Magistère d'Informatique et Modélisation
deuxième semestre 2000/2001

cours de

Calcul Formel

cours : Jean-Louis NICOLAS
TD : Marc DELÉGLISE
rédaction : Sébastien BRIAIS

Introduction

Que fait un système de calcul formel ?

- travailler sur des grands nombres entiers, rationnels, réels, ...
- travailler sur des polynômes, fractions rationnelles, en plusieurs variables. Factorisation de polynômes.
- analyse : calcul de limites, de dérivées, ...
- simplification, manipulation de formules
- résolution d'équations exactes et approchées
- intégration formelle
- résolution d'équations différentielles
- algèbre linéaire : résolution de systèmes, calcul de valeurs propres
- calcul dans les corps de nombres
  exemple :
  $$\mathbf{Q}[\sqrt{2}] = \left\{a + b\sqrt{2}; a, b \in \mathbf{Q}\right\}$$
- calcul de sommes
  exemple :
  $$\sum_{i=1}^{n} \mathrm{f}(i)$$
  $$\int_a^b \mathrm{f}(x)\,dx$$
  $$\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$
- calcul modulaire : calcul modulo n, dans $\mathbf{Z}/n\mathbf{Z}$
- simplification

  exemple :
  en Maple : expand, normal, collect, simplify, factor
  ```
  expand((1+X)^20);
    1+20X+190X^2+...+X^20
  factor(\%);
    (1+X)^20
  expand((1+X)^20+1);
    2+20X+190X^2+...+X^20
  factor(\%);
    2+20X+190X^2+...+X^20
  ```
  exemple : Simplifier des expressions n'est pas facile ; ainsi, il n'est pas évident

de se rendre compte que l'expression suivante désigne un entier.

$$\sqrt[3]{27+6\sqrt{21}}+\sqrt[3]{27-6\sqrt{21}}$$

exemple : De même, on ne voit pas facilement que $\alpha = \beta$.

$$\left\{\begin{array}{lcc} \alpha & = & \sqrt{5}+\sqrt{22+2\sqrt{5}} \\ \beta & = & \sqrt{11+2\sqrt{29}}+\sqrt{16-2\sqrt{29}+2\sqrt{55-10\sqrt{29}}} \end{array}\right.$$

Table des matières

premier chapitre

Rappels d'arithmétique et multiprécision

1.1 Nombres et chiffres

$$2001 = 2 \times 10^3 + 0 \times 10^2 + 0 \times 10 + 1$$

Le zéro comme chiffre date de 450, il a été inventé par les mathématiciens hindous.

Soit $B \in \mathbf{N}$ la base et $N \in \mathbf{N}$. On décompose N sur B en :

$$N = c_k B^k + c_{k-1} B^{k-1} + \ldots + c_1 B + c_0, \text{ avec } \forall i, c_i \in \{0, 1, \ldots, B-1\}$$

1.1.1 Décomposition d'un nombre sur une base

N et B étant donnés, trouver les c_i.

$$2001 = \underbrace{200}_{quotient} \times 10 + \underbrace{1}_{reste}$$

On notera $a \div b$ le quotient de la division euclidienne de a par b et $a \bmod b$ le reste. (en MAPLE : `iquo` et `irem`)

---

algorithme 1 calcul des c_i

étant donné : N, B

fournit : $N = \sum_{i=0}^{+\infty} c_i B^i, 0 \leq c_i < B$

```
i ← 0
M ← N
tant que M ≠ 0 faire
  c_i ← M mod B
  i ← i + 1
  M ← M ÷ B
fin tant que
```

---

exemple : écrire 23 en base 2

$$
\begin{array}{r|rrrrr}
23 & 2 \\ \cline{2-2}
\boxed{1} & \multicolumn{1}{r|}{11} & 2 \\ \cline{3-3}
 & \multicolumn{1}{r|}{\boxed{1}} & \multicolumn{1}{r|}{5} & 2 \\ \cline{4-4}
 & \multicolumn{1}{r|}{} & \multicolumn{1}{r|}{\boxed{1}} & \multicolumn{1}{r|}{2} & 2 \\ \cline{5-5}
 & \multicolumn{1}{r|}{} & \multicolumn{1}{r|}{} & \multicolumn{1}{r|}{\boxed{0}} & \multicolumn{1}{r|}{1} & 2 \\ \cline{6-6}
 & & & & \multicolumn{1}{r|}{\boxed{1}} & 0
\end{array}
$$

d'où $23 = \overline{10111}_2$

Maple La fonction `convert(N,base,B)` décompose N sur la base B.

1.1.2 Evaluation d'un nombre connaissant sa décomposition sur une base

c_i et B étant donnés, trouver N.

Il s'agit en fait d'évaluer un polynôme en un point, on utilise pour cela la méthode de Horner.

---

algorithme 2 calcul de N

étant donné : B, k, $c_i, 0 \leq i \leq k$

fournit : $N = \sum_{i=0}^{k} c_i B^i$

$N \leftarrow 0$

pour $i = k$ **à** 0 **par pas de** -1 **faire**

$N \leftarrow N \times B + c_i$

fin pour

1.2 Algorithme des puissances

1.2.1 Algorithme gauche-droite

exemple :

$$3^{16} = ?$$

$$\underbrace{3 \times 3 \times \cdots \times 3}_{\text{15 multiplications}}$$

$$\underbrace{\left(\left(\left(3^2\right)^2\right)^2\right)^2}_{\text{4 multiplications}}$$

exemple :

calcul de a^{23}

$$23 = \overline{\cancel{1}0111}_2$$

algorithme 3 calcul de $c = a^b$

étant donné : a, b

fournit : $c = a^b$

écrire b en base 2

rayer le 1 de gauche

remplacer 0 par Q, 1 par QX

en partant de a, exécuter les opérations

$$\mathrm{Q}(t) = t^2$$

$$\mathrm{X}(t) = a \times t$$

On obtient les opérations

$$\text{QQXQXQX}$$
$$a \to a^2 \to a^4 \to a^5 \to a^{10} \to a^{11} \to a^{22} \to a^{23}$$

Le coût de l'opération est inférieure à deux fois le nombre de chiffre de b en base 2 moins 1.

En base B, un nombre de k chiffres est compris entre B^{k-1} et $B^k - 1$.

Soit k le nombre de chiffre de b en base 2.

$$2^{k-1} \leq b < 2^k$$

$$k - 1 \leq \log_2 b < k$$

Le coût de l'opération est donc inférieure à $2 \log_2 b$.

preuve :

1. Par récurrence sur le nombre de chiffres de b en base 2.

$$b = 2b' + \varepsilon, \varepsilon \in \{0, 1\}$$

$$a^b = \left(a^{b'}\right)^2 \times a^\varepsilon$$

2. Horner

$$\begin{aligned} b &= c_k 2^k + c_{k-1} 2^{k-1} + \cdots + c_0 \\ &= ((c_k \times 2 + c_{k-1}) \times 2 + c_{k-2}) \times 2 + \cdots \end{aligned}$$

■

1.2.2 La multiplication des paysans russes

exemple : Soit à calculer 19×23

19	23	1
38	11	1
76	5	1
152	2	0
304	1	1
		↑
437		écriture binaire de 23

On ignore les lignes qui ont un nombre pair dans la colonne de 23 (ce qui correspond à un 0 dans son écriture binaire)

$$23 = 16 + 0 \times 8 + 4 + 2 + 1$$

$$19 \times 23 = 19 \times (1 + 2 + 4 + 0 \times 8 + 16)$$
$$19 \times 23 = 19 + 19 \times 2 + 19 \times 4 + 19 \times 0 \times 8 + 19 \times 16$$

algorithme 4 calcul de $y = a \times b$

étant donné : a, b

fournit : $y = a \times b$

$z \leftarrow a$
$y \leftarrow 0$
$w \leftarrow b$
tant que $w \neq 0$ **faire**
  $r \leftarrow w \bmod 2$
  $w \leftarrow w \div 2$
  si $r = 1$ **alors**
    $y \leftarrow y + z$
  fin si
  $z \leftarrow 2 \times z$
fin tant que

1.2.3 Algorithme droite-gauche

multiplication

$$a \times b = \underbrace{a + a + \cdots + a}_{\text{b fois}}$$

exponentiation

$$a^b = \underbrace{a \times a \times \cdots \times a}_{\text{b fois}}$$

On remplace + par $\times$ et 0 par 1 dans l'algorithme 4 obtenant ainsi l'algorithme 5.

1.2.4 Calcul de $a^b \bmod n$

méthode bête

1. Calculer a^b
2. Prendre le reste dans la division par n

méthode meilleure Dans les algorithmes 3 ou 5, travailler modulo n.

algorithme 5 calcul de $y = a^b$

étant donné : a, b
fournit : $y = a^b$

$z \leftarrow a$
$y \leftarrow 1$
$w \leftarrow b$
tant que $w \neq 0$ **faire**
  $r \leftarrow w \bmod 2$
  $w \leftarrow w \div 2$
  si $r = 1$ **alors**
    $y \leftarrow y \times z$
  fin si
  $z \leftarrow z \times z$
fin tant que

Conclusion $a^b \bmod n$ se calcule si a, b, n ont 100 chiffres décimaux en moins de $\log(100) = 670$ opérations élémentaires, chaque opération étant une multiplication de deux nombres de 100 chiffres suivie par une division par un nombre de 100 chiffres : c'est rapide.

Application au test de primalité Étant donné n impair, n est-il premier ?

1. Diviser n par $2, 3, 5, 7, 11, \ldots \leq \sqrt{n}$. Si une division a un reste nul, n n'est pas premier. Si aucune division n'a un reste nul, n est premier.
   Pour un n de 30 chiffres : $n \approx 10^{30}$, $\sqrt{n} \approx 10^{15}$.
   On note $\Pi(x)$ le nombre de nombres premiers inférieurs à x. On sait que $\Pi(x) \sim \frac{x}{\log x}$.
   $$\Pi\big(10^{15}\big) \geq 10^{13}$$
   On doit donc faire 10^{13} divisions. En admettant qu'un ordinateur actuel permet de faire 10^9 divisions par secondes, il faut alors attendre 10^4 secondes, c'est-à-dire 3 heures !
2. Utiliser le théorème de FERMAT, à savoir :
   Si p est premier et $p \nmid a$ alors $a^{p-1} \equiv 1 \bmod p$.
   Si n est impair, on calcule $2^{n-1} \bmod n$ par l'algorithme des puissances. Si le résultat est différent de 1, n n'est pas premier. En revanche, si le résultat est égal à 1, n est probablement premier.
   Par exemple, pour $n = 341 = 11 \times 31$, $2^{340} \equiv 1 \bmod 341$, le test précédent échoue.

Maple

```
a &^ b mod n;
power(a,b) mod n;
```

1.3 Multiprécision

De nos jours, nous disposons d'ordinateurs travaillant sur 32 ou 64 bits. Les opérations dont le résultat est inférieure à $2^{31}-1$ ou $2^{63}-1$ sont exactes.

On choisit B tel que B^2 soit plus petit que le plus grand entier représenté par l'ordinateur.

$$B^2 < 2^{31}-1$$

On choisit généralement pour B une puissance paire de 2. Pour un ordinateur 32 bits, on choisit $B = 2^{14}$. On représente alors un grand nombre N par :

$$N = c_k B^k + c_{k-1} B^{k-1} + \cdots + c_1 B + c_0, 0 \leq c_i < B$$

On va voir dans cette partie comment faire les opérations élémentaires sur ces grands nombres représentés par la liste de leurs coefficients.

1.3.1 Addition

algorithme 6 calcul de $W = U + V$

étant donné : $U = \sum_{i=0}^{m} u_i B^i$, $V = \sum_{j=0}^{n} v_j B^j$

fournit : $W = U + V = \sum_{k=0}^{l} w_k B^k$

`// alignement`
$l \leftarrow \max(m, n)$
si $l = m$ **alors**
  Compléter $v_l = v_{l-1} = \cdots = v_{n+1} = 0$
sinon
  Compléter $u_l = u_{l-1} = \cdots = u_{m+1} = 0$
fin si
`// addition`
$retenue \leftarrow 0$
pour $i = 0$ **à** l **faire**
  $t \leftarrow u_i + v_i + retenue$
  $w_i \leftarrow t \bmod B$
  $retenue \leftarrow t \div B$
fin pour
si $retenue \neq 0$ **alors**
  $l \leftarrow l + 1$
  $w_l \leftarrow retenue$
fin si

1.3.2 Multiplication

algorithme 7 calcul de $W = U \times V$

étant donné : $U = \sum_{i=0}^{m} u_i B^i$, $V = \sum_{j=0}^{n} v_j B^j$

fournit : $W = U \times V = \sum_{k=0}^{l} w_k B^k$

```
// initialisation
```

pour $l = 0$ **à** $m + n + 1$ **faire**
  $w_l \leftarrow 0$
fin pour

```
// calcul des produits partiels
```

pour $j = 0$ **à** n **faire**
  $retenue \leftarrow 0$
  pour $i = 0$ **à** m **faire**
    $t \leftarrow u_i \times v_j + w_{i+j} + retenue$
    $w_{i+j} \leftarrow t \bmod B$
    $retenue \leftarrow t \div B$
  fin pour
  $w_{j+m+1} \leftarrow retenue$
fin pour

Il n'y a pas de dépassements car $t < B^2$. En effet :

$$w_k < B$$

$$t = u_i \times v_j + w_{i+j} + retenue$$

$$t \leq (B-1)^2 + (B-1) + (B-1)$$

$$t \leq B^2 - 2B + 1 + 2B - 2 = B^2 - 1$$

1.3.3 Division

exemple :

$$\begin{array}{r|l} 410\,000 & 588 \\ \cline{2-2} & \end{array}$$

$$588 \leq 4100 < 5880$$

$$\begin{array}{r|c} 41\,00 & 588 \\ \cline{2-2} 572 & \cancel{8} \\ & \cancel{7} \\ & 6 \end{array}$$

Division élémentaire

$$\text{Soit } \begin{cases} V &= v_n B^n + \cdots + v_0 \\ U &= u_{n+1}B^{n+1} + u_n B^n + \cdots + u_0 \quad u_{n+1} \text{ pouvant être nul} \end{cases}$$

tels que

$$V \leq U < BV$$

On pose

$$\begin{aligned} q &= \left\lfloor \frac{U}{V} \right\rfloor & \text{(quotient exact)} \\ x &= \frac{u_{n+1}B + u_n}{v_n} \\ \hat{q} &= \min(\lfloor x \rfloor, B-1) & \text{(quotient approché)} \end{aligned}$$

théorème 1.1 (*Division élémentaire*)

> *1.* $q \leq \hat{q}$
> *2. Si* $v_n \geq \left\lfloor \frac{B}{2} \right\rfloor$*, alors* $\hat{q} - 2 \leq q \leq \hat{q}$.

preuve : 1. On a :

$$v_n B^n \leq V \leq v_n B^n + (B-1)\big(1 + B + \cdots + B^{n-1}\big)$$

$$v_n B^n \leq V \leq v_n B^n + B^n - 1$$

On majore q :

$$\begin{aligned} q &= \left\lfloor \frac{u_{n+1}B^{n+1} + u_n B^n + \cdots + u_0}{v_n B^n + \cdots + v_0} \right\rfloor \\ &\leq \left\lfloor \frac{u_{n+1}B^{n+1} + u_n B^n + B^n - 1}{v_n B^n} \right\rfloor \\ &\leq \left\lfloor \frac{u_{n+1}B + u_n + 1 - \frac{1}{B^n}}{v_n} \right\rfloor \end{aligned}$$

On effectue la division euclidienne de $u_{n+1}B + u_n$ par v_n :

$$u_{n+1}B + u_n = \lfloor x \rfloor v_n + r, 0 \leq r < v_n$$

D'où

$$\begin{aligned} q &\leq \left\lfloor \frac{u_{n+1}B + u_n + 1 - \frac{1}{B^n}}{v_n} \right\rfloor \\ &\leq \left\lfloor \frac{\lfloor x \rfloor v_n + r + 1 - \frac{1}{B^n}}{v_n} \right\rfloor \end{aligned}$$

Or

$$r + 1 - \frac{1}{B^n} < v_n$$

Donc

$$\left\lfloor \frac{\lfloor x\rfloor v_n + r + 1 - \frac{1}{B^n}}{v_n} \right\rfloor = \lfloor x\rfloor$$

Ainsi

$$q \leq \lfloor x\rfloor \leq \hat{q}$$

2. On suppose

$$v_n \geq \left\lfloor \frac{B}{2} \right\rfloor$$

Montrons que

$$\hat{q} \leq q + 2$$

Comme $\hat{q} \leq B - 1$, si $q \geq B - 3$, c'est évident.
Supposons donc que $q < B - 3$.
Montrons que

$$\lfloor x\rfloor \leq q + 2$$

$$x = \frac{u_{n+1}B + u_n}{v_n} = \frac{u_{n+1}B^{n+1} + u_nB^n}{v_nB^n} \leq \frac{U}{V - (B^n - 1)}$$

$$q = \left\lfloor \frac{U}{V} \right\rfloor \geq \frac{U}{V} - 1$$

D'où

$$\begin{aligned} x - q - 1 &\leq \frac{U}{V - (B^n - 1)} - \frac{U}{V} \\ &\leq \frac{U}{V}\left(\frac{V}{V - (B^n - 1)} - 1\right) \\ &\leq \frac{U}{V}\left(\frac{V - (V - (B^n - 1))}{V - (B^n - 1)}\right) \\ &\leq \frac{U}{V}\left(\frac{B^n - 1}{V - B^n + 1}\right) \\ &< \frac{U}{V}\left(\frac{B^n}{V - B^n}\right) \end{aligned}$$

Or

$$V \geq v_nB^n \geq \left\lfloor \frac{B}{2} \right\rfloor B^n \geq \frac{B-1}{2}B^n$$

D'où

$$\begin{aligned} x - q - 1 &< \frac{U}{V}\left(\frac{B^n}{V - B^n}\right) \\ &< \frac{U}{V}\left(\frac{B^n}{\frac{B-1}{2}B^n - B^n}\right) \\ &< \frac{U}{V}\left(\frac{1}{\frac{B-1}{2} - 1}\right) \\ &< \frac{U}{V}\left(\frac{2}{B - 3}\right) \end{aligned}$$

Mais

$$\frac{U}{V} < q + 1 \leq B - 4 + 1 = B - 3$$

D'où

$$x - q - 1 < 2$$

i.e.

$$x < q + 3$$

Donc

$$\lfloor x \rfloor \leq q + 2$$

■

théorème 1.2 (*Lemme de normalisation*)

Soit v tel que $1 \leq v \leq B - 1$.
Alors

$$\left\lfloor \frac{B}{2} \right\rfloor \leq v \left\lfloor \frac{B}{v+1} \right\rfloor < B$$

preuve :

$$v \left\lfloor \frac{B}{v+1} \right\rfloor \leq v \frac{B}{v+1} < B \tag{1.1}$$

On effectue la division euclidienne de B par $v + 1$.

$$B = a(v+1) + r, 0 \leq r \leq v$$

$$\left\lfloor \frac{B}{v+1} \right\rfloor = a$$

Il faut donc montrer

$$av \geq \left\lfloor \frac{B}{2} \right\rfloor$$

Comme

$$B \geq v + 1$$

On a

$$a \geq 1$$

Et comme

$$r \leq v$$

On a

$$B \leq a(v+1) + v$$

i.e.

$$B \leq av + a + v = 2av - (a-1)(v-1) + 1$$

D'où

$$B \leq 2av + 1$$

Ainsi

$$\frac{B}{2} \leq av + \frac{1}{2}$$

D'où

$$\left\lfloor \frac{B}{2} \right\rfloor \leq av \tag{1.2}$$

■

Comment faire la division de U par V si $v_n < \frac{B}{2}$?
On multiplie tout par $a = \left\lfloor \frac{B}{v_n+1} \right\rfloor$, obtenant $U' = aU$ et $V' = aV$. On faire alors la division de U' par V'. On a

$$\frac{U'}{V'} = \frac{U}{V}$$

Le reste de la division est multiplié par a.

$$V' = aV \leq a(v_n + 1)B^n < B^{n+1}$$

Ainsi

$$a(v_n + 1) < B$$

Donc V et V' ont le même nombre de chiffres.

$$V' = aV \geq av_n B^n \geq \left\lfloor \frac{B}{2} \right\rfloor B^n$$

Donc le chiffre dominant de V' est supérieur à $\left\lfloor \frac{B}{2} \right\rfloor$.

1.3.4 Multiplier rapidement

Si U a $n+1$ chiffres, V a $n+1$ chiffres, la multiplication de U par V est en $\mathcal{O}\left(n^2\right)$.

1 milliard de décimales de π occupent 100 millions de chiffres en base $B = 2^{30}$. Multiplier deux tels nombres nécessitent $\left(10^8\right)^2 = 10^{16}$ opérations élémentaires.

L'algorithme de KARATSUBA a une complexité de $\mathcal{O}\left(n^{\frac{\log 3}{\log 2}}\right)$.

Exercice 1.1 — *Algorithme de Karatsuba*

Soit P et Q deux polynômes de degré inférieur à $2m$, où $m = 2^n$. L'algorithme de Karatsuba fonde son approche diviser pour régner sur la formule :

$$P \times Q = \left(X^{2m} + X^m\right)P_1 \times Q_1 - X^m(P_1 - P_0) \times (Q_1 - Q_0) + (X^m + 1)P_0 \times Q_0$$

avec

$$\left\{ \begin{array}{lcl} P & = & P_1 X^m + P_0 \\ Q & = & Q_1 X^m + Q_0 \end{array} \right.$$

Montrer que la complexité de l'algorithme de Karatsuba pour la multiplication de deux polynômes de degré N est $\mathcal{O}\left(N^{\frac{\log 3}{\log 2}}\right)$.

solution page 101

L'algorithme de transformée de FOURIER rapide fonctionne, quant à lui, en $\mathcal{O}(n \log n \log\log n)$. Cette méthode, difficile à implémenter, ne devient intéressante que pour n supérieur à plusieurs milliers.

Exercice 1.2 — *Calcul de π*

Montrer la formule

$$\pi = \sum_{i=0}^{+\infty} \frac{1}{16^i} \left(\frac{4}{8i+1} - \frac{2}{8i+4} - \frac{1}{8i+5} - \frac{1}{8i+6} \right)$$

solution page 101

deuxième chapitre

Rappels d'arithmétique

2.1 pgcd

On calcule le pgcd de deux entiers en utilisant l'algorithme d'EUCLIDE.

lemme 2.1

Si $a = bq + r$ *avec* $0 \leq r < b$ *alors* $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r)$.

preuve : Soit $d = \mathrm{pgcd}(a, b) \in \mathbf{N}$ et $d' = \mathrm{pgcd}(b, r) \in \mathbf{N}$.

$d \mid a$ et $d \mid b$ donc $d \mid r = a - bq$, ainsi $d \mid d'$.

$d' \mid b$ et $d' \mid r$ donc $d' \mid a = bq + r$, ainsi $d' \mid d$.

Comme $d \mid d'$ et que $d' \mid d$, on a $d = d'$. ■

On en déduit un algorithme pour le calcul du pgcd.

algorithme 8 $\mathrm{pgcd}(a, b)$ version récursive

étant donné : $a \in \mathbf{N}$, $b \in \mathbf{N}$
fournit : $\mathrm{pgcd}(a, b)$
  si $b = 0$ **alors**
    retourner a
  sinon
    retourner $\mathrm{pgcd}(b, a \bmod b)$
  fin si

algorithme 9 pgcd(a,b) version itérative

étant donné : $a \in \mathbf{N}$, $b \in \mathbf{N}$

fournit : $d = \text{pgcd}(a,b)$

$m \leftarrow a$

$n \leftarrow b$

$r \leftarrow m \bmod n$

tant que $r \neq 0$ **faire**

  $m \leftarrow n$

  $n \leftarrow r$

  $r \leftarrow m \bmod n$

fin tant que

$d \leftarrow r$

exemple : Algorithme d'Euclide de A et de B, avec $A \geq B$.

$$\begin{array}{rcll}
A & = & a_0 B + r_0 & a_0 \geq 1, 1 \leq r_0 < B \\
B & = & a_1 r_0 + r_1 & a_1 \geq 1, 1 \leq r_1 < r_0 \\
r_0 & = & a_2 r_1 + r_2 & a_2 \geq 1, 1 \leq r_2 < r_1 \\
 & \vdots & & \\
r_i & = & a_{i+2} r_{i+1} + r_{i+2} & a_{i+2} \geq 1, 1 \leq r_{i+2} < r_{i+1} \\
r_{i+1} & = & a_{i+3} r_{i+2} + r_{i+3} & a_{i+3} \geq 1, 1 \leq r_{i+3} < r_{i+2} \\
r_{i+2} & = & a_{i+4} r_{i+3} + r_{i+4} & a_{i+4} \geq 1, 1 \leq r_{i+4} < r_{i+3} \\
 & \vdots & & \\
r_{n-5} & = & a_{n-3} r_{n-4} + r_{n-3} & a_{n-3} \geq 1, 1 \leq r_{n-3} < r_{n-4} \\
r_{n-4} & = & a_{n-2} r_{n-3} + r_{n-2} & a_{n-2} \geq 1, 1 \leq r_{n-2} < r_{n-3} \\
r_{n-3} & = & a_{n-1} r_{n-2} & a_{n-1} \geq 2, r_{n-1} = 0
\end{array}$$

Le pgcd de A et de B est le dernier reste non nul, c'est-à-dire r_{n-2}. Dans l'algorithme ci-dessus, il y a n divisions ($n \geq 2$).

définition 2.1 (*suite de Fibonacci*)

La suite de Fibonacci $(F_n)_{n \in \mathbf{N}}$ est définie par

$$\left\{ \begin{array}{rcll} F_0 & = & 0 & \\ F_1 & = & 1 & \\ F_{n+2} & = & F_{n+1} + F_n & n \geq 0 \end{array} \right.$$

proposition 2.2

Dans l'algorithme d'Euclide de A et B, avec $A \geq B$, on pose $r_{-2} = A$, $r_{-1} = B$. On a alors

$$\forall j \in \{-2, -1, 0, 1, \ldots, n-3\}, r_j \geq F_{n-j}$$

preuve : On montre l'inégalité par récurrence descendante.

L'hypothèse de récurrence $\mathrm{H}(i)$ est $\forall j \geq i+1, r_j \geq F_{n-j}$

- $i = n-2$

$$r_{n-3} = a_{n-1} r_{n-2} \geq 2 \times 1 = F_3$$

- Soit $i < n-2$ tel que $\mathrm{H}(i)$.
  Montrons $\mathrm{H}(i-1)$, c'est-à-dire, montrons que $r_i \geq F_{n-i}$.
  Par hypothèse de récurrence, on a

$$\begin{cases} r_{i+1} & \geq & F_{n-i-1} \\ r_{i+2} & \geq & F_{n-i-2} \end{cases}$$

  De plus

$$r_i = a_{i+2} r_{i+1} + r_{i+2}$$

  Or

$$a_{i+2} \geq 1$$

  Donc

$$r_i \geq r_{i+1} + r_{i+2} \geq F_{n-i-1} + F_{n-i-2} = F_{n-i}$$

D'où le résultat. ■

théorème 2.3

Si dans l'algorithme d'Euclide de A et de B, où $A \geq B$, il y a n divisions, alors $A \geq F_{n+2}$.

preuve : Évident d'après la proposition précédente. ■

corollaire 2.4

Soit A et B deux nombres strictement inférieurs à F_{n+2}. Alors l'algorithme d'Euclide de A et de B nécessite au plus n divisions.

preuve : On effectue l'algorithme d'Euclide de A et de B.

- Si $A \geq B$, il y a au plus $n-1$ divisions.
- Sinon la première division $A = 0 \times B + A$ permute A et B et il y a au plus n divisions. ■

lemme 2.5

$$\forall n \geq 0, F_{n+2} \geq 10^{\frac{n}{5}}$$

Exercice 2.1 — *Suite de Fibonacci*

1) Calculer F_n.

2) Montrer que

$$\forall n \geq 0, F_{n+2} \geq 10^{\frac{n}{5}}$$

3) Montrer que F_n peut se calculer en $\mathcal{O}(\log_2 n)$ opérations portant sur des entiers.

solution page 102

théorème 2.6 (*Lamé,* 1845)

Si A et B ont au plus k chiffres en base 10, l'algorithme d'Euclide de A et de B nécessite au plus $5k$ divisions.

preuve :

$$A, B < 10^k \leq F_{5k+2}$$

On applique alors le corollaire précédent. ■

2.2 Bézout

théorème 2.7 (*Bézout*)

Soit $a, b \in \mathbf{N}$ et $d = \mathrm{pgcd}(a, b)$.
Alors

$$\exists u, v \in \mathbf{Z} \left\{ \begin{array}{ccc} d & = & au + bv \\ \mid u \mid & < & b \\ \mid v \mid & < & a \end{array} \right.$$

De plus, on a

$$\mathrm{pgcd}(a, b) = 1 \Leftrightarrow \exists u, v \in \mathbf{Z} | au + bv = 1$$

preuve :

1. La preuve utilise l'algorithme d'Euclide étendu.
   Dans l'algorithme d'Euclide de A et de B, on pose, en notant $(a_i)_{0 \leq i \leq n-1}$ la suite des quotients,

$$\left\{ \begin{array}{ccc} u_{-2} & = & 0 \\ u_{-1} & = & 1 \\ u_i & = & -a_i u_{i-1} + u_{i-2} \\ v_{-2} & = & 1 \\ v_{-1} & = & 0 \\ v_i & = & -a_i v_{i-1} + v_{i-2} \end{array} \right.$$

   On montre alors par récurrence que

$$v_i A + u_i B = r_i$$

   En faisant $i = n - 2$, on obtient le résultat :

$$v_{n-2} A + u_{n-2} B = r_{n-2} = \mathrm{pgcd}(A, B)$$

2. Soit

$$d = \mathrm{pgcd}(a, b)$$

   On a

$$d \mid a$$
$$d \mid b$$

   Donc

$$d \mid au + bv$$

i.e.

$$d \mid 1$$

Donc

$$d = 1$$

i.e.

$$\mathrm{pgcd}(a, b) = 1$$

■

2.3 Fonction de Möbius

Maple

```
with(numtheory);
```

définition 2.2 (*sans facteurs carrés*)

Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ avec p_i premier deux à deux distincts et $\alpha_i \geq 1$.
n est sans facteur carrés si $\alpha_1 = \cdots = \alpha_k = 1$

définition 2.3 (*fonction de Möbius*)

On définit $\mu : \mathbf{N} \setminus \{0\} \to \{-1, 0, 1\}$ par :

$$\begin{cases} \mu(1) & = & 1 & \\ \mu(n) & = & (-1)^k & \text{si } n = p_1 \cdots p_k \text{ est sans facteurs carrés} \\ \mu(n) & = & 0 & \text{sinon} \end{cases}$$

théorème 2.8

$$\sum_{d \mid n} \mu(d) = \begin{matrix} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{matrix}$$

preuve :

– Si $n = 1$

$$\sum_{d \mid n} \mu(d) = \mu(1) = 1$$

– Sinon

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

On note

$$\overline{n} = p_1 \cdots p_k$$

Si $d \mid n$ et $\mu(d) \neq 0$ alors $d \mid \overline{n}$.
On a donc

$$\sum_{d \mid n} \mu(d) = \sum_{d \mid \overline{n}} \mu(d)$$

On note $\omega(d)$ le nombre de facteurs premiers de d. On a $\omega(n) = k$.

On a alors

$$\sum_{d|n} \mu(d) = \sum_{j=0}^{k} \left(\sum_{\substack{d \mid \overline{n} \\ \omega(d)=j}} \mu(d) \right)$$

Or si $\omega(d) = j$ et $d \mid \overline{n}$ alors $\mu(d) = (-1)^j$
Donc

$$\sum_{d|n} \mu(d) = \sum_{j=0}^{k} (-1)^j \left(\sum_{\substack{d \mid \overline{n} \\ \omega(d)=j}} 1 \right)$$

Or

$$\sum_{\substack{d \mid \overline{n} \\ \omega(d)=j}} 1 = \mathrm{C}_k^j$$

D'où

$$\sum_{d|n} \mu(d) = \sum_{j=0}^{k} (-1)^j \mathrm{C}_k^j = (1-1)^k = 0$$

■

théorème 2.9 (*Formule d'inversion de Möbius*)

Soit $f : \mathbf{N} \setminus \{0\} \to \mathbf{C}$ *et* g *définie par* $\mathrm{g}(n) = \sum_{d|n} \mathrm{f}(d)$ *alors*

$$\begin{aligned} \mathrm{f}(n) &= \sum_{d|n} \mu(d)\mathrm{g}\left(\tfrac{n}{d}\right) \\ &= \sum_{d|n} \mu\left(\tfrac{n}{d}\right)\mathrm{g}(d) \\ &= \sum_{dd'=n} \mu(d)\mathrm{g}(d') \end{aligned}$$

preuve :

$$\begin{aligned} \sum_{d|n} \mu(d)\mathrm{g}\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{\delta | \frac{n}{d}} \mathrm{f}(\delta) \\ &= \sum_{\delta | n} \mathrm{f}(\delta) \underbrace{\sum_{d | \frac{n}{\delta}} \mu(d)}_{0 \text{ sauf si } \frac{n}{\delta} = 1} \\ &= \mathrm{f}(n) \end{aligned}$$

■

2.4 Fonction d'Euler

définition 2.4 (*fonction d'Euler*)

On définit $\varphi : \mathbf{N} \to \mathbf{N}$ la fonction d'Euler par :

$$\varphi(n) = \mathrm{card}(\{a | 1 \leq a \leq n, \mathrm{pgcd}(a,n) = 1\})$$

théorème 2.10

$$\sum_{d|n} \varphi(d) = n$$

preuve : On compte les fractions $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{a}{n}, \ldots, \frac{n}{n}$. Il y en a n.

Pour a tel que $1 \leq a \leq n$, il existe b, d uniques tels que :

$$\begin{gathered} \tfrac{a}{n} = \tfrac{b}{d} \\ d \mid n \\ \mathrm{pgcd}(b,d) = 1 \\ 1 \leq b \leq d \end{gathered}$$

Réciproquement, à chaque fraction $\frac{b}{d}$ tel que

$$\begin{gathered} d \mid n \\ \mathrm{pgcd}(b,d) = 1 \\ 1 \leq b \leq d \end{gathered}$$

correspond un unique a tel que $1 \leq a \leq n$ et $\frac{b}{d} = \frac{a}{n}$.

Il y a $\varphi(d)$ fractions $\frac{b}{d}$ avec $\mathrm{pgcd}(b,d) = 1$ et $1 \leq b \leq d$.

D'où

$$\sum_{d|n} \varphi(d) = n$$

■

théorème 2.11

Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, p_i premiers deux à deux distincts et $\alpha_i > 0$ alors

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

preuve : On utilise la formule d'inversion de Möbius et le théorème précédent. On obtient :

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|\overline{n}} \frac{\mu(d)}{d}$$

$$
\begin{aligned}
\sum_{d|\overline{n}} \frac{\mu(d)}{d} &= \sum_{j=0}^{k} \sum_{\substack{d \,|\, \overline{n} \\ \omega(d)=j}} \frac{1}{p_{i_1}\cdots p_{i_j}} \\
&= 1 - \sum_{p|n} \frac{1}{p} + \sum \frac{1}{p_{i_1}p_{i_2}} - \cdots \\
&= \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)
\end{aligned}
$$

■

2.5 $\mathbf{Z}/n\mathbf{Z}$

définition 2.5 (*congruence modulo n*)

Soit $n \in \mathbf{N}$. On définit la relation de congruence modulo n sur $\mathbf{Z}^2$ par :

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b)$$

lemme 2.12

Soit $n \in \mathbf{N}$. La relation de congruence modulo n est une relation d'équivalence stable par addition et multiplication.

preuve : Évident. ■

lemme 2.13

Soit $n \in \mathbf{N}$, $a, b \in \mathbf{Z}$ tels que $a \equiv b \pmod{n}$.

Si $\begin{cases} d \mid a \\ d \mid b \\ d \mid n \end{cases}$, *alors* $\frac{a}{d} \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{n}{d}\right)$.

preuve : On écrit

$$
\begin{aligned}
a &= da' \\
b &= db' \\
n &= dn'
\end{aligned}
$$

Or

$$n \mid (a-b)$$

Donc

$$(a-b) = nm$$

i.e.

$$d\big(a'-b'\big) = dn'm$$

D'où

$$\big(a'-b'\big) = n'm$$

i.e.

$$\frac{a}{d} \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{n}{d}\right)$$

■

théorème 2.14 (*Lemme de Gauss*)

Si $n \mid ab$ *et* $\text{pgcd}(n, a) = 1$ *alors* $n \mid b$.

preuve : On utilise Bézout :

$$au + nv = 1$$

On multiplie par b :

$$abu + nbv = b$$

Or

$$n \mid ab$$

Donc

$$n \mid abu$$

De plus

$$n \mid nbv$$

Donc

$$n \mid abu + nbv$$

i.e.

$$n \mid b$$

■

corollaire 2.15

Si $d \mid a$, $d \mid b$ *et* $\text{pgcd}(n, d) = 1$ *alors*

$$a \equiv b \pmod{n} \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{n}$$

preuve : $\Rightarrow$ Par hypothèse :

$$b - a = d(b' - a')$$
$$n \mid (b - a)$$

Donc

$$n \mid d(b' - a')$$

Or

$$\text{pgcd}(n, d) = 1$$

Donc

$$n \mid (b' - a')$$

i.e.

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{n}$$

$\Leftarrow$ Évident. ■

Pour $a \in \mathbf{Z}$, on note $\overline{a}$ la classe de a modulo n. Le représentant canonique de $\overline{a}$ est l'unique élément compris entre 0 et $n - 1$ congru à a modulo n. On choisit aussi quelquefois, pour n impair, l'unique élément compris entre $-\frac{n-1}{2}$ et $\frac{n-1}{2}$.

Maple

```
mod
mods
```

définition 2.6 (*anneau quotient $\mathbf{Z}/n\mathbf{Z}$*)

On quotiente $\mathbf{Z}$ par la relation $\equiv_{\text{modulo } n}$, on obtient ainsi $\mathbf{Z}/n\mathbf{Z}$. On définit sur $\mathbf{Z}/n\mathbf{Z}$:

- *la somme*
$$\overline{a} + \overline{b} = \overline{a+b}$$
- *le produit*
$$\overline{a} \times \overline{b} = \overline{a \times b}$$

Ces définitions ont bien un sens car $\equiv$ est stable par addition et multiplication. On identifie $\overline{a}$ et le représentant de $\overline{a}$. Les éléments de $\mathbf{Z}/n\mathbf{Z}$ sont donc les nombres compris entre 0 et $n-1$.

lemme 2.16

$a \in \mathbf{Z}/n\mathbf{Z}$ est inversible si et seulement si $\operatorname{pgcd}(a, n) = 1$.

preuve : $\Rightarrow$ $a \in \mathbf{Z}/n\mathbf{Z}$ a un inverse signifie qu'il existe $a' \in \mathbf{Z}/n\mathbf{Z}$ tel que $aa' \equiv 1 \pmod n$. Donc
$$n \mid \left(aa' - 1\right)$$
i.e.
$$aa' - 1 = nd$$
i.e.
$$aa' - nd = 1$$
d'après le théorème de Bézout, cela signifie que
$$\operatorname{pgcd}(a, n) = 1$$

$\Leftarrow$ D'après le théorème de Bézout, il existe $u, v \in \mathbf{Z}$ tels que
$$au + nv = 1$$
D'où
$$\overline{au + nv} = \overline{1}$$
i.e.
$$\overline{au} = \overline{1}$$
ainsi a est inversible. ∎

Résolution de $ax \equiv b \pmod n$

1. Si $\operatorname{pgcd}(a, n) = 1$, a est inversible
$$a^{-1}ax \equiv a^{-1}b \pmod n$$
i.e.
$$x \equiv a^{-1}b \pmod n$$
$$x = a^{-1}b \bmod n$$

2. Sinon $\operatorname{pgcd}(a, n) = d > 1$
   - Si $d \nmid b$, pas de solutions
     En effet, sinon on a
     $$ax = b + kn$$
     i.e.
     $$b = ax - kn$$
     et d divise le membre de droite mais pas celui de gauche : absurde.
   - Si $d \mid b$, l'équation devient
     $$\frac{a}{d}x \equiv \frac{b}{d} \left(\bmod \frac{n}{d}\right)$$
     et on se ramène au premier cas.

Maple

```
msolve(ax=b,n);
```

Système de congruences
A matrice carrée à coefficients entiers, b vecteurs à coefficients entiers

$$AX \equiv b \pmod n$$

On a

$$\det A \in \mathbf{Z}$$

Si $\operatorname{pgcd}(\det A, n) = 1$, le système admet une unique solution modulo n.
La méthode du pivot de Gauss s'avère difficile à appliquer systématiquement.

2.6 $\mathbf{Z}/p\mathbf{Z}$, p premier

Si p est un nombre premier, $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ est un corps. ${\mathbf{F}_p}^\star$ est un groupe multiplicatif.

théorème 2.17

Le groupe ${\mathbf{F}_p}^\star$ est cyclique, c'est-à-dire qu'il existe $g \in \mathbf{F}_p$ générateur (ou racine primitive) tel que

$$\{1, \ldots, p-1\} = \left\{g \bmod p, \ldots, g^{p-1} \bmod p\right\}$$

Maple

```
primroot
```

exemple : Considérons $\mathbf{F}_7$

$$p = 7$$
$$g = 3$$
$$g^2 = 9 = 2$$

$$g^3 = 6$$
$$g^4 = 4$$
$$g^5 = 5$$
$$g^6 = 1$$

proposition 2.18

Si g est un générateur de $\mathbf{F}_p$, les autres générateurs sont les g^a tels que $\text{pgcd}(a, p-1) = 1$.

exemple :

$$p - 1 = 6$$
$$a = 1 \text{ ou } a = 5$$

théorème 2.19 (*Lucas*)

Soit n un entier strictement positif et a tel que $a^{n-1} \equiv 1 \pmod n$.
On suppose que pour tout nombre premier q divisant $n-1$,

$$a^{\frac{n-1}{q}} \not\equiv 1 \pmod n$$

Alors n est premier et a est un générateur de $\mathbf{F}_n$.

preuve : On a

$$a^{n-1} \equiv 1 \pmod n$$

Donc a est inversible et $\text{pgcd}(a, n) = 1$.
Notons $\text{ord}(a)$ l'ordre de a.
On a $\text{ord}(a) \mid n-1$
Soit la décomposition de $n-1$ en facteurs premiers

$$n - 1 = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$$

Comme

$$\text{ord}(a) \mid n - 1$$

On a

$$\text{ord}(a) = p_1^{\beta_1} \cdots p_n^{\beta_n}, \text{avec } \forall i, \beta_i \leq \alpha_i$$

Supposons

$$\text{ord}(a) \neq n - 1$$

Alors il existe i_0 tel que $\beta_{i_0} < \alpha_{i_0}$
Mais alors

$$\text{ord}(a) \mid \frac{n-1}{p_{i_0}}$$

C'est-à-dire

$$a^{\frac{n-1}{p_{i_0}}} \equiv 1 \pmod n$$

C'est absurde, car cela contredit l'hypothèse.
Donc $\text{ord}(a) = n - 1$.
Les éléments $a, a^2, \ldots, a^{n-1}$ sont donc distincts deux à deux et inversibles.
Donc $\mathbf{F}_n$ est un corps, n est premier et a est générateur. ∎

Remarque Il faut connaitre les facteurs premiers de $n-1$.

Recherche d'un générateur
Il n'existe pas (encore) de méthodes pour construire un générateur de $\mathbf{F}_p$.
En pratique, on essaie $a=2, a=3$, les carrés ne peuvent pas être générateurs, $a=5, a=6, \ldots$
Sous l'hypothèse de Riemann généralisé, on peut montrer qu'il existe un générateur g de $\mathbf{F}_p$ tel que $g \leq 2\log(p)^2$.

On sait construire des grands nombres premiers avec un générateur connu. En revanche, on ne sait pas trouver un générateur pour des nombres premiers p à plus de 160 chiffres. Le problème est la factorisation de $p-1$.

Construction des grands nombres premiers
On suppose connu k nombre premiers $q_1, \ldots, q_k$.
On pose $M = q_1 \cdots q_k$ de telle manière que M ait à peu près la taille souhaitée.
On pose $n = \lambda M + 1$ avec λ petit entier.
On connait les facteurs premiers de $n-1$.

$$\Pi(x) = \mathrm{card}(\{p \text{ premier} | p \leq x\})$$

$$\Pi(x) \sim \frac{x}{\log x}$$

Au voisinage de x, la probabilité de trouver un nombre premier est environ $\frac{1}{\log x}$.
Si on choisit $\log x$ nombres, il y aura probablement un nombre premier.
Si $n = 10^{100}$, $\log n \approx 230$.
On fait varier λ entre 1 et 1000, et on élimine les n qui sont multiples de $2, 3, 5, \ldots, p$ premier ≤ 1000.

2.7 Polynômes irréductibles

Si $\mathbf{K}$ est un corps, $\mathbf{K}[X]$ désigne l'anneau des polynômes sur $\mathbf{K}$.

définition 2.7 (*polynôme irréductible sur* K)

$P \in \mathbf{K}[X]$ est irréductible si pour tout $A, B \in \mathbf{K}[X]$ tels que $\deg A \geq 1$ et $\deg B \geq 1$, $P \neq AB$

- Dans $\mathbf{C}[X]$,
  les polynômes irréductibles sont exactement ceux de degré 1.
- Dans $\mathbf{R}[X]$,
  les polynômes irréductibles sont
  1. ceux de degré 1
  2. ceux de degré 2 à discriminant strictement négatif
- Dans $\mathbf{Q}[X]$,
  c'est beaucoup plus compliqué !

Exercice 2.2 — *Majoration des racines d'un polynôme*

Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbf{C}[X]$.
Soit $z_1, \ldots, z_n \in \mathbf{C}$ les racines de P avec $\mid z_1 \mid \leq \cdots \leq \mid z_n \mid = M$.
Soit $Q = X^n - \mid a_{n-1} \mid X^{n-1} - \cdots - \mid a_0 \mid$

1) Montrer que si les a_i ne sont pas tous nuls, Q admet une unique racine réelle strictement positive, que l'on notera r.

2) Montrer que $M \leq r$

3) Montrer que $M \leq 1 + \max\limits_{0 \leq k \leq n-1} \mid a_k \mid$

solution page 103

On va s'intéresser dans la suite aux polynômes irréductibles sur $\mathbf{F}_p[X]$.

exemple :

$$p = 2$$

– degré 1

$$\begin{array}{c} X \\ X+1 \end{array}$$

– degré 2

$$\begin{array}{c} X^2 \\ X^2+1 \\ X^2+X \\ X^2+X+1 \end{array}$$

– degré 3

$$\begin{array}{c} X^3 \\ X^3+1 \\ X^3+X \\ X^3+X^2 \\ X^3+X+1 \\ X^3+X^2+1 \\ X^3+X^2+X \\ X^3+X^2+X+1 \end{array}$$

définition 2.8 ($I_{n,p}$)

On note $I_{n,p}$ le nombre de polynômes irréductibles unitaires sur $\mathbf{F}_p$ de degré n.

exemple :

$$I_{1,2} = 2$$
$$I_{2,2} = 1$$
$$I_{3,2} = 2$$

théorème 2.20 (*Lemme combinatoire*)

Soit $a_1, \ldots, a_k$ des entiers positifs non nuls. On note $\mathrm{N}(n)$ le nombre de solutions entières de l'équation

$$a_1x_1 + \cdots + a_kx_k = n$$

Alors

$$\sum_{n=0}^{+\infty} \mathrm{N}(n)X^n = \prod_{i=1}^{k} \frac{1}{1 - X^{a_i}}$$

preuve : pour $k = 3$

$$\begin{aligned}
\frac{1}{1-X^{a_1}} &= 1 + X^{a_1} + X^{2a_1} + \cdots + X^{ra_1} + \cdots \\
\frac{1}{1-X^{a_2}} &= 1 + X^{a_2} + X^{2a_2} + \cdots + X^{sa_2} + \cdots \\
\frac{1}{1-X^{a_3}} &= 1 + X^{a_3} + X^{2a_3} + \cdots + X^{ta_3} + \cdots \\
\prod_{i=1}^{3} \frac{1}{1-X^{a_i}} &= \sum_{n=0}^{+\infty} X^n \left(\sum_{ra_1+sa_2+ta_3=n} 1 \right)
\end{aligned}$$

■

théorème 2.21

$$\sum_{n=0}^{+\infty} p^n X^n = \prod_{m=1}^{+\infty} \left(\frac{1}{1-X^m} \right)^{I_{m,p}}$$

preuve : On note $I_n = I_{n,p}$.

Tout polynôme unitaire de $\mathbf{F}_p[X]$ s'écrit de façon unique comme produit de polynômes irréductibles.

Soit

$$\begin{array}{rl}
P_1, \ldots, P_{I_1} & \text{les polynômes irréductibles de degré 1} \\
P_{I_1+1}, \ldots, P_{I_1+I_2} & \text{les polynômes irréductibles de degré 2} \\
\vdots & \\
P_{I_1+\cdots+I_{m-1}+1}, \ldots, P_{I_1+\cdots+I_m} & \text{les polynômes irréductibles de degré m}
\end{array}$$

Soit P un polynôme unitaire de degré $n \leq m$.

P s'écrit :

$$P = P_1^{\alpha_1} \cdots P_{I_1}^{\alpha_{I_1}} \cdots P_{I_1+\cdots+I_m}^{\alpha_{I_1+\cdots+I_m}}$$

avec

$$\begin{aligned}
n &= \deg P \\
&= \alpha_1 + \cdots + \alpha_{I_1} + 2\alpha_{I_1+1} + \cdots + 2\alpha_{I_1+I_2} + \cdots \\
&\quad \cdots + m\alpha_{I_1+\cdots+I_{m-1}+1} + \cdots + m\alpha_{I_1+\cdots+I_m}
\end{aligned}$$

Combien y a-t-il de solutions ?

Si on note a_n le nombre de polynômes unitaires de degré n dont tous les facteurs irréductibles sont de degré inférieur à m, on obtient en appliquant le lemme combinatoire

$$\sum_{n=0}^{+\infty} a_n X^n = \left(\frac{1}{1-X} \right)^{I_1} \left(\frac{1}{1-X^2} \right)^{I_2} \cdots \left(\frac{1}{1-X^m} \right)^{I_m}$$

Si $n \leq m$, $a_n = p^n$ est le nombre de polynômes unitaires de degré n.

D'où

$$\sum_{n=0}^{+\infty} p^n X^n = \prod_{m=1}^{+\infty} \left(\frac{1}{1-X^m} \right)^{I_{m,p}}$$

■

théorème 2.22

$$\sum_{d|n} dI_{d,p} = p^n$$

preuve : La formule du théorème précédent s'écrit :

$$\frac{1}{1-pX} = \prod_{m=1}^{+\infty} \left(\frac{1}{1-X^m}\right)^{I_{m,p}}$$

On passe aux dérivées logarithmiques :

$$\frac{-p}{1-pX} = \sum_{m=1}^{+\infty} I_m \frac{-mX^{m-1}}{1-X^m}$$

i.e.

$$\frac{pX}{1-pX} = \sum_{m=1}^{+\infty} \frac{mI_mX^m}{1-X^m}$$

c'est-à-dire

$$pX\left(1+pX+p^2X^2+\cdots\right) = \sum_{m=1}^{+\infty} mI_mX^m\left(1+X^m+X^{2m}+\cdots\right)$$

Le coefficient de X^n dans la formule de gauche est p^n et dans la formule de droite est $\sum\limits_{m|n} mI_m$.

D'où

$$\sum_{d|n} dI_{d,p} = p^n$$

■

théorème 2.23

$$I_{n,p} = \frac{1}{n}\sum_{d|n} \mu(d)p^{\frac{n}{d}}$$

preuve : On utilise la formule d'inversion de Möbius et le théorème précédent. ■

corollaire 2.24

$$\frac{1}{n}\left(p^n - 2p^{\frac{n}{2}}\right) \leq I_{n,p} \leq \frac{1}{n}p^n$$

corollaire 2.25

$$\forall n \in \mathbf{N} \setminus \{0\}, \forall p \text{ premier}, I_{n,p} \geq 1$$

Exercice 2.3 — *Méthode de Hensel*

Soit $P \in \mathbf{Z}[X]$, p un nombre premier et $x_0 \in \mathbf{Z}$ tel que

$$\begin{cases} \mathrm{P}(x_0) \equiv 0 \pmod{p} \\ \mathrm{P}'(x_0) \not\equiv 0 \pmod{p} \end{cases}$$

Montrer que

$$\forall n \in \mathbf{N}, \exists! x \text{ modulo } p^n \mid \begin{cases} x \equiv x_0 \pmod{p} \\ \mathrm{P}(x) \equiv 0 \pmod{p^n} \end{cases}$$

solution page 104

2.8 Construction des corps finis

2.8.1 $\mathbf{F}_9$

Les éléments de $\mathbf{F}_9$ sont les $a + bi$, avec $a, b \in \mathbf{F}_3$, et $i = \sqrt{-1}$. On obtient ainsi 9 éléments.

On définit ensuite les opérations de base :

– addition

$$a + bi + (a' + b'i) = a + a' + (b + b')i$$

– multiplication

$$(a + bi)(a' + b'i) = aa' - bb' + (ab' + a'b)i$$

– division

$$\frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2}$$

Or

$$a^2 + b^2 \equiv 0 \pmod{3} \Leftrightarrow a \equiv b \equiv 0 \pmod{3}$$

Donc si a, b non nuls, $\frac{1}{a^2+b^2}$ existe dans $\mathbf{F}_3$.

$$\frac{1}{a + bi} = a\big(a^2 + b^2\big)^{-1} - b\big(a^2 + b^2\big)^{-1} i$$

Or si $\mathbf{K}$ est un corps fini, alors $\mathbf{K}^\star = \mathbf{K} \setminus \{0\}$ est un groupe multiplicatif cyclique.

$g = 1 + i$ est générateur de $\mathbf{F}_9$. Les autres générateurs sont les g^a avec $\mathrm{pgcd}(a, 8) = 1$, c'est-à-dire g^3, g^5 et g^7.

2.8.2 Cas général

Soit p premier et $n \geq 2$.

Il existe un polynôme irréductible unitaire sur $\mathbf{F}_p$ de degré n (car $I_{n,p} \geq 1$).

Soit $\mathrm{f}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ un tel polynôme ($a_i \in \mathbf{F}_p$).

Soit α une racine (complexe) de f, i.e. $\mathrm{f}(\alpha) = 0$.

On définit $\mathbf{K} = \mathbf{F}_{p^n}$ comme l'ensemble des éléments de la forme

$$b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0, \text{ avec } b_i \in \mathbf{F}_p$$

On définit ensuite les opérations de base :

– addition

$$\begin{array}{rl} & b_{n-1}\alpha^{n-1}+\cdots+b_1\alpha+b_0+\left(c_{n-1}\alpha^{n-1}+\cdots+c_1\alpha+c_0\right) \\ = & \underbrace{\left(b_{n-1}+c_{n-1}\right)}_{\text{calculé dans } \mathbf{F}_p}\alpha^{n-1}+\cdots+\underbrace{\left(b_0+c_0\right)}_{\text{calculé dans } \mathbf{F}_p} \end{array}$$

– multiplication

$$\begin{array}{rcl} \alpha^n & = & -a_{n-1}\alpha^{n-1}-\cdots-a_1\alpha-a_0 \\ \alpha^{n+1} & = & -a_{n-1}\alpha^n-\cdots-a_1\alpha^2-a_0\alpha \\ & = & -a_{n-1}\left(-a_{n-1}\alpha^{n-1}-\cdots-a_1\alpha-a_0\right)-\cdots-a_0\alpha \end{array}$$

On précalcule $\alpha^n, \alpha^{n+1}, \ldots, \alpha^{2n-2}$ en fonction de $1, \alpha, \ldots, \alpha^{n-1}$.

$$\begin{array}{rl} & \left(b_{n-1}\alpha^{n-1}+\cdots+b_1\alpha+b_0\right)\times\left(c_{n-1}\alpha^{n-1}+\cdots+c_1\alpha+c_0\right) \\ = & \text{polynôme en } \alpha \text{ de degré inférieur à } 2n-2 \end{array}$$

On y remplace donc $\alpha^n, \alpha^{n+1}, \ldots, \alpha^{2n-2}$ par leurs valeurs et on trouve

$$d_{n-1}\alpha^{n-1}+\cdots+d_1\alpha+d_0$$

– inverse
Soit $\mathrm{Q}(\alpha)=b_{n-1}\alpha^{n-1}+\cdots+b_1\alpha+b_0$
Si $\mathrm{Q}(\alpha)\neq 0$, Q est premier avec f, on peut donc appliquer Bezout. En prenant la valeur en α, on obtient :

$$\begin{array}{c} \mathrm{Q}(\alpha)\mathrm{u}(\alpha)+\mathrm{f}(\alpha)\mathrm{v}(\alpha)=1 \\ \deg u<\deg f \\ \deg v<\deg Q \end{array}$$

i.e.

$$\mathrm{Q}(\alpha)\mathrm{u}(\alpha)=1$$

$\mathrm{u}(\alpha)$ est un inverse de $\mathrm{Q}(\alpha)$.

On cherche alors un générateur g, c'est-à-dire un élément tel que $g^{p^n-1}=1$ et pour tout q nombre premier divisant p^n-1, $g^{\frac{p^n-1}{q}}\neq 1$.

On calcule alors la table donnant pour chaque élément x son logarithme discret en base g, c'est-à-dire le a compris entre 0 et p^n-1 tel que $x=g^a$.

Les éléments du groupe multiplicatif sont :

$$g, g^2, \ldots, g^{p^n-1}$$

Il est commode d'utiliser la fonction de Zech tel que $g^a+1=g^{\lambda(a)}$.
$\lambda(a)$ n'est pas définie pour $g^a=-1$, c'est-à-dire pour $a=\frac{p^n-1}{2}$.
Dans cette représentation, les opérations deviennent :
– multiplication

$$g^a g^b=g^{a+b \bmod (p^n-1)}$$

– addition
Si $a\geq b$

$$g^a+g^b=g^b\left(g^{a-b}+1\right)=g^b g^{\lambda(a-b)}=g^{b+\lambda(a-b)}$$

2.9 Propriétés des corps finis

On se place dans le corps $\mathbf{K} = \mathbf{F}_{p^n}$.
Tout $a \in \mathbf{K}^\star$ vérifie $a^{p^n-1} = 1$.
On a donc

$$X^{p^n-1} - 1 = \prod_{a \in \mathbf{K}^\star} (X - a)$$

théorème 2.26

On note K_p^d l'ensemble des polynômes irréductibles unitaires de degré d sur $\mathbf{F}_p$.

$$X^{p^n} - X = \prod_{d|n} \prod_{Q \in K_p^d} Q$$

Remarque En passant au degré dans le théorème précédent, on retrouve

$$p^n = \sum_{d|n} d I_{d,p}$$

théorème 2.27

Deux corps finis à p^n éléments sont isomorphes.

Soit deux polynômes irréductibles unitaires f_1 et f_2 de degré n sur $\mathbf{F}_p$. On peut construire deux corps $\mathbf{K}_1$ et $\mathbf{K}_2$ avec f_1 et f_2. Le théorème précédent nous dit qu'il existe $\sigma : \mathbf{K}_1 \to \mathbf{K}_2$ bijection tel que :

$$\begin{array}{rcl} \sigma(a+b) & = & \sigma(a) + \sigma(b) \\ \sigma(a \times b) & = & \sigma(a) \times \sigma(b) \end{array}$$

Choix de f le plus simple possible

$$\text{Si } p = 2, f_n = x^n + x + 1$$

Existe-t-il une infinité de n avec f_n irréductible ?

définition 2.9 (*Frobénius*)

Dans $\mathbf{K} = \mathbf{F}_{p^n}$, on définit le Frobénius σ par

$$\sigma : \begin{array}{ccc} \mathbf{F}_{p^n} & \to & \mathbf{F}_{p^n} \\ x & \mapsto & x^p \end{array}$$

Lemme 2.28

Dans $\mathbf{K} = \mathbf{F}_{p^n}$, le Frobénius est un morphisme de corps.

preuve :

$$\sigma(xy) = (xy)^p = x^p y^p = \sigma(x)\sigma(y)$$
$$\sigma(x+y) = x^p + y^p + \sum_{k=1}^{p-1} \mathrm{C}_p^k x^k y^{p-k} = x^p + y^p = \sigma(x) + \sigma(y)$$

Car $p \mid \mathrm{C}_p^k$ pour $k = 1, \ldots, p-1$. ■

Dans **K**, le polynôme irréductible f qui a servi à construire **K** se décompose en facteurs de degré 1. En effet, si α est une racine de f, les autres racines sont $\alpha^2, \ldots, \alpha^{p^n-1}$ car si α est racine, α^p est aussi racine.

$$\mathrm{f}(\alpha^p) = \mathrm{f}(\alpha)^p = 0$$

Construction de $\mathbf{F}_8$

$$\mathrm{f}(x) = x^3 + x + 1$$

α racine de f est générateur, en effet :

$$\begin{gathered} \alpha \\ \alpha^2 \\ \alpha^3 = \alpha + 1 \\ \alpha^4 = \alpha^2 + \alpha \\ \alpha^5 = \alpha^2 + \alpha + 1 \\ \alpha^6 = \alpha^2 + 1 \\ \alpha^7 = 1 \end{gathered}$$

$$\begin{aligned} X^8 - X &= \prod_{d \mid 3} \prod_{Q \in K_2^d} Q \\ &= X(X+1)\big(X^3+X+1\big)\big(X^3+X^2+1\big) \text{sur } \mathbf{F}_2 \end{aligned}$$

Mais

$$X^3 + X + 1 = (X+\alpha)\big(X+\alpha^2\big)\big(X+\alpha^4\big)$$
$$X^8 - X = X(X+\alpha)\big(X+\alpha^2\big)\cdots\big(X+\alpha^7\big)$$

Donc

$$X^3 + X^2 + 1 = \big(X+\alpha^3\big)\big(X+\alpha^6\big)\left(X + \underbrace{\alpha^{12}}_{=\alpha^5}\right)$$

Si on avait choisi $\mathrm{f}(x) = x^3 + x^2 + 1$

$$\beta^3 = \beta^2 + 1$$

$$\beta = \alpha^3$$

troisième chapitre

Codes correcteurs d'erreurs

3.1 Introduction

Un message $M = m_1, \ldots, m_k$ est un mot sur un alphabet fini quelconque. Nous nous restreindrons à l'alphabet $\{0, 1\}$.

Problème Le message est envoyé de A à B. Lors de la transmission ce message est altéré, B reçoit $\bar{M} = \bar{m}_1, \ldots, \bar{m}_k$. On note r le pourcentage d'erreurs. Pour $k(1-r)$ indices i, on a $\bar{m}_i = m_i$ et pour les autres, $\bar{m}_i \neq m_i$.

Modélisation On considérera que sur k bits consécutifs, il y a aura au plus e erreurs. On choisit $\frac{e}{k} = r$. Pour corriger les éventuelles erreurs de transmission, on envoie des messages redondants.

Exemple du code répétition Dans ce code, on duplique chaque lettre du message d fois. Ainsi, dans le cas où $k = 1$ et si l'on envoie 3 fois la lettre, on a :

$$m, m, m \to \bar{m}_1, \bar{m}_2, \bar{m}_3$$

Si l'on suppose qu'il y a au plus une erreur sur les 3 bits, on déchiffre $\bar{m}_1, \bar{m}_2, \bar{m}_3$ à la majorité absolue.

$$\begin{array}{ccc} 000 & \to & m = 0 \\ 001 & \to & m = 0 \\ 011 & \to & m = 1 \\ 111 & \to & m = 1 \end{array}$$

Si on répète la lettre 5 fois, on pourra corriger 2 erreurs sur 5 bits. L'inconvénient de cette méthode est que le message produit est très long.

3.2 Le code de Hamming $7-4$

Dans ce code, il y a :
- 4 bits d'information a, b, c, d
- 3 bits de redondance x, y, z

définition 3.1 (*matrice de contrôle (parity check matrice)*)

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Cette matrice est obtenue en écrivant de bas en haut et en binaire les chiffres de 1 à 7.

Le code de Hamming $7-4$ noté $\mathcal{C}$ est une partie $\mathbf{F}_2{}^7$. Concrètement,

$$C=(x,y,a,z,b,c,d)\in\mathcal{C}\Leftrightarrow H^tC=0$$

Les bits x,y et z de redondance sont définis par :

$$\left\{\begin{array}{lcll} x & = & a+b+d & \pmod 2 \\ y & = & a+c+d & \pmod 2 \\ z & = & b+c+d & \pmod 2 \end{array}\right.$$

Si l'on veut transmettre le message $M=(a,b,c,d)$, on calcule $C=(x,y,a,z,c,d)$ et on envoie C. Le receveur reçoit $R=C+E$.

$$E=\left\{\begin{array}{ll} 0 & \\ e_i & \text{erreur sur le } i^{\text{ème}} \text{ bit} \end{array}\right.$$

Le receveur calcule le syndrome S.

$$\begin{array}{rcl} S & = & H^tR \\ & = & H^tC+H^tE \\ & = & \left\{\begin{array}{c} 0 \\ H^te_i \end{array}\right. \end{array}$$

En faisant l'hypothèse qu'il y a au plus une erreur dans les 7 bits, on peut déduire que :
- Si $S=0$, alors il n'y a pas d'erreur.
- Si $S=\begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix}\neq 0$, alors il y a une erreur sur le $4s_3+2s_2+s_1$-ième bit.

3.3 Le code de Hamming $8-4$

Ce code permet de corriger une erreur et d'en détecter deux. Dans ce code, il y a :
- 4 bits d'information a,b,c et d.
- 4 bits de redondance x,y,z et w.

définition 3.2 (*matrice de contrôle*)

$$H=\begin{pmatrix} 1&1&1&1&1&1&1&1 \\ 0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&0&1&1 \\ 0&0&0&0&1&1&1&1 \end{pmatrix}$$

H_{8-4} s'obtient à partir de H_{7-4} en rajoutant une ligne de 1 et en complétant avec une colonne de 0.

Le code de Hamming $8-4$ noté $\mathcal{C}$ est une partie de $\mathbf{F}_2{}^8$ définie par

$$C=(w,x,y,a,z,b,c,d)\in\mathcal{C}\Leftrightarrow H^tC=0$$

Les bits redondants sont calculés par :

$$\left\{\begin{array}{lllll} x & = & a+b+d & \pmod 2 \\ y & = & a+c+d & \pmod 2 \\ z & = & b+c+d & \pmod 2 \\ w & = & a+b+c & \pmod 2 \end{array}\right.$$

Le procédé est identique au précédent. L'envoyeur calcul w, x, y et z puis envoie C. Le receveur reçoit $R = C + E$ où,

$$E = \left\{\begin{array}{cc} 0 & \\ e_i & \text{erreur sur le } i^{\text{ème}} \text{ bit} \\ e_i + e_j & \text{avec } i \neq j \end{array}\right.$$

Il calcule le syndrome S.

$$\begin{array}{rcl} S & = & H^t R \\ & = & H^t C + H^t E \\ & = & \left\{\begin{array}{c} 0 \\ H^t e_i = h_i \\ H^t(e_i + e_j) = h_i + h_j \end{array}\right. \end{array}$$

S'il y a 0 ou 2 erreurs, $s_1 = 0$.

- Si $S = 0$, alors il n'y a pas d'erreurs
- Sinon $S = \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s4 \end{pmatrix} \neq 0$
  - Si $s_1 = 1$, il y a une erreur en $i = 4s_4 + 2s_3 + s_2$.
  - Si $s_1 = 0$, il y a deux erreurs.

3.4 Distance de Hamming

définition 3.3 (*Distance de Hamming*)

Soit $V = (v_1, \ldots, v_n) \in \mathbf{F}_2{}^n$ et $W = (w_1, \ldots, w_n) \in \mathbf{F}_2{}^n$. On définit la distance de Hamming de V à W par

$$\delta(V, W) = \sum_{i=1}^{n} \mid v_i - w_i \mid$$

(calculé dans $\mathbf{R}$).

C'est bien une distance.

Remarque Dans $\mathbf{R}^n$, il y a trois distances classiques :

- $\| (x_1, \ldots, x_n) \|_\infty = \max_{1 \leq i \leq n} | x_i |$
- $\| (x_1, \ldots, x_n) \|_1 = \sum_{1=i}^{n} | x_i |$
- $\| (x_1, \ldots, x_n) \|_2 = \sqrt{\sum_{1=i}^{n} x_i^2}$

On peut voir ${\mathbf{F}_2}^n$ comme une partie de $\mathbf{R}^n$ (ce sont les points à coordonnées 0 ou 1). La distance de Hamming sur ${\mathbf{F}_2}^n$ est la trace de $\| \,.\, \|_1$.

définition 3.4 (*Poids d'un élément*)

On définit le poids de $V = (v_1, \ldots, v_n) \in {\mathbf{F}_2}^n$ par

$$\mathrm{w}(V) = \sum_{i=1}^{n} v_i = \delta(V, 0)$$

.

Remarque On a $\delta(V, W) = \mathrm{w}(V + W)$.

définition 3.5 (*Code, code linéaire*)

Un code $\mathcal{C}$ de longueur n et de dimension k est une partie à 2^k éléments de ${\mathbf{F}_2}^n$.

Un code linéaire de longueur n et de dimension k est un sous-espace vectoriel de dimension k de ${\mathbf{F}_2}^n$.

exemple : Le code de Hamming $7-4$ est un code linéaire de longueur 7 et de dimension 4. Il y a $2^4 = 16$ messages distincts.

définition 3.6 (*Distance minimale d'un code $\mathcal{C}$*)

C'est $d = \min_{V \neq W \in \mathcal{C}} \delta(V, W)$.

Si $\mathcal{C}$ est linéaire, on a $d = \min_{V \in \mathcal{C} \setminus \{0\}} \mathrm{w}(V)$.

exemple : Pour le code de Hamming $7-4$, $d = 3$.

théorème 3.1

Un code $\mathcal{C}$ de distance minimale d corrige $t = \lfloor \frac{d-1}{2} \rfloor$ erreurs.

preuve : On suppose que $\mathcal{C}$ corrige e erreurs.

Par définition de d, les boules de rayon t centrées sur les mots du code $\mathcal{C}$ sont disjointes. En effet, supposons avoir un $w \in {\mathbf{F}_2}^n$ et $u, v \in \mathcal{C}$ tels que $\delta(u, w) \leq t$ et $\delta(v, w) \leq t$. Alors $\delta(u, v) \leq \delta(u, w) + \delta(w, v) < 2t < d$, absurde.

Donc, si le mot reçu v a subi moins de t erreurs, il existe un unique mot u de $\mathcal{C}$ tel que $\delta(u, v) \leq t$ et on décode alors v par u de manière sure. On peut donc corriger au moins t erreurs, i.e. $e \geq t$.

On a $e \leq t$ car sinon, il existe deux mots $u, v \in \mathcal{C}$ qui ont leur $(t+1)^{\text{ème}}$ orbite non disjointes, ce qui entraine qu'on ne sait pas décoder les mots se trouvant dans l'intersection. ■

3.5 Codes parfaits

Un code linéaire $\mathcal{C}$ de longueur n, de dimension k est un sous-espace vectoriel de dimension k de $\mathbf{F}_2{}^n$. Il y a 2^k mots de code. Si ce code corrige e erreurs, les orbites d'ordre $1, 2, \ldots, e$ sont disjointes.

D'où

$$\left(1 + \mathrm{C}_n^1 + \mathrm{C}_n^2 + \cdots + \mathrm{C}_n^e\right) \times 2^k \leq 2^n$$

$\mathcal{C}$ est dit parfait quand il y a égalité dans l'inégalité précédente.

Si le code n'est pas parfait, il y a des mots de $\mathbf{F}_2{}^n$ qui ne sont dans aucune orbite : c'est le no man's land.

exemple : Le code de Hamming $7-4$ est parfait.

En effet, $k = 4$ donc il y a 16 mots de code.

Ce code corrige une erreur, il y a donc une seule orbite par mot de code. L'orbite contient $\mathrm{C}_7^1 = 7$ éléments.

On a $(1+7) \times 16 = 128 = 2^7$.

3.6 Code BCH $7-4$

On se place dans $\mathbf{F}_8$ généré par le polynome $P = X^3 + X + 1$.

Soit α une racine de P.

On vérifie que α est générateur de $\mathbf{F}_8$.

Lemme 3.2

Soit $A \in \mathbf{F}_2[X]$.
On suppose que $\mathrm{A}(\alpha) = 0$ dans $\mathbf{F}_8$.
Alors A est multiple de $X^3 + X + 1$ dans $\mathbf{F}_2[X]$.

Remarque Soit $P \in \mathbf{R}[X]$ tel que $\mathrm{P}(i) = 0$ dans $\mathbf{C}$, alors P est multiple de $X^2 + 1$ dans $\mathbf{R}[X]$.

preuve : On propose deux preuves différentes.

1. Comme $X^3 + X + 1$ est irréductible sur $\mathbf{F}_2$, $\mathrm{pgcd}\big(A, X^3 + X + 1\big)$ est soit 1 soit $X^3 + X + 1$.
   Si $\mathrm{pgcd}\big(A, X^3 + X + 1\big) = 1$, Bezout nous donne l'existence de deux polynomes U et V tels que $AU + \big(X^3 + X + 1\big)V = 1$. En prenant la valeur en α dans $\mathbf{F}_8$, on trouve $0 = 1$, c'est absurde.
   Donc $\mathrm{pgcd}\big(A, X^3 + X + 1\big) = X^3 + X + 1$, d'où $X^3 + X + 1 \mid A$.
2. En passant au Frobénius, on trouve que α^2 et α^4 sont aussi racines de A, donc A est multiple de $(X+\alpha)\big(X+\alpha^2\big)\big(X+\alpha^4\big)$, c'est-à-dire A est multiple de $X^3 + X + 1$. ■

Construction du code BCH $7-4$
Dans le code BCH[1] $7-4$, on a 4 bits d'informations : a_6, a_5, a_4, a_3. On leur associe le polynôme $C_1 = a_6X^6 + a_5X^5 + a_4X^4 + a_3X^3$.
Effectuons la division euclidienne de C_1 par $X^3 + X + 1$.
On a $C_1 = \left(X^3 + X + 1\right)Q + C_2$ avec $\deg C_2 \leq 2$.
C_2 s'écrit $C_2 = a_2X^2 + a_1X + a_0$.
Les bits de redondance sont a_0, a_1, a_2.
Le mot de code est $(a_6, a_5, a_4, a_3, a_2, a_1, a_0)$, soit aussi le polynôme $C = C_1 + C_2$.

théorème 3.3

$$C \in \mathcal{C} \Leftrightarrow \mathrm{C}(\alpha) = 0 \ (\textit{dans } \mathbf{F}_8)$$

preuve : $\Rightarrow$

$C = C_1 + C_2 = \left(X^3 + X + 1\right)Q$.
On a donc $\mathrm{C}(\alpha) = 0$.

$\Leftarrow$

Soit C tel que $\mathrm{C}(\alpha) = 0$
C s'écrit $C = a_6X^6 + \cdots + a_0$
Soit $C_1 = a_6X^6 + \cdots + a_3X^3$ et posons $C_2 = C - C_1$
$C_1 = \left(X^3 + X + 1\right)Q + \tilde{C_2}$
On a $\tilde{\mathrm{C}_2}(\alpha) = \mathrm{C}_1(\alpha)$
De plus $\mathrm{C}_2(\alpha) = \mathrm{C}(\alpha) - \mathrm{C}_1(\alpha) = \mathrm{C}_1(\alpha)$
Donc $\tilde{\mathrm{C}_2}(\alpha) = \mathrm{C}_2(\alpha)$
i.e. $\left(\tilde{\mathrm{C}_2} - \mathrm{C}_2\right)(\alpha) = 0$
D'après le lemme précédent, $X^3 + X + 1$ divise $\tilde{C_2} - C_2$.
Or $\deg\left(\tilde{C_2} - C_2\right) \leq 2$, donc $\tilde{C_2} = C_2$ et $C \in \mathcal{C}$. ∎

Le code BCH $7-4$ permet de corriger une erreur.
L'envoyeur a son message $a_6, \ldots, a_3$. Il calcule $C = a_6X^6 + \cdots + a_1X + a_0$.
Il envoie C.
Le receveur reçoit $R = C + E$ avec $\begin{cases} E = 0 & \text{pas d'erreur} \\ E = X^i & 0 \leq i \leq 6 \end{cases}$
Il calcule le syndrome $S = \mathrm{R}(\alpha) = \mathrm{C}(\alpha) + \mathrm{E}(\alpha) = \mathrm{E}(\alpha)$
S est un élément de $\mathbf{F}_8$, il s'écrit $S = s_2\alpha^2 + s_1\alpha + s_0$
- Si $S = 0$, pas d'erreur
- Sinon, $S \neq 0$, comme α générateur, $S = \alpha^i$ avec $0 \leq i \leq 6$. L'exposant de α donne la place de l'erreur.

Le code BCH $7-4$ est un code linéaire.
$\mathcal{C}$ est donc un sous-espace vectoriel de l'espace des polynômes de degré inférieur à 6 sur $\mathbf{F}_2[X]$

[1] Bose Chaudury Hocquengheim

Matrice de contrôle On exprime $\mathrm{C}(\alpha) = 0$ et on remplace α^3, α^4, α^5 et α^6 par leur valeur.

$$\begin{aligned}\mathrm{C}(\alpha) &= a_6\big(\alpha^2+1\big) + a_5\big(\alpha^2+\alpha+1\big) + a_4\big(\alpha^2+\alpha\big) + a_3(\alpha+1) + a_2\alpha^2 + a_1 \\ &= \alpha^2 \times (a_6+a_5+a_4+a_2) + \alpha \times (a_5+a_4+a_3+a_1) \\ &\qquad + 1 \times (a_6+a_5+a_3+a_0) \\ &= 0\end{aligned}$$

On en déduit

$$\begin{cases} a_6+a_5+a_4+a_2 &= 0 \\ a_5+a_4+a_3+a_1 &= 0 \\ a_6+a_5+a_3+a_0 &= 0 \end{cases}$$

D'où

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

On reconnait la matrice de contrôle du code de Hamming $7-4$ à une permutation des colonnes près.

3.7 Code BCH $15-11$

On se place dans $\mathbf{F}_{16}$ généré par le polynôme X^4+X+1.
Soit α une racine de P.
On vérifie que α est générateur de $\mathbf{F}_{16}$.

Construction du code BCH $15-11$
Dans le code BCH $15-11$, on a 11 bits d'informations : $a_{14}, a_{13}, \ldots, a_4$. On leur associe le polynôme $C_1 = a_{14}X^{14} + a_{13}X^{13} + \cdots + a_4X^4$.
On fait la division euclidienne de C_1 par X^4+X+1.
On a $C_1 = \big(X^4+X+1\big)Q + C_2$ avec $\deg C_2 \leq 3$.
C_2 s'écrit $C_2 = a_3X^3 + a_2X^2 + a_1X + a_0$.
Le mot de code est $(a_{14}, \ldots, a_0)$, soit aussi le polynôme $C = C_1 + C_2$.

théorème 3.4

$$C \in \mathcal{C} \Leftrightarrow \mathrm{C}(\alpha) = 0$$

Le code BCH $15-11$ permet de corriger une erreur.
L'envoyeur a son message $a_{14}, \ldots, a_4$. Il calcule $C = a_{14}X^{14} + \cdots + a_1X + a_0$.
Il envoie C.
Le receveur reçoit $R = C + E$ avec $\begin{cases} E = 0 & \text{pas d'erreur} \\ E = X^i & 0 \leq i \leq 14 \end{cases}$
Il calcule le syndrome $S = \mathrm{R}(\alpha) = \mathrm{C}(\alpha) + \mathrm{E}(\alpha) = \mathrm{E}(\alpha)$
S est un élément de $\mathbf{F}_{16}$

- Si $S = 0$, pas d'erreur
- Sinon, $S \neq 0$, comme α générateur, $S = \alpha^i$ avec $0 \leq i \leq 14$. L'exposant de α donne la place de l'erreur.

3.8 Code BCH $15-7$

Les racines dans $\mathbf{F}_{16}$ de X^4+X+1 sont $\alpha, \alpha^2, \alpha^4, \alpha^8$.
On cherche un polynôme irréductible de $\mathbf{F}_2[X]$ qui admet α^3 comme racine.
On sait que $\alpha^{15}=1$, c'est-à-dire $\left(\alpha^3\right)^5=1$.
α^3 annule le polynôme $X^5-1=(X-1)\left(1+X+X^2+X^3+X^4\right)$.
Comme $\alpha^3 \neq 1$, α^3 annule $1+X+X^2+X^3+X^4$, qui est irréductible.
On pose

$$\left\{\begin{array}{lll} M_1 & = & X^4+X+1 \\ M_3 & = & X^4+X^3+X^2+X+1 \end{array}\right.$$

Construction du code BCH $15-7$
Soit $M=M_1M_3$. M est de degré 8.
Dans le code BCH $15-7$, on a 7 bits d'informations : $a_{14}, a_{13}, \ldots, a_8$. On leur associe le polynôme $C_1=a_{14}X^{14}+a_{13}X^{13}+\cdots+a_8X^8$.
On fait la division euclidienne de C_1 par M.
On a $C_1=MQ+C_2$ avec $\deg C_2 \leq 7$.
C_2 s'écrit $C_2=a_7X^7+\cdots+a_1X+a_0$.
Le mot de code est $(a_{14}, \ldots, a_0)$, soit aussi le polynôme $C=C_1+C_2$.

théorème 3.5

$$C \in \mathcal{C} \Leftrightarrow \mathrm{C}(\alpha)=\mathrm{C}\left(\alpha^3\right)=0$$

Remarque Comme α est racine de $C \in \mathcal{C}$, en passant au Frobénius, α^2, α^4 et α^8 sont aussi racines de C. De même, puisque α^3 est racine de C, α^6, α^{12} et $\alpha^{24}=\alpha^9$ sont aussi racines de C.
On a donc

$$C \in \mathcal{C} \Rightarrow \mathrm{C}\left(\alpha^i\right)=0, 1 \leq i \leq 4$$

Le code BCH $15-7$ permet de corriger deux erreurs.
L'envoyeur a son message $a_{14}, \ldots, a_8$. Il calcule $C=a_{14}X^{14}+\cdots+a_1X+a_0$.
Il envoie C.

Le receveur reçoit $R=C+E$ avec $\left\{\begin{array}{cc} E=0 & \text{pas d'erreur} \\ E=X^i & \text{une erreur} \\ E=X^i+X^j & \text{deux erreurs} \end{array}\right.$

Il calcule le syndrome $S_t=\mathrm{R}(\alpha^t)=\mathrm{C}(\alpha^t)+\mathrm{E}(\alpha^t)=\mathrm{E}(\alpha^t)$ pour $t=1,2,3$.
Il calcule alors le polynôme $P=S_1X^2+S_2X+S_3+S_1S_2$.

- Si $E=0$, alors $S_t=0$ et $P=0$, pas d'erreur
- Sinon, si $E=X^i$, alors $S_t=\alpha^{it}$ et

$$P=\alpha^iX^2+\alpha^{2i}X+\underbrace{\alpha^{3i}+\alpha^i\alpha^{2i}}_{=0}=\alpha^iX\left(X+\alpha^i\right)$$

  P a donc une racine nulle et une autre racine α^i qui indique la place de l'erreur.
- Sinon, $E=X^i+X^j$,alors

- $S_1 = \alpha^i + \alpha^j$
- $S_2 = \alpha^{2i} + \alpha^{2j}$
- $S_3 = \alpha^{3i} + \alpha^{3j} = \big(\alpha^i + \alpha^j\big)\big(\alpha^{2i} + \alpha^{2j} + \alpha^i\alpha^j\big)$

$$\begin{array}{rcl} P & = & \big(\alpha^i + \alpha^j\big)X^2 + \big(\alpha^{2i} + \alpha^{2j}\big)X + \alpha^{3i} + \alpha^{3j} + \big(\alpha^i + \alpha^j\big)\big(\alpha^{2i} + \alpha^{2j}\big) \\ & = & \big(\alpha^i + \alpha^j\big)\big(X^2 + \big(\alpha^i + \alpha^j\big)X + \alpha^i\alpha^j\big) \\ & = & \big(\alpha^i + \alpha^j\big)\big(X + \alpha^i\big)\big(X + \alpha^j\big) \end{array}$$

P a deux racines α^i et α^j qui indiquent la place des erreurs.

Autre justification
Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbf{K}[X]$ et soit $x_1, \ldots, x_n$ ses racines dans une extension.

$$\begin{array}{rcl} \sigma_1 & = & x_1 + \cdots + x_n = -a_1 \\ \sigma_2 & = & x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = a_2 \\ & \vdots & \\ \sigma_n & = & x_1x_2\cdots x_n = (-1)^n a_n \end{array}$$

On pose $S_k = x_1^k + \cdots + x_n^k \in \mathbf{K}$ (sommes de Newton). On a

$$S_1 = \sigma_1 = -a_1$$

c'est-à-dire

$$S_1 + a_1 = 0$$

$$S_2 = \sigma_1^2 - 2\sigma_2 = -a_1S_1 - 2a_2$$

i.e.

$$S_2 + a_1S_1 + 2a_2 = 0$$

et plus généralement

- Pour $k \leq n$
$$S_k + a_1S_{k-1} + \cdots + a_{k-1}S_1 + ka_k = 0$$
- Pour $k > n$
$$S_k + a_1S_{k-1} + \cdots + a_nS_{k-n} = 0$$
- Si il y a deux erreurs, α^i et α^j sont racines du polynôme localisateur des erreurs.
$$\begin{array}{rcl} \sigma_1 & = & \alpha^i + \alpha^j \\ \sigma_2 & = & \alpha^i\alpha^j \\ S_t & = & \alpha^{it} + \alpha^{jt} \end{array}$$

D'après ce qui précède (on est en caractéristique 2, donc $\sigma_i = a_i$)

$$\left\{ \begin{array}{rcl} S_3 + \sigma_1S_2 + \sigma_2S_1 & = & 0 \\ S_4 + \sigma_1S_3 + \sigma_2S_2 & = & 0 \end{array} \right.$$

En posant

$$M = \begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix}$$

On a le système d'équations suivant :

$$M\begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_3 \\ S_4 \end{pmatrix}$$

Si il y a deux erreurs,

$$\begin{aligned}
\det M &= S_1S_3 - S_2^2 \\
&= \left(\alpha^i+\alpha^j\right)\left(\alpha^{3i}+\alpha^{3j}\right) - \left(\alpha^{2i}+\alpha^{2j}\right)^2 \\
&= \left(\alpha^i+\alpha^j\right)\Big(\alpha^{3i}+\alpha^{3j}+\left(\alpha^i+\alpha^j\right)^3\Big) \\
&= \left(\alpha^i+\alpha^j\right)\left(\alpha^{2i}\alpha^j+\alpha^i\alpha^{2j}\right) \\
&= \left(\alpha^i+\alpha^j\right)^2\alpha^i\alpha^j \\
&\neq 0
\end{aligned}$$

Ainsi M est inversible, on peut donc trouver σ_1 et σ_2 en résolvant le système précédent dans $\mathbf{F}_{16}$.

– S'il y a une seule erreur

$$M = \begin{pmatrix} \alpha^i & \alpha^{2i} \\ \alpha^{2i} & \alpha^{3i} \end{pmatrix}$$

$$\det M = 0$$

Or $M \neq 0$, donc $\mathrm{rg}(M) = 1$
On remarque d'ailleurs que le rang de M donne le nombre d'erreurs.
S'il y a une erreur, $\mathcal{C}(15-7) \subset \mathcal{C}(15-11)$, on peut donc décoder comme on le faisait pour le code BCH $15-11$.

Autre façon de décoder
Il y a en tout 2^{15} mots possibles et il y a 2^7 mots de code. On génère un tableau avec 2^{15} entrées, chaque entrée contient le mot de code le plus proche.

Le code BCH $15-7$ n'est pas parfait
En effet,

$$128(1+15+105) = 128 \times 121 < 128 \times 256$$

3.9 Code BCH $15-5$

La technique est la même que pour le code BCH $15-7$.

On cherche un polynôme irréductible qui admet α^5 comme racine. Le polynôme $X^3-1 = (X-1)\left(1+X+X^2\right)$ annule α^5. Le polynôme $1+X+X^2$ annule α^5 et est irréductible sur $\mathbf{F}_2$.

On pose

$$M_5 = X^2+X+1$$

Construction du code BCH $15-5$
Soit $M = M_1M_3M_5$. M est de degré 10.
Dans le code BCH $15-5$, on a 5 bits d'informations : $a_{14}, a_{13}, \ldots, a_{10}$. On leur associe le polynôme $C_1 = a_{14}X^{14} + a_{13}X^{13} + \cdots + a_{10}X^{10}$.
On fait la division euclidienne de C_1 par M.
On a $C_1 = MQ + C_2$ avec $\deg C_2 \leq 9$.
C_2 s'écrit $C_2 = a_9X^9 + \cdots + a_1X + a_0$.
Le mot de code est $(a_{14}, \ldots, a_0)$, soit aussi le polynôme $C = C_1 + C_2$.

théorème 3.6

$$C \in \mathcal{C} \Leftrightarrow \mathrm{C}(\alpha) = \mathrm{C}(\alpha^3) = \mathrm{C}(\alpha^5) = 0$$

Remarque

$$C \in \mathcal{C} \Rightarrow \mathrm{C}(\alpha^i) = 0, 1 \leq i \leq 6$$

Le code BCH $15-5$ permet de corriger trois erreurs.
L'envoyeur a son message $a_{14}, \ldots, a_{10}$. Il calcule $C = a_{14}X^{14} + \cdots + a_1 X + a_0$. Il envoie C.

Le receveur reçoit $R = C + E$ avec $\begin{cases} E = 0 & \text{pas d'erreur} \\ E = X^i & \text{une erreur} \\ E = X^i + X^j & \text{deux erreurs} \\ E = X^i + X^j + X^k & \text{trois erreurs} \end{cases}$

Il calcule le syndrome $S_t = \mathrm{R}(\alpha^t) = \mathrm{C}(\alpha^t) + \mathrm{E}(\alpha^t) = \mathrm{E}(\alpha^t)$ pour $1 \leq t \leq 6$.
Il calcule la matrice suivante

$$M = \begin{pmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{pmatrix}$$

Comme précédemment, le rang de M donne le nombre d'erreurs.

- Si $\mathrm{rg}(M) \leq 2$, on utilise le fait que $\mathcal{C}(15-5) \subset \mathcal{C}(15-7)$ et on décode avec les méthodes vues pour le code BCH $15-7$.
- Si $\mathrm{rg}(M) = 3$, il y a trois erreurs.
  Le receveur résout le système

  $$M \begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_4 \\ S_5 \\ S_6 \end{pmatrix}$$

  Il cherche alors les racines de

  $$X^3 + \sigma_1 X^2 + \sigma_2 X + \sigma_1$$

  donnant la place des erreurs.

Rendement Le rendement de ce code est $\frac{k}{n} = \frac{5}{15} = \frac{1}{3}$. C'est le même rendement que le code répétition 3 fois.

Conclusion Un code BCH corrigeant trois erreurs peut être construit dans $\mathbf{F}_{32}, \mathbf{F}_{64}, \ldots$. Il suffit de choisir trois polynômes tels que

$$\mathrm{M}(\alpha) = \mathrm{M}(\alpha^2) = \cdots = \mathrm{M}(\alpha^6) = 0$$

quatrième chapitre

Factorisation des polynômes

4.1 Les carrés dans $\mathbf{F}_p{}^\star$

exemple : $p = 7$

				-3	-2	-1
x	1	2	3	4	5	6
x^2	1	4	2	2	4	1

Il y a 3 carrés. Chaque carré a deux racines carrées distinctes.

théorème 4.1

Soit $p \neq 2$ un nombre premier. Il y a dans $\mathbf{F}_p{}^\star$ $\frac{p-1}{2}$ carrés et $\frac{p-1}{2}$ non carrés. Chaque carré a deux racines carrées.

preuve : Soit g un générateur de $\mathbf{F}_p{}^\star$.

$$\mathbf{F}_p{}^\star = \left\{g, g^2 \bmod p, \ldots, g^{p-1} \bmod p\right\}$$

Soit $u = g^{\frac{p-1}{2}}$.
On a $u^2 = g^{p-1} = 1$, donc $u = \pm 1$.
Or $u = g^{\frac{p-1}{2}} \neq g^{p-1} = 1$ donc $u = -1$.

x	g	g^2	$\cdots$	$g^{\frac{p-1}{2}}$	$g^{\frac{p+1}{2}}$	$\cdots$	g^{p-1}
x^2	g^2	g^4	$\cdots$	$g^{p-1} = 1$	g^2		$g^{2p-2} = 1$

Les carrés sont donc les éléments qui s'écrivent comme g élevé à une puissance paire, il y a donc $\frac{p-1}{2}$ carrés.

$$\sqrt{g^2} = \left\{g, g^{\frac{p+1}{2}}\right\} = \pm g$$

On a donc plus généralement

$$\sqrt{g^{2i}} = \left\{g^i, g^{\frac{p+i}{2}}\right\} = \pm g^i$$

Chaque carré a bien deux racines carrées distinctes. ∎

Comment savoir si $a \in \mathbf{Z}$ est un carré ?
On introduit pour cela le symbole de Legendre.

définition 4.1 (*Symbole de Legendre*)

Soit $a \in \mathbf{Z}$ et $p \neq 2$ un nombre premier. On définit le symbole de Legendre par

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si } \bar{a} \text{ est un carré} \\ -1 & \text{si } \bar{a} \text{ n'est pas un carré} \\ 0 & \text{si } p \mid a \end{cases}$$

théorème 4.2 (*Critère d'Euler*)

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

preuve :

– Si $p \mid a$

$$\left(\frac{a}{p}\right) = 0$$

$$a^{\frac{p-1}{2}} \equiv 0 \pmod p$$

– Si a est un carré

$$\left(\frac{a}{p}\right) = 1$$

a est une puissance paire de g, i.e. $a = g^{2i}$
d'où

$$a^{\frac{p-1}{2}} \equiv g^{(p-1)i} \equiv 1 \pmod p$$

– Si a est un non carré

$$\left(\frac{a}{p}\right) = -1$$

a est une puissance impaire de g, i.e. $a = g^{2i+1}$
d'où

$$a^{\frac{p-1}{2}} \equiv g^{(p-1)i} g^{\frac{p-1}{2}} \equiv -1 \pmod p$$

■

proposition 4.3

Propriétés du symbole de Legendre

1.
$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow a \text{ est un carré } \bmod p$$

2.
$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

3.
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

c'est-à-dire

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \textit{si } p \equiv 1 \pmod 4 \\ -1 & \textit{si } p \equiv 3 \pmod 4 \end{cases}$$

4. *périodicité*
pour $\lambda \in \mathbf{Z}$

$$\left(\frac{a+\lambda p}{p}\right) = \left(\frac{a}{p}\right)$$

5. *multiplicativité*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

preuve :

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p$$

■

6.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

i.e.

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \textit{si } p \equiv \pm 1 \pmod 8 \\ -1 & \textit{si } p \equiv \pm 3 \pmod 8 \end{cases}$$

7.

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$$

Autrement dit :

– *Si* $p \equiv q \equiv 3 \pmod 4$

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

– *Sinon, si* $p \equiv 1 \pmod 4$ *ou* $q \equiv 1 \pmod 4$

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

Symbole de Jacobi

Le symbole de Jacobi généralise le symbole de Legendre.

définition 4.2 (*Symbole de Jacobi*)

On définit le symbole de Jacobi pour $a \in \mathbf{Z}$ *et* n *positif impair.*
On décompose $n = p_1 \dots p_r$ *en facteurs premiers avec* $p_1 \leq \dots \leq p_r$.
Alors

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right)$$

proposition 4.4

Propriétés du symbole de Jacobi

1.
$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

2. <u>*périodicité*</u>
pour $\lambda \in \mathbf{Z}$
$$\left(\frac{a+\lambda n}{n}\right) = \left(\frac{a}{n}\right)$$

3. <u>*multiplicativité*</u>
$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

4.
$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

5.
$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right)$$

exemple :
$$\left(\frac{30}{43}\right) = \left(\frac{2}{43}\right)\left(\frac{15}{43}\right) = -\left(\frac{15}{43}\right)$$
$$\left(\frac{15}{43}\right) = -\left(\frac{43}{15}\right) = -\left(\frac{13}{15}\right) = -\left(\frac{15}{13}\right) = -\left(\frac{2}{13}\right) = -(-1) = +1$$
d'où
$$\left(\frac{30}{43}\right) = -1$$

4.2 Résolution de $x^2 \equiv a \pmod p$

Si $\left(\frac{a}{p}\right) = +1$, a est un carré.
$\sqrt{a}$?

Premier cas simple
Si $p \equiv 3 \pmod 4$, $\sqrt{a} = \pm a^{\frac{p+1}{4}} \bmod p$.
En effet,
$$\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} a \equiv \left(\frac{a}{p}\right) a \equiv a \pmod p$$

Cas général
On a besoin, lorsque $p \equiv 1 \bmod 4$, d'un non résidu b.
Soit donc b un non résidu
$$\left(\frac{b}{p}\right) = -1$$

algorithme 10 Calcul du symbole de Jacobi $\left(\frac{a}{n}\right)$

étant donné : $a \in \mathbf{Z}$, $n \in \mathbf{N}$ impair

fournit : $\left(\frac{a}{n}\right)$

si $a < 0$ **alors**

$a' \leftarrow -a$

$\left(\frac{a}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{a'}{n}\right)$ $\{ \quad \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} \quad \}$

sinon si $a \geq n$ **alors**

$a = nq + r$ $\{ \quad 0 \leq r < n \quad \}$

$\left(\frac{a}{n}\right) = \left(\frac{nq+r}{n}\right) = \left(\frac{r}{n}\right)$

sinon

si $a = 0$ **alors**

$\left(\frac{a}{n}\right) = \left(\frac{0}{n}\right) = \begin{cases} +1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$

sinon si a est pair **alors**

$a = 2^\alpha a'$ $\{ \quad a' \textit{ impair} \quad \}$

$\left(\frac{a}{n}\right) = \left(\frac{2}{n}\right)^\alpha \left(\frac{a'}{n}\right)$ $\{ \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} \quad \}$

sinon

$\left(\frac{a}{n}\right) = (-1)^{\frac{a-1}{2}\frac{n-1}{2}} \left(\frac{n}{a}\right)$ $\{ \quad a \textit{ est impair}, 0 \leq a < n \quad \}$

fin si

fin si

Si $p \equiv 5 \bmod 8$, on peut prendre $b = 2$. Si $p \equiv 1 \bmod 8$, voir plus loin.
On a par hypothèse

$$\left(\frac{a}{p}\right) = +1$$

On cherche e_1 et e_2 tels que

$$a^{e_1} b^{e_2} \equiv 1 \pmod{p} \tag{4.1}$$

On part de

$$\begin{cases} e_1 & = & \frac{p-1}{2} \\ e_2 & = & 0 \end{cases}$$

L'équation 4.1 implique que e_2 est pair.

- Si e_1 est impair

  $$r = \pm a^{\frac{e_1+1}{2}} b^{\frac{e_2}{2}}$$

  r est solution.

  $$r^2 = a^{e_1+1} b^{e_2} = a(a^{e_1} b^{e_2}) \equiv a \pmod{p}$$

- Si e_1 est pair
  Soit $u = a^{\frac{e_1}{2}} b^{\frac{e_2}{2}} \bmod p$

  $$u^2 = a^{e_1} b^{e_2} \equiv 1 \pmod{p}$$

  Donc

  $$u \equiv \pm 1 \pmod{p}$$

  - Si $u = 1$

    $$a^{\frac{e_1}{2}} b^{\frac{e_2}{2}} = 1$$

    est une nouvelle relation 4.1.
  - Si $u = -1$

    $$\begin{array}{lcc} a^{\frac{e_1}{2}} b^{\frac{e_2+p-1}{2}} & \equiv & \underbrace{a^{\frac{e_1}{2}} b^{\frac{e_2}{2}}}_{=1 \text{ d'après l'équation } 4.1} \quad b^{\frac{p-1}{2}} \\ & \equiv & u\left(\frac{b}{p}\right) \\ & = & (-1)(-1) \\ & = & +1 \end{array}$$

    D'où encore une relation de type 4.1.

Retour au cas $p \equiv 3 \pmod{4}$
a et $-a$ ne sont pas carrés simultanément car

$$\left(\frac{-a}{p}\right) = -\left(\frac{a}{p}\right)$$

l'algorithme précédent calcule la racine carrée de celui a ou $-a$ qui est un carré.

algorithme 11 Calcul de racine carrée modulaire

étant donné : a, p premier

fournit : $\sqrt{a}$ en cas d'existence

$e_1 \leftarrow \frac{p-1}{2}$
$e_2 \leftarrow 0$
tant que e_1 est pair **faire**
  $u \leftarrow a^{\frac{e_1}{2}} b^{\frac{e_2}{2}} \bmod p$
  si $u = +1$ **alors**
    $e_1 \leftarrow \frac{e_1}{2}$
    $e_2 \leftarrow \frac{e_2}{2}$
  sinon
    $e_1 \leftarrow \frac{e_1}{2}$
    $e_2 \leftarrow \frac{e_2+p-1}{2}$
  fin si
fin tant que
$r \leftarrow a^{\frac{e_1+1}{2}} b^{\frac{e_2}{2}} \bmod p$
si $r^2 \equiv a \pmod{p}$ **alors**
  écrire $\pm r$
sinon
  pas de solutions
fin si

Pêche aux non résidus
On dispose d'un algorithme probabiliste :

1. Choisir b au hasard en 1 et $p-1$
2. Si $\left(\frac{b}{p}\right) = -1$ alors on a gagné, sinon on recommence.

On ne sait pas s'il existe un bon algorithme déterministe.

Trouver un résidu

- Choisir $a = 1, 4, 9, 16, 25, \ldots$
- Choisir x au hasard entre 1 et $p-1$ et $a = x^2 \bmod p$
- 1. Choisir a au hasard
  2. - Si $\left(\frac{a}{p}\right) = 1$ on a gagné.
     - Sinon, recommencer avec a'
       - Si $\left(\frac{a'}{p}\right) = 1$, on a gagné.
       - Sinon, on pose $c = aa'$ et $\left(\frac{c}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right) = +1$, on a encore gagné.

4.3 Résolution de $x^2 \equiv a \pmod{n}$

Si $n = pq$, $p \neq q$, $p, q \neq 2$

$$x^2 \equiv a \pmod{n} \Leftrightarrow \begin{cases} x^2 \equiv a \pmod{p} \\ x^2 \equiv a \pmod{q} \end{cases}$$

D'où

$$x^2 \equiv a \pmod{n} \Rightarrow \begin{cases} \left(\frac{a}{p}\right) = +1 \\ \left(\frac{a}{q}\right) = +1 \end{cases}$$

$$\begin{array}{lcl} x^2 \equiv a \pmod{p} & \to & x \equiv \pm\alpha \pmod{p} \\ x^2 \equiv a \pmod{q} & \to & x \equiv \pm\beta \pmod{q} \end{array}$$

On résout alors les systèmes

$$\begin{cases} x \equiv \varepsilon\alpha \pmod{p} \\ x \equiv \varepsilon'\beta \pmod{q} \end{cases}$$

où $\varepsilon, \varepsilon' \in \{-1, +1\}$. On trouve quatre solutions.

$$x \equiv \pm\gamma, \pm\delta \pmod{n}$$

Maple

```
mcombine
msolve
```

Retour sur le symbole de Jacobi
On a $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1) \times (-1) = +1$, or 2 n'est pas un carré modulo 15, car 2 n'est pas un carré modulo 3 et n'est pas un carré modulo 5.
On a donc, pour le symbole de Jacobi,

$$\left(\frac{a}{n}\right) = +1 \not\Rightarrow a \text{ est un carré modulo } n$$

En revanche, supposons $\left(\frac{a}{n}\right) = -1$ et soit $n = p_1 \cdots p_r$ la décomposition de n en facteurs premiers.
Par définition,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right)$$

Comme $\left(\frac{a}{n}\right) = -1$, il existe i_0 tel que $\left(\frac{a}{p_{i_0}}\right) = -1$ et donc a n'est pas un carré modulo n.

$$\left(\frac{a}{n}\right) = -1 \Rightarrow a \text{ n'est pas un carré modulo } n$$

4.4 Résolution de $x^2 \equiv a \pmod{p^\alpha}$

On utilise la méthode de Hensel.

théorème 4.5

*Soit $\alpha \geq 2$,
$x^2 \equiv a \pmod{p^\alpha}$ a deux racines si et seulement si $x^2 \equiv a \pmod{p}$ est résoluble, c'est-à-dire si et seulement si $\left(\frac{a}{p}\right) = +1$.*

exemple : On cherche à résoudre :

$$x^2 \equiv 19 \pmod{125}$$

Comme

$$\left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = +1$$

d'après le théorème précédent, il y a deux solutions.
On résout

$$x^2 \equiv 4 \pmod{5}$$

On trouve

$$x \equiv \pm 2 \pmod{5}$$

i.e.

$$x = 2 + 5t$$

On remplace dans

$$x^2 \equiv 19 \pmod{25}$$

On a

$$(2+5t)^2 = 4 + 20t + 25t^2 \equiv 19 \pmod{25}$$

i.e.

$$4 + 20t \equiv 19 \pmod{25}$$

i.e.

$$20t \equiv 15 \pmod{25}$$

c'est-à-dire

$$4t \equiv 3 \pmod 5$$

D'où

$$t = 2$$

Et

$$x = 2 + 5t = 12$$

On cherche donc x sous la forme

$$x = 12 + 25z$$

De même que précédemment, on exprime z en résolvant

$$(12 + 25z)^2 \equiv 19 \pmod{125}$$

4.5 Factorisation de $X^4 + 1$ dans $\mathbf{F}_p[X]$

théorème 4.6

$X^4 + 1$ est irréductible dans $\mathbf{Q}$.
Pour tout nombre premier p, $X^4 + 1$ est réductible dans $\mathbf{F}_p[X]$.

preuve :

- Dans $\mathbf{Q}$
  Si $X^4 + 1$ est réductible dans $\mathbf{Q}$, la décomposition dans $\mathbf{Q}$ est une décomposition dans $\mathbf{R}$. Or dans $\mathbf{R}$, X^4+1 a une unique décomposition qui est

  $$X^4 + 1 = \left(X^2 + 1\right)^2 - 2X^2 = \left(X^2 + 1 + \sqrt{2}X\right)\left(X^2 + 1 - \sqrt{2}X\right)$$

  Or $\sqrt{2} \notin \mathbf{Q}$
- Soit p un nombre premier
  - Si $p = 2$
    Alors

    $$X^4 + 1 = (X + 1)^4$$
  - Si $p \equiv 1 \pmod 8$
    Alors -1 est une puissance quatrième.

    $$u = g^{\frac{p-1}{8}}$$

    $$u^4 = g^{\frac{p-1}{2}} = -1$$

    Il y a quatre racines quatrièmes de -1
    Si

    $$g^{4x} \equiv -1 = g^{\frac{p-1}{2}}$$

    Alors

    $$4x \equiv \frac{p-1}{2} \pmod{p-1}$$

    i.e.

    $$x \equiv \frac{p-1}{8} \left(\mathrm{mod}\ \frac{p-1}{4}\right)$$

On pose, pour $k = 1, 2, 3, 4$,

$$u_k = g^{\frac{p-1}{8} + k\frac{p-1}{4}}$$

On a alors

$$X^4 + 1 = (X - u_1)(X - u_2)(X - u_3)(X - u_4)$$

– Si $p \not\equiv 1 \pmod 8$
-1 n'a pas de racines quatrièmes, donc X^4+1 n'a pas de facteurs linéaires.
  – Si $p \equiv 7 \pmod 8$

$$\left(\frac{2}{p}\right) = +1$$

  Il existe a tel que

$$a^2 \equiv a \pmod p$$

$$\begin{aligned} X^4 + 1 &= \left(X^2+1\right)^2 - 2X^2 \\ &= \left(X^2+1\right)^2 - (aX)^2 \\ &= \left(X^2+1-aX\right)\left(X^2+1+aX\right) \end{aligned}$$

  – Si $p \equiv 3 \pmod 8$

$$\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right) = -1$$

  Donc

$$\left(\frac{-2}{p}\right) = +1$$

  Il existe a tel que

$$a^2 \equiv -2 \pmod p$$

$$\begin{aligned} X^4 + 1 &= \left(X^2-1\right)^2 - (-2)X^2 \\ &= \left(X^2-1\right)^2 - (aX)^2 \\ &= \left(X^2-1-aX\right)\left(X^2-1+aX\right) \end{aligned}$$

  – Si $p \equiv 5 \pmod 8$

$$\left(\frac{-1}{p}\right) = +1$$

  Il existe a tel que

$$a^2 \equiv -1 \pmod p$$

$$\begin{aligned} X^4 + 1 &= \left(X^2\right)^2 - (-1) \\ &= \left(X^2\right)^2 - (a)^2 \\ &= \left(X^2-a\right)\left(X^2+a\right) \end{aligned}$$

Dans tous les cas, on a pu réduire $X^4 + 1$. ■

4.6 Polynômes sans facteurs carrés

Soit $\mathbf{K}$ un corps, $P \in \mathbf{K}[X]$ et $\hat{\mathbf{K}}$ la cloture de $\mathbf{K}$. P est donc scindé dans $\hat{\mathbf{K}}$.

théorème 4.7

Les assertions suivantes sont équivalentes

1. *les racines de P sont simples dans $\hat{\mathbf{K}}$*
2. $\mathrm{pgcd}(P, P') = 1$

preuve :

- non 1 $\rightarrow$ non 2
  Soit θ une racine de P d'ordre au moins 2.
  $$P = (X - \theta)^2 Q$$
  $$P' = 2(X - \theta)Q + (X - \theta)^2 Q'$$
  Si $\mathrm{pgcd}(P, P') = 1$, on utilise Bezout dans $\mathbf{K}[X]$
  $$uP + vP' = 1$$
  prenant la valeur en θ, on obtient
  $$0 + 0 = 1$$
  ce qui est absurde.
- non 2 $\rightarrow$ non 1
  Soit $D = \mathrm{pgcd}(P, P')$. On suppose $D \neq 1$.
  Dans $\hat{\mathbf{K}}$, il existe θ tel que $\mathrm{D}(\theta) = 0$. Alors $\mathrm{P}(\theta) = \mathrm{P}'(\theta) = 0$.
  $$P = (X - \theta)Q_1$$
  $$P' = Q_1 + (X - \theta)Q_1'$$
  d'où
  $$\mathrm{Q}_1(\theta) = 0$$
  Q_1 est donc multiple de $X - \theta$, donc θ est racine au moins double de P. ■

théorème 4.8

$\dfrac{P}{\mathrm{pgcd}(P, P')}$ *est un polynôme sans facteurs carrés.*

preuve :

$$P = (X - \theta_1)^{\alpha_1} \cdots (X - \theta_n)^{\alpha_n}$$

Si θ est racine d'ordre k de P alors θ est racine d'ordre $k-1$ de P'. $X - \theta_1$ apparait à l'ordre α_1 au numérateur et à l'ordre $\alpha_1 - 1$ au dénominateur, il apparait donc à l'ordre 1 dans le quotient. ■

théorème 4.9

> *Si $P' \neq 0$ il existe des polynômes calculables $P_1, \ldots, P_r \in \mathbf{K}[X]$ tels que P_i soit sans facteurs carrés et $P = P_1 \cdots P_r$.*

preuve :

$$P = \underbrace{\frac{P}{\mathrm{pgcd}(P, P')}}_{\text{sans facteurs carrés}} \underbrace{\mathrm{pgcd}\big(P, P'\big)}_{\text{degré} < \deg P}$$ ■

En caractéristique p

Que signifie $P' = 0$ en caractéristique p ?
Si $\mathrm{P}(X) = \mathrm{Q}(X^p)$, alors $\mathrm{P}'(X) = p\mathrm{Q}'\big(X^{p-1}\big) = 0$. La réciproque est vraie.
Si $\mathrm{P}'(X) = 0$, poser $Y = X^p$ et $\mathrm{P}(X) = \mathrm{Q}(Y)$, si $\mathrm{Q}'(Y) = 0$, on recommence en posant $Z = Y^p$,...

On supposera dans la suite qu'on cherche à factoriser P sans facteurs carrés.

4.7 Recherche des racines de P dans $\mathbf{F}_p$

4.7.1 Si p petit

---

algorithme 12 Recherche des racines de P dans $\mathbf{F}_p$

étant donné : p premier, $P \in \mathbf{F}_p[X]$
fournit : racines de P dans $\mathbf{F}_p$
  pour $x = 0$ à $p - 1$ **faire**
    si $\mathrm{P}(x) = 0$ **alors**
      écrire x
    fin si
  fin pour

4.7.2 Si p grand, $p > 2$

On utilise le polynôme $X^p - X$

$$X^p - X = \prod_{a \in \mathbf{F}_p} (X - a) = X\left(X^{\frac{p-1}{2}} - 1\right)\left(X^{\frac{p-1}{2}} + 1\right)$$

En utilisant le critère d'Euler pour le symbole de Legendre

$$X^{\frac{p-1}{2}} - 1 = \prod_{\substack{a \in \mathbf{F}_p{}^\star \\ \left(\frac{a}{p}\right) = +1}} (X - a)$$

$$X^{\frac{p-1}{2}}+1=\prod_{\substack{a\in\mathbf{F}_p{}^\star\\ \left(\frac{a}{p}\right)=-1}}(X-a)$$

On a aussi

$$\mathrm{pgcd}(P,X^p-X)=\prod_{\substack{a\in\mathbf{F}_p\\ \mathrm{P}(a)=0}}(X-a)$$

Pour le calcul de ce pgcd, on calcule d'abord $A = X^p \bmod P$ en utilisant l'algorithme des puissances puis en faisant une division euclidienne. On a alors $\mathrm{pgcd}(P, X^p - X) = \mathrm{pgcd}(P, A - X)$.

Notons $D = \mathrm{pgcd}(P, X^p - X)$

- Si $D = 1$
  P n'a pas de racines
- Si $\deg D = 1$
  P a une racine dans $\mathbf{F}_p$
- Si $\deg D = 2$
  P a deux racines dans $\mathbf{F}_p$
- Si $\deg D = 3$ ou $\deg D = 4$
  On peut utiliser les formules de Cardan.

Maple

```
solve(x^3+p*x+q,x);
solve(a*x^4+b*x^3+c*x^2+d*x+e,x);
```

Si $\deg D \geq 2$, on dispose d'un algorithme probabiliste

On pose

$$D_1=\mathrm{pgcd}\big(P,X^{p-1}-X\big)$$

On calcule

$$\begin{cases} A_- &= \mathrm{pgcd}\Big(P,X^{\frac{p-1}{2}}-1\Big)\\ A_+ &= \mathrm{pgcd}\Big(P,X^{\frac{p-1}{2}}+1\Big)\end{cases}$$

On a

$$A_-A_+=D_1$$

On a

$$A_-=\prod_{\substack{a\in\mathbf{F}_p{}^\star\\ \mathrm{P}(a)=0\\ \left(\frac{a}{p}\right)=+1}}(X-a)$$

et

$$A_+=\prod_{\substack{a\in\mathbf{F}_p{}^\star\\ \mathrm{P}(a)=0\\ \left(\frac{a}{p}\right)=-1}}(X-a)$$

Il se peut que $A_- = 1$ ou $A_+ = 1$, et dans ce cas, on échoue.
Sinon, $A_- \neq 1$ et $A_+ \neq 1$, on a alors factorisé $D_1 = A_- A_+ = \mathrm{pgcd}\big(P, X^{p-1} - 1\big)$.

proposition 4.10

$\left(\frac{a}{p}\right) = \pm 1$ *et* $\left(\frac{a+1}{p}\right) = \pm 1$ *sont indépendants (presque).*

On dispose d'une factorisation de $D_1 = U_1 \cdots U_k$ avec $k \geq 1$. Pour chaque i, $1 \leq i \leq k$, on calcule

$$\begin{cases} A_-^i &= \mathrm{pgcd}\Big(U_i, (X+1)^{\frac{p-1}{2}} - 1\Big) \\ A_+^i &= \mathrm{pgcd}\Big(U_i, (X+1)^{\frac{p-1}{2}} + 1\Big) \end{cases}$$

On a

$$U_i = A_-^i A_+^i$$

et

$$A_-^i = \prod_{\substack{a \in \mathbf{F}_p{}^\star \\ \mathrm{U_i}(a) = 0 \\ \left(\frac{a+1}{p}\right) = +1}} (X - a)$$

On itère ensuite en remplaçant $X+1$ par $X+2$, $X+3$, ...
Le calcul de $\mathrm{pgcd}\Big(U, (X-s)^{\frac{p-1}{2}} - 1\Big)$ s'effectue en faisant le changement de variables $Y = X - s$, on est ramené alors à calculer $\mathrm{pgcd}\Big(\mathrm{U}(Y+s), Y^{\frac{p-1}{2}} - 1\Big)$.
On calcule $\mathrm{U}(Y+s)$ soit en utilisant Taylor, soit en utilisant Horner. Le second terme se calcule avec l'algorithme des puissances.

4.8 Le théorème chinois

théorème 4.11 (*Théorème des restes chinois*)

Soit $P_1, \ldots, P_r$ des polynômes de $\mathbf{K}[X]$ premiers entre eux deux à deux et soit $A_1, \ldots, A_r$ des polynômes quelconques de $\mathbf{K}[X]$.
Le système

$$\begin{cases} \mathrm{P}(X) &\equiv A_1 \pmod{P_1} \\ &\vdots \\ \mathrm{P}(X) &\equiv A_r \pmod{P_r} \end{cases} \tag{4.2}$$

admet une unique solution $\mathrm{P}(X) \in \mathbf{K}[X]$ *tel que*

$$\deg P < \deg P_1 + \cdots + \deg P_r = \deg P_1 \cdots P_r$$

preuve :

– Unicité
Supposons que P et $\hat{P}$ soient solutions de 4.2 avec la condition sur le degré.

On pose $Q = P - \hat{P}$ et on suppose $Q \neq 0$.
On a alors

$$\begin{cases} \mathrm{Q}(X) & \equiv & 0 \pmod{P_1} & \Rightarrow & P_1 \mid Q \\ \vdots & & & & \\ \mathrm{Q}(X) & \equiv & 0 \pmod{P_r} & \Rightarrow & P_r \mid Q \end{cases}$$

Comme les P_i sont premiers entre eux deux à deux, on a

$$P_1 \cdots P_r \mid Q$$

En passant au degré,

$$\deg P_1 \cdots P_r \leq \deg Q$$

Or

$$\deg Q = \deg \left(P - \hat{P}\right) \leq \max\left(\deg P, \deg Q\right) < \deg P_1 \cdots P_r$$

D'où une contradiction.
Ainsi $Q = 0$ et $P = \hat{P}$.

– Existence

On s'intéresse dans un premier temps aux systèmes chinois élémentaires.
Le système chinois élémentaire d'indice i est

$$\begin{cases} \mathrm{P}(X) & \equiv & 0 \pmod{P_1} & \Rightarrow & P_1 \mid P \\ \vdots & & & & \\ \mathrm{P}(X) & \equiv & 0 \pmod{P_{i-1}} & \Rightarrow & P_{i-1} \mid P \\ \mathrm{P}(X) & \equiv & 1 \pmod{P_i} & & \\ \mathrm{P}(X) & \equiv & 0 \pmod{P_{i+1}} & \Rightarrow & P_{i+1} \mid P \\ \vdots & & & & \\ \mathrm{P}(X) & \equiv & O \pmod{P_r} & \Rightarrow & P_r \mid P \end{cases}$$

On pose

$$Q_i = \frac{P_1 \cdots P_r}{P_i}$$

Comme les P_i sont premiers entre eux

$$Q_i \mid P$$

Donc il existe un polynôme S tel que

$$Q_i S = P$$

En utilisant la $i^{\text{ème}}$ équation, on a

$$P = Q_i S \equiv 1 \pmod{P_i}$$

On a aussi

$$\mathrm{pgcd}(Q_i, P_i) = 1$$

Donc, par Bezout

$$u_i Q_i + v_i P_i = 1$$

D'où

$$u_i Q_i \equiv 1 \pmod{P_i}$$

Une solution du système élémentaire d'indice i est

$$P = u_i Q_i$$

On revient ensuite à 4.2.
Le polynôme

$$P = u_1Q_1A_1 + \cdots + u_rQ_rA_r$$

est solution du système 4.2.
En effet, pour $1 \leq i \leq r$

$$P \equiv u_iQ_iA_i \pmod{P_i} \equiv A_i \pmod{P_i}$$

Il se peut que $\deg P$ soit trop grand, on effectue alors la division euclidienne de P par $P_1 \cdots P_r$, i.e.

$$P = (P_1 \cdots P_r)Q + R$$

et R est solution de 4.2 avec la condition sur le degré. ■

4.9 La méthode de Berlekamp

On cherche à factoriser $\mathrm{u}(x)$ sur $\mathbf{F}_p$. On suppose que u est sans facteurs carrés et que u est le produit de r facteurs irréductibles sur $\mathbf{F}_p$.

$$u = u_1u_2 \cdots u_r$$

On s'intéresse à la congruence

$$\mathrm{v}(x)^p \equiv \mathrm{v}(x) \pmod{\mathrm{u}(x)} \tag{4.3}$$

Quel est le nombre de $\mathrm{v}(x)$ solutions de 4.3 telles que $\deg v < \deg u$?

théorème 4.12

Le nombre de solutions de 4.3 est p^r où r est le nombre de facteurs irréductibles de u.

preuve :

$$X^p - X = X(X-1)\cdots(X-(p-1))$$
$$\mathrm{v}(x)^p - \mathrm{v}(x) = \mathrm{v}(x)(\mathrm{v}(x)-1)\cdots(\mathrm{v}(x)-(p-1))$$

Si v satisfait 4.3 alors $\mathrm{v}(x)^p - \mathrm{v}(x)$ est multiple de $\mathrm{u}(x) = u_1 \cdots u_r$.

$$u_1 \cdots u_r \mid \mathrm{v}(x)(\mathrm{v}(x)-1)\cdots(\mathrm{v}(x)-(p-1))$$

u_i divise le produit donc il existe un unique s_i tel que $u_i \mid \mathrm{v}(x) - s_i$. En effet, si $u_i \mid \mathrm{v}(x) - s$ et $u_i \mid \mathrm{v}(x) - t$ avec $s \neq t$, alors $u_i \mid s - t$, ce qui est absurde.

D'où, il existe $s_1, \ldots, s_r$ tel que si $\mathrm{v}(x)$ est solution de 4.3 alors $\mathrm{v}(x)$ est solution du système chinois

$$\left\{\begin{array}{lcl} \mathrm{v}(x) & \equiv & s_1 \pmod{u_1} \\ & \vdots & \\ \mathrm{v}(x) & \equiv & s_r \pmod{u_r} \end{array}\right.$$

Réciproquement

$$\begin{gathered} u_1 \mid \mathrm{v}(x) - s_1 \\ \vdots \\ u_r \mid \mathrm{v}(x) - s_r \end{gathered}$$

donc

$$u_1 \cdots u_r \mid (\mathrm{v}(x) - s_1) \cdots (\mathrm{v}(x) - s_r)$$

d'où

$$u \mid \mathrm{v}(x)^p - \mathrm{v}(x)$$

On a
- p choix pour s_1
- $\vdots$
- p choix pour s_r

p^r choix au total ∎

définition 4.3 (*Matrice de Berlekamp*)

Soit $\mathrm{u}(x)$ *de degré* n. *Soit, pour* $0 \leq k \leq n-1$, *le reste*

$$q_{k,n-1}x^{n-1} + \cdots + q_{k,1}x + q_{k,0}$$

de la division euclidienne de x^{kp} *par* $\mathrm{u}(x)$. *On définit la matrice de Berlekamp par*

$$Q = \begin{pmatrix} q_{0,0} & q_{0,1} & \cdots & q_{0,n-1} \\ q_{1,0} & q_{1,1} & \cdots & q_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots \\ q_{n-1,0} & q_{n-1,1} & \cdots & q_{n-1,n-1} \end{pmatrix}$$

Si p *est grand, on peut calculer ces coefficients en utilisant l'algorithme des puissances*

$$x^{kp} \bmod \mathrm{u}(x)$$

exemple :

$$\begin{gathered} p = 5, \mathrm{u}(x) = x^4 + 1 \\ x^0 = 1 \\ x^5 = -x \\ x^{10} = x^2 \\ x^{15} = -x^3 \\ Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \end{gathered}$$

Remarque La première ligne de la matrice de Berlekamp est toujours $1\ 0\ \cdots\ 0$.

théorème 4.13 (*Théorème de Berlekamp*)

Soit Φ *l'application définie par*

$$\Phi : \begin{array}{ccc} \mathbf{F}_p[X]_n & \to & \mathbf{F}_p[X]_n \\ P & \mapsto & \mathrm{P}(X)^p \bmod \mathrm{u}(X) \end{array}$$

Alors Φ est linéaire, sa matrice dans la base canonique est ${}^tQ$ et les solutions de 4.3 sont les vecteurs propres de Φ associés à la valeur propre 1.

Remarque
1 est toujours valeur propre.

preuve : Φ est trivialement linéaire (Frobénius).
La base canonique de $\mathbf{F}_p[X]_n$ est $1, X, \ldots, X^{n-1}$.

$$\begin{aligned} \Phi(X^k) &= X^{pk} \bmod \mathrm{u}(X) \\ &= q_{k,n-1}X^{n-1} + \cdots + q_{k,0} \end{aligned}$$

Si v est un vecteur propre associé à la valeur propre 1, alors $\Phi(v) = v$ i.e. $\mathrm{v}(X)^p = \mathrm{v}(X) \bmod \mathrm{u}(X)$ et v est solution de 4.3. ■

Corollaire 4.14

Le nombre r de facteurs irréductibles de u est égal à $r = n - \mathrm{rg}(Q - I)$.

preuve : Les solutions de 4.3 forment un sous-espace vectoriel de dimension r, sous-espace propre correspondant à la valeur propre 1 et par la formule du rang $\dim \mathrm{Ker}(\Phi - I) + \mathrm{rg}(\Phi - I) = n$. ■

Calcul du rang
Le rang d'une matrice se calcule en $\mathcal{O}\left(n^3\right)$. C'est égal à la dimension du plus grand déterminant non nul extrait de la matrice.
exemple : Calculons le nombre de facteurs irréductibles de $X^4 + 1$ sur $\mathbf{F}_5$.

$$Q - I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}$$

$\mathrm{rg}(Q - I) = 2$ d'où $r = 4 - 2 = 2$.

Calcul de $u_1, \ldots, u_r$ (p petit)

- Si $r = 1$, u est irréductible.
- Si $r \geq 2$, on calcule une base de vecteurs propres correspondant à $\lambda = 1$: $\mathcal{B} = v_1, \ldots, v_r$ avec $v_1 = 1$.
  On calcule alors pour $s = 0, 1, \ldots, p - 1$,

  $$A_s = \mathrm{pgcd}(\mathrm{v}_2(x) - s, \mathrm{u}(x))$$

  on a

  $$\prod_{0 \leq s \leq p-1} A_s = u$$

obtenant une factorisation de u.
v_2 correspond à un système chinois

$$\begin{cases} v_2 & \equiv & s_1 \bmod u_1 \\ & \vdots & \\ v_2 & \equiv & s_r \bmod u_r \end{cases}$$

$$A_s = \prod_{s_i = s} u_i$$

On a donc après utilisation de v_2 une factorisation de u en

$$u = A_1 \cdots A_j$$

Si $r = 2$, on peut montrer que c'est fini.
Si $r \geq 3$, on calcule pour chaque A_i avec $1 \leq i \leq j$, $\mathrm{pgcd}(\mathrm{v}_3(x) - s, A_i)$ pour $s = 0, 1, \ldots, p-1$ et on continue jusqu'à obtenir r facteurs.
L'algorithme converge.

Calcul de $u_1, \ldots, u_r$ (p grand)
Comme précédemment, on calcule une base $\mathcal{B} = v_1, \ldots, v_r$ des vecteurs propres associés à $\lambda = 1$, avec $v_1 = 1$.
On choisit alors un vecteur au hasard

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots \lambda_r v_r$$

avec λ_i choisi au hasard entre 0 et $p-1$.

$$\mathrm{v}(x)^{p-1} - 1 = \Big(\mathrm{v}(x)^{\frac{p-1}{2}} + 1\Big)\Big(\mathrm{v}(x)^{\frac{p-1}{2}} - 1\Big)$$

On calcule

$$U_1 = \mathrm{pgcd}\Big(\mathrm{u}(X), \mathrm{v}(X)^{\frac{p-1}{2}} - 1\Big)$$

$$U_2 = \mathrm{pgcd}\Big(\mathrm{u}(X), \mathrm{v}(X)^{\frac{p-1}{2}} + 1\Big)$$

On a

$$\mathrm{u}(X) = \mathrm{U}_1(X)\mathrm{U}_2(X)$$

On recommence avec un autre vecteur v sur U_1 et U_2.

$$U_{11} = \mathrm{pgcd}\Big(\mathrm{U}_1(X), \mathrm{v}(X)^{\frac{p-1}{2}} - 1\Big)$$

$$U_{12} = \mathrm{pgcd}\Big(\mathrm{U}_1(X), \mathrm{v}(X)^{\frac{p-1}{2}} + 1\Big)$$

On arrête dès que l'on a trouvé r facteurs.

4.10 Factorisation en degrés distincts

On cherche à décomposer $u = u_1 \cdots u_r$, avec u_i irréductibles sur $\mathbf{F}_p$ en

$$u = U_1 \cdots U_s$$

avec

$$U_k = \prod_{\deg u_i = k} u_i$$

Il est facile d'obtenir les U_k.

$$X^{p^n} - X = \prod_{d|n} (\text{polynômes irréductibles unitaires de degré } d)$$

$$X^p - X = \prod_{a \in \mathbf{F}_p} (X - a)$$

On a donc

$$U_1 = \operatorname{pgcd}(u, X^p - X)$$

On pose

$$V_1 = \frac{u}{U_1}$$

V_1 n'a pas de facteurs irréductibles de degré 1.
On a donc

$$U_2 = \operatorname{pgcd}\Big(V_1, X^{p^2} - X\Big)$$

En effet, c'est le produit des polynômes irréductibles de degré 1 ou 2 de V_1 donc de u, mais il n'y en a pas de degré 1.
Par récurrence, on suppose que c'est vrai jusqu'à U_{k-1}.
$V_{k-1} = \frac{u}{U_1 \cdots U_{k-1}}$ n'a pas de facteurs de degré inférieur à $k-1$.
On a donc

$$U_k = \operatorname{pgcd}\Big(V_{k-1}, X^{p^k} - X\Big)$$

En effet, c'est le produit des polynômes irréductibles unitaires de degré $d \mid k$ de V_{k-1} donc c'est U_k.
On s'arrête dès que $\deg V_{k-1} < 2k$.

$$V_{k-1} = \frac{u}{U_1 \cdots U_{k-1}}$$

Si $V_k = 1$, c'est terminé Si $V_k \neq 1$, alors V_k est irréductible. En effet, si V_k avait deux facteurs, ils seraient de degré supérieur à $2k$.

$$u = U_1 \cdots U_{k-1} \underbrace{V_{k-1}}_{U_{\deg V_{k-1}}}$$

théorème 4.15 (*Critère d'irréductibilité*)

Soit P unitaire de degré n sur $\mathbf{F}_p[X]$.

Si $\begin{cases} \mathrm{P}(X) \mid X^{p^n} - X \\ \forall d \mid n, \operatorname{pgcd}\Big(\mathrm{P}(X), X^{p^d} - X\Big) = 1 \end{cases}$ *alors P est irréductible.*

preuve : Comme P divise $X^{p^n} - X$, ses facteurs éventuels sont $Q_1, \dots, Q_r$ et Q_i est un polynôme irréductible de degré d_i avec $d_i \mid n$, ce qui est impossible car alors $\mathrm{pgcd}\left(X^{p^{d_i}} - X, P\right) \neq 1$ (car multiple de Q_i). ∎

4.11 Factorisation dans $\mathbf{Z}[X]$

Théorie 4.16

> *Soit* $P \in \mathbf{Z}[X]$ *unitaire,*
> $\mathrm{P}(X)$ *est irréductible dans* $\mathbf{Z}[X] \Leftrightarrow \mathrm{P}(X)$ *est irréductible dans* $\mathbf{Q}[X]$.

$\Phi : \begin{array}{ccc} \mathbf{Z} & \to & \mathbf{Z}/p\mathbf{Z} \\ n & \mapsto & n \bmod p \end{array}$ est un morphisme d'anneau.

On peut l'étendre en un morphisme d'anneau de $\mathbf{Z}[X]$ dans $\mathbf{Z}/p\mathbf{Z}[X]$.

$$\Phi : \begin{array}{ccc} \mathbf{Z}[X] & \to & \mathbf{Z}/p\mathbf{Z}[X] \\ a_0 + a_1 X + \cdots + a_n X^n & \mapsto & \Phi(a_0) + \Phi(a_1)X + \cdots \Phi(a_n)X^n \end{array}$$

Si $\mathrm{P}(X) = \mathrm{A}(X)\mathrm{B}(X)$ dans $\mathbf{Z}[X]$ alors $\Phi(P) = \Phi(A)\Phi(B)$ dans $\mathbf{F}_p[X]$. La réciproque est fausse car $X^4 + 1$ est irréductible sur $\mathbf{Z}[X]$ et réductible dans chaque $\mathbf{F}_p[X]$.

Si $P \in \mathbf{Z}[X, Y] = (\mathbf{Z}[X])[Y]$, i.e.

$$P = \mathrm{a_n}(X)Y^n + \mathrm{a_{n-1}}(X)Y^{n-1} + \cdots + \mathrm{a_0}(X)$$

et si Y est fixé égal à y_0

$$\mathrm{P}(X, Y) = \mathrm{A}(X, Y)\mathrm{B}(X, Y)$$

entraine

$$\mathrm{P}(X, y_0) = \mathrm{A}(X, y_0)\mathrm{B}(X, y_0)$$

théorème 4.17 (*Hilbert*)

> *Si* $\mathrm{P}(X, Y)$ *est irréductible, il existe une infinité de* $y_0 \in \mathbf{Z}$ *tels que* $\mathrm{P}(X, y_0)$ *soit irréductible.*

théorème 4.18 (*La borne de Landau-Mignotte*)

> *Soit* $\mathrm{P}(X) \in \mathbf{C}[X]$, $\mathrm{P}(X) = a_n X^n + \cdots + a_0$. *On note*
>
> $$\| P \| = \sqrt{\mid a_n \mid^2 + \cdots + \mid a_0 \mid^2} = \| P \|_2$$
>
> $$\mathrm{L}(P) = \sum_{i=0}^{n} \mid a_i \mid = \| P \|_1$$
>
> $$\mathrm{H}(P) = \max_{0 \le i \le n} \mid a_i \mid = \| P \|_\infty$$
>
> *Soit* $\mathrm{Q}(X) = b_d X^d + \cdots + b_0 \in \mathbf{C}[X]$ *tel que* $Q \mid P$.

On a alors

$$\mathrm{H}(Q) \leq \mathrm{L}(Q) \leq 2^d | \frac{b_d}{a_n} ||| P ||$$

Remarque Ce théorème est très utile pour majorer les coefficients des polynômes cyclotomiques.

$$X^n - 1 = \prod_{d|n} \Phi_{\mathrm{d}}(X)$$

exemple :

$$P = X^4 + 1$$
$$\| P \| = \sqrt{2}$$

Si Q est unitaire, divisant P, de degré 1 ou 2, on a

$$\mathrm{H}(Q) \leq 2^2\sqrt{2} \approx 5,6$$

Si $Q \in \mathbf{Z}[X]$, ses coefficients sont en valeur absolue inférieur à 5.

Une première méthode de factoriser
Choisir un nombre premier $p > 2 \times$ (Borne de Landau-Mignotte de P) pour $d \leq \frac{n}{2}$. (On suppose P unitaire, $a_n = b_d = 1$). On factorise alors le polynôme P sur $\mathbf{F}_p$.

$$P = u_1 \cdots u_r$$

Pour chaque $I \subset \{1, \ldots, r\}$

$$A = \prod_{i \in I} u_i$$

$$B = \prod_{i \notin I} u_i$$

On a $P = AB$ dans $\mathbf{F}_p[X]$. On peut supposer $\deg A \leq \frac{n}{2}$ quitte à échanger A et B.
Alors, si P se factorise en $P = VW$ dans $\mathbf{Z}[X]$ alors $\Phi(P) = \Phi(V)\Phi(W)$. Il existera donc $I \subset \{1, \ldots, r\}$ tel que $\Phi(V) \equiv A \pmod p$ et $\Phi(W) \equiv B \pmod p$.
Les coefficients de V sont en valeur absolue inférieurs à $\frac{p}{2}$.
En utilisant la représentation symétrique, $\Phi(V) = V = A$. On vérifie alors pour chaque factorisation de P en $P = AB$ dans $\mathbf{F}_p[X]$ avec $\deg A \leq \frac{n}{2}$ si A divise P dans $\mathbf{Z}[X]$. Sinon, P est irréductible.
exemple :

$$P = X^4 + 1$$

La borne de Landau-Mignotte est $B \approx 5,6$, on prend $p = 13$.
Dans $\mathbf{F}_{13}$,

$$X^4 + 1 = \left(X^2 - 5\right)\left(X^2 + 5\right)$$

S'il y a un facteur $\mathrm{V}(X)$ de $X^4 + 1$ dans $\mathbf{Z}[X]$, il est de degré 2, de coefficients en valeur absolue inférieurs à 5.
On a aussi

$$V \equiv \begin{cases} X^2 - 5 \\ X^2 + 5 \end{cases} \mod 13$$

V est donc de la forme

$$V = X^2 + \lambda 13X + \varepsilon 5 + 13\mu$$

La contrainte sur les coefficients impose $\lambda = \mu = 0$.
On en déduit que

$$V = \begin{cases} X^2 - 5 \\ X^2 + 5 \end{cases}$$

On vérifie que ni $X^2 - 5$, ni $X^2 + 5$ ne divise P, ce qui montre que $P = X^4 + 1$ est irréductible dans $\mathbf{Z}[X]$.

Remarque
Supposons que P est de degré $n = 20$.

- Dans $\mathbf{F}_{p_1}$
  P se factorise en produit de 5 facteurs de degré 4
- Dans $\mathbf{F}_{p_2}$
  P se factorise en produit de 4 facteurs de degré 5

Alors P est irréductible dans $\mathbf{Z}[X]$.
En effet, si $P = UV$ dans $\mathbf{Z}[X]$ alors

- dans $\mathbf{Z}/p_1\mathbf{Z}[X]$
$$\Phi_1(P) = \Phi_1(U)\Phi_1(V)$$
$$\deg U = \deg \Phi_1(U) = 4, 8, 12 \text{ ou } 16$$
- dans $\mathbf{Z}/p_2\mathbf{Z}[X]$
$$\Phi_2(P) = \Phi_2(U)\Phi_2(V)$$
$$\deg U = \deg \Phi_2(U) = 5, 10 \text{ ou } 15$$

C'est impossible.
Cela revient donc à chercher les sous-sommes communes

$$n = n_1 + \cdots + n_k = n'_1 + \cdots + n'_r$$

La méthode de Hensel
Nous allons maintenant voir une deuxième méthode pour factoriser dans $\mathbf{Z}[X]$. On utilise pour cela la méthode de Hensel qui permet de relever une factorisation modulo p en une factorisation modulo p^n.

Lemme 4.19

Soit $\mathbf{K}$ un corps, h_1 et $g_1 \in \mathbf{K}[X]$.
On suppose

$$\begin{cases} \deg g_1 \geq 1 \\ \deg h_1 \geq 1 \\ \operatorname{pgcd}(g_1, h_1) = 1 \end{cases}$$

Soit $C \in \mathbf{K}[X]$ tel que $\deg C < \deg g_1 + \deg h_1$.
Alors il existe $A, B \in \mathbf{K}[X]$ uniques tels que

$$\begin{cases} Ag_1 + Bh_1 = C \\ \deg A < \deg h_1 \\ \deg B < \deg g_1 \end{cases}$$

preuve :

- Existence
  - Si $C = 1$, c'est Bezout
  - Si $C \neq 1$
    Par le théorème de Bezout, il existe u et v tels que
    $$ug_1 + vh_1 = 1$$
    En multipliant par C, il vient
    $$uCg_1 + vCh_1 = C$$
    On effectue la division euclidienne de uC par h_1
    $$uC = h_1 q + r_1$$
    avec $\deg r_1 < \deg h_1$.
    On a alors
    $$h_1 q g_1 + r_1 g_1 + vCh_1 = C$$
    i.e.
    $$r_1 g_1 + h_1(qg_1 + vC) = C$$
    On pose $A = r_1$ et $B = qg_1 + vC$.
    On a $\deg B < \deg g_1$ car sinon $\deg(r_1 g_1 + Bh_1)$ serait plus grand que $\deg g_1 + \deg h_1$ qui est strictement plus grand que $\deg C$ par hypothèse. On aurait $\deg C > \deg C$, ce qui est absurde.
    D'où l'existence.
- Unicité
  On suppose que A, B et A_1, B_1 conviennent.
  On a alors
  $$(A - A_1)g_1 + (B - B_1)h_1 = 0$$
  i.e.
  $$(A - A_1)g_1 = (B_1 - B)h_1$$
  Donc
  $$g_1 \mid (B_1 - B)h_1$$
  Or
  $$\operatorname{pgcd}(g_1, h_1) = 1$$
  Donc
  $$g_1 \mid (B_1 - B)$$
  Ce qui est absurde car $\deg(B_1 - B) < \deg g_1$.
  D'où l'unicité. ■

Lemme de Hensel 4.20

Soit p un nombre premier. Soit $f, g, h \in \mathbf{Z}[X]$ unitaires.
On suppose que
$$\begin{cases} f \equiv gh \pmod p \\ \operatorname{pgcd}(g,h) = 1 \text{ dans } \mathbf{F}_p[X] \end{cases}$$
Alors pour tout $k \geq 1$, il existe des polynômes $g_k, h_k \in \mathbf{Z}[X]$ unitaires tels que
$$\begin{cases} f & \equiv & g_k h_k \pmod{p^k} \\ g_k & \equiv & g \pmod p \\ h_k & \equiv & h \pmod p \end{cases}$$

preuve : On fait une récurrence sur k

- $k = 1$
  c'est l'hypothèse en posant $g_1 = g$ et $h_1 = h$.
- Montrons le principe de la récurrence pour $k = 2$

$$g_2 = g_1 + p\hat{g}_2$$
$$h_2 = h_1 + p\hat{h}_2$$
$$f \equiv g_2 h_2 \equiv g_1 h_1 + p\Big(\hat{g}_2 h_1 + \hat{h}_2 g_1\Big) + p^2 \hat{g}_2 \hat{h}_2 \pmod{p^2}$$

i.e.

$$f \equiv g_1 h_1 + p\Big(\hat{g}_2 h_1 + \hat{h}_2 g_1\Big) \pmod{p^2}$$
$$\frac{f - g_1 h_1}{p} \equiv \hat{g}_2 h_1 + \hat{h}_2 g_1 \pmod{p}$$

On applique alors le lemme précédent avec $C = \frac{f - g_1 h_1}{p}$, ce qui détermine $\hat{g}_2$ et $\hat{h}_2$. ■

Méthode de factorisation de $P \in \mathbf{Z}[X]$
On suppose P unitaire

1. Choix de p premier
   On veut p assez petit tel que P soit sans facteur carré modulo p.
   On choisit p ne divisant pas le discriminant de P, on fait ensuite quelques essais afin de minimiser r.
2. Calculer B, la borne de Landau-Mignotte de P avec $d = \frac{n}{2}$
3. Factoriser P sur $\mathbf{F}_p$
$$P = u_1 \cdots u_r \pmod{p}$$
4. Choisir k tel que $p^k > 2B$ et étendre la factorisation par la méthode de Hensel.
$$P = u_1^{(k)} \cdots u_r^{(k)} \pmod{p^k}$$
5. Pour chaque sous-produit $A = u_{i_1}^{(k)} \cdots u_{i_j}^{(k)}$ avec $\deg A \leq \frac{n}{2}$, tester si A divise P dans $\mathbf{Z}[X]$. Si aucun A ne divise P, P est irréductible.

Un meilleur algorithme du à Lenstra, Lenstra et Levász (LLL) (1982)
Cet algorithme polynômial s'appuie sur la notion de réseau de $\mathbf{R}^n$.
Si $b_1, \ldots, b_n$ est une base de $\mathbf{R}^n$, $\{\lambda_1 b_1 + \cdots + \lambda_n b_n, \lambda_i \in \mathbf{Z}\}$ est le réseau de base $b_1, \ldots, b_n$.
Soit $\mathcal{R}$ un réseau de base $(b_1, \ldots, b_n)$. Soit $v_1, \ldots, v_n \in \mathcal{R}$. On se demande si $(v_1, \ldots, v_n)$ forme une base.
v_1 a pour composante $v_1^{(i)}$ avec $1 \leq i \leq n$ dans la base b_i, i.e. $v_1 = \sum\limits_{i=1}^{n} v_1^{(i)} b_i$ avec $v_1^{(i)} \in \mathbf{Z}$.
La matrice de changement de base est

$$M = \begin{pmatrix} v_1^{(1)} & \cdots & v_n^{(1)} \\ \vdots & \vdots & \vdots \\ v_1^{(n)} & \cdots & v_n^{(n)} \end{pmatrix}$$

On a

$$(v_1, \ldots, v_n) \text{ est une base } \Leftrightarrow \det M = \pm 1$$

exemple : Dans $\mathbf{R}^2$

$$v_1 = b_1 = (1, 0)$$
$$v_2 = (a, 1)$$

(v_1, v_2) base ?

$$\det \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = 1$$

(v_1, v_2) est une base.
Le problème est de trouver une base sympathique, avec des vecteurs aussi courts que possible.
L'algorithme LLL permet de trouver

- Un vecteur court dans un réseau
- Une base à peu près orthogonale

Dans la factorisation,
$\mathrm{h}(x)$ polynôme de degré d dans $\mathbf{Z}$.
Les polynômes de $\mathbf{Z}[X]$ de degré inférieur à m et multiples de $\mathrm{h}(x)$ dans $\mathbf{Z}/n\mathbf{Z}$ forment un réseau.
En appliquant l'algorithme LLL à ce réseau avec $n = p$

$$\mathrm{P}(x) = u_1 \cdots u_r$$

Pour chaque i, $\mathrm{h}(x) = u_i$ et l'algorithme LLL fournit le facteur de p dans $\mathbf{Z}[X]$ qui est multiple de u_i dans $\mathbf{F}_p[X]$.

Cas des polynômes à coefficient dominant $\neq 1$

$$\mathrm{f}(x) = a_n x^n + \cdots + a_0, a_n \neq 1$$

On considère $a_n \mathrm{f}(x)$

$$\mathrm{f}(x) = \mathrm{B}(x)\mathrm{C}(x)$$
$$B = b_k x^k + \cdots$$
$$C = c_j x^j + \cdots$$
$$a_n = b_k c_j$$
$$a_n \mathrm{f}(x) = (c_j B)(b_k C)$$

$c_j B$ et $b_k C$ ont a_n comme coefficient dominant.
On a factorisé $a_n f$ en deux polynômes de coefficient dominant a_n.
On choisit p premier tel que $p \nmid a_n$.
On factorise $a_n^{-1} f$ sur $\mathbf{F}_p[X]$

$$a_n^{-1} f = B_1 C_1$$

Par la méthode de Hensel

$$a_n f = (a_n B_1)(a_n C_1)$$

$$a_n f \equiv B_h C_h \bmod p$$

Le coefficient dominant de B_h et C_h est a_n.

Cas des polynômes à plusieurs variables
Si $\mathrm{f}(X,Y) \in \mathbf{Z}[X,Y]$ est irréductible, le nombre de $y_0 \in [-N,N]$ tel que $\mathrm{f}(x,y_0)$ est irréductible dans $\mathbf{Z}[X]$ est inférieur à N^α avec $\alpha < 1$.
Essayer des valeurs de y_0 et calculer le nombre de facteurs irréductibles de $\mathrm{f}(x,y_0)$

- Si $\mathrm{f}(x,y)$ est unitaire, c'est assez facile.
  On factorise $\mathrm{f}(x,y_0) = \mathrm{B}(x,y_0)\mathrm{C}(x,y_0)$
  On remonte par la formule de Taylor

$$\mathrm{f}(x,y) = \mathrm{f}(x,y_0) + (y-y_0)\mathrm{f}'_{\mathrm{y}}(x,y_0) + \cdots$$

$$\mathrm{B}(x,y) = \mathrm{B}(x,y_0) + (y-y_0)\mathrm{B}'_{\mathrm{y}}(x,y_0) + \cdots$$

$$\mathrm{C}(x,y) = \mathrm{C}(x,y_0) + (y-y_0)\mathrm{C}'_{\mathrm{y}}(x,y_0) + \cdots$$

  $\mathrm{B}(x,y_0)$ et $\mathrm{C}(x,y_0)$ sont connus, par une méthode analogue au lemme de Hensel, on calcule alors B'_y, C'_y,... (c'est possible car f unitaire)
- Si f n'est pas unitaire, c'est plus compliqué.

cinquième chapitre

Intégration formelle

5.1 Résultant

théorème 5.1

Soit $f, g \in \mathbf{K}[X]$

$$f = a_m x^m + \cdots + a_0$$

$$g = b_n x^n + \cdots + b_0$$

Les assertions suivantes sont équivalentes :

i) f *et* g *ne sont pas premiers entre eux*

ii) il existe $u, v \in \mathbf{K}[X]$, $\deg u < \deg g$, $\deg v < \deg f$ *tels que* $fu + gv = 0$.

preuve :

– $i \Rightarrow ii$
Soit $d = \operatorname{pgcd}(f, g)$, $\deg d \geq 1$.

$$f = df_1$$

$$g = dg_1$$

On pose $u = g_1$ et $v = -f_1$.

$$fu + gv = df_1g_1 - df_1g_1 = 0$$

– $ii \Rightarrow i$
Par contraposée,
On suppose que f et g sont premiers entre eux i.e. $\operatorname{pgcd}(f, g) = 1$.
Si $fu + gv = 0$ alors $fu = -gv$, donc $f \mid gv$. De plus $\operatorname{pgcd}(f, g) = 1$, donc $f \mid v$ et donc $\deg f \leq \deg v$, absurde. D'où non i. ∎

définition 5.1 (*Matrice de Sylvester de f et g*)

$$\mathrm{S}(f,g) = \begin{pmatrix} \underbrace{\begin{matrix} a_m & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ \vdots & & & a_m \\ a_0 & & & \vdots \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_0 \end{matrix}}_{n} & \underbrace{\begin{matrix} b_n & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ \vdots & & & b_n \\ b_0 & & & \vdots \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & b_0 \end{matrix}}_{m} \end{pmatrix}$$

définition 5.2 (*Résultant*)

Le résultant de f et g est défini par

$$\mathrm{R}(f,g) = \det \mathrm{S}(f,g)$$

proposition 5.2

$$\operatorname{pgcd}(f,g) \neq 1 \Leftrightarrow \mathrm{R}(f,g) = 0$$

preuve :

- Si $\operatorname{pgcd}(f,g) \neq 1$
  il existe $u = u_{n-1}x^{n-1} + \cdots + u_0$ et $v = v_{m-1}x^{m-1} + \cdots + v_0$ tels que $uf + vg = 0$.
  On a
  $$\mathrm{S}(f,g) \begin{pmatrix} u_{n-1} \\ \vdots \\ u_0 \\ v_{m-1} \\ \vdots \\ v_0 \end{pmatrix} = 0$$
  On a donc $\det \mathrm{S}(f,g) = \mathrm{R}(f,g) = 0$
- Si $\mathrm{R}(f,g) = 0$
  il existe $X \neq 0$ tel que $SX = 0$. L'existence de X induit l'existence de deux polynômes u et v (construits comme ci-dessus) tels que $uf + vg = 0$ avec $\deg u < \deg g$ et $\deg v < \deg f$.
  Donc $\operatorname{pgcd}(f,g) \neq 1$. ∎

Application
Soit $f \in \mathbf{Z}[X]$. On a $\mathrm{R}(f,f') \in \mathbf{Z}$.
Si $\mathrm{R}(f,f') = 0$ alors f a un facteur carré dans $\mathbf{Z}$.
Sinon, $\mathrm{R}(f,f') = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, on choisit $p \neq p_i$ et alors f est sans facteurs carrés dans $\mathbf{F}_p$.

Propriétés du résultant

1. $$\mathrm{R}(\lambda f, \mu g) = \lambda^n \mu^m \mathrm{R}(f,g)$$

2. $$\mathrm{R}(g,f) = (-1)^{mn}\mathrm{R}(f,g)$$

preuve : La colonne $n+1$ est amenée en première place en n sauts. De même pour chaque colonne de b_j. D'où mn inversions et le facteur $(-1)^{mn}$. ∎

3. Supposons
$$\mathrm{f}(x) = a_m(x-\alpha_1)\cdots(x-\alpha_m)$$
$$\mathrm{g}(x) = b_n(x-\beta_1)\cdots(x-\beta_n)$$

Alors
$$\begin{aligned} \mathrm{R}(f,g) &= a_m^n \prod_{i=1}^m \mathrm{g}(\alpha_i) \\ &= b_n^m \prod_{j=1}^n \mathrm{f}(\beta_i) \\ &= a_m^n b_n^m \prod_{i,j} (\alpha_i - \beta_j) \end{aligned}$$

preuve :
$$\begin{aligned} a_m^n \prod_{i=1}^m \mathrm{g}(\alpha_i) &= a_m^n \prod_{i=1}^m (b_n(\alpha_i-\beta_1)\cdots(\alpha_i-\beta_n)) \\ &= a_m^n b_n^m \prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j) \\ &= a_m^n b_n^m \prod_{i,j} (\alpha_i - \beta_j) \end{aligned}$$

Montrons donc que
$$\mathrm{R}(f,g) = a_m^n b_n^m \prod_{i,j} (\alpha_i - \beta_j)$$

$$^t\mathrm{S}(f,g) \begin{pmatrix} \beta_1^{m+n-1} & \cdots & \beta_n^{m+n-1} & \alpha_1^{m+n-1} & \cdots & \alpha_m^{m+n-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ \beta_1 & \cdots & \beta_n & \alpha_1 & \cdots & \alpha_m \\ 1 & \cdots & 1 & 1 & \cdots & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \beta_1^{n-1}\mathrm{f}(\beta_1) & \cdots & \beta_m^{n-1}\mathrm{f}(\beta_m) & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & 0 & \cdots & 0 \\ \vdots & & \vdots & \alpha_1^{m-1}\mathrm{g}(\alpha_1) & \cdots & \alpha_n^{m-1}\mathrm{g}(\alpha_n) \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathrm{f}(\beta_1) & \cdots & \mathrm{f}(\beta_m) & \vdots & & \vdots \\ 0 & \cdots & 0 & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \mathrm{g}(\alpha_1) & \cdots & \mathrm{g}(\alpha_n) \end{pmatrix}$$

En passant au déterminant, on reconnait à gauche un déterminant de Vandermonde multiplié par $\mathrm{R}(f,g)$.

$$\begin{vmatrix} x_1^{n-1} & \cdots & x_n^{n-1} \\ \vdots & & \vdots \\ x_1 & \cdots & x_n \\ 1 & \cdots & 1 \end{vmatrix} = \prod_{1\leq i<j\leq n} (x_i - x_j)$$

■

4. Soit la division euclidienne de g par f

$$g = fq + h$$

Alors

$$\mathrm{R}(f,g) = a_m^{n-\deg h}\mathrm{R}(f,h)$$

preuve :

$$\mathrm{R}(f,g) = a_m^n \prod_{i=1}^{m} \mathrm{g}(\alpha_i)$$

$$\mathrm{g}(\alpha_i) = \mathrm{f}(\alpha_i)\mathrm{q}(\alpha_i) + \mathrm{h}(\alpha_i)$$

i.e.

$$\mathrm{g}(\alpha_i) = \mathrm{h}(\alpha_i)$$

Donc

$$\mathrm{R}(f,g) = a_m^n \prod_{i=1}^{m} \mathrm{h}(\alpha_i)$$

Or

$$\mathrm{R}(f,h) = a_m^{\deg h} \prod_{i=1}^{m} \mathrm{h}(\alpha_i)$$

D'où

$$\mathrm{R}(f,g) = a_m^{n-\deg h}\mathrm{R}(f,h)$$

■

De cette relation découle naturellement un algorithme pour calculer $\mathrm{R}(f,g)$.

définition 5.3 (*Discriminant de f*)

Si $f \in \mathbf{K}[X]$

$$\mathrm{Disc}(f) = \frac{(-1)^{\frac{m(m-1)}{2}}}{a_m}\mathrm{R}(f,f')$$

exemple :

$$f = ax^2 + bx + c$$

$$\mathrm{R}(f,f') = \begin{vmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{vmatrix}$$

i.e.

$$\mathrm{R}(f,f') = a(4ac - b^2)$$

D'où

$$\mathrm{Disc}(f) = \frac{-1}{a}a(4ac - b^2) = b^2 - 4ac$$

théorème 5.3

$$\mathrm{Disc}(f) = a_m^{2m-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

preuve :

$$\mathrm{R}\big(f, f'\big) = a_m^{m-1} \prod_{i=1}^{m} \mathrm{f}'(\alpha_i)$$

$$\mathrm{f}(x) = a_m(x - \alpha_1) \cdots (x - \alpha_m)$$

$$\mathrm{f}'(\alpha_i) = a_m(\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \cdots (\alpha_i - \alpha_m)$$

D'où

$$\begin{aligned}
\mathrm{R}(f, f') &= a_m^{2m-1} \prod_{i=1}^{m} \prod_{j \neq i} (\alpha_i - \alpha_j) \\
&= (-1)^{\frac{m(m-1)}{2}} a_m^{2m-1} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2
\end{aligned}$$

D'où le résultat. ■

Application
Chercher le polynôme dont les racines sont les cubes des α_i.

$$\mathrm{f}(x) = (x - \alpha_1) \cdots (x - \alpha_m)$$

Le polynôme cherché est

$$\mathrm{F}(x) = \big(x - \alpha_1^3\big) \cdots \big(x - \alpha_m^3\big)$$

Posons

$$\mathrm{g}(x) = y - x^3$$

où y est indéterminé.

$$\mathrm{R_x}(f, g) = \prod_{i=1}^{m} \mathrm{g}(\alpha_i) = \prod_{i=1}^{m} \big(y - \alpha_i^3\big) = \mathrm{F}(y)$$

Le polynôme cherché est donc $\mathrm{R_x}(f, g) = \mathrm{R_x}\big(f, y - x^3\big)$.

Application aux nombres algébriques
α est algébrique si il existe $f \in \mathbf{Z}[X]$ tel que $\mathrm{f}(\alpha) = 0$.
Soit α, β deux nombres algébriques.
Montrer que $\alpha+\beta$ est algébrique en trouvant un polynôme entier annulant $\alpha+\beta$.

$$\mathrm{f}(\alpha) = 0$$

$$\mathrm{g}(\beta) = 0$$

On choisit $\alpha_1 = \alpha$, $\beta_1 = \beta$ (avec les notations précédentes).
On définit P par

$$\mathrm{P}(y) = \mathrm{R_x}(f, \mathrm{g}(y-x)) = a_m^n \prod_{i=1}^{m} \mathrm{g}(y-\alpha_i)$$

$$\mathrm{g}(y-\alpha_i) = 0 \Leftrightarrow y - \alpha_i = \beta_j \Leftrightarrow y = \alpha_i + \beta_j$$

P est le polynôme cherché.

Exercice 5.1

Trouver $P \in \mathbf{Z}[X]$ tel que $\mathrm{P}(\alpha\beta) = 0$ puis tel que $\mathrm{P}\left(\frac{\alpha}{\beta}\right) = 0$.

solution page 106

5.2 Position du problème

On cherche à intégrer $\frac{P}{Q} \in \mathbf{Z}(X)$ avec $\deg P < \deg Q$.

Lemme 5.4

L'ensemble des fractions $\frac{P}{Q}$ avec $\deg P < \deg Q$ est stable par addition et multiplication.

preuve : Immédiat. ∎

Revenons à notre problème.
On factorise Q sur $\mathbf{C}[X]$.

$$\mathrm{Q}(X) = (X-a_1)^{\alpha_1} \cdots (X-a_k)^{\alpha_k}$$

On décompose en éléments simples

$$\frac{P}{Q} = \sum_{i=1}^{k} \sum_{1 \leq j \leq \alpha_i} \frac{A_{ij}}{(X-a_i)^j}$$

– Si $j \geq 2$

$$\int \frac{A_{ij}}{(X-a_i)^j} = -\frac{A_{ij}}{(j-1)(X-a)^{j-1}}$$

– Si $j = 1$

$$\int \frac{A_{ij}}{(X-a_i)} = A_{ij}\log(X-a)$$

Remarque

$$\int \frac{P'}{P} = \log(P)$$

5.3 Algorithme de Yun

On cherche à écrire Q sous la forme

$$Q = \prod_{i=1}^{\max \alpha_j} R_i^i$$

avec

$$R_i = \prod_{\alpha_j = i} (X - a_j)$$

Lemme 5.5

Si $\mathrm{Q}(X) \in \mathbf{Q}[X]$ *alors* $\forall i, R_i \in \mathbf{Q}[X]$.

preuve : L'algorithme calculant les R_i le montre. ∎

---

algorithme 13 calcul des R_i

étant donné : $Q = \prod_{j=1}^{k} (X - a_j)^{\alpha_k}$

fournit : $R_i = \prod_{\alpha_j = i} (X - a_j)$

$C_1 \leftarrow \mathrm{pgcd}(Q, Q')$
$D_1 \leftarrow \frac{Q}{C_1}$
$i \leftarrow 1$
tant que $D_i \neq 1$ **faire**
  $D_{i+1} \leftarrow \mathrm{pgcd}(C_i, D_i)$
  $C_{i+1} \leftarrow \frac{C_i}{D_{i+1}}$
  $R_i = \frac{D_i}{D_{i+1}}$
  $i \leftarrow i + 1$
fin tant que

---

preuve :

$$Q = R_1 R_2^2 \cdots R_s^s$$
$$C_1 = R_2 R_3^2 \cdots R_s^{s-1}$$
$$D_1 = R_1 R_2 \cdots R_s$$
$$D_2 = R_2 R_3 \cdots R_s$$
$$C_2 = R_3 R_4^2 \cdots R_s^{s-2}$$
$$R_1 = \frac{D_1}{D_2}$$

L'invariant de boucle est

$$C_i = R_{i+1} R_{i+2}^2 \cdots R_s^{s-i}$$

$$D_i = R_i R_{i+1} \cdots R_s$$

On a alors

$$D_{i+1} = \text{pgcd}(C_i, D_i) = R_{i+1} R_{i+2} \cdots R_s$$

$$C_{i+1} = \frac{C_i}{D_{i+1}} = R_{i+2} R_{i+3}^2 \cdots R_s^{s-(i+1)}$$

$$R_i = \frac{D_i}{D_{i+1}} = R_i$$

■

définition 5.4 (*Partie rationnelle, partie logarithmique*)

- *Partie rationnelle :*

$$\sum \int \textit{éléments simples de degré} \geq 2$$

C'est une fraction rationnelle !

- *Partie logarithmique :*

$$\sum \int \textit{éléments simples de degré } 1$$

5.3.1 Méthode de Hermite

$$\int \frac{P}{Q} = \int \frac{P}{\prod_{i=1}^{s} R_i^i} \text{ avec } \text{pgcd}(R_i, R_j) = 1$$

Décomposons en éléments simples $\frac{P}{Q_1 Q_2}$ avec $\text{pgcd}(Q_1, Q_2) = 1$.

$$\frac{P}{Q_1 Q_2} = \frac{A}{Q_1} + \frac{B}{Q_2} = \frac{AQ_2 + BQ_1}{Q_1 Q_2}$$

$\deg P < \deg Q_1 Q_2$, il existe A, B uniques tels que $AQ_2 + BQ_1 = P$.
En itérant le principe

$$\frac{P}{Q} = \frac{P}{\prod_{i=1}^{s} R_i^i} = \sum_{i=1}^{s} \frac{A_i}{R_i^i}$$

Si $i \geq 2$

$$\int \frac{A_i}{R_i^i} = \text{ fraction rationnelle } + \underbrace{\int \frac{B}{R_i}}_{\text{logarithmique}}$$

En effet, R_i est sans facteurs carrés donc $\text{pgcd}(R_i, R_i') = 1$. Il existe u et v tel que

$$uR_i + vR_i' = 1$$

$$\begin{aligned}\int \frac{P}{R_i^i} &= \int \frac{P(uR_i + vR_i')}{R_i^i}\\ &= \int \frac{Pu}{R_i^{i-1}} + \int \frac{PvR_i'}{R_i^i}\\ &= \int \frac{Pu}{R_i^{i-1}} + \int \frac{VR_i'}{R_i^i} \quad \text{en posant } V = Pv\end{aligned}$$

En intégrant par partie le terme de droite

$$\int \frac{VR_i'}{R_i^i} = -\frac{V}{(i-1)R_i^{i-1}} + \int \frac{V'}{(i-1)R_i^{i-1}}$$

5.3.2 Méthode de Horowitz

théorème 5.6

Soit $P, Q \in \mathbf{Q}[X]$ tels que $\deg(P) < \deg(Q)$.
Alors il existe $P_1, P_2, Q_1, Q_2 \in \mathbf{Q}[X]$ avec $\deg(P_i) < \deg(Q_i)$ tels que

$$\int \frac{P}{Q} = \frac{P_1}{Q_1} + \int P_2 Q_2 \tag{5.1}$$

Plus précisément, on a

$$Q_1 = \mathrm{pgcd}(Q, Q')$$

et

$$Q_2 = \frac{Q}{Q_1}$$

preuve :

$$\mathrm{Q}(X) = (X - a_1)^{\alpha_1} \cdots (X - a_k)^{\alpha_k}$$

On a alors

$$\mathrm{Q}_1(X) = (X - a_1)^{\alpha_1 - 1} \cdots (X - a_k)^{\alpha_k - 1}$$

$$\mathrm{Q}_2(X) = (X - a_1) \cdots (X - a_k)$$

$$\begin{aligned}\frac{P}{Q} &= \sum_{i=1}^{k} \sum_{j=1}^{\alpha_i} \frac{A_{ij}}{(X - a_i)^j}\\ &= \underbrace{\sum_{i=1}^{k} \frac{A_{i1}}{(X - a_i)}}_{\frac{P_2}{Q_2}} + \sum_{i=1}^{k} \sum_{j=2}^{\alpha_i} \frac{A_{ij}}{(X - a_i)^j}\end{aligned}$$

avec

$$\deg(P_2) < \deg(Q_2)$$

et

$$P_2 \in \mathbf{C}[X]$$

D'où

$$\int \frac{P}{Q} = \int \frac{P_2}{Q_2} + \underbrace{\sum_{i=1}^{k} \sum_{j=2}^{\alpha_i} \frac{-A_{ij}}{(j-1)(X-a_i)^{j-1}}}_{\frac{P_1}{Q_1}}$$

avec

$$\deg(P_1) < \deg(Q_1)$$

et

$$P_1 \in \mathbf{C}[X]$$

Il ne reste plus qu'à montrer que

$$P_1, P_2 \in \mathbf{Q}[X]$$

Dérivons 5.1.

$$\begin{aligned}
\frac{P}{Q} &= \frac{P_2}{Q_2} + \frac{Q_1 P_1' - Q_1' P_1}{Q_1^2} \\
&= \frac{P_2 Q_1}{Q} + \frac{P_1' Q_2}{Q} - \frac{Q_1' P_1 Q_2^2}{Q^2} \\
&= \frac{P_2 Q_1 + P_1' Q_2 - S P_1}{Q}
\end{aligned}$$

avec

$$S = \frac{Q_1' Q_2^2}{Q}$$

On a le résultat suivant :
S est un polynôme.
En effet, si a est une racine de Q d'ordre α alors

- a est racine de Q_1 d'ordre $\alpha - 1$
- a est racine de Q_1' d'ordre $\alpha - 2$
- a est racine de Q_2 d'ordre 1

Si $\alpha \geq 2$, a est d'ordre ≥ 0.
Si $\alpha = 1$, a est d'ordre ≥ 1.
S est bien un polynôme.
On en déduit alors que

$$P = P_2 Q_1 + P_1' Q_2 - S P_1$$

Q_1, Q_2 et S sont connus.
En écrivant

$$P_1 = c_k X^k + \cdots$$

$$P_2 = d_j X^j + \cdots$$

on obtient un système linéaire en c_i et d_i ayant une unique solution dans $\mathbf{C}$.
Le système étant à coefficients dans $\mathbf{Q}$, sa solution est dans $\mathbf{Q}$.
Donc $P_1, P_2 \in \mathbf{Q}[X]$. ∎

5.3.3 Intégration de la partie logarithmique

On cherche à calculer

$$\int \frac{P}{Q}$$

avec

$$\deg(P) < \deg(Q)$$

et Q sans facteurs carrés.

$$\mathrm{Q}(X) = (X - a_1) \cdots (X - a_n) \text{ (dans } \mathbf{C})$$

$$\frac{P}{Q} = \sum_{i=1}^{n} \frac{A_i}{X - a_i}$$

$$\int \frac{P}{Q} = \sum_{i=1}^{n} A_i \log(X - a_i)$$

On regroupe alors les A_i égaux.

$$I = \mathrm{card}(\{A_1, \ldots, A_n\})$$

On écrit donc

$$\{A_1, \ldots, A_n\} = \{c_1, \ldots, c_I\}$$

avec les c_i deux à deux distincts.

On pose, pour $1 \leq i \leq I$, $v_i = \displaystyle\prod_{j=1, A_j = c_i}^{n} (X - a_i)$.

exemple : On considère l'expression

$$2\log(X-1) + 2\log(X-2) + 3\log(X-3)$$

On a alors

$$A_1 = A_2 = 2$$
$$A_3 = 3$$
$$I = 2$$
$$\{c_1, c_2\} = \{2, 3\}$$
$$v_1 = (X-1)(X-2)$$
$$v_2 = (X-3)$$

théorème 5.7

Soit $1 \leq k \leq I$, alors

- *Si $c \neq c_k$,*

$$\mathrm{pgcd}(P - cQ', v_k) = 1$$

- *Si $c = c_k$,*

$$\mathrm{pgcd}(P - cQ', v_k) = v_k$$

On en déduit en particulier que v_k divise $P - c_k Q'$.

preuve : On a

$$\int \frac{P}{Q} = \sum_{i=1}^{n} A_i \log(X - a_i) = \sum_{i=1}^{I} c_i \log(v_i)$$

Donc, en dérivant

$$\frac{P}{Q} = \sum_{i=1}^{I} c_i \frac{v_i'}{v_i}$$

De plus

$$Q = v_1 v_2 \cdots v_I$$

Posons $u_i = \dfrac{Q}{v_i} = \prod_{j \neq i} v_j$

Alors

$$Q' = \sum_{i=1}^{I} u_i v_i'$$

Or

$$P = \sum_{i=1}^{I} c_i v_i' \frac{Q}{v_i} = \sum_{i=1}^{I} c_i u_i v_i'$$

D'où

$$P - cQ' = \sum_{i=1}^{I} (c_i - c) u_i v_i'$$

Fixons k entre 1 et I

Comme v_k divise tous les u_i sauf u_k, on a

$$\mathrm{pgcd}\big(P - cQ', v_k\big) = \mathrm{pgcd}\big((c_k - c) u_k v_k', v_k\big)$$

Comme v_k n'a que des racines simples, $\mathrm{pgcd}(v_k, v_k') = 1$

De plus, $\mathrm{pgcd}(u_k, v_k) = 1$

D'où

- Si $c = c_k$
$$\mathrm{pgcd}\big(P - cQ', v_k\big) = \mathrm{pgcd}(0, v_k) = v_k$$
- Si $c \neq c_k$
$$\mathrm{pgcd}\big(P - cQ', v_k\big) = \mathrm{pgcd}((c_k - c) u_k v_k, v_k) = \mathrm{pgcd}(c_k - c, v_k) = 1 \quad ■$$

Calcul de $\int \frac{P}{Q}$

On calcule $\mathrm{R_x}(P - yQ', Q)$. C'est un déterminant où y figure dans n colonnes, c'est donc un polynôme en y de degré n qui a n racines.
Soit $y_1, \ldots, y_n$ ces racines et $c_1, \ldots, c_I$ les valeurs distinctes de ces racines.
Pour $y = c_k$, on obtient que $P - c_k Q'$ et Q ne sont pas premiers entre eux.
On a alors

$$\int \frac{P}{Q} = \sum_{i=1}^{I} c_i \log(v_i)$$

avec $v_i = \mathrm{pgcd}(P - c_k Q', Q)$.
Les c_i appartiennent à un corps où le polynôme en y a toutes ses racines. Les coefficients de v_k sont dans ce corps.

exemple :

$$\int \frac{2x+1}{x^2+x+1}$$

$$Q = x^2 + x + 1$$

$$Q' = 2x + 1$$

$$\begin{aligned}
\mathrm{R_x}\big((2x+1)(1-y), x^2+x+1\big) &= \begin{vmatrix} 2(1-y) & 0 & 1 \\ 1-y & 2(1-y) & 1 \\ 0 & 1-y & 1 \end{vmatrix} \\
&= (1-y)^2 \begin{vmatrix} 2 & 0 & 1 \\ 1 & 2 & 1 \\ 0 & 1 & 1 \end{vmatrix} \\
&= 3(1-y)^2
\end{aligned}$$

$y = 1$ est racine double.
D'où

$$\int \frac{2x+1}{x^2+x+1} = 1 \times \log(Q) = \log\big(x^2+x+1\big)$$

exemple : Dû à Tobey et Trager

$$\int \frac{7x^{13} + 10x^8 + 4x^7 - 7x^6 - 4x^3 - 4x^2 + 3x + 3}{x^{14} - 2x^8 - 2x^7 - 2x^4 - 4x^3 - x^2 + 2x + 1}$$

$$\mathrm{R_x}\big(P - yQ', Q\big) = \big(4y^2 - 4y - 1\big)^7$$

Les racines de R_x sont

$$y = \frac{1 \pm \sqrt{2}}{2}$$

$$c_1 = \frac{1+\sqrt{2}}{2} \qquad\qquad c_2 = \frac{1-\sqrt{2}}{2}$$

$$v_1 = x^7 - \sqrt{2}x^2 - \left(\sqrt{2}+1\right)x - 1 \qquad\qquad v_2 = x^7 + \sqrt{2}x^2 + \left(\sqrt{2}-1\right)x - 1$$

$$v_1 v_2 = Q$$

$$\int \frac{P}{Q} = c_1 \log(v_1) + c_2 \log(v_2)$$

5.4 Conclusion

On doit ensuite s'intéresser à intégrer des fractions rationnelles en X et $\log(X)$, ce qui revient à poser $Y = \log(X)$ et intégrer une fraction rationnelle à deux variables.

On peut aussi étendre la "base" des fonctions pour exprimer les primitives, par exemple en ajoutant le logarithme intégrale $\mathrm{Li}(x) = \displaystyle\int \frac{\mathrm{d}x}{\log(x)}$, on peut essayer de calculer $\displaystyle\int \frac{\mathrm{d}x}{\log^2(x)}$.

Pour approfondir, on peut se reporter au travail de James Davenport qui est un des grands noms du domaine.

sixième chapitre

Séries formelles

6.1 Introduction

L'idée est d'étendre la notion de série entière.

Pour les séries entières $\sum_{n=0}^{+\infty} a_n z^n$ avec $a_n \in \mathbf{C}$, on calcule habituellement le rayon de convergence (qui donne le domaine de définition de la série entière). On sait ajouter, multiplier, inverser et composer des séries entières (modulo certaines conditions).

Cependant, que dire de $\sum_{n=0}^{+\infty} n! z^n$ qui a un rayon nul ?

Dans les séries formelles, on ne se soucie pas du rayon.

Le premier problème qui apparait informatiquement est comment définir les coefficients ?

Nombres de Bernouilli

$$\frac{x}{e^x - 1} = \frac{x}{x + \frac{x^2}{2} + \cdots} = \sum_{n=0}^{+\infty} b_n x^n$$

Par définition, les b_n sont les nombres de Bernouilli. Ces coefficients sont intéressants car ils permettent d'exprimer certains autres coefficients de manière assez simple.

$$\tan(x) = \sum_{n=0, n \text{ impair}}^{+\infty} t_n x^n$$

Les t_n s'expriment en fonction des b_n.

$$\operatorname{cotan}(x) = \frac{1}{x} + \sum_{n=0, n \text{ impair}}^{+\infty} c_n x^n$$

Les c_n s'expriment en fonction des b_n.

En effet,

$$\operatorname{cotan}(x) = 1 + \frac{2}{e^{2ix} - 1}$$

Fonction de partition

$$\sum_{n=0}^{+\infty} \mathrm{p}(n)x^n = \prod_{m=1}^{+\infty} \frac{1}{1-x^m}$$

$\mathrm{p}(n)$ est le nombre de façons d'écrire n comme somme d'entiers plus petits.
Le calcul de $\mathrm{p}(n)$ ne nécessite le calcul que des n premiers termes du produit.
Identité d'Euler

$$\prod_{m=1}^{+\infty}(1-X^m) = 1 + \sum_{n\geq 1}(-1)^n\left(x^{\frac{n(3n+1)}{2}} + x^{\frac{n(3n-1)}{2}}\right)$$

C'est une manière commode de calculer les $\mathrm{p}(n)$.

Fonction τ de Ramanujan

$$q\prod_{n=1}^{+\infty}(1-q^n)^{24} = \sum_{n=1}^{+\infty}\tau(n)q^n$$

τ est multiplicative i.e. si $\mathrm{pgcd}(m,n) = 1$, $\tau(mn) = \tau(m)\tau(n)$.
Existe-t-il une infinité de n tel que $\tau(n) = 0$? (pour l'instant, on n'en connait aucun)
Ramanujan a utilisé cette fonction pour expliquer une bizarrerie mathématique, à savoir $e^{\pi\sqrt{163}}$ est presque entier.

$$e^{\pi\sqrt{163}} \approx 262537412640768743,9999999999992\cdots$$

Posons

$$q = e^{2i\pi\tau}, \mid q \mid < 1$$

On définit aussi

$$\Delta(\tau) = q\prod_{n=1}^{+\infty}(1-q^n)^{24}$$

$$\mathrm{f}(\tau) = \frac{\Delta(2\tau)}{\Delta(\tau)}$$

L'invariant modulaire est

$$\mathrm{j}(\tau) = \frac{(256\mathrm{f}(\tau)+1)^3}{\mathrm{f}(\tau)}$$

On peut montrer

$$\mathrm{j}(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{+\infty} c_n q^n,\ \text{avec } c_n \in \mathbf{Z}$$

On a également le résultat
Si τ est racine d'une équation du second degré à coefficients entiers, alors $\mathrm{j}(\tau)$ est simple.
Ici

$$\mathrm{j}\left(\frac{1+i\sqrt{163}}{2}\right) = -640320^3$$

$$\tau = \frac{1 + i\sqrt{163}}{2}$$

$$q = e^{2i\pi\tau} = -e^{-\pi\sqrt{163}}$$

q est très petit donc $\frac{1}{q}$ est très grand.

$$\mathrm{j}(\tau) = -e^{-\pi\sqrt{163}} + 744 + \varepsilon$$

i.e.

$$e^{\pi\sqrt{163}} = 744 - \mathrm{j}(\tau) + \varepsilon = 640320^3 + 744 + \varepsilon$$

ε étant très petit, $e^{\pi\sqrt{163}}$ est presque entier.

6.2 Opérations sur les séries formelles

$$\mathrm{u}(z) = u_0 + u_1 z + \cdots + u_n z^n + \cdots$$

$$\mathrm{v}(z) = v_0 + v_1 z + \cdots + v_n z^n + \cdots$$

6.2.1 addition

La calcul de $w = u + v$ est évident.
Pour calculer w jusqu'à l'ordre N, la complexité est $\mathcal{O}(N)$.

6.2.2 produit

On cherche à calculer $w = u \times v$.

$$\mathrm{w}(z) = w_0 + w_1 z + \cdots + w_n z^n + \cdots$$

$$w_n = u_0 v_n + u_1 v_{n-1} + \cdots + u_n v_0$$

Le calcul de w_n nécessite $n + 1$ produits.
Pour calculer w jusqu'à l'ordre N, la complexité est $\mathcal{O}\left(N^2\right)$.

6.2.3 quotient

On cherche à calculer $w = \frac{u}{v}$, on suppose $v_0 \neq 0$.
Si $v_0 = v_1 = \cdots = v_{k-1} = 0$ et $v_k \neq 0$, w est une série de Laurent.

$$\mathrm{v}(z) = z^k \left(v_k + v_{k+1} z^{k+1} + \cdots\right)$$

$$\mathrm{w}(z) = \frac{\mathrm{u}(z)}{\mathrm{v}(z)} = \frac{1}{z^k} \frac{\mathrm{u}(z)}{v_k + v_{k+1} z + \cdots}$$

On peut donc toujours se ramener au cas $v_0 \neq 0$.
Pour calculer w, on dispose de plusieurs méthodes

- Division suivant les puissances croissantes

– Identification
  On a la relation

$$u = vw$$

  On a donc

$$v_n w_0 + v_{n-1} w_1 + \cdots + v_0 w_n = u_n$$

  On peut calculer les w_i par récurrence

$$\begin{cases} w_0 &= \dfrac{u_0}{v_0} \\ w_n &= \dfrac{1}{v_0}(u_n - v_n w_0 - v_{n-1} w_1 - \cdots - v_1 w_{n-1}) \end{cases}$$

  Le calcul de w_n nécessite n multiplications et une division.
  Pour calculer w jusqu'à l'ordre N, la complexité est $\mathcal{O}\left(N^2\right)$.
La division coûte aussi cher que la multiplication.

Application

$$\sum_{n=0}^{+\infty} \mathrm{p}(n) x^n = \frac{1}{1 + \sum\limits_{n \geq 1} (-1)^n \left(x^{\frac{n(3n+1)}{2}} + x^{\frac{n(3n-1)}{2}} \right)}$$

On calcule $\mathrm{p}(n)$ en $\mathcal{O}\left(N\sqrt{N}\right)$ opérations.

Remarque
Ici, on dispose d'un algorithme "on line", c'est à dire que si l'on a calculé jusqu'à l'ordre N, on peut calculer le w_{N+1} sans tout recommencer.

6.3 Calcul de $\mathrm{v}(x)^\alpha, \alpha \in \mathbf{R}$

$$\mathrm{v}(x) = v_0 + v_1 x + \cdots$$

On suppose $v_0 = 1$.
Si $v_0 = 0$, on met $v_k x^k$ en facteur comme pour le calcul du quotient.
On dispose de deux méthodes

– Méthode classique

$$\mathrm{u}(x) = \mathrm{v}(x) - 1 = v_1 x + v_2 x^2 + \cdots$$

$$\mathrm{v}(x)^\alpha = (1 + \mathrm{u}(x))^\alpha = 1 + \alpha \mathrm{u}(x) + \frac{\alpha(\alpha-1)}{2} \mathrm{u}(x)^2 + \cdots$$

  Pour aller jusqu'à l'ordre N, il faut calculer $u^2, u^3, \ldots, u^N$, chaque calcul nécessitant $\mathcal{O}\left(N^2\right)$ opérations. La complexité est donc $\mathcal{O}\left(N^3\right)$.
– Méthode de l'équation différentielle
  Cette méthode est bien meilleure puisque en $\mathcal{O}\left(N^2\right)$.

$$\mathrm{w}(x) = \mathrm{v}(x)^\alpha$$

En dérivant

$$\mathrm{w}'(x) = \alpha \mathrm{v}(x)^{\alpha-1}\mathrm{v}'(x) = \alpha \mathrm{v}(x)^{\alpha}\frac{\mathrm{v}'(x)}{\mathrm{v}(x)}$$

D'où

$$\mathrm{w}'(x)\mathrm{v}(x) - \alpha \mathrm{w}(x)\mathrm{v}'(x) = 0$$

On exprime v et w

$$\begin{aligned}
\mathrm{v}(x) &= 1 + v_1 x + \cdots + v_n x^n + \cdots \\
\mathrm{v}'(x) &= v_1 + 2v_2 x + \cdots + n v_n x^{n-1} + \cdots \\
\mathrm{w}(x) &= 1 + w_1 x + \cdots + w_n x^n + \cdots \\
\mathrm{w}'(x) &= w_1 + 2w_2 x + \cdots + n w_n x^{n-1} + \cdots
\end{aligned}$$

Le coefficient de x^{n-1} dans $w'v$ est

$$nw_n + (n-1)w_{n-1}v_1 + \cdots + v_1 w_{n-1} = \sum_{k=0}^{n} k w_k v_{n-k}$$

Le coefficient de x^{n-1} dans wv' est

$$\sum_{k=0}^{n} k v_k w_{n-k} = \sum_{k=0}^{n} (n-k) w_k v_{n-k}$$

Le coefficient de x^{n-1} dans $w'v - \alpha w v'$ est nul.
i.e.

$$\sum_{k=0}^{n} w_k v_{n-k}(k - \alpha(n-k)) = 0$$

D'où

$$nw_n = \sum_{k=0}^{n-1} w_k v_{n-k}(\alpha(n-k) - k)$$

On a donc une relation de récurrence pour calculer les w_n.
Pour calculer jusqu'à l'ordre N, il faut $\mathcal{O}\left(N^2\right)$ multiplications.

Remarque
Par des techniques voisines de la seconde méthode, on peut calculer :

–

$$\mathrm{w}(x) = e^{\mathrm{v}(x)}, v_0 = 0$$
$$w' = e^{v}v' = wv'$$

D'où

$$w' - wv' = 0$$

Calcul en $\mathcal{O}\left(N^2\right)$

–

$$\mathrm{w}(x) = \log(1 + \mathrm{v}(x)), v_0 = 0$$
$$w' = \frac{v'}{1+v}$$
$$w'(1+v) - v' = 0$$

Calcul en $\mathcal{O}\left(N^2\right)$

6.4 Inversion de séries formelles

On cherche à calculer la fonction réciproque, c'est-à-dire, si

$$z = \mathrm{v}(t) = t + v_2 t^2 + \cdots + v_n t^n + \cdots$$

on veut exprimer t en fonction de z

$$t = \mathrm{w}(z) = z + w_2 z^2 + \cdots + w_n z^n + \cdots$$

Encore une fois, il existe plusieurs méthodes

- On utilise la formule d'inversion de Lagrange.
  Pour n fixé, $n \geq 2$, on calcule

  $$\left(\frac{\mathrm{v}(t)}{t}\right)^{-n} = 1 + u_1^{(n)} + \cdots + u_k^{(n)} t^k + \cdots$$

  Le théorème de Lagrange dit que

  $$w_n = \frac{1}{n} u_{n-1}^{(n)}$$

  On calcule par récurrence $\left(\frac{\mathrm{v}(t)}{t}\right)^{-n}$ en divisant par $\frac{\mathrm{v}(t)}{t}$, ce qui se fait en $\mathcal{O}\left(N^2\right)$, d'où une complexité totale de $\mathcal{O}\left(N^3\right)$.
- Méthode d'itération
  Montrons son principe sur un exemple

  $$y = \arctan(x) = x - \frac{x^3}{3} + \frac{x^5}{5} + \mathcal{O}\left(x^7\right)$$

  D'où

  $$x = y + \frac{x^3}{3} - \frac{x^5}{5} + \mathcal{O}\left(y^7\right) = y + \mathcal{O}\left(y^3\right)$$

  En itérant

  $$x = y + \frac{1}{3}\big(y + \mathcal{O}\left(y^3\right)\big)^3 + \mathcal{O}\left(y^5\right) = y + \frac{y^3}{3} + \mathcal{O}\left(y^5\right)$$

  Puis

  $$x = y + \frac{1}{3}\left(y + \frac{y^3}{3} + \mathcal{O}\left(y^5\right)\right)^3 - \frac{1}{5}\left(y + \frac{y^3}{3} + \mathcal{O}\left(y^5\right)\right)^5 + \mathcal{O}\left(y^7\right)$$

  D'où

  $$x = y + \frac{y^3}{3} + \frac{2}{15} y^5 + \mathcal{O}\left(y^7\right)$$

  On ne gagne qu'un coefficient à chaque étape.
- Méthode de Newton

  $$x_{n+1} = x_n - \frac{\mathrm{f}(x_n)}{\mathrm{f}'(x_n)}$$

La convergence est quadratique, i.e. le nombre de chiffres significatifs double à chaque étape. On peut, comme ceci, obtenir assez rapidement une bonne approximation de $\sqrt{2}$

$$\mathrm{f}(x) = x^2 - 2$$

$$x_{n+1} = x_n - \frac{x_n^2 - 2}{2x_n}$$

On adapte cette méthode au cas des séries formelles.

$$z = t + v_2 t^2 + \cdots = \mathrm{v}(t)$$

$$t = \mathrm{w}(z) = z + w_2 z^2 + \cdots$$

$$t_{n+1} = t_n - \frac{\mathrm{v}(t_n) - z}{\mathrm{v}'(t_n)}$$

où

$$t_n = z + \cdots + w_{n-1} z^{n-1} + \mathcal{O}\left(z^n\right)$$

t_{n+1} sera en $\mathcal{O}\left(z^{2n}\right)$.
On double le nombre de coefficients à chaque étape.

6.5 Composition des séries formelles

$$\mathrm{u}(z) = z + u_2 z^2 + \cdots + u_n z^n + \cdots$$

$$\mathrm{v}(z) = v_0 + v_1 t + \cdots + v_n t^n + \cdots$$

On veut calculer $\mathrm{w}(z) = \mathrm{v}(\mathrm{u}(z))$.
Il existe plusieurs méthodes :

–

$$\begin{array}{rcl} t & = & \mathrm{u}(z) \\ t^2 & = & \mathrm{u}(z)^2 \\ & \vdots & \\ t^n & = & \mathrm{u}(z)^n = z^n + \mathcal{O}\left(z^{n+1}\right) \end{array}$$

Chaque calcul, excepté le dernier, se fait en $\mathcal{O}\left(n^2\right)$ d'où une complexité en $\mathcal{O}\left(N^3\right)$.

– Diviser pour régner

$$\mathrm{V}(t) = \underbrace{t + \cdots + v_{m-1} t^{m-1}}_{V_0} + t^m \underbrace{\left(v_m + v_{m+1} t^{m+1} + \cdots + v_n t^{n-m}\right)}_{V_1} + \mathcal{O}\left(t^{n+1}\right)$$

Le meilleur choix pour m est $\sqrt{n \log n}$. On peut aussi prendre $m = \sqrt{n}$.
Sur les séries formelles, la formule de Taylor est vraie.
On a

$$\mathrm{V}(t) = V_0 + t^m V_1 + \mathcal{O}\left(t^{n+1}\right)$$

$$\mathrm{U}(z) = \mathrm{U}\big(V_0 + t^m V_1 + \mathcal{O}\left(t^{n+1}\right)\big)$$

D'où

$$\mathrm{U}(z) = \mathrm{U}(V_0) + t^m V_1 \mathrm{U}'(V_0) + \frac{t^{2m} V_1^2}{2} \mathrm{U}''(V_0) + \cdots$$

Pour aller jusqu'à l'ordre N, la complexité est $\mathcal{O}\left((N \log N)^{\frac{3}{2}}\right)$.

6.6 Deux exemples d'application des séries formelles

6.6.1 Premier exemple

Soit $u_0 \in \mathbf{R}$, on définit $(u_n)_{n\in\mathbf{N}}$ par la formule de récurrence $u_{n+1} = \sin(u_n)$. Montrer que $u_n \to 0$ et trouver un équivalent de u_n.
Quitte à poser $v_n = -u_n$, on peut supposer $u_1 \geq 0$.
On a alors, pour $n \geq 1$, $0 \leq u_n \leq 1$ et comme $\sin(x) \leq x$, (u_n) est décroissante. Comme elle est positive, elle admet une limite l. La fonction sin étant continue, on a à la limite $\sin(l) = l$, donc $l = 0$.

On va utiliser la méthode en α, c'est-à-dire on cherche α tel que

$$u_{n+1}^{\alpha} - u_n^{\alpha} \to l$$

lemme 6.1

$$\lim_{x\to 0}\left(\frac{1}{\sin^2(x)} - \frac{1}{x^2}\right) = \frac{1}{3}$$

preuve :

$$\begin{aligned}
\frac{1}{\sin(x)^2} - \frac{1}{x^2} &= \frac{x^2 - \sin^2(x)}{x^2\sin^2(x)} \\
&= \frac{(x-\sin(x))(x+\sin(x))}{x^2\sin^2(x)} \\
&\sim \frac{\frac{x^3}{6}2x}{x^2x^2} \\
&\sim \frac{1}{3}
\end{aligned}$$

■

théorème 6.2 (*Césaro*)

Si $a_n \to l$, $\dfrac{a_1 + \cdots + a_n}{n} \to l$.

On a

$$\lim_{n\to+\infty}\left(\frac{1}{u_{n+1}^2} - \frac{1}{u_n^2}\right) = \frac{1}{3}$$

Par le théorème de Césaro

$$\frac{1}{n-1}\sum_{k=1}^{n-1}\left(\frac{1}{u_{k+1}^2} - \frac{1}{u_k^2}\right) \to \frac{1}{3}$$

De plus

$$\frac{1}{n-1}\sum_{k=1}^{n-1}\left(\frac{1}{u_{k+1}^2}-\frac{1}{u_k^2}\right)=\frac{1}{n-1}\left(\frac{1}{u_n^2}-\frac{1}{u_1^2}\right)$$

Or

$$\frac{1}{n-1}\left(\frac{1}{u_n^2}-\frac{1}{u_1^2}\right)\sim\frac{1}{nu_n^2}$$

Donc

$$\frac{1}{nu_n^2}\sim\frac{1}{3}$$

D'où

$$u_n\sim\sqrt{\frac{3}{n}}$$

Maple

```
rsolve(u(i+1)=sin(u(i)),u(i));
-
asympt(%,i,10);
```

$$\sqrt{\frac{3}{n}}\left(1-\frac{3}{10}\frac{\log(n)}{n}-\frac{3}{2}\frac{B}{n}+\frac{27}{200}\frac{\log^2(n)}{n^2}+\sum_k\frac{\mathrm{P_k}(\log(n),B)}{n^k}\right)$$

6.6.2 Second exemple

$$\mathrm{li}(x)=\int_2^x\frac{\mathrm{d}t}{\log(t)}$$

On peut montrer

$$\mathrm{li}(x)\sim\frac{x}{\log(x)}$$

En faisant une intégration par parties, on écrit

$$\mathrm{li}(x)=\frac{x}{\log(x)}+\frac{x}{\log^2(x)}+\frac{2x}{\log^3(x)}+\cdots+\frac{(k-1)!\,x}{\log^{\mathrm{k}}(x)}+\mathcal{O}\left(\frac{x}{\log^{\mathrm{k}+1}(x)}\right)$$

li est croissante, continue donc admet une fonction réciproque. On souhaite un développement asymptotique de $x=\mathrm{li}^{-1}(y)$ en fonction de $y=\mathrm{li}(x)$.
On utilise la méthode d'itération

$$y\sim\frac{x}{\log(x)}$$

D'où

$$\log(y)\sim\log(x)-\log(\log(x))\sim\log(x)$$

Or

$$x\sim y\log(x)$$

Donc

$$x\sim y\log(y)$$

i.e.
$$x = y\log(y)(1 + \mathrm{o}(1))$$

D'où
$$\log(x) = \log(y) + \log(\log(y)) + \log(1 + \mathrm{o}(1))$$

i.e.
$$\log(x) = \log(y) + \log(\log(y)) + \mathrm{o}(1)$$

On remplace dans $x = y\log(x)$.
En itérant, on arrive finalement à

$$x = y\left(\log(y) + \log(\log(y)) - 1 + \sum_{k=1}^{K} \frac{\mathrm{P_k}(\log(\log(y)))}{(\log(y))^k} + \mathcal{O}\left(\ldots\right)\right)$$

Application
On désigne par $\Pi(x)$ le nombre de nombres premiers inférieurs à x.

$$\Pi(x) = \mathrm{li}(x) + \text{ reste assez petit} \sim \frac{x}{\log(x)}$$

En fait, on a

$$\Pi(x) = \frac{x}{\log(x)} + \frac{x}{\log^2(x)} + \cdots + \frac{(k-1)!\,x}{\log^{\mathrm{k}}(x)} + \mathcal{O}\left(\frac{x}{\log^{\mathrm{k}+1}(x)}\right)$$

Si on note p_n le $n^{\text{ème}}$ nombre premier, on a

$$\Pi(p_n) = n \approx \mathrm{li}(p_n)$$

D'où
$$p_n \approx \mathrm{li}^{-1}(n)$$

On a donc
$$p_n = n(\log(n) + \log(\log(n)) - 1 + \cdots)$$

On obtient donc une approximation du $n^{\text{ème}}$ nombre premier.

septième chapitre

Cryptographie

7.1 Les méthodes alphabétiques

La méthode de César
Il s'agit simplement de décaler les lettres de trois.

$$\begin{array}{ccc} A & \to & D \\ B & \to & E \\ & \vdots & \\ X & \to & A \\ Y & \to & B \\ Z & \to & C \end{array}$$

La méthode de Hill
Dans cette approche, on numérote les lettres de l'alphabet de 0 à 25. On peut ensuite voir tout nombre comme une lettre. Si n est un entier, en effectuant la division de n par 26, $n = 26q + r$, n code la $r^{\text{ème}}$ lettre de l'alphabet.
On choisit ensuite une matrice carrée 2×2 inversible dans $\mathbf{Z}/26\mathbf{Z}$.
Par exemple

$$M = \begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix}$$

Codons le mot `universite`.
On le découpe en morceaux de deux lettres, à savoir `un`, `iv`, `er`, `si` et `te`.

$$\texttt{un} = \begin{pmatrix} 21 \\ 14 \end{pmatrix}$$

`un` est codé en $M \begin{pmatrix} 21 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \end{pmatrix} = \texttt{eh}$.
Pour le décodage, on utilise $M^{-1} \bmod 26$.

Faiblesse de ces deux méthodes
Des méthodes linguistiques permettent de casser ces algorithmes de cryptage.
- Une analyse de la lettre la plus fréquente dans les messages codés par la méthode de César permet de casser la méthode.
- Pour casser la méthode de Hill, il faut étudier les doublons les plus fréquents. (méthode polyalphabétique)

7.2 RSA

Cette méthode tire son nom de ses auteurs : Rivest, Shamir et Adleman.
Si p et q sont deux nombres premiers, il est facile de calculer $n = pq$. En revanche, connaissant n, le calcul des facteurs premiers de n est difficile. On appelle une telle fonction une fonction à sens unique.
La méthode RSA ne permet de crypter que des messages numériques. Pour coder des lettres, on peut par exemple utiliser le code ASCII.

Algorithme RSA

- Choisir p et q deux nombres premiers de 100 chiffres environ.
- Calculer $n = pq$
- Calculer $\varphi = (p-1)(q-1)$
- Choisir d premier avec φ (par des méthodes probabilistes).
- Calculer e tel que $ed \equiv 1 \pmod{\varphi}$
- n et e sont publics
- p, q, φ et d sont privés
- Pour envoyer un message numérique M avec $M < n$, on calcule

  $$C = M^e \bmod n$$

  et on envoie le cryptogramme C.
- Pour décoder, on calcule $M = C^d \bmod n$

Connaissant e, calculer d est équivalent à factoriser n.
Le théorème d'Euler donne :
Si a et n sont premiers entre eux alors $a^{\varphi(n)} \equiv 1 \pmod{n}$.
Supposons

$$C = M^e \pmod{n}$$

Soit

$$M' = C^d \bmod n$$

Montrons que

$$M' = M$$

On a

$$M' \equiv M^{ed} \pmod{n}$$

Or

$$ed = 1 + k\varphi(n)$$

D'où

$$M' = M \times \left(M^{\varphi(n)}\right)^k \equiv M \pmod{n}$$

Comme M et M' sont compris entre 0 et n et qu'ils sont congrus modulo n, ils sont égaux.
On retrouve donc bien le message envoyé.

7.3 DES : Data Encryption Standard

Ce standard est vu comme une boite prenant en entrée une clé codée sur 64 bits et un message de 64 bits et qui renvoie un cryptogramme de 64 bits, i.e. c'est une fonction booléenne :

$$f : \mathbf{F}_2{}^{64} \times \mathbf{F}_2{}^{64} \to \mathbf{F}_2{}^{64}$$

L'avantage de ce standard est que la fonction est rapide à calculer (cela peut même être implémenté de manière matérielle) et que le procédé est symétrique, c'est-à-dire si $\mathrm{f}(\mathtt{key}, \mathtt{message}) = \mathtt{code}$, on a $\mathrm{f}(\mathtt{key}, \mathtt{code}) = \mathtt{message}$.
De nos jours, le codage sur 64 bits commencent à devenir facile à casser par la méthode qui essaie toutes les possibilités (à cause de la puissance des ordinateurs actuels), c'est pour cela qu'un nouveau standard va remplacer le DES : l'AES. La méthode employée sera certainement la méthode Rijndael qui est à l'essai actuellement.

annexe A

Solution des exercices

Exercice 1.1 — *Algorithme de Karatsuba* *énoncé page 11*

Soit $\mathrm{T}(m)$ le nombre d'opérations élémentaires demandées par le calcul de $P \times Q$ (P et Q étant de dégré inférieur à $2m = 2^{n+1}$).

On a la relation de récurrence :

$$\mathrm{T}(m) = \underbrace{3\mathrm{T}\left(\frac{m}{2}\right)}_{\text{diviser pour régner}} + \underbrace{\mathcal{O}(m)}_{\text{addition des polynômes}} + \underbrace{\mathcal{O}(1)}_{\text{multiplication par } X^m \text{ et } X^{2m}}$$

En effet, les multiplications par X^m et X^{2m} ne sont que des décalages et ne coûtent que $\mathcal{O}(1)$, l'addition de deux polynômes de degré n demande un temps $\mathcal{O}(n)$, les multiplications $P_1 \times Q_1$, $(P_1 - P_0) \times (Q_1 - Q_0)$ et $P_0 \times Q_0$ sont effectuées en appelant récursivement l'algorithme de multiplication.

On a donc :

$$\mathrm{T}(m) = 3\mathrm{T}\left(\frac{m}{2}\right) + \mathcal{O}(n)$$

D'où

$$\mathrm{T}(m) = \mathcal{O}\left(m^{\log_2 3}\right)$$

i.e.

$$\mathrm{T}(2^n) = \mathcal{O}\left(2^{n \log_2 3}\right)$$

Ainsi, si P et Q sont de degré inférieur à N, $n = \log_2 N$ et

$$\mathrm{T}(N) = \mathcal{O}\left(2^{\log_2 N \log_2 3}\right) = \mathcal{O}\left(N^{\frac{\log 3}{\log 2}}\right)$$

Exercice 1.2 — *Calcul de* π *énoncé page 11*

La clé est

$$\sum_{i=0}^{+\infty} \frac{1}{16^i} \frac{1}{8i+k} = \sqrt{2}^k \int_0^{\frac{1}{\sqrt{2}}} \frac{x^{k-1}}{1-x^8}\, dx$$

$$\begin{aligned}
\sqrt{2}^k \int_0^{\frac{1}{\sqrt{2}}} \tfrac{x^{k-1}}{1-x^8}\, dx &= \sqrt{2}^k \int_0^{\frac{1}{\sqrt{2}}} x^{k-1} \sum_{i=0}^{+\infty} x^{8i}\, dx \\
&= \sqrt{2}^k \int_0^{\frac{1}{\sqrt{2}}} \sum_{i=0}^{+\infty} x^{8i+k-1}\, dx \\
&\quad \text{(convergence normale de la série sur le segment } [0, \tfrac{1}{\sqrt{2}}]) \\
&= \sqrt{2}^k \sum_{i=0}^{+\infty} \int_0^{\frac{1}{\sqrt{2}}} x^{8i+k-1}\, dx \\
&= \sqrt{2}^k \sum_{i=0}^{+\infty} [\tfrac{x^{8i+k}}{8i+k}]_0^{\frac{1}{\sqrt{2}}} \\
&= \sum_{i=0}^{+\infty} \tfrac{1}{\sqrt{2}^{8i}} \tfrac{1}{8i+k} \\
&= \sum_{i=0}^{+\infty} \tfrac{1}{16^i} \tfrac{1}{8i+k}
\end{aligned}$$

Il ne reste plus qu'à montrer que :

$$\pi = \int_0^{\frac{1}{\sqrt{2}}} \frac{4\sqrt{2} - 8x^3 - 4\sqrt{2}x^4 - 8x^5}{1 - x^8}\, dx$$

Exercice 2.1 — *Suite de Fibonacci* *énoncé page 15*

question 1 – Le polynôme caractéristique de l'équation est $P = X^2 - X - 1$. Les racines de P sont

$$\begin{cases} \varphi = \frac{1+\sqrt{5}}{2} & \varphi \text{ est le nombre d'or} \\ \hat{\varphi} = \frac{1-\sqrt{5}}{2} & \end{cases}$$

D'où

$$F_n = \frac{1}{\sqrt{5}}(\varphi^n - \hat{\varphi}^n)$$

On peut aussi montrer que F_n est l'entier le plus proche de $\frac{\varphi^n}{\sqrt{5}}$.

question 2 – On raisonne par récurrence :

- $n = 0$
$$F_2 = 1 \geq 10^0$$
- $n = 1$
$$F_3 = 2 \geq 10^{\frac{1}{5}} \approx 1.58$$
- $n, n+1 \to n+2$
$$F_{n+2} = F_n + F_{n+1} \geq 10^{\frac{n-2}{5}} + 10^{\frac{n-1}{5}} \geq 10^{\frac{n-2}{5}} \left(1 + 10^{\frac{1}{5}}\right)$$
Or
$$\mathrm{P}\left(10^{\frac{1}{5}}\right) < 0$$
i.e.
$$1 + 10^{\frac{1}{5}} > 10^{\frac{2}{5}}$$

D'où

$$F_{n+2} \geq 10^{\frac{n-2}{5}} \times 10^{\frac{2}{5}} = 10^{\frac{n}{5}}$$

question 3 – On pose

$$X_n = \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

On a

$$\begin{cases} X_{n+1} & = & AX_n \\ X_0 & = & \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{cases}$$

D'où

$$X_n = A^n X_0$$

En utilisant l'algorithme des puissances, A^n se calcule en $\mathcal{O}(\log_2 n)$, d'où un algorithme efficace calculant F_n.

Exercice 2.2 — *Majoration des racines d'un polynôme* *énoncé page 25*

question 1 – Soit $x > 0$

$$\begin{aligned} \mathrm{Q}(x) = 0 \quad & \Leftrightarrow \quad |\, a_0 \,| + \cdots + |\, a_{n-1} \,| x^{n-1} = x^n \\ & \Leftrightarrow \quad \frac{|a_0|}{x^n} + \cdots + \frac{|a_{n-1}|}{x} = 1 \end{aligned}$$

On définit $g : \mathbf{R}_+^\star \to \mathbf{R}$ par $\mathrm{g}(x) = \frac{|a_0|}{x^n} + \cdots + \frac{|a_{n-1}|}{x}$.
g est continue et strictement décroissante sur $\mathbf{R}_+^\star$.

$$\lim_{x \to 0^+} \mathrm{g}(x) = +\infty$$

$$\lim_{x \to +\infty} \mathrm{g}(x) = 0^+$$

Ainsi g réalise une bijection de $\mathbf{R}_+^\star$ sur $\mathbf{R}_+^\star$. Donc il existe un unique $r > 0$ tel que $\mathrm{g}(r) = 1$, i.e. il existe un unique $r > 0$ tel que $\mathrm{Q}(r) = 0$.
question 2 – g est strictement décroissante sur $\mathbf{R}_+^\star$.

$$\mathrm{P}(z_n) = 0$$

i.e.

$$z_n^n = -a_{n-1} z_n^{n-1} - \cdots - a_0$$

D'où, en appliquant l'inégalité triangulaire,

$$|\, z_n \,|^n \leq |\, a_{n-1} \,||\, z_n \,|^{n-1} + \cdots + |\, a_0 \,|$$

i.e.

$$M^n \leq |\, a_{n-1} \,| M^{n-1} + \cdots + |\, a_0 \,|$$

i.e.

$$\mathrm{g}(r) = 1 \leq \mathrm{g}(M)$$

Donc
$$M \leq r$$

question 3 – Posons $B = \max\limits_{0 \leq k \leq n-1} \mid a_k \mid$

- Si $r \leq 1$, c'est évident d'après la question précédente.
- Sinon $r > 1$
$$r^n = \mid a_{n-1} \mid r^{n-1} + \cdots + \mid a_0 \mid$$
D'où
$$r^n \leq B\big(r^{n-1} + \cdots + 1\big)$$
i.e.
$$r^n \leq B\frac{r^n - 1}{r - 1}$$
Donc
$$\frac{r^{n+1} - r^n}{r^n - 1} \leq B$$
i.e.
$$\frac{r - 1}{1 - \frac{1}{r^n}} \leq B$$
Or
$$0 < 1 - \frac{1}{r^n} \leq 1$$
Donc
$$\frac{1}{1 - \frac{1}{r^n}} \geq 1$$
D'où
$$\frac{r - 1}{1 - \frac{1}{r^n}} \geq r - 1$$
Ainsi
$$B \geq r - 1$$
i.e.
$$r \leq 1 + B$$

On a montré que
$$M \leq 1 + \max_{0 \leq k \leq n-1} \mid a_k \mid$$

Exercice 2.3 — *Méthode de Hensel*

énoncé page 28

On raisonne par récurrence sur n

- $n = 1$
  c'est l'hypothèse

– $n \to n+1$
Soit x_n donné par l'hypothèse de récurrence
On cherche x_{n+1} sous la forme $x_{n+1} = x_n + \lambda p^n$
On utilise la formule de Taylor

$$\mathrm{P}(x_{n+1}) \equiv \mathrm{P}(x_n) + \lambda p^n \mathrm{P}'(x_n) \pmod{p^{n+1}}$$

En effet, pour $k \geq 2$

$$\frac{\mathrm{P}^{(\mathrm{k})}(x_n)}{k!} \in \mathbf{Z}$$

On montre ceci pour les monômes

$$P = X^l$$

Alors

$$P^{(k)} = l(l-1)\cdots(l-k)X^{l-k}$$

Donc

$$\frac{\mathrm{P}^{(\mathrm{k})}(x_n)}{k!} = \frac{l(l-1)\cdots(l-k)}{k!} {x_n}^{l-k} = \mathrm{C}_l^k {x_n}^{l-k} \in \mathbf{Z}$$

Or

$$\mathrm{P}(x_n) \equiv 0 \pmod{p^n}$$

Donc

$$\exists a \in \mathbf{Z} | \mathrm{P}(x_n) = p^n a$$

D'où

$$\mathrm{P}(x_{n+1}) \equiv p^n(a + \lambda \mathrm{P}'(x_n)) \pmod{p^{n+1}}$$

On cherche donc λ tel que

$$p^n(a + \lambda \mathrm{P}'(x_n)) \equiv 0 \pmod{p^{n+1}}$$

c'est-à-dire tel que

$$a + \lambda \mathrm{P}'(x_n) \equiv 0 \pmod{p}$$

Or

$$\mathrm{P}'(x_n) \not\equiv 0 \pmod{p}$$

Car

$$\left\{ \begin{array}{c} \mathrm{P}'(x_n) \equiv \mathrm{P}'(x_0) \pmod{p} \\ \mathrm{P}'(x_0) \not\equiv 0 \pmod{p} \end{array} \right.$$

Donc

$$\lambda = -\frac{a}{\mathrm{P}'(x_n)} \pmod{p}$$

On a donc

$$\mathrm{P}(x_{n+1}) \equiv 0 \pmod{p^n}$$

et

$$x_{n+1} \equiv x_n \equiv x_0 \pmod{p}$$

Montrons l'unicité :
Soit x et y tels que :

$$\begin{array}{c} x \not\equiv y \pmod{p^{n+1}} \\ x \equiv y \equiv x_0 \pmod{p} \\ \mathrm{P}(x) \equiv 0 \pmod{p^{n+1}} \\ \mathrm{P}(y) \equiv 0 \pmod{p^{n+1}} \end{array}$$

Donc
$$P \equiv (X-x)(X-y)Q \pmod{p^{n+1}}$$
Donc
$$P \equiv (X-x_0)^2 Q \pmod{p}$$
Alors x_0 est au moins racine double de P modulo p, contredisant ainsi $\mathrm{P}'(x_0) \not\equiv 0 \pmod{p}$.

Exercice 5.1

énoncé page 78

$$\mathrm{f}(x) = a_m(x-\alpha_1)\cdots(x-\alpha_m)$$
$$\mathrm{g}(x) = b_n(x-\beta_1)\cdots(x-\beta_n)$$

avec $\alpha_1 = \alpha$ et $\beta_1 = \beta$.

- Montrons que $\alpha\beta$ est algébrique
  On pose
  $$\mathrm{h}(x) = x^n \mathrm{g}\left(\frac{y}{x}\right)$$
  $\mathrm{h}(x)$ est bien un polynôme.
  On définit P par
  $$\mathrm{P}(y) = \mathrm{R_x}(f,h) = a_m^n \prod_{i=1}^{m} \alpha_i^n \mathrm{g}\left(\frac{y}{\alpha_i}\right)$$
  Si on suppose $\alpha \neq 0$, alors $\forall i, \alpha_i \neq 0$ car sinon f ne serait pas le polynôme minimal de α.
  On a alors
  $$\mathrm{P}(y) = 0 \Leftrightarrow \mathrm{g}\left(\frac{y}{\alpha_i}\right) = 0 \Leftrightarrow \frac{y}{\alpha_i} = \beta_j \Leftrightarrow y = \alpha_i\beta_j$$
- Montrons que $\frac{\alpha}{\beta}$ est algébrique
  On définit P par
  $$\mathrm{P}(y) = \mathrm{R_x}(\mathrm{f}(yx), g) = b_n^m \prod_{j=1}^{n} \mathrm{f}(\beta_j y)$$
  Si on suppose $\beta \neq 0$, alors $\forall j, \beta_j \neq 0$ car sinon g ne serait pas le polynôme minimal de β.
  On a alors
  $$\mathrm{P}(y) = 0 \Leftrightarrow \mathrm{f}(\beta_j y) = 0 \Leftrightarrow \beta_j y = \alpha_i \Leftrightarrow y = \frac{\alpha_i}{\beta_j}$$

annexe B

Listes

B.1 Liste des définitions

B.2 Liste des théorèmes

B.3 Liste des exercices