

# Algorithmique avancée : Polynômes et séries

Serge Haddad

LMF, ENS Paris-Saclay & CNRS

L3

- 1 Produit rapide de polynômes
- 2 Produit rapide de polynômes sans racines primitives de l'unité
- 3 Inversion de série
- 4 Division de polynômes

# Plan

## 1 Produit rapide de polynômes

Produit rapide de polynômes sans racines primitives de l'unité

Inversion de série

Division de polynômes

# Un premier algorithme

**Hypothèses.** Soit  $\mathbb{A}$  un anneau. On suppose que :

- ▶  $\mathbb{A}$  est *commutatif*, i.e.  $\forall x, y \in \mathbb{A} \ xy = yx$
- ▶  $2 = 1 + 1$  est *invertible*, i.e.  $\exists 2^{-1} \ 2^{-1}2 = 1$

On dit que  $a$  est un *diviseur de 0*, noté  $a \mid 0$  s'il existe  $b \neq 0$  tel que  $ab = 0$ .

On ne suppose pas que  $\mathbb{A}$  est *intègre* : il peut exister  $a \neq 0$  diviseur de 0.

Soit  $P, Q$ , deux polynômes de degré  $< n$ .

```
For  $i$  from 0 do  $2n - 2$  do  $R[i] \leftarrow 0$   
For  $i$  from 0 do  $n - 1$  do  
  For  $j$  from 0 do  $n - 1$  do  
     $R[i + j] \leftarrow R[i + j] + P[i]Q[j]$   
Return( $R$ )
```

Complexité en  $\Theta(n^2)$

# L'algorithme de Karatsuba (1)

Supposons  $n = 2^k$ .

$$P = P^{(0)} + P^{(1)}X^{\frac{n}{2}} \text{ et } Q = Q^{(0)} + Q^{(1)}X^{\frac{n}{2}}$$

avec  $P^{(0)}, P^{(1)}, Q^{(0)}, Q^{(1)}$  des polynômes de degré  $< \frac{n}{2}$ .

$R$  s'exprime alors comme suit :

$$R = P^{(0)}Q^{(0)} + (P^{(1)}Q^{(0)} + P^{(0)}Q^{(1)})X^{\frac{n}{2}} + P^{(1)}Q^{(1)}X^n$$

ou encore :

$$R = P^{(0)}Q^{(0)} + ((P^{(0)} + P^{(1)})(Q^{(0)} + Q^{(1)}) - P^{(0)}Q^{(0)} - P^{(1)}Q^{(1)})X^{\frac{n}{2}} + P^{(1)}Q^{(1)}X^n$$

qui a l'avantage de nécessiter uniquement trois multiplications de matrices.

# L'algorithme de Karatsuba (2)

**ProduitRec**( $P, Q, n$ )

**If**  $n = 1$  **then**  $R[0] \leftarrow P[0]Q[0]$ ; **Return**( $R$ )

**For**  $i$  **from** 0 **to**  $\frac{n}{2} - 1$  **do**

$P^{(0)}[i] \leftarrow P[i]$ ;  $P^{(1)}[i] \leftarrow P[i + \frac{n}{2}]$ ;  $Q^{(0)}[i] \leftarrow Q[i]$ ;  $Q^{(1)}[i] \leftarrow Q[i + \frac{n}{2}]$

$SP[i] \leftarrow P[i] + P[i + \frac{n}{2}]$ ;  $SQ[i] \leftarrow Q[i] + Q[i + \frac{n}{2}]$

$R^{(0)} \leftarrow \mathbf{ProduitRec}(P^{(0)}, Q^{(0)}, \frac{n}{2})$ ;  $R^{(1)} \leftarrow \mathbf{ProduitRec}(P^{(1)}, Q^{(1)}, \frac{n}{2})$

$SR \leftarrow \mathbf{ProduitRec}(SP, SQ, \frac{n}{2})$

**For**  $i$  **from** 0 **to**  $\frac{n}{2} - 1$  **do**

$R[i] \leftarrow R^{(0)}[i]$

$R[i + \frac{n}{2}] \leftarrow R^{(0)}[i + \frac{n}{2}] + SR[i] - R^{(0)}[i] - R^{(1)}[i]$

$R[i + n] \leftarrow R^{(1)}[i] + SR[i + \frac{n}{2}] - R^{(0)}[i + \frac{n}{2}] - R^{(1)}[i + \frac{n}{2}]$

$R[i + \frac{3n}{2}] \leftarrow R^{(1)}[i + \frac{n}{2}]$

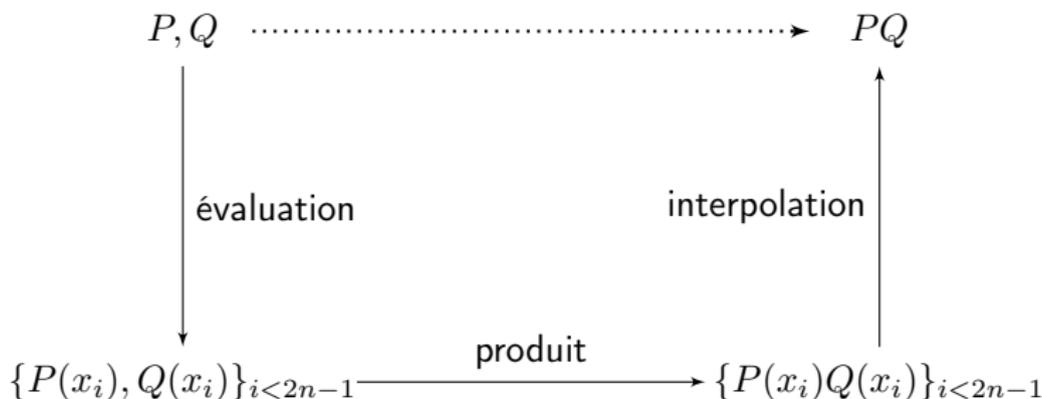
**Return**( $R$ )

D'après les équations de récurrence, complexité en  $\Theta(n^{\log_2(3)})$ .

# Multiplication par évaluation-interpolation

Soit  $\mathbb{A}$  un corps.

Le produit  $PQ$  de degré inférieur à  $2n - 1$  peut se calculer à l'aide de  $2n - 1$  valeurs distinctes  $\{x_i\}_{0 \leq i < 2n-1}$ .



Le produit des évaluations s'effectue en  $\Theta(n)$ .

Quid de l'évaluation et de l'interpolation ?

# L'algorithme de Horner

Soit  $P$  un polynôme de degré inférieur à  $n$  et  $v$  une valeur.

```
 $s \leftarrow P[n - 1]$   
For  $i$  from  $n - 2$  downto  $0$  do  
   $(s = \sum_{k=i+1}^{n-1} P[k]v^{k-i-1})$   
   $s \leftarrow s \times v + P[i]$   
   $(s = \sum_{k=i}^{n-1} P[k]v^{k-i})$   
Return( $s$ )
```

- $n - 1$  multiplications et additions.
- L'étape d'évaluation s'effectue en  $\Theta(n^2)$ .

# L'interpolation de Lagrange

Soit  $\{x_i, y_i\}_{i < n}$  ( $\{X[i], Y[i]\}_{i < n}$ ) les  $n$  points. Alors  $P = \sum_{i=1}^n y_i \frac{\prod_{j \neq i} X - x_j}{\prod_{j \neq i} x_i - x_j}$  est l'unique polynôme de degré inférieur à  $n$  qui les rencontre.

```
Q[0] ← -X[1]; Q[1] ← 1;
```

```
For i from 2 to n do (Q =  $\prod_{j < i} X - x_j$ )
```

```
Q[i] ← 1
```

```
For j from i - 1 downto 1 do Q[j] ← -X[i]Q[j] + Q[j - 1]
```

```
Q[0] ← -X[i]Q[0]
```

```
For i from 0 to n - 1 do P[i] ← 0
```

```
For i from 1 to n do (P =  $\sum_{j < i} y_j \frac{\prod_{j=1}^n X - x_j}{(\prod_{j \neq i} (x_i - x_j)(X - x_i))}$ )
```

```
c ← Y[i]; For j from 1 to n do if j ≠ i then c ←  $\frac{c}{X[i] - X[j]}$ 
```

```
R[n - 1] ← Q[n]; For j from n - 1 downto 1 do R[j - 1] ← Q[j] + X[i]R[j]
```

```
For j from 0 to n - 1 do P[j] ← P[j] + cR[j]
```

L'étape d'interpolation s'effectue en  $\Theta(n^2)$ .

# Racine primitive de l'unité

Soit  $n \in \mathbb{N}^*$ .  $\omega \in \mathbb{A}$  est une racine  $n$ ième de l'unité si  $\omega^n = 1$ .

$\omega$  est primitive si  $\forall 1 \leq i < n, \neg \omega^i - 1 \mid 0$ .

1.  $\omega^0, \omega^1, \dots, \omega^{n-1}$  sont des racines  $n$ ïèmes de l'unité toutes distinctes.
2. Si  $n$  est pair alors  $\omega^2$  est une racine  $\frac{n}{2}$ ième primitive de l'unité et  $\omega^{\frac{n}{2}} = -1$ .
3. Pour tout  $1 \leq i < n$ , on a  $\sum_{j=0}^{n-1} (\omega^i)^j = 0$ .

## Preuve.

1.  $(\omega^i)^n = (\omega^n)^i = 1$ . S'il existe  $0 \leq i < j < n$  tels que  $\omega^j = \omega^i$  alors  $(\omega^{j-i} - 1)\omega^i = 0$ . Donc  $\omega^{j-i} - 1 \mid 0$ , une contradiction.
2.  $(\omega^2)^{\frac{n}{2}} = \omega^n = 1$  et pour tout  $0 \leq i < \frac{n}{2}$   $(\omega^2)^i = \omega^{2i}$ , d'où  $\neg \omega^{2i} - 1 \mid 0$ .  
 $(\omega^{\frac{n}{2}} - 1)(\omega^{\frac{n}{2}} + 1) = \omega^n - 1 = 0$ . Puisque  $\neg \omega^{\frac{n}{2}} - 1 \mid 0$ ,  $\omega^{\frac{n}{2}} + 1 = 0$ .
3.  $(\sum_{j=0}^{n-1} (\omega^i)^j)(\omega^i - 1) = (\omega^i)^n - 1 = 0$ . Puisque  $\neg \omega^i - 1 \mid 0$ ,  $\sum_{j=0}^{n-1} (\omega^i)^j = 0$ .

# Polynôme et racine primitive

Soit  $P = \sum_{i < n} p_i X^i$  et  $\omega$  une racine  $n$ ième primitive avec  $n = 2^k$ .

Notons  $P^{(0)} = \sum_{i < \frac{n}{2}} p_{2i} X^i$  et  $P^{(1)} = \sum_{i < \frac{n}{2}} p_{2i+1} X^i$

$$P(X) = P^{(0)}(X^2) + X P^{(1)}(X^2)$$

D'où, en notant que  $\omega^{k+\frac{n}{2}} = \omega^{\frac{n}{2}} \omega^k = -\omega^k$  :

- ▶  $\forall 0 \leq k < \frac{n}{2} \quad P^{(0)}(\omega^{2k}) = P^{(0)}(\omega^{2(\frac{n}{2}+k)}) = \sum_{i < \frac{n}{2}} p_{2i} (\omega^{2k})^i$
- ▶  $\forall 0 \leq k < \frac{n}{2} \quad P^{(1)}(\omega^{2k}) = P^{(1)}(\omega^{2(\frac{n}{2}+k)}) = \sum_{i < \frac{n}{2}} p_{2i+1} (\omega^{2k})^i$
- ▶  $\forall 0 \leq k < \frac{n}{2} \quad P(\omega^k) = P^{(0)}(\omega^{2k}) + \omega^k P^{(1)}(\omega^{2k})$
- ▶  $\forall 0 \leq k < \frac{n}{2} \quad P(\omega^{\frac{n}{2}+k}) = P^{(0)}(\omega^{2k}) - \omega^k P^{(1)}(\omega^{2k})$

# Transformée de Fourier rapide

- Evaluation de  $P$  sur les  $n$  racines  $\omega^0, \dots, \omega^{n-1}$  (stockées dans  $T$ ).

**FFT**( $P, T, n$ ) :

**If**  $n = 1$  **then**  $F[0] \leftarrow P[0]$  ; **Return**( $F$ )

**For**  $i$  **from** 0 **to**  $\frac{n}{2} - 1$  **do**

$P^{(0)}[i] \leftarrow P[2i]$  ;  $P^{(1)}[i] \leftarrow P[2i + 1]$  ;  $T'[i] \leftarrow T[2i]$

$F^{(0)} \leftarrow \mathbf{FFT}(P^{(0)}, T', \frac{n}{2})$  ;  $F^{(1)} \leftarrow \mathbf{FFT}(P^{(1)}, T', \frac{n}{2})$

**For**  $i$  **from** 0 **to**  $\frac{n}{2} - 1$  **do**

$v \leftarrow T[i]F^{(1)}[i]$  ;  $F[i] \leftarrow F^{(0)}[i] + v$  ;  $F[\frac{n}{2} + i] \leftarrow F^{(0)}[i] - v$

**Return**( $F$ )

- D'après les équations de récurrence, cette étape s'effectue en  $\Theta(n \log(n))$ .

# Anneau de polynômes quotient

Soit  $D = \sum_{i \leq n} d_i X^i$  avec  $d_n$  inversible.

$\mathbb{A}[X]/D$  est l'ensemble des classes d'équivalence de  $A[X]$

par la relation  $P \sim Q$  si  $P \bmod D = Q \bmod D$ .

Le représentant de la classe d'équivalence de  $P$  est  $P \bmod D$  (de degré  $< n$ ).

$\mathbb{A}[X]/D$  est un anneau et on note  $P \cdot_D Q$  le produit dans  $\mathbb{A}[X]/D$ .

**Deux anneaux quotients particuliers.**

$$P \cdot_{X^{n-1}} Q = \sum_{k < n} \left( \sum_{i+j=k} p_i q_j + \sum_{i+j=k+n} p_i q_j \right) X^k$$

$$P \cdot_{X^{n+1}} Q = \sum_{k < n} \left( \sum_{i+j=k} p_i q_j - \sum_{i+j=k+n} p_i q_j \right) X^k$$

# Anneau quotient et racine primitive

- Soit  $\omega$  une racine  $n$ ième primitive,  $P = \sum_{i < n} p_i X^i$  et  $Q = \sum_{i < n} q_i X^i$ .

$$PQ = H(X^n - 1) + P \cdot_{X^{n-1}} Q \text{ pour un certain } H$$

D'où pour tout  $i$ ,  $P(\omega^i)Q(\omega^i) = PQ(\omega^i) = P \cdot_{X^{n-1}} Q(\omega^i)$ .

- Soit  $\theta$  une racine  $2n$ ième primitive. Notons  $\widehat{P} = \sum_{i < n} \theta^i p_i X^i$ .

$$\begin{aligned} P \widehat{\cdot_{X^{n+1}}} Q &= \sum_{k < n} \theta^k \left( \sum_{i+j=k} p_i q_j - \sum_{i+j=k+n} p_i q_j \right) X^k \\ &= \sum_{k < n} \left( \sum_{i+j=k} \theta^i p_i \theta^j q_j - \theta^{-n} \sum_{i+j=k+n} \theta^i p_i \theta^j q_j \right) X^k \\ &= \sum_{k < n} \left( \sum_{i+j=k} \theta^i p_i \theta^j q_j + \sum_{i+j=k+n} \theta^i p_i \theta^j q_j \right) X^k = \widehat{P} \cdot_{X^{n-1}} \widehat{Q} \end{aligned}$$

# Interpolation et racine primitive

Soit  $P = \sum_{i < n} p_i X^i$  et l'application  $f_{n,\omega}$  qui associe à  $(p_0, \dots, p_{n-1})$ ,

$$f_{n,\omega}(p_0, \dots, p_{n-1}) = (P(\omega^0), \dots, P(\omega^{n-1}))$$

C'est une application linéaire.

$\mathbf{M}_{n,\omega}$ , sa matrice  $\{0, \dots, n-1\} \times \{0, \dots, n-1\}$  est définie par :  $\mathbf{M}_{n,\omega}[i, j] = \omega^{ij}$ .

$$\mathbf{M}_{n,\omega} \mathbf{M}_{n,\omega^{-1}} = n \mathbf{Id}$$

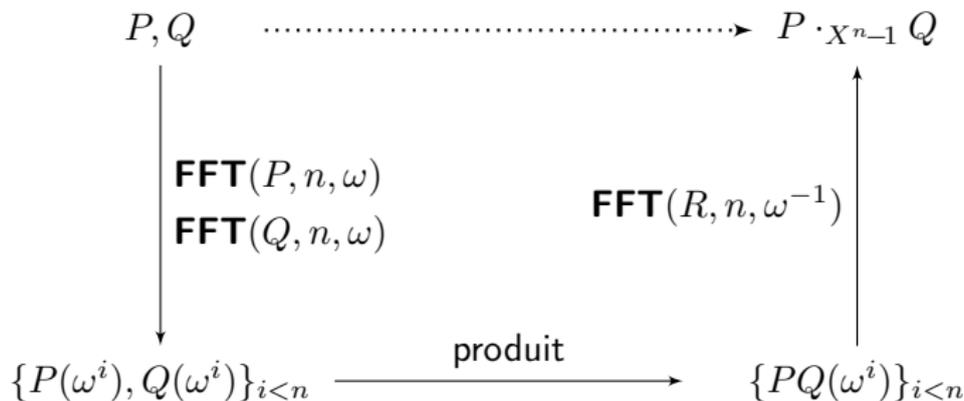
**Preuve.**

$$\mathbf{M}_{n,\omega} \mathbf{M}_{n,\omega^{-1}}[i, i] = \sum_{k < n} \omega^{ik} \omega^{-ki} = n$$

$$i \neq j \quad \mathbf{M}_{n,\omega} \mathbf{M}_{n,\omega^{-1}}[i, j] = \sum_{k < n} \omega^{ik} \omega^{-kj} = \sum_{k < n} (\omega^{i-j})^k = 0$$

# Multiplication rapide dans $\mathbb{A}[X]/X^n - 1$

On note  $R = n^{-1} \sum_{i < n} PQ(\omega^i) X^i$ .

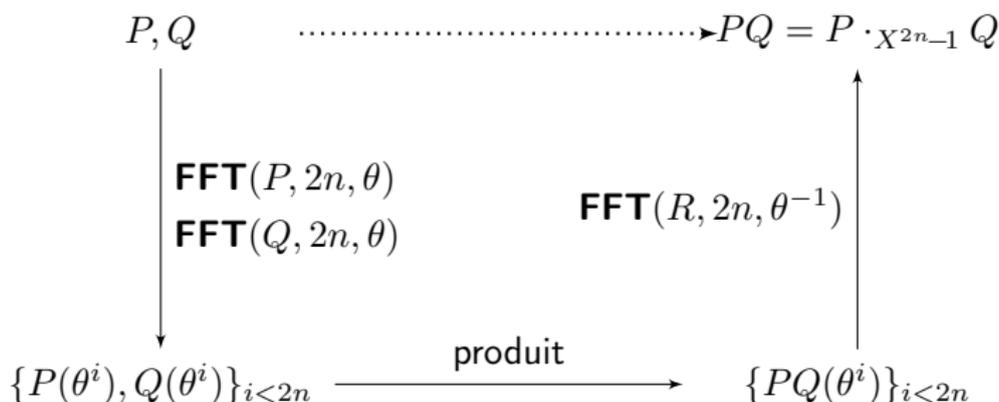


La complexité de cet algorithme est en  $\Theta(n \log(n))$ .

# Multiplication rapide dans $\mathbb{A}[X]$

On se place dans  $\mathbb{A}[X]/X^{2n}-1$ . Soit  $\theta$  une racine  $2n$ ième primitive.

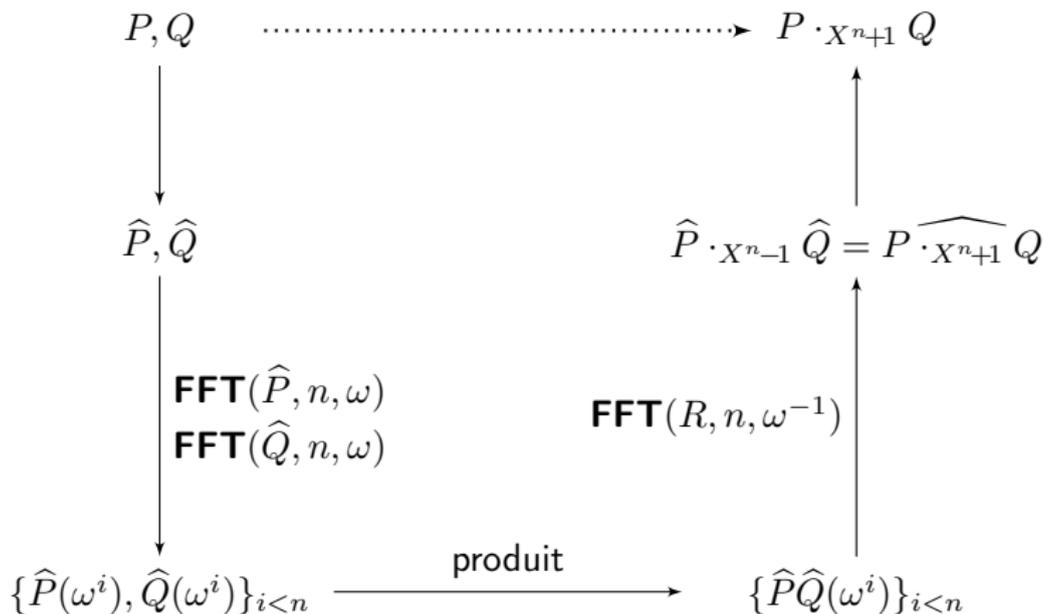
$$R = (2n)^{-1} \sum_{i < 2n} PQ(\theta^i) X^i.$$



Application à  $\mathbb{A} = \mathbb{R}$  en plongeant  $\mathbb{R}$  dans  $\mathbb{C}$  avec  $\omega = e^{\frac{2i\pi}{n}}$ .

# Multiplication rapide dans $\mathbb{A}[X]/X^n+1$

On note  $R = n^{-1} \sum_{i < n} \widehat{P} \widehat{Q}(\omega^i) X^i$ .



Les opérations supplémentaires s'effectuent en  $\Theta(n)$ .

# Plan

Produit rapide de polynômes

② Produit rapide de polynômes sans racines primitives de l'unité

Inversion de série

Division de polynômes

# Une racine primitive dans $\mathbb{A}[X]/X^n + 1$

Soit  $n = 2^k$  avec  $k \in \mathbb{N}^*$ . Alors :

$\theta = X$  est une racine  $2n$ -ième primitive de l'unité dans  $\mathbb{A}[X]/X^n + 1$ .

**Preuve.**  $\theta^n = -1$ . Donc  $\theta$  est une racine  $2n$ -ième de l'unité.

Montrons que pour tout  $1 \leq t < 2n$ ,  $\neg \theta^t - 1 \mid 0$ .

**Observation.** Soient  $p, q \in \mathbb{Z}$  avec  $q > 0$ ,

$$\theta^{pq} - 1 = (\theta^p - 1)(1 + \theta^p + \theta^{2p} + \dots + \theta^{(q-1)p}).$$

Donc, si  $\neg \theta^{pq} - 1 \mid 0$  alors  $\neg \theta^p - 1 \mid 0$ .

• Soit  $q < 0$ ,  $\theta^{pq} - 1 = \theta^{pq}(1 - \theta^{-pq})$ ,  $\theta^{pq} - 1 \mid 0$  si et seulement si  $\theta^{-pq} - 1 \mid 0$ .

D'où pour tout  $p, q \in \mathbb{Z}$ , si  $\neg \theta^{pq} - 1 \mid 0$  alors  $\neg \theta^p - 1 \mid 0$ .

•  $\theta^n - 1 = -2$  inversible donc  $\neg \theta^n - 1 \mid 0$ .

Posons  $g = \text{pgcd}(t, 2n)$ ,  $g$  s'écrit  $2^{k'}$  avec  $k' \leq k$ , donc  $g$  divise  $n$ .

D'après l'observation,  $\neg \theta^g - 1 \mid 0$ .

• D'après le théorème de Bezout, il existe  $u, v \in \mathbb{Z}$  tels que  $tu + 2nv = g$ .

$$\theta^{tu} - 1 = \theta^{tu} \theta^{2nv} - 1 = \theta^g - 1$$

Puisque  $t$  divise  $tu$ ,  $\neg \theta^t - 1 \mid 0$ .

# Une racine non primitive dans $\mathbb{A}[X]/X^6+1$

Considérons les puissances successives de  $X$  dans  $\mathbb{A}[X]/X^6+1$  :

- ▶  $1, X, X^2, X^3, X^4, X^5$  ;
- ▶  $-1, -X, -X^2, -X^3, -X^4, -X^5$ .

$$\boxed{-X^2 - 1 \text{ est un diviseur de } 0.}$$

**Preuve.**

$$X^6 + 1 = (X^2 + 1)(X^4 - X^2 + 1)$$

L'interpolation dans  $\mathbb{A}[X]/X^6+1$  avec les puissances de  $X^2$  est fautive car :

$$\sum_{i<6} (-X^2)^i = 1 - X^2 + X^4 + 1 - X^2 + X^4 = 2 - 2X^2 + 2X^4 \neq 0$$

# FFT dans $(\mathbb{A}[X]/X^n+1)[Y]/Y^m-1$

Soit un polynôme  $P \in (\mathbb{A}[X]/X^n+1)[Y]/Y^m-1$  avec  $m \leq n$   
à évaluer sur  $\omega^0, \dots, \omega^{m-1}$  avec  $\omega = X^{\frac{2n}{m}}$ . ( $T[i] = \omega^i$ )

**FFT**( $P, T, m, n$ ) :

**If**  $m = 1$  **then**  $F[0] \leftarrow P[0]$ ; **Return**( $F$ )

**For**  $i$  **from** 0 **to**  $\frac{m}{2} - 1$  **do**

$P^{(0)}[i] \leftarrow P[2i]$ ;  $P^{(1)}[i] \leftarrow P[2i+1]$ ;  $T'[i] \leftarrow T[2i]$

$F^{(0)} \leftarrow \mathbf{FFT}(P^{(0)}, T', \frac{m}{2})$ ;  $F^{(1)} \leftarrow \mathbf{FFT}(P^{(1)}, T', \frac{m}{2})$

**For**  $i$  **from** 0 **to**  $\frac{m}{2} - 1$  **do**

$v \leftarrow T[i] \cdot F^{(1)}[i]$ ;  $F[i] \leftarrow F^{(0)}[i] + v$ ;  $F[\frac{m}{2} + i] \leftarrow F^{(0)}[i] - v$

**Return**( $F$ )

**Complexité.** Les opérations (en rouge) sont des copies, additions et multiplications de polynômes de degré inférieur à  $n$ .

L'un des termes de chaque multiplication est  $\pm X^k$  pour un certain  $k$ .

Cette multiplication correspond à une translation circulaire des coefficients avec changement de signe pour certains coefficients.

Toutes ces opérations s'effectuent en  $\Theta(n)$ . Donc la FFT opère en  $\Theta(nm \log(m))$ .

# Changement d'anneau

**Objectif.** Multiplication rapide dans  $\mathbb{A}[X]/X^n+1$  où  $n = 2^k$  pour  $n \geq 16$ .

1.  $n = dd'$  avec  $d = 2^{\lceil \frac{k}{2} \rceil}$  et  $d' = 2^{\lfloor \frac{k}{2} \rfloor}$ .
2. On associe à  $P = \sum_{i < n} p_i X^i \in \mathbb{A}[X]/X^n+1$   
 $P^y \in (\mathbb{A}[X]/X^{2d}+1)[Y]/Y^{d'}+1$  défini par :

$$P^y = \sum_{i < d'} \left( \sum_{j < d} p_{id+j} X^j \right) Y^i$$

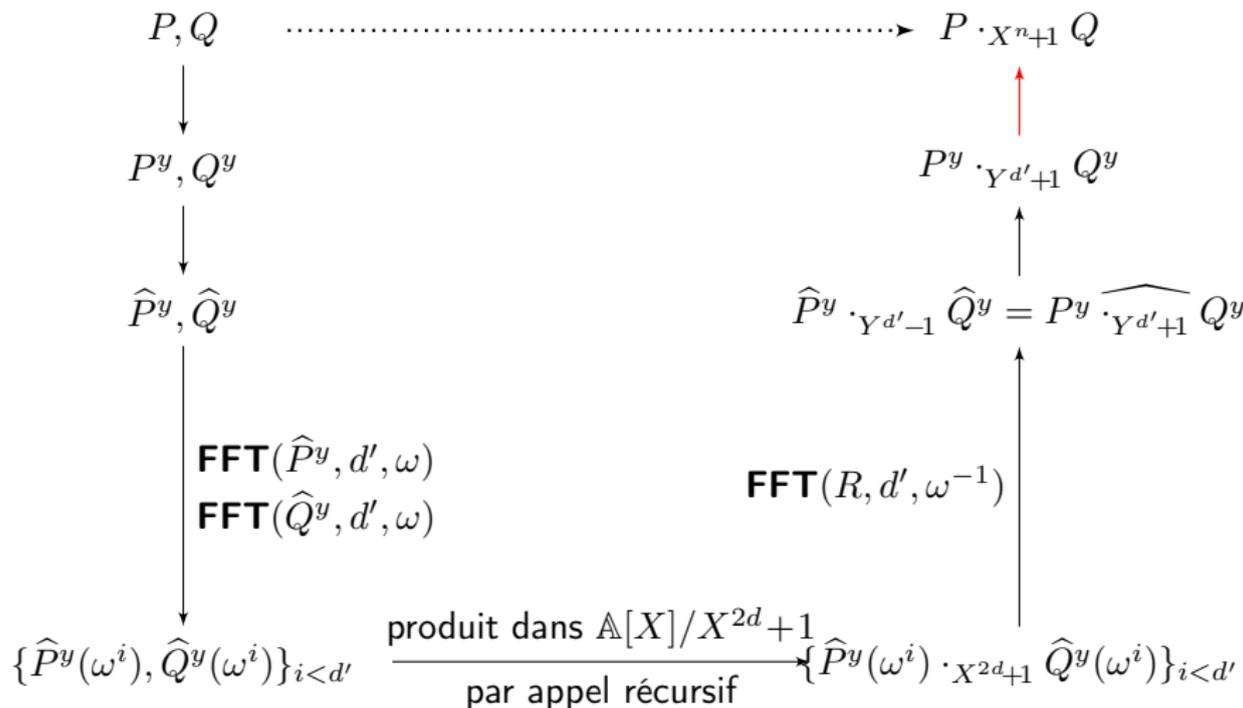
**Illustration.**  $n = 16$ ,  $d = 4$ ,  $d' = 4$ .

$$P^y = \left( \sum_{i < 4} p_i X^i \right) + \left( \sum_{i < 4} p_{i+4} X^i \right) Y + \left( \sum_{i < 4} p_{i+8} X^i \right) Y^2 + \left( \sum_{i < 4} p_{i+12} X^i \right) Y^3$$

3. Pour calculer  $P \cdot_{X^n+1} Q$  (à coefficients dans  $\mathbb{A}$ ), on calcule  $P^y \cdot_{Y^{d'}+1} Q^y$   
(à coefficients dans  $\mathbb{A}[X]/X^{2d}+1$ ).

**Observation.** Les produits de coefficients de  $P^y$  et de  $Q^y$  sont identiques dans  $\mathbb{A}[X]/X^{2d}+1$  et  $\mathbb{A}[X]$  car ces coefficients ont un degré inférieur à  $d$ .

# Schéma de l'algorithme



avec  $R = d'^{-1} \sum_{i < d'} (\widehat{P}^y(\omega^i) \cdot X^{2d+1} \widehat{Q}^y(\omega^i)) Y^i$  et  $\omega = X^{\frac{4d}{d'}}$ .

# De $P^y \cdot Y^{d'+1} Q^y$ à $P \cdot X^{n+1} Q$ (1)

Soit :

- ▶  $P^y = \sum_{i < d'} p_i^y Y^i$
- ▶  $Q^y = \sum_{j < d'} q_j^y Y^j$
- ▶  $P^y \cdot Y^{d'+1} Q^y = \sum_{a < d'} c_a^y Y^a$  avec  $c_a^y = \sum_{b < 2d} c_{a,b}^y X^b$

$$\begin{aligned} c_a^y &= \sum_{i+j=a} p_i^y q_j^y - \sum_{i+j=d'+a} p_i^y q_j^y \\ &= \sum_{i+j=a} \left( \sum_{h < d} p_{id+h} X^h \right) \left( \sum_{l < d} q_{jd+l} X^l \right) - \sum_{i+j=d'+a} \left( \sum_{h < d} p_{id+h} X^h \right) \left( \sum_{l < d} q_{jd+l} X^l \right) \end{aligned}$$

D'où :

$$c_{a,b}^y = \sum_{i+j=a} \sum_{h+l=b} p_{id+h} q_{jd+l} - \sum_{i+j=d'+a} \sum_{h+l=b} p_{id+h} q_{jd+l}$$

**Observation.**  $c_{d'-1,b}^y$  se réduit à :

$$c_{d'-1,b}^y = \sum_{i+j=d'-1} \sum_{h+l=b} p_{id+h} q_{jd+l}$$

# De $P^y \cdot_{Y^{d'+1}} Q^y$ à $P \cdot_{X^{n+1}} Q$ (2)

Soit :

- ▶  $P = \sum_{s < n} p_s X^s$ ,  $Q = \sum_{t < n} q_t X^t$
- ▶  $P \cdot_{X^{n+1}} Q = \sum_{u < n} c_u X^u$  avec  $c_u = \sum_{s+t=u} p_s q_t - \sum_{s+t=n+u} p_s q_t$

Posons  $s = id + h$ ,  $t = jd + l$ ,  $u = ad + b$ , avec  $0 \leq i, j, a < d'$  et  $0 \leq h, l, b < d$ .

$$c_u = \sum_{i+j=a} \sum_{h+l=b} p_{id+h} q_{jd+l} - \sum_{i+j=d'+a} \sum_{h+l=b} p_{id+h} q_{jd+l} \\ + \sum_{i+j=a-1} \sum_{h+l=d+b} p_{id+h} q_{jd+l} - \sum_{i+j=d'+a-1} \sum_{h+l=d+b} p_{id+h} q_{jd+l}$$

**Cas  $a = 0$ .** D'où  $0 \leq u = b < d$ .

$$c_u = \sum_{i+j=0} \sum_{h+l=u} p_{id+h} q_{jd+l} - \sum_{i+j=d'} \sum_{h+l=u} p_{id+h} q_{jd+l} \\ - \sum_{i+j=d'-1} \sum_{h+l=d+u} p_{id+h} q_{jd+l} = c_{0,u}^y - c_{d'-1,d+u}^y$$

**Cas  $a > 0$ .**

$$c_u = \sum_{i+j=a} \sum_{h+l=b} p_{id+h} q_{jd+l} - \sum_{i+j=d'+a} \sum_{h+l=b} p_{id+h} q_{jd+l} \\ + \sum_{i+j=a-1} \sum_{h+l=d+b} p_{id+h} q_{jd+l} - \sum_{i+j=a-1} \sum_{h+l=d+b} p_{id+h} q_{jd+l} = c_{a,b}^y + c_{a-1,d+b}^y$$

# Analyse de complexité

Soit  $n = 2^k$  et  $T(n)$  le temps d'exécution. On considère ici le logarithme en base 2.

- ▶ Si  $k$  est pair  $T(n) \leq cn \log(n) + \sqrt{n}T(2\sqrt{n})$
- ▶ Si  $k$  est impair  $T(n) \leq cn \log(n) + \sqrt{\frac{n}{2}}T(2\sqrt{2n})$

Il existe  $n_0$  et  $e$  tel que pour tout  $n \geq n_0$ ,  $T(n) \leq en \log(n) \log(\log(n))$ .

**Preuve.** Démontrons-le par induction. Supposons que  $k$  est pair.

$$T(n) \leq cn \log(n) + \sqrt{n}T(2\sqrt{n})$$

$$T(n) \leq cn \log(n) + e\sqrt{n}(2\sqrt{n} \log(2\sqrt{n}) \log(\log(2\sqrt{n})))$$

$$T(n) \leq cn \log(n) + 2en \log(2\sqrt{n}) \log(\log(2\sqrt{n}))$$

$$T(n) \leq cn \log(n) + en(\log(n) + 2) \log(\log(2\sqrt{n}))$$

$$T(n) \leq cn \log(n) + en(\log(n) + 2) \log(\frac{1}{2} \log(n) + 1)$$

$$T(n) \leq cn \log(n) + en(\log(n) + 2)(\log(\frac{1}{2} \log(n)) + \frac{1}{2}) \text{ (avec } n_0 \text{ suffisamment grand)}$$

$$T(n) \leq cn \log(n) + en(\log(n) + 2)(\log(\log(n)) - \frac{1}{2})$$

$$T(n) \leq en \log(n) \log(\log(n)) + (c - \frac{e}{2})n \log(n) + 2 \log(\log(n))$$

$$T(n) \leq en \log(n) \log(\log(n)) \text{ (avec } e > 2c \text{ et } n_0 \text{ suffisamment grand)}$$

Le cas  $k$  impair se traite de manière similaire.

# Plan

Produit rapide de polynômes

Produit rapide de polynômes sans racines primitives de l'unité

3 Inversion de série

Division de polynômes

# Séries formelles

Une série formelle à coefficients dans  $\mathbb{A}$  est de la forme  $P = \sum_{i \in \mathbb{N}} p_i X^i$ .

Les opérations de  $\mathbb{A}[[X]]$ , l'anneau des séries formelles sont définies ainsi

avec  $Q = \sum_{i \in \mathbb{N}} q_i X^i$  :

- ▶  $P + Q = \sum_{i \in \mathbb{N}} (p_i + q_i) X^i$
- ▶  $PQ = \sum_{k \in \mathbb{N}} (\sum_{i+j=k} p_i q_j) X^k$

$P$  est inversible ssi  $p_0$  est inversible. Son inverse  $Q$  est alors définie par :

$$q_0 = p_0^{-1} \text{ et } q_i = -q_0 \sum_{j < i} p_{i-j} q_j$$

**Preuve.**

$Q$  doit vérifier  $p_0 q_0 = 1$  et pour tout  $k > 0$ ,  $\sum_{i+j=k} p_i q_j = 0$ .

La première équation implique  $p_0$  inversible d'inverse  $q_0$ .

Les équations suivantes se résolvent alors inductivement :

$$p_0 q_i = - \sum_{j < i} p_{i-j} q_j \text{ d'où } q_i = -q_0 \sum_{j < i} p_{i-j} q_j.$$

**Observation.**  $q_1 = -p_1 q_0^2$

# Calcul de l'inverse

Les séries sont définies de manière implicite :

- ▶ par une fonction  $p(n)$  qui renvoie  $p_n$  ;
- ▶ par une équation de récurrence comme  $p_n = p_{n-1} + p_{n-2}$ , etc.

Dans la suite on suppose qu'on peut calculer  $p_n$  en  $\Theta(1)$ ,  
une fois calculés  $p_0, \dots, p_{n-1}$ .

**Objectif.** Calcul efficace des  $n$  premiers coefficients de l'inverse d'une série.

**Inverse**( $p, n$ )

$Q[0] \leftarrow p(0)^{-1}$

**For**  $i$  **from** 1 **to**  $n - 1$  **do**

$Q[i] \leftarrow 0$

**For**  $j$  **from** 1 **to**  $i$  **do**  $Q[i] \leftarrow Q[i] + Q[i - j]p(j)$  ;

$Q[i] \leftarrow -Q[0]Q[i]$

Complexité en  $\Theta(n^2)$ .

# Analyse de l'inverse

Soit  $n = 2^k$ . Décomposons  $Q$ , l'inverse de  $P$  de la façon suivante :

- ▶  $Q = Q_0 + Q_1 + Q_2$
- ▶  $Q_0 = \sum_{i < \frac{n}{2}} q_i X^i$ ,  $Q_1 = \sum_{\frac{n}{2} \leq i < n} q_i X^i$  et  $Q_2 = \sum_{i \geq n} q_i X^i$

$$Q_1 = -PQ_0^2 \text{ tronqué aux coefficients d'indice compris entre } \frac{n}{2} \text{ et } n - 1$$

**Preuve.**  $P(Q_0 + Q_1 + Q_2) = 1$

D'où :  $1 - PQ_0 = PQ_1 + PQ_2$

En multipliant par  $Q_0$  :  $(1 - PQ_0)Q_0 = PQ_0Q_1 + PQ_0Q_2$

puis en utilisant à nouveau  $P(Q_0 + Q_1 + Q_2) = 1$  :

$$(1 - PQ_0)Q_0 = (1 - PQ_1 - PQ_2)Q_1 + PQ_0Q_2$$

$$\text{D'où : } Q_0 - PQ_0^2 = Q_1 - PQ_1^2 - PQ_1Q_2 + PQ_0Q_2$$

Puisque  $Q_1^2$  et  $Q_2$  sont des séries dont les coefficients inférieurs à  $n$  sont nuls et  $Q_0$  est de degré strictement inférieur à  $\frac{n}{2}$ , on obtient le résultat.

# Calcul efficace de l'inverse

```
Inverse( $P, n$ )  
If  $n = 1$  then  $Q[0] \leftarrow P[0]^{-1}$ ; Return( $Q$ )  
 $Q_0 \leftarrow$  Inverse( $P, \frac{n}{2}$ )  
 $Q_a \leftarrow$  Produit( $Q_0, Q_0, \frac{n}{2}$ )  
 $Q_a \leftarrow$  Produit( $P, Q_a, n$ )  
For  $i$  from 0 to  $\frac{n}{2} - 1$  do  $Q[i] \leftarrow Q_0[i]$   
For  $i$  from  $\frac{n}{2}$  to  $n - 1$  do  $Q[i] \leftarrow -Q_a[i]$   
Return( $Q$ )
```

## Analyse de complexité.

$$\text{Pour } n \geq 2 \quad T(n) \leq cn \log(n) \log(\log(n)) + T\left(\frac{n}{2}\right)$$

D'où :

$$T(n) \leq d + \sum_{0 \leq i < k} c \frac{n}{2^i} \log\left(\frac{n}{2^i}\right) \log(\log(\frac{n}{2^i})) \leq d + 2cn \log(n) \log(\log(n))$$

# Plan

Produit rapide de polynômes

Produit rapide de polynômes sans racines primitives de l'unité

Inversion de série

4 Division de polynômes

# Calcul de la division

Soit  $P = \sum_{i \leq n} p_i X^i$  et  $D = \sum_{i \leq m} d_i X^i$  avec  $m \leq n$  et  $d_m$  inversible.

La division euclidienne de  $P$  par  $D$  est définie par la paire  $(Q, R)$  telle que :

$$P = QD + R \text{ avec } \deg(R) < m$$

**Quotient**( $P, D, n, m$ )

**For**  $i$  **from**  $n - m$  **downto** 0 **do**

$$Q[i] \leftarrow P[i + m]D[m]^{-1}$$

**For**  $j$  **from**  $i + m - 1$  **downto**  $i$  **do**  $P[j] \leftarrow P[j] - D[j - i]Q[i]$

**For**  $i$  **from** 0 **to**  $m - 1$  **do**  $R[i] \leftarrow P[i]$

**Return**( $Q, R$ )

## Analyse de complexité.

La division s'effectue en  $\Theta((n + 1 - m)m)$ .

# Division via les séries

On introduit une nouvelle variable formelle  $T$  telle que  $X = \frac{1}{T}$ .

L'équation  $P = QD + R$  peut se réécrire :

$$T^n P\left(\frac{1}{T}\right) = (T^{n-m} Q\left(\frac{1}{T}\right))(T^m D\left(\frac{1}{T}\right)) + T^n R\left(\frac{1}{T}\right)$$

où  $T^n P\left(\frac{1}{T}\right)$ ,  $T^{n-m} Q\left(\frac{1}{T}\right)$ ,  $T^m D\left(\frac{1}{T}\right)$  et  $T^n R\left(\frac{1}{T}\right)$  appartiennent à  $\mathbb{A}[T] \subseteq \mathbb{A}[[T]]$ .

Le terme constant de  $T^m D\left(\frac{1}{T}\right)$  est  $d_m$ . Donc  $T^m D\left(\frac{1}{T}\right)$  est inversible dans  $\mathbb{A}[[T]]$  :

$$T^n P\left(\frac{1}{T}\right)(T^m D\left(\frac{1}{T}\right))^{-1} = T^{n-m} Q\left(\frac{1}{T}\right) + T^n R\left(\frac{1}{T}\right)(T^m D\left(\frac{1}{T}\right))^{-1}$$

Le terme non nul de plus petit degré de  $T^n R\left(\frac{1}{T}\right)$  a un degré  $\geq n - m + 1$ .

Par conséquent :

$$T^{n-m} Q\left(\frac{1}{T}\right) = T^n P\left(\frac{1}{T}\right)(T^m D\left(\frac{1}{T}\right))^{-1} \text{ tronqué aux } n - m + 1 \text{ premiers coefficients}$$

# Calcul efficace de la division

```
For  $i$  from 0 to  $n - 1$  do  $P'[i] \leftarrow P[n - i]$   
For  $i$  from 0 to  $m - 1$  do  $D'[i] \leftarrow D[n - i]$   
 $D'' \leftarrow \text{Inverse}(D', n - m + 1)$   
 $Q' \leftarrow \text{Produit}(P', D'', n)$   
For  $i$  from 0 to  $n - m$  do  $Q[i] \leftarrow Q'[n - i]$   
 $QD \leftarrow \text{Produit}(Q, D, n)$   
For  $i$  from 0 to  $m - 1$  do  $R[i] \leftarrow P[i] - QD[i]$   
Return( $Q, R$ )
```

## Analyse de complexité.

La division s'effectue en  $\Theta(n \log(n) \log(\log(n)))$ .