence par chercher un nombre premier p tel que P dans $\mathbb{Z}/p\mathbb{Z}$ conserve le même degré et reste sans facteur multiple (donc pgcd(P, P')=1 dans $\mathbb{Z}/p\mathbb{Z}$), ce qui est toujours possible (il suffit de prendre p plus grand que le plus grand entier apparaissant dans l'algorithme du sous-résultant pour calculer le pgcd de P et P' dans $\mathbb{Z}$).

Convention

Tous les polynômes ayant leurs coefficients dans un corps fini sont supposés avoir comme coefficient dominant 1 lorsque le choix existe (par exemple les facteurs d'un polynôme modulo p).

2.1 Factorisation dans $\mathbb{Z}/p\mathbb{Z}[X]$

On suppose qu'on a un polynôme P à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ sans facteur multiple. Il s'agit de factoriser P dans $\mathbb{Z}/p\mathbb{Z}[X]$. Il existe essentiellement deux stratégies, l'une commence par factoriser par groupes de facteurs de même degré puis casse les facteurs et l'autre plus directe à base d'algèbre linéaire modulaire (méthode de Berlekamp). Dans les deux cas, on utilise le fait que si F est un polynôme, alors les polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ modulo F forment un anneau A qui est aussi un espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$ de dimension le degré de F (si F est irréductible, alors A est un corps). On s'intéresse alors aux propriétés de l'application $\varphi : x \in A \mapsto x^p$. On observe d'abord que cette application est une application *linéaire*. Cela découle du petit théorème de Fermat pour $\varphi(\lambda x) = \lambda\varphi(x)$ et de la formule de Newton et de la primalité de p pour $\varphi(x+y) = \varphi(x) + \varphi(y)$.

Calcul de φ

Pour mettre en oeuvre ces algorithmes, on commence par déterminer la matrice de l'endomorphisme $\varphi : x \mapsto x^p$ dans $\mathbb{Z}/p\mathbb{Z}[X] \pmod{P(X)}$ muni de sa base canonique $\{1, X, ..., X^{\deg(P)-1}\}$.

2.1.1 Distinct degree factorization

Cette méthode consiste à détecter les groupes de facteurs ayant un degré donné (distinct degree factorization). Si nécessaire, on utilise ensuite un autre algorithme pour casser ces groupes. On utilise ici les propriétés des itérées de l'application linéaire φ sur des espaces vectoriels de corps de base $\mathbb{Z}/p\mathbb{Z}$. On va déterminer le produit P_k de tous les facteurs de P de degré k en calculant le pgcd de P et de $X^{(p^k)} - X$ dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Pour $k = 1$, $X^p - X$ est le produit des $X - k$ pour tout $k \in \mathbb{Z}/p\mathbb{Z}$ par le petit théorème de Fermat ($k^p = k \pmod p$), donc le pgcd de P et de $X^{(p^1)} - X$ dans $\mathbb{Z}/p\mathbb{Z}[X]$ est le produit des facteurs de P de degré 1.

Pour $k > 1$, le raisonnement se généralise de la manière suivante : on considère un facteur irréductible $F(X)$ de P de degré k et le corps $K = (\mathbb{Z}/p\mathbb{Z})[Y] \pmod{F(Y)}$. Le corps K est un corps fini, c'est aussi un espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$ de dimension k, donc K possède p^k éléments et K^* est un groupe multiplicatif à p^k-1 éléments, donc tout élément de K^* vérifie l'équation $x^{p^k-1} = 1$ donc tout élément de K vérifie $x^{(p^k)} = x$. En particulier pour $x = Y \pmod{F(Y)}$ on trouve que $Y^{(p^k)} = Y \pmod{F(Y)}$ donc $F(X)$ divise $X^{(p^k)} - X$ dans $\mathbb{Z}/p\mathbb{Z}$.

Réciproquement, si on se donne un facteur irréductible F qui divise $X^{p^k} - X$, soit K le corps correspondant à F, alors le noyau de l'application linéaire

$$x \in K \mapsto x^{p^k} - x \in K$$

est K tout entier, car $Y = Y^{p^k} \pmod F$ entraine $(Y^2)^{(p^k)} = Y^{2p^k} = (Y^{p^k})^2 = Y^2 \pmod F$ et de même pour les autres puissances de Y qui, avec $Y^0 = 1$ également dans le noyau, forment une base de l'espace vectoriel K sur $\mathbb{Z}/p\mathbb{Z}$. Donc le nombre d'éléments de K est inférieur ou égal au degré du polynôme $X^{p^k} - X$ (puisque $X^{(p^k)} - X$ est divisible par $X - x$ pour tout $x \in K$), donc le degré de F est inférieur ou égal à k.

Donc P_k est égal au pgcd de $P/\Pi_{j<k}P_j$ avec $X^{p^k} - X$.

Algorithme distinct degree factorization
Argument : un polynôme P à coefficients entiers sans facteur multiple et primitif.
Valeur renvoyée : la liste L des produits des facteurs irréductibles et du degré correspondant de P (ordonné par ordre croissant de degré).
On commence par initialiser L à vide et un polynôme auxiliaire Q à X (il contiendra les valeurs de $X^{p^k} - X \pmod P$), on fait une boucle indéfinie sur k commençant à 1 et incrémenté de 1 à chaque itération

- Si k est strictement plus grand que le degré de P divisé par 2, on rajoute le couple (P,degre(P)) à L et on renvoie L
- On remplace Q par $Q^p \pmod P$ en utilisant le calcul de φ modulo P
- On calcule le pgcd G de $Q - X$ et de P.
- Si G vaut 1, on passe à l'itération suivante
- On rajoute le couple (G,k) à la liste L et on remplace P par le quotient de P par G.

Exemple : factorisation en degré distincts de $(X^3 + X + 1)(X^4 - X + 1)$ dans $\mathbb{Z}/5\mathbb{Z}$. On regarde d'abord si P reste sans facteur multiple après réduction modulo 5.

```
P:=normal((x^3+x+1)*(x^4-x+1) mod 5);
gcd(P,diff(P,x));
    1 mod 5  -> ok P est sans facteur multiple
P1:=gcd(P,(x^5-x)mod 5);
    (1 mod 5)*x -2 mod 5  -> P1
P:=normal(P/P1);
P2:=gcd(P,(x^(5^2)-x)mod 5);
    1 mod 5  -> pas de facteur de degre 2
P3:=gcd(P,(x^(5^3)-x)mod 5);
    (x^6+2*x^5+x^2+x+2) mod 5
```

Donc P admet 3 facteurs dans $\mathbb{Z}/5\mathbb{Z}$: un de degré 1 $(x - 2)$ et deux de degré 3 (dont le produit est $x^6 + 2x5 + x^2 + x + 2$).

Le même calcul dans $\mathbb{Z}/7\mathbb{Z}$ donne

```
P:=normal((x^3+x+1)*(x^4-x+1) mod 7);
gcd(P,diff(P,x));
    1 mod 7  -> ok P est sans facteur multiple
P1:=gcd(P,(x^7-x)mod 7);
    1 mod 7
P2:=gcd(P,(x^(7^2)-x)mod 7);
    1 mod 7
P3:=gcd(P,(x^(7^3)-x)mod 7);
    (x^3+x+1) mod 7
```

donc P possède un facteur de degré 3 modulo 7, donc le facteur restant de degré 4 est forcément irréductible.

On remarque sur cet exemple que 7 est plus intéressant que 5, car la factorisation modulo 7 donne moins de facteurs (à recombiner pour trouver la factorisation dans $\mathbb{Z}$) et la factorisation est complète modulo 7 alors que modulo 5 il faut casser le facteur de degré 6 en deux facteurs de degré 3. La plupart des algorithmes de factorisation effectuent la factorisation en degré distinct modulo plusieurs entiers (ce qui peut de plus être parallélisé) et choisissent le meilleur.

2.1.2 La méthode de Cantor-Zassenhaus

Cet algorithme sert à casser des groupes de facteurs de même degré, c'est une méthode probabiliste. On suppose donc qu'on a un produit P d'au moins deux facteurs irréductibles de degré d à casser. Soit D l'un des polynôme irréductible de degré d à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, et soit $K = \mathbb{Z}/p\mathbb{Z}[Y] \pmod{D(Y)}$, on a :

$$X^{p^d} - X = \Pi_{\alpha \in K}(X - \alpha)$$

puisque le corps K possède p^d éléments tous racines de l'équation $X^{p^d} = X$.

On considère un polynôme T non constant, et le polynôme $T^{p^d} - T$. En remplaçant X par T ci-dessus, on en déduit :

$$T^{p^d} - T = \Pi_{\alpha \in K}(T - \alpha)$$

Donc pour tout élément $\beta \in K = \mathbb{Z}/p\mathbb{Z}[Y] \pmod{D(Y)}$, on a

$$(T^{p^d} - T)(\beta) = \Pi_{\alpha \in K}(T(\beta) - \alpha) = 0$$

Donc $T^{p^d} - T$ est divisible par $X^{p^d} - X$ (puisque toutes les racines du second sont racines du premier), donc est divisible par tout polynôme irréductible de degré inférieur ou égal à d à coefficients dans $Z/p\mathbb{Z}$. Comme

$$T^{p^d} - T = T(T^{\frac{p^d-1}{2}} - 1)(T^{\frac{p^d+1}{2}} - 1) \quad (1)$$

et que ces trois facteurs sont premiers entre eux, on en déduit que tout polynôme irréductible de degré inférieur ou égal à d à coefficients dans $Z/p\mathbb{Z}$ divise l'un des trois facteurs ci-dessus. Pour casser P, l'idée consiste alors à calculer le pgcd de P et $T^{\frac{p^d-1}{2}} - 1$ pour un polynôme pris au hasard. On sait que P divise le produit des 3 termes de (1), et on espère que les facteurs irréductibles de P ne diviseront pas tous le même terme.

On va montrer que si T est un polynôme de degré $\leq 2d-1$ choisi au hasard, la probabilité que deux facteurs irréductibles de P ne divisent pas $T^{p^d} - T$ est proche de 0.5. Soient donc A et B deux facteurs irréductibles de P de degré d. D'après l'identité de Bézout, tout polynôme T de degré $\leq 2d - 1$ s'écrit de manière unique sous la forme :

$$T = AU + BV \quad (2)$$

avec degre($U \leq d - 1$) et degre($V \leq d - 1$) et réciproquement une combinaison linéaire de cette forme est un polynôme de degré $\leq 2d - 1$. Choisir T au hasard revient donc à choisir un couple (U, V) de polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ au hasard et de manière indépendante. D'autre part, A et B étant de degré d, on sait que dans $K = \mathbb{Z}/p\mathbb{Z}[Y] \pmod{D(Y)}$ ces polynômes admettent d racines.

Soit donc α [respectivement β] une racine de A [resp. B] dans K. Alors A divise $T^{\frac{p^d-1}{2}}-1$ si et seulement si $T(\alpha)^{\frac{p^d-1}{2}}=1$ (et de même pour B et β) car $T^{\frac{p^d-1}{2}}-1$ a ses coefficients dans $\mathbb{Z}/p\mathbb{Z}$ (et non dans K). En appliquant (2), A divise $T^{\frac{p^d-1}{2}}-1$ si et seulement si :

$$B(\alpha)^{\frac{p^d-1}{2}}V(\alpha)^{\frac{p^d-1}{2}}=1$$

Le premier terme de cette égalité est une constante égale à 1 ou -1, le second a une probabilité proche de 0.5 (égale à $\frac{p^d-1}{2p^d}$) de valoir 1 ou -1 car, comme A est irréductible, $V(\alpha)$ décrit K lorsque V décrit les polynômes de degré $\leq d-1$. De même, B a une probabilité proche de 0.5 de diviser $T^{\frac{p^d-1}{2}}-1$, et ces 2 probabilités sont indépendantes puisque U et V le sont, donc la probabilité que soit A soit B divise divise $T^{\frac{p^d-1}{2}}-1$ est proche de 0.5.

Algorithme de Cantor-Zassenhaus
Argument : Un polynôme P à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ de degré k dont tous les facteurs irréductibles sont de degré d.
Valeur renvoyée : la liste des facteurs irréductibles de P.

- Si $k=d$ renvoyer une liste contenant P.
- Déterminer un polynôme T aléatoire de degré inférieur ou égal à $2d-1$ et de coefficient dominant 1. Calculer le pgcd D de P et de $T^{(p^d-1)/2}-1$. Si le degré de T est égal à 0 ou à k recommencer cette étape.
- Appeler récursivement cet algorithme avec T et P/T et renvoyer la liste réunion des deux listes renvoyées.

Exemple : cassons le polynôme de degré 6 obtenu dans l'exemple précédent (modulo 5). Donc $P:=(x^6+2*x^5+x^2+x+2) \pmod 5$ et $d=3$. On choisit au hasard un polynôme de degré 5, par exemple $T=x^4-x^3+x+1$, puis on calcule T^62 modulo P ce qui donne $(x^5+x^3+x^2+1) \pmod 5$ puis le pgcd de T^62-1 et de P qui vaut $x^3+x+1 \pmod 5$, on a donc cassé P en deux. En prenant $T:=x^4-x^3+x+2$, on trouve $T^62=1 \pmod P$, donc ce T n'aurait pas permi de casser P.

2.1.3 La méthode de Berlekamp

Cette méthode permet de factoriser un polynôme sans facteurs multiples, elle peut aussi servir à casser des groupes de facteurs de même degré. Ici on travaille dans l'anneau des polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ modulo le polynôme P et on s'intéresse au noyau de $\varphi-Id$ (où $\varphi: x\mapsto x^p$). On suppose que $P=\Pi_{j=1}^n F_j$ où les F_j sont irréductibles et premiers entre eux. On va montrer que le noyau de $\varphi-Id$ est composé des polynômes Q tels que $Q \pmod{F_j}$ est dans $\mathbb{Z}/p\mathbb{Z}$ pour tout j.

Si $Q \pmod{F_j}=s_j\in\mathbb{Z}/p\mathbb{Z}$, alors $Q^p \pmod{F_j}=s_j^p=s_j$, donc par le théorème des restes chinois, $Q=Q^p \pmod P$.

Réciproquement, si $Q^p - Q = 0 \pmod P$, en utilisant la factorisation :

$$X^p - X = \Pi_{j \in \mathbb{Z}/p\mathbb{Z}}(X - j)$$

on en tire P divise $Q^p - Q = \Pi_{j\in\mathbb{Z}/p\mathbb{Z}}(Q(X)-j)$, donc F_j divise l'un des facteurs et $Q(X) \pmod{F_j} \in \mathbb{Z}/p\mathbb{Z}$. Le noyau de $\varphi - Id$ est donc un espace vectoriel de dimension n, le nombre de facteurs irréductibles de P et possède donc p^n éléments (en effet pour tout n uplet de s_j, on peut construire un polynôme Q du noyau par le théorème des restes chinois en posant $Q \pmod{F_j} = s_j$).

L'intérêt du noyau de $\varphi - Id$ est qu'on peut le calculer sans connaitre les F_j. Une fois ce calcul fait, voyons comment on peut remonter aux F_j. On connait déjà la dimension du noyau donc le nombre de facteurs irréductibles. De plus, on remarque que le polynome constant est un élément du noyau qu'on appelera T_1, on note alors $T_2, ..., T_n$ les autres polynômes du noyau. Ensuite, on calcule le pgcd de P avec $T_2 - jT_1$ pour $j \in \mathbb{Z}/p\mathbb{Z}$. On sait que $T_2 = s_{2j} \pmod{F_j}$, donc ce pgcd est égal au produit des facteurs F_j tels que $s_{2j} = jT_1$. L'un au moins des pgcd calculés est non trivial car sinon $T_2 = T_1 \pmod{F_j}$ pour tout j donc $T_2 = T_1$. Si on a de la chance tous les s_{2j} seront distincts et les pgcd non triviaux de P avec $T_2 - jT_1$ donneront les F_k. Sinon il faudra continuer avec $T_3 - jT_1$ etc.

Exemple : revenons sur la factorisation de $P := (x^6 + 2 * x^5 + x^2 + x + 2) \pmod 5$. Commençons par calculer la matrice de φ dans la base $\{1, x, x^2, ..., x^5\}$. On a évidemment $\varphi(1) = 1$ et $\varphi(x) = x^5$, puis $\varphi(x^2) = x^10 = x^5 + x^4 - 2x^3 + x \pmod P$, puis en multipliant par x^5 et en divisant par P, $\varphi(x^3) = -x^4 + 2x^3$, de la même manière on obtient $\varphi(x^4) = -x^5 + 2x^4 + x^3 - x^2 - 2$ et $\varphi(x^5) = x^3 + x^2 - x$. La matrice de φ est donc :

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & -2 & 2 & 1 & 1 \\ 0 & 0 & 1 & -1 & 2 & 0 \\ 0 & 1 & 1 & 0 & -1 & 0 \end{pmatrix}$$

On calcule ensuite le noyau de $\varphi - Id$ modulo 5, on obtient une base du noyau en prenant par exemple les vecteurs $(-1, 0, 0, 0, 0, 0)$ et $(0, 0, -1, -1, 0, -1)$. Donc ce polynôme possède 2 facteurs dans $\mathbb{Z}/5\mathbb{Z}$. Pour déterminer les facteurs, on calcule le pgcd de P avec le polynôme $T_2 - s$ où $T_2 = -x^5 - x^3 - x^2$ correspond au 2ème vecteur de la base du noyau. On obtient pour $s = 0$ un pcgd non trivial $(x^3 + x + 1)$, ce qui permet de calculer les 2 facteurs. Si on avait essayé d'autres valeurs de s, pour $s = 1$ on obtient comme pgcd 1, pour $s = 2$ on trouve le 2ème facteur $x^3 + 2x^2 - x + 2$.

2.2 Remontée (Hensel)

Il s'agit de passer d'une factorisation de P dans $\mathbb{Z}/p\mathbb{Z}[X]$ à une factorisation de P dans $\mathbb{Z}/p^k Z[X]$, la méthode est analogue à celle de l'algorithme EZGCD de calcul de pgcd de polynômes.

On suppose donc que

$$P = \Pi_{j=1}^n P_j \pmod p$$

où les P_j sont premiers entre eux deux à deux dans $\mathbb{Z}/p\mathbb{Z}$. Il s'agit de trouver des polynômes $P_{j,k} = P_j \pmod p$ tels que

$$P = \Pi_{j=1}^n P_{j,k} \pmod{p^k}$$

Commençons par le cas $k = 2$. On pose

$$P_{j,2} = P_j + pQ_j = P_j \pmod p$$

On a alors :

$$\begin{aligned} P &= \Pi_{j=1}^n P_{j,2} \pmod{p^2} = \Pi_{j=1}^n (P_j + pQ_j) \pmod{p^2} \\ &= \Pi_{j=1}^n P_j + p \sum_{j=1}^n Q_j \Pi_{k \neq j} P_k \pmod{p^2} \end{aligned}$$

Donc :

$$\sum_{j=1}^n Q_j \Pi_{k\neq j} P_k = \frac{P - \Pi_{j=1}^n P_j}{p} \pmod p$$

On est ramené à résoudre une identité de Bézout généralisée. On montrera dans l'appendice le :

Théorème 1 *(Identité de Bézout généralisée) Soit P_1, ..., P_n ($n \geq 2$) des polynômes premiers entre eux deux à deux modulo p. Alors pour tout polynôme Q, il existe des polynômes Q_1, ..., Q_n tels que :*

$$\sum_{j=1}^n Q_j \Pi_{k\neq j} P_k = Q \pmod p$$

On a donc réussi à lifter l'égalité $P = \Pi P_j \pmod p$ à $P = \Pi P_{j,2} \pmod{p^2}$. Le passage de $P = \Pi P_{j,l} \pmod{p^l}$ à $P = \Pi P_{j,l+1} \pmod{p^{l+1}}$ est identique, on a :

$$P_{j,l+1} = P_{j,l} + p^l Q_j$$

où les Q_j sont les solutions de l'identité de Bézout généralisée avec :

$$Q = \frac{P - \Pi_{j=1}^n P_{j,l}}{p^l}$$

Lorsqu'on programme cet algorithme, on calcule une fois pour toutes les solutions de l'identité de Bézout pour $Q = 1$, et on multiplie par Q.

Algorithme de remontée de Hensel linéaire

Arguments : Un polynôme P à coefficients entiers, la liste $L = \{P_j\}$ de ses facteurs dans $\mathbb{Z}/p\mathbb{Z}[X]$

Valeur renvoyée : la liste des facteurs de P dans $\mathbb{Z}/p^l\mathbb{Z}[X]$

On calcule la borne de Landau sur les facteurs de P, on multiple par le coefficient dominant de P et on calcule l tel que p^l est strictement plus grand que deux fois cette quantité. On calcule aussi les polynômes Q_j de l'identité de Bézout généralisée pour $Q = 1$

Puis on fait une boucle pour k variant de 2 à l :

- On détermine $P - \Pi_j P_j \pmod{p^k}$, on divise par p^{k-1} et on place le résultat dans Q
- On multiplie les polynômes Q_j de l'identité de Bézout généralisée (correspondants au polynôme 1) par Q et on détermine le reste de la division euclidienne de QQ_j par P_j, on multiplie par p^{k-1} et on ajoute le résultat à P_j.

Il existe une version quadratique de cette méthode. On passe alors de $P = \Pi P_{j,l} \pmod{p^l}$ à $P = \Pi P_{j,2l} \pmod{p^{2l}}$. Pour cela, il faut trouver les polynômes Q_j solutions de l'équation :

$$\sum_{j=1}^{n} Q_j \Pi_{k \neq j} P_{k,l} = Q \pmod{p^l}$$

Pour $l = 1$, c'est l'identité de Bézout généralisée, mais ce n'est plus le cas pour $l > 1$. En fait, on résout cette égalité en liftant l'identité de Bézout quadratiquement, plus précisément pour trouver les S_j solutions de

$$\sum_{j=1}^{n} S_j \Pi_{k \neq j} P_{k,2l} = Q \pmod{p^{2l}}$$

on pose $S_j = Q_j + p^l R_j$, il s'agit donc de trouver les R_j solutions de

$$\sum_{j=1}^{n} (Q_j + p^l R_j) \Pi_{k \neq j} P_{k,2l} = Q \pmod{p^{2l}}$$

soit :

$$\sum_{j=1}^{n} R_j \Pi_{k \neq j} P_{k,l} = \frac{Q - \sum_{j=1}^{n} Q_j \Pi_{k \neq j} P_{k,l}}{p^l} \pmod{p^l}$$

on en déduit les R_j.

Algorithme de remontée de Hensel quadratique

Arguments et valeur renvoyée identiques à l'algorithme de remontée de Hensel linéaire ci-dessus.

On commence comme dans le cas linéaire par calculer les coefficients de l'identité de Bézout généralisée pour $Q = 1$ et la valeur de l telle que p^{2^l} soit supérieur à deux fois la borne de Landau des facteurs de P fois le coefficient dominant de P.

On fait une boucle sur k variant de 1 à l :

- On calcule $P - \Pi_j P_j \pmod{p^{2^k}}$, on divise par $p^{2^{k-1}}$ et on place le résultat dans Q

- On multiplie par Q les polynômes Q_j de l'identité de Bézout généralisée (avec comme second membre le polynôme 1), on calcule le reste euclidien du résultat par P_j (modulo $p^{2^{k-1}}$), on multiplie par $p^{2^{k-1}}$ et on ajoute à P_j (avec les notations précédentes, on passe ainsi des $P_{j,2^{k-1}}$ aux $P_{j,2^k}$)
- Si $k = l$ on renvoie la liste des P_j
- On calcule $1 - \sum_j Q_j \Pi_{k \neq j} P_k \pmod{p^{2^k}}$, on divise par $p^{2^{k-1}}$ et on place le résultat dans Q
- On multiplie par Q les polynômes Q_j de l'identité de Bézout, généralisée et on calcule le reste euclidien du résultat par P_j (modulo $p^{2^{k-1}}$), on multiplie par $p^{2^{k-1}}$ et on ajoute à Q_j (ce qui ajuste les polynômes Q_j qui vérifient maintenant l'identité de Bézout modulo p^{2^k})

Remarque

Pendant l'étape de remontée de Hensel, une optimisation classique consiste à tester la divisibilité dans $\mathbb{Z}$ du polynôme P par le facteur lifté P_j ([1]) lorsqu'il n'a pas subi de modification pendant 2 étapes successives (autrement dit lorsque $P_j \pmod{p^l} = P_j \pmod{p^{l+1}}$ (ou $\pmod{p^{2l}}$ pour le lift quadratique). Si la division est exacte, on obtient un facteur irréductible de P dans $\mathbb{Z}$. On recalcule alors la borne de Landau de P/P_j pour diminuer le nombre d'itérations à effectuer dans cette étape.

Exemple : Reprenons le polynôme $P(X) = (X^3 + X + 1)(X^4 - X + 1)$ et supposons qu'on ait choisi de le factoriser modulo 5 puis de remonter. On a 3 facteurs $a = x - 2$, $b = x^3 + x + 1$ et $c = x^3 + 2x^2 - x + 2$. Si on développe P, on trouve 6 coefficients non nuls de valeur absolue 1, on peut calculer la borne de Landau-Mignotte correspondante sur les coefficients d'un facteur entier : $2^5(\sqrt(6) + 1)$ soit un peu plus de 110, il suffit donc d'effectuer 3 étapes de remontée linéaire ($5^4 = 625 > 111/2$). On commence par trouver 3 polynômes A, B, C tels que

$$A(x^3+x+1)(x^3+2x^2-x+2)+B(x-2)(x^3+2x^2-x+2)+C(x-2)(x^3+x+1) = 1 \pmod 5$$

On commence par résoudre $D(x^3 + 2x^2 - x + 2) + C(x - 2)(x^3 + x + 1) = 1 \pmod 5$, on trouve $C = 2x^2 - 2$ et $D = -2x^3 - 2x^2 + 2x + 1$. Puis on calcule A et B en résolvant $E(x^3+x+1)+F(x-2) = 1$ qui donne $E = 1$ et $F = -x^2-2x$ qu'on multiplie par D, donc $A = D$ et $B = 2x^5 + x^4 + 2x^3 - 2x$. Ce qui donne l'identité de Bézout généralisée.

Passons aux calculs de remontée. On a $abc = x^7 - 4x^5 + 5x^4 + -9x^3 - x^2 - 4$ et $P = x^7 + x^5 + x^3 - x^2 + 1$, donc $Q = (P - abc)/5 = x^5 - x^4 + 2x^3 + 1$. On pose alors

$$a_1 = a+5(QA \pmod a) \pmod 2)5, b_1 = b+5(QB \pmod b) \pmod 2)5, c_1 = c+5(QC \pmod c) \quad (\mathrm{mo}$$

donc :

$$a_1 = a + 5(-2), \quad b_1 = b + 5 \times 0, \quad c_1 = c + 5 \times (2x^2 - x)$$

[1] Plus exactement, on multiplie P_j par le coefficient dominant de P modulo p^l

En principe, on continue encore 2 itérations de la même manière. La 2ème itération donne :

$$Q = (P - a_1 b_1 c_1)/25 = 6x^5 - 3x^4 + 7x^3 + 3x^2 - 2x + 1$$

$a_2 = a_1 + 25(QA \pmod a) \pmod 2)5, b_2 = b_1 + 25(QB \pmod b) \pmod 2)5, c_2 = c_1 + 25(QC \pmod c))$

donc :

$$a_2 = a_1 + 25(-1) = x - 37, \quad b_2 = b_1 = b, \quad c_2 = c_1 + 25(x^2 + 1) = x^3 + 37x^2 - 6 * x + 27$$

On peut aussi observer que $b_1 = b$, ceci laisse à penser que b est un facteur de P dans $\mathbb{Z}$ ce qu'on vérifie en effectuant la division euclidienne de P par $b = x^3 + x + 1$. Comme elle tombe juste, on est ramené à factoriser $x^4 - x + 1$ et donc à remonter la factorisation de ac. La borne de Landau diminue à $8(\sqrt{3}+1)$ puisque le degré est 4 et la norme euclidienne du polynôme est $\sqrt{3}$. Il suffit alors de remonter dans $\mathbb{Z}/125\mathbb{Z}$ au lieu de $\mathbb{Z}/625\mathbb{Z}$ (on gagne ainsi une itération).

2.3 Combinaison de facteurs

Lorsqu'on a les facteurs de P dans $\mathbb{Z}/p^k\mathbb{Z}$ avec p^k plus grand que le produit du coefficient dominant de P multiplié par la borne de Landau-Mignotte sur les coefficients de P, on commence par tester la divisibilité dans $\mathbb{Z}$ de P par chaque facteur trouvé multiplié par le coefficient dominant de P. Si la division est exacte, on a un facteur irréductible, mais si elle n'est pas exacte il peut se produire qu'un facteur irréductible de P dans $\mathbb{Z}$ soit un produit de deux, voir plusieurs, facteurs modulaires. Il faut donc tester la divisibilité de P dans $\mathbb{Z}$ par toutes les combinaisons possibles de produits de facteurs modulaires (toujours multiplié par le coefficient dominant de P). Cette étape peut être exponentiellement longue si le nombre de facteurs modulaires est grand et si par exemple P est irréductible, bien que les cas soient très rares.

Algorithme de recombinaison

Arguments : un polynôme à coefficients entiers, primitif et sans facteur multiple P de coefficient dominant p_n, la liste L des facteurs de P dans $\mathbb{Z}/p^l Z[X]$ pour l assez grand et p^l

Valeur de retour : la liste F des facteurs de P dans $\mathbb{Z}$.

Initialiser F à vide, initialiser le nombre de facteurs à combine c à 1, entamer une boucle infinie :

- Si c est strictement supérieur au cardinal de L divisé par 2, ajouter le quotient de P par le produit des facteurs de F à F et retourner F
- Initialiser un vecteur $v = (v_1, ..., v_c)$ à c composantes à la valeur $(1, ..., c)$
- Boucle indéfinie intérieure :
  1. Faire le produit des facteurs de F d'indice v, multiplier par p_n dans $\mathbb{Z}/p^l Z$, écrire le facteur en représentation symétrique, le rendre primitif et tester si c'est un facteur de P dans $\mathbb{Z}$.
  2. Si on a trouvé un facteur, le rajouter à la liste F et supprimer les indices de v de la liste L, terminer cette boucle intérieure.

3. Sinon, incrémenter v de la manière suivante :
   On fait une boucle sur un index m initialisé à la taille de v, diminuant de 1 à chaque itération : on ajoute 1 à l'élement de v d'indice m, si l'élément obtenu est inférieur ou égal au cardinal de $L+m-n$, on arrête cette boucle, sinon on passe à l'itération suivante. Si $m=0$ à la fin de la boucle, v ne peut pas être incrémenté.
4. Si v ne peut être incrémenté, on incrémente c et on termine la boucle intérieure.
5. Sinon on fait une boucle à nouveau sur m en partant de la valeur actuelle incrémentée de 1, et tant que $m \leq n$ on pose $v_m = v_{m-1}+1$. Puis on passe à l'itération suivante de la boucle intérieure.

Il existe différentes méthodes qui améliorent la complexité de cette étape :
- La recherche des degré possibles de facteurs fondée sur la factorisation en degrés distincts pour différents nombres premiers permet d'éviter des tests de division si une combinaison de facteurs est d'un degré exclu par la factorisation pour d'autres nombres premiers.
- Le test de divisibilité du coefficient dominant ou du coefficient constant permet aussi d'éviter des divisions complètes de polynômes.

Mais ces astuces n'évitent pas l'énumération de toutes les combinaisons possibles de facteurs et donc la complexité exponentielle. Lorsque les combinaisons d'un petit nombre de facteurs (par exemple 3) échouent, les systèmes récents utilisent l'algorithme knapsack de Van Hoeij basé sur l'algorithme LLL (recherche de base d'un réseau ayant des vecteurs de petite norme) qui permet d'eliminer complètement cette complexité exponentielle.

Exemple : Toujours le même exemple, il nous restait deux facteurs dans $\mathbb{Z}/125\mathbb{Z}$, le facteur x^3+x+1 ayant été détecté comme un facteur de $P = x^7+x^5+x^3-x^2+1$ dans $\mathbb{Z}$. On teste chacun des facteurs $a_2 = x-37$ et $c_2 = x^3+37x^2-6*x+27$ séparément, sans succès. On les multiplie alors modulo 125, ce qui donne x^4-x+1 en représentation symétrique qui est bien un facteur de P (donc un facteur irréductible).

3 Factorisation à plusieurs variables

Comme pour le PGCD en plusieurs variables, on se ramène d'abord en une variable, en général on évalue toutes les variables sauf celle correspondant au degré partiel le plus faible. On factorise ensuite en une variable puis on remonte. A chaque étape de remontée, il peut être à nouveau nécessaire de combiner plusieurs facteurs. Différentes stratégies existent, comme pour le PGCD : factorisarion heuristique (avec reconstruction z-adique), remontée variable par variable ou toutes les variables en même temps comme dans EZGCD. On va présenter ici plus en détails l'algorithme de factorisation heuristique.

Soit P un polynôme en $X_1,...,X_n$ à coefficients entiers avec $n>1$, on choisit une des variables par exemple X_n, qu'on notera X dans la suite. On considère P comme un polynôme en $X_1,...,X_{n-1}$ à coefficients dans $\mathbb{Z}[X]$. On suppose que P est primitif (quitte à extraire son contenu qui est dans $\mathbb{Z}[X]$). On calcule ensuite $P(z)$ pour un entier z tel que $|z| \geq 2|P| + 2$. On factorise $P(z)$ dans $\mathbb{Z}[X_1, ..., X_{n-1}]$:

$$P(z)(X_1, ..., X_{n-1}) = c(z)\Pi_{j=1}^{k} p_j(X_1, ..., X_{n-1}) \tag{3}$$

où c est le contenu du polynôme $P(z)$ (comme polynôme en $n-1$ variables à coefficients entiers). Il s'agit de reconstruire les facteurs de P à partir des p_j et de c. Deux problèmes se posent alors, celui de la recombinaison possible de plusieurs facteurs p_j pour obtenir un facteur irréductible de P, et l'existence d'un facteur entier du contenu c à combiner avec un ou plusieurs p_j pour obtenir ce facteur irréductible. Plus précisément, si P_k est un facteur irréductible de P, on a :

$$P_k(z) = d(z)\Pi_{\text{certains } j} p_j, \quad \text{où } d(z) \text{ divise } c(z) \tag{4}$$

On a le :

Théorème 2 *Soit $P(X_1, ..., X_{n-1}, X)$ un polynôme à coefficients entiers ayant au moins 2 variables. On suppose que P est primitif vu comme polynôme en les variables $X_1, ..., X_{n-1}$ à coefficients dans $Z[X]$. Il existe une majoration C du contenu $|c(z)|$ de P évalué en $X = z$.*
Il existe un nombre fini de z tels que l'un des facteurs irréductibles P_k de P évalué en $X = z$ soit réductible (c'est-à-dire tels que (4) admette plusieurs facteurs p_j distincts)

Preuve
Pour déterminer C, on remarque que les facteurs du contenu de $P(z)$ sont des facteurs communs des coefficients de P évalués en z vu comme polynôme en $X_1, ..., X_{n-1}$ à coefficients dans $\mathbb{Z}[X]$. Donc $c(z)$ divise le générateur de l'idéal engendré par ces coefficients (ce générateur est un polynôme de $\mathbb{Z}[X]$ qui est constant car on a supposé P primitif), on peut aussi dire que deux au moins des coefficients dans $\mathbb{Z}[X]$ de P sont premiers entre eux, alors $c(z)$ divise le coefficient de l'identité de Bézout de ces 2 coefficients vu comme polynômes en X.

Considérons maintenant un facteur irréductible P_k de P de degré d par rapport à X. Pour $X_1, ..., X_{n-1}$ fixés, on factorise P_k sur $\mathbb{C}$:

$$P_k(X) = p_k \Pi_{j=1}^{d} (X - z_j)$$

On va maintenant se restreindre à un domaine des $X_1, ..., X_{n-1}$ sur lequel les z_j ont une dépendance analytique par rapport à $X_1, ..., X_{n-1}$. Pour cela on veut appliquer le théorème des fonctions implicites pour déterminer z_j au voisinage d'une solution donnée. On calcule donc la dérivée P_k' de P_k par rapport à X. On sait que P n'a pas de facteurs multiples, donc P_k et P_k' sont premiers entre eux, donc d'après l'identité de Bézout, il existe un polynôme non nul D dépendant de $X_1, ..., X_{n-1}$ et deux polynômes U et V dépendant de $X_1, ..., X_{n-1}, X$ tels que :

$$UP_k + VP_k' = D$$

Si $D(X_1, ..., X_{n-1})$ ne s'annule pas, on va pouvoir appliquer le théorème des fonctions implicites. On se fixe $x_1, .., x_{n-1}$, on calcule dans $\mathbb{C}$ les racines z_j du polynôme $P(x_1, .., x_{n-1}, X)$ pour une solution z_j telle que $P(x_1, .., x_{n-1}, z_j) = 0$, comme D est non nul, on a $P'(x_1, ..., x_{n-1}, z_j) \neq 0$, donc on peut écrire au voisinage de $(x_1, .., x_{n-1})$

$$z_j = z_j(X_1, ..., X_{n-1}), \quad P(X_1, ..., X_{n-1}, z_j) = 0$$

avec des fonctions z_j analytiques. Si D est constant, D ne s'annule pas, sinon quitte à permuter les variables, on peut supposer que le degré de D par rapport à X_1 est non nul. On peut alors se restreindre à une zone $X_1 >> X_2 >> .. >> X_{n-1} >> 1$ où D sera non nul ce qui permet de suivre analytiquement les z_j.

Supposons maintenant qu'il existe un nombre infini de z tels $P_k(z)$ soit réductible. Alors il existe un ensemble infini Z de ces valeurs de z pour lesquels l'un des facteurs à coefficients entiers f_j de $P_k(z)$ correspond à un même sous-ensemble R des racines z_j de P_k et à un même contenu c (puisqu'il y a un nombre fini de combinaisons possibles des racines en facteur et un nombre fini de diviseurs possibles du contenu de P_k). Pour $z \in Z$, on a :

$$f_j(X_1, ..., X_n, z) = c\Pi_{l \in R}(z - z_j), \quad f_j \in \mathbb{Z}[X_1, ..., X_{n-1}]$$

Soit $L(X)$ le polynôme obtenu par interpolation de Lagrange en cardinal$(R)+1$ points z de Z, égal à f_j en $X = z$. Pour des raisons de degré, on a :

$$L = c\Pi_{l \in R}(X - z_j)$$

donc L est un facteur de P. De plus L est un polynôme en $X_1, ..., X_{n-1}, X$ à coefficients rationnels (par construction). Ceci vient en contradiction avec l'hypothèse P_k irréductible, car on a construit un facteur de P_k à coefficients rationnels L de degré strictement inférieur.

Corollaire

Pour z assez grand, la reconstruction z-adique de $c(z)p_j(z)$ est un polynôme dont la partie primitive est un facteur irréductible de P.

Preuve du corollaire

On prend z assez grand pour que tous les facteurs irréductibles de P évalués en z aient un seul facteur polynomial (i.e. soient de la forme $d(z)p_j(z)$). Quitte à augmenter z, on peut supposer que $|z| > 2CL$ où C est la majoration de $|c(z)|$ et L est la borne de Landau sur les facteurs de P. Alors la reconstruction z-adique de $c(z)p_j(z)$ est $c(z)/d(z)P_j$, donc sa partie primitive est un facteur irréductible de P.

Algorithme de factorisation heuristique à plusieurs variables

Argument : un polynôme P primitif en au moins 2 variables.
Valeur renvoyée : les facteurs irréductibles de P
Choisir la variable X par rapport à laquelle P est de plus bas degré puis factoriser le contenu de P vu comme polynôme à coefficients dans $\mathbb{Z}[X]$. Initialiser un entier z à $2|P| + 2$ (où $|P|$ est le plus grand coefficient entier de P en valeur absolue) et une liste L à la factorisation de du contenu de P.
Boucle indéfinie :

- Si $P = 1$ renvoyer la liste L des facteurs de P.
- Tant que $\mathrm{pgcd}(P(z), P'(z)) = 0$ incrémenter z de 1.
- Factoriser $P(z) = c(z)\Pi p_j$
- Pour tous les facteurs p_j, déterminer le polynôme P_j tel que $c(z)p_j = P_j(z)$ par remontée z-adique (avec les coefficients de P_j écrit en représentation symétrique, de valeur absolue plus petite que $|z|/2$). Tester si la partie primitive de P_j divise P. Si oui, rajouter un facteur irréductible à la liste L, et diviser P par ce facteur.
- Augmenter z, par exemple remplacer z par la partie entière de $\sqrt{2}z$.

4 Pour en savoir plus

Pour factoriser des polynômes ayant des coefficients dans des extensions algébriques, il existe un algorithme assez simple, l'algorithme de Trager, qui n'est pas forcément le plus performant (la recherche est encore active dans ce domaine), cf. le livre de Henri Cohen pp. 142-144.

Pour factoriser sur des corps finis, on peut consulter la thèse de Bernardin disponible sur le web (`http://www.bernardin.lu`).

On peut aussi consulter le code source de Mupad, les routines de factorisation se trouvent dans le répertoire `lib/POLYLIB/FACLIB` après avoir désarchivé la `lib.tar`. Le point d'entrée pour factoriser des polynômes à plusieurs variables sur $\mathbb{Z}$ est le fichier `mfactor.mu`, on observera que l'algorithme utilisé par Mupad est assez différent de celui qu'on a détaillé dans la section précédente.

A Preuve de l'identité de Bézout généralisée

Elle se fait par récurrence. Pour $n = 2$, c'est l'identité de Bézout usuelle. Pour passer du rang $n-1$ au rang n, on isole P_n dans l'identité à résoudre :

$$\left(\sum_{j=1}^{n-1} Q_j (\Pi_{1 \leq k \leq n-1, k \neq j} P_k) \right) P_n + Q_n \Pi_{k \leq n-1} P_k = Q \pmod{p}$$

Comme P_n est premier avec $\Pi_{k \leq n-1} P_k$, en appliquant Bézout, on trouve deux polynômes Q_n et R_n tels que :

$$R_n P_n + Q_n \Pi_{k \leq n-1} P_k = Q \pmod{p} \tag{5}$$

Il reste à résoudre

$$\sum_{j=1}^{n-1} Q_j \Pi_{1 \leq k \leq n-1, k \neq j} P_k = R_n \pmod{p}$$

ce que l'on peut faire par hypothèse de récurrence.

B Algorithme de Bézout généralisé

Arguments : une liste $P_1, ..., P_n$ de polynômes premiers entre eux 2 à 2 et un polynôme Q à coefficients dans $\mathbb{Z}/p\mathbb{Z}$
Valeur renvoyée : la liste de polynômes $Q_1, ..., Q_n$ tels que

$$\sum_{j=1}^{n} Q_j \Pi_{k\neq j} P_k = Q \pmod p$$

On peut commencer par calculer le produit de tous les P_k puis faire une boucle sur j pour calculer les produits des P_k pour $k \neq j$ en divisant le produit complet par P_j (on fait ainsi $n-1$ multiplications et n divisions au lieu de $n(n-1)$ multiplications).
Boucle indéfinie sur n décrémenté de 1 par itération :

- Si $n = 2$, on rajoute à la liste résultat les polynômes Q_1 et Q_2 de l'algorithme de Bézout usuel et on renvoie la liste
- Sinon, on calcule les polynômes R_n et Q_n vérifiant (5), on rajoute Q_n en début de liste, on remplace Q par R_n.

Remarquons que lorsque nous utiliserons cet algorithme, Q sera la différence entre deux polynôme de même degré (le degré de P) et de même coefficient dominant 1, on peut donc remplacer les Q_i par le reste euclidien de Q_i par P_i sans changer l'égalité.