

# Algorithmique rapide des sommes de Newton en petite caractéristique

Alin Bostan (ALGO, INRIA)

collaboration avec Laureano González Vega,  
Hervé Perdry et Éric Schost

## Contexte et résultat principal

Conversion **sommes de Newton**  $\rightarrow$  **symétriques élémentaires**  
 $(x+y+z, x^2+y^2+z^2, x^3+y^3+z^3) \rightarrow (x+y+z, xy+yz+zx, xyz)$

- bien comprise en caractéristique zéro (e.g.  $\mathbb{Q}$ ),
- plus compliquée en petite caractéristique (e.g.  $\mathbb{F}_p$ ), à cause des divisions par **2, 3, ...** et de la non-unicité du résultat.

**Théorème (BGPS'05, voir plus loin pour un énoncé précis).**

- *On peut faire marcher la conversion en petite caractéristique “pour quelques décimales de plus” ;*
- *Cela améliore la complexité de certains algorithmes pour l’algèbre linéaire et pour les nombres algébriques en petite caractéristique.*

# Motivation

Dans beaucoup de cas, il est plus facile d'accéder aux sommes de Newton d'un polynôme qu'à ses coefficients.

**Algèbre linéaire** : polynômes caractéristiques, **Le Verrier (1840)**,  
résolution de systèmes à la Wiedemann, **Kaltofen, Pan, Villard**.

**Nombres algébriques** :  $+$ ,  $\times$ ,  $\dots$ , **Dvornicich-Traverso (1989)**.

**Calcul parallèle** : pgcd, approx. de Padé–Hermite, **Bini, Pan,...**

**Systèmes polynomiaux** : calculs de polynômes éliminant dans des  
algèbres quotient, **Rouillier (1999)**.

**Théorie des codes** : décodage des codes BCH, **Pan (1997)**.

**Et en général** : tout algorithme basé sur une **formule de trace**.

# Polynômes symétriques élémentaires et de Newton

Soit  $F$  dans  $k[X]$ ,  $k$  corps.

- Les **polynômes symétriques élémentaires** (des racines de  $F$ ) sont les coefficients de  $F$  :

$$F = X^d + A_1 X^{d-1} + \dots + A_d.$$

- Les **sommes symétriques de Newton**  $S_1, S_2, \dots$  de  $F$  sont

$$S_i = \sum_{F(x)=0} x^i,$$

la somme étant prise sur toutes les racines de  $F$  (avec leur multiplicité) dans une clôture algébrique de  $k$ .

## Quelques relations importantes

**Théorème** (folklore). Soit  $F^*$  le polynôme réciproque de  $F$  :

$$F^* = 1 + A_1 X + \cdots + A_d X^d.$$

Alors :

$$\frac{(F^*)'}{F^*} = - \sum_{i \geq 0} S_{i+1} X^i$$

et donc en caractéristique nulle

$$F^* = \exp \left( - \int \sum_{i \geq 0} S_{i+1} X^i \right).$$

**Corollaire** (relations de Newton, extraction de coefficients).

$$i A_i + S_1 A_{i-1} + \cdots + S_i = 0, \quad 1 \leq i \leq d.$$

## Conséquences algorithmiques

Soit  $\mathbf{M}$  la complexité du produit des polynômes dans  $k[X]$ .

Avec la FFT  $\implies \mathbf{M}(d) \in \mathcal{O}(d \log d \log \log d)$ , **Schönhage-Strassen**.

**Coefficients  $\rightarrow$  sommes de Newton.** Étant donnés les coefficients  $A_1, \dots, A_d$ , les  $d$  premières sommes de Newton se calculent en

- $\mathcal{O}(d^2)$  (par les relations de Newton).
- $\mathcal{O}(\mathbf{M}(d))$  (itération de Newton pour l'inverse, **Sieveking-Kung**).

**Sommes de Newton  $\rightarrow$  coefficients.** Si  $\text{char}(k) = 0$ , les coefficients peuvent se calculer à partir des  $d$  premières sommes de Newton en

- $\mathcal{O}(d^2)$  (par les relations de Newton).
- $\mathcal{O}(\mathbf{M}(d))$  (itération de Newton pour l'exponentielle, **Brent**).

## En petite caractéristique

Soit  $p$  la caractéristique de  $k$ . L'application

**coefficients  $\rightarrow$  sommes de Newton**

**n'est pas injective** pour les polynômes de degré  $\geq p$ .

**Obstruction :** les sommes de Newton des polynômes en  $X^p$  valent 0

$$\text{NewtonSums}(X^{2p+1} + X^{p+1} + X) = \text{NewtonSums}(X^{2p+1} + 2X).$$

**Conséquence :** Le problème de la conversion n'a plus de sens sans hypothèses supplémentaires (e.g.  $F$  sans carré).

**Pire :** Même quand le résultat est unique, les algorithmes peuvent échouer, à cause des divisions par zéro.

## Solutions possibles

Dans toute la suite,  $\mathbf{k} = \mathbb{F}_p$ .

**Approche rationnelle.** Toute fonction symétrique sur  $\mathbf{k}$  est une *fraction rationnelle* en les sommes de Newton  $S_j$  avec  $p \nmid j$ , e.g.

$$A_2(x, y) = (S_1^3 - S_3)/S_1, A_2(x, y, z) = (S_1^2 S_3 - S_5)/(S_1^3 - S_3).$$

Idée de Schönhage (1993), méthode de Le Verrier en caractéristique  $p$ .

Améliorée par Pan (1997, 2000). Faiblesse : sortie partielle.

**Approche  $p$ -adique.** Calculer dans  $\mathbb{Z}/p^N\mathbb{Z}$  au lieu de  $\mathbb{F}_p$ .

Les divisions feront perdre de la précision, mais de combien ?

Idée de González Vega et Perdry (EACA 2004), avec  $N \approx d/p$ .

Cet exposé :  $N = \log_p(d)$  suffit.

## Algorithme de Schönhage et Pan

**Théorème.** *On suppose que toutes les racines de  $F$  ont multiplicité au plus  $p - 1$ . Alors, étant données les  $2d$  premières sommes de Newton de  $F$ , on peut calculer ses coefficients en*

$$\mathcal{O}(M(d) + p M(d/p) \log(d/p)) \quad \text{ops dans } \mathbb{F}_p.$$

**Esquisse de l'algorithme :**

- calculer  $G$  de degré  $2d$  en appliquant les relations de Newton quand cela est possible et en mettant les autres coefficients à  $0$ .  
→  $\mathcal{O}(M(d))$  opérations par un calcul d'exponentielle tordue.
- on a  $G^* = F^* / F_0(X^p) \bmod X^{2d}$  (même dérivée logarithmique !)  
→  $\mathcal{O}(p M(d/p) \log(d/p))$  ops par  $p - 1$  approximations de Padé.

## L'algorithme de Le Verrier, l'approche rationnelle

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



Schönhage-Pan : calculer l'approximant de Padé  $(7, 7)$  de la série

$$\sum \text{trace}(M^i) X^i = 1 + X + X^2 + X^4 + X^7 + X^8 + X^9 + X^{11} + X^{14} + \mathcal{O}(X^{15})$$

On obtient  $1/(X^3 + X + 1)$  et la sortie est  $X^3 + X^2 + 1$ , alors que le vrai polynôme caractéristique est  $\chi_M = (X^2 + X)^2 \times (X^3 + X^2 + 1)$ .

## L'algorithme de Le Verrier, l'approche $p$ -adique

remontée arbitraire de $M$ à $\mathbb{Z}/8\mathbb{Z}$	sommes de Newton dans $\mathbb{Z}/8\mathbb{Z}$
$\overline{M} = \begin{pmatrix} 7 & 0 & 3 & 0 & 1 & 5 & 0 \\ 0 & 0 & 3 & 1 & 5 & 0 & 0 \\ 7 & 5 & 0 & 3 & 0 & 0 & 7 \\ 3 & 5 & 1 & 3 & 0 & 5 & 3 \\ 1 & 0 & 0 & 0 & 0 & 3 & 1 \\ 0 & 5 & 0 & 0 & 0 & 7 & 0 \\ 5 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$	$S = \left( \text{trace}(\overline{M}^i) \right)_{i \geq 1}$ $= (1, 7, 4, 7, 0, 0, 5)$

$$A_1 := -S_1 = 7,$$

$$A_2 := -\frac{1}{2}(S_1 A_1 + S_2) = -(7 + 7)/2 = 10/2 = 1 + 4\alpha,$$

$$A_3 := -\frac{1}{3}(S_1 A_2 + S_2 A_1 + S_3) = \dots = 4\alpha + 6,$$

$$A_4 := -\frac{1}{4}(S_1 A_3 + \dots + S_4) = -(4\alpha + 5 + 4\alpha + 3)/4 = 0/4 = 2\beta + 4\gamma,$$

$$A_5 := -\frac{1}{5}(S_1 A_4 + \dots + S_5) = \dots = 4\alpha + 6\beta + 4\gamma + 5,$$

$$A_6 := -\frac{1}{6}(S_1 A_5 + \dots + S_6) = \dots = (4\beta + 4)/6 = 6\beta + 4\delta + 6,$$

$$A_7 := -\frac{1}{7}(S_1 A_6 + \dots + S_7) = \dots = 4\gamma + 4\delta.$$

Sortie correcte :  $\chi_M = \sum A_i X^{7-i} \pmod{2} = X^7 + X^6 + X^5 + X^2.$

## Valuation $p$ -adique et divisions dans $\mathbb{Z}/p^N\mathbb{Z}$

**La valuation  $p$ -adique.** Soit  $v(\cdot)$  la valuation  $p$ -adique dans  $\mathbb{Z} \setminus \{0\}$  : si  $x \neq 0$ ,  $v(x)$  est  $v$  maximal tel que  $p^v$  divise  $x$ .

Si  $N > 0$ ,  $v(\cdot)$  s'étend uniquement à  $\mathbb{Z}/p^N\mathbb{Z} \setminus \{0\}$ .

**Divisions dans  $\mathbb{Z}/p^N\mathbb{Z}$ .** Soient  $a, b$  dans  $\mathbb{Z}/p^N\mathbb{Z}$ , tq  $b \neq 0$ . Alors :

- soit il n'y a aucun  $c$  dans  $\mathbb{Z}/p^N\mathbb{Z}$  tel que  $a = bc$  ;
- soit il en existe plusieurs : seulement  $c \pmod{p^{N-v(b)}}$  est unique.

Autrement dit, **on perd une précision  $v(b)$  après division par  $b$ .**

## Le résultat de González Vega et Perdry

**Théorème.** Soit  $F$  dans  $\mathbb{F}_p[X]$ ,  $d = \deg F$ , et  $N > v(d!)$ .

Soit  $\bar{F}$  une remontée arbitraire de  $F$  à coefficients dans  $\mathbb{Z}/\mathfrak{p}^N\mathbb{Z}$ .

Données les  $d$  premières sommes de Newton de  $\bar{F}$ , on peut calculer les coeffs de  $F$  en  $\mathcal{O}(d^2)$  opérations  $(+, -, \times)$  et  $d$  divisions dans  $\mathbb{Z}/\mathfrak{p}^N\mathbb{Z}$ .

**Preuve.** Les relations de Newton requièrent des divisions par  $2, \dots, d$  dans  $\mathbb{Z}/\mathfrak{p}^N\mathbb{Z}$ . Si  $N > \sum v(i) = v(d!)$ , le résultat est correct mod  $p$ .

**Faiblesse.**  $v(d!) \approx \frac{d}{p}$ , donc les coefficients deviennent  $\frac{d}{p}$  plus gros.

## La vie est plus belle

Soient  $p = 2$ ,  $d = 10$ ,  $N = 10$  et :

- $F = X^{10} + X^9 + X^8 + X^4 + X^3 + X^2 + X + 1$  dans  $\mathbb{F}_2[X]$ .
- $\overline{F} = X^{10} + X^9 + X^8 + X^4 + X^3 + X^2 + X + 1$  dans  $\mathbb{Z}/1024\mathbb{Z}[X]$ .

Supposons connues les premières sommes de Newton de  $\overline{F}$

**1023, 1023, 2, 1023, 1023, 1020, 1023, 1023, 1017, 1023, 10, ...**

Dans les relations de Newton, on divise par  $2^1, 2^2, 3 \times 2^1, 2^3, 5 \times 2^1$ , donc on attend une perte de  $8 = 1 + 2 + 1 + 3 + 1$  bits de précision, *i.e.* **2** bits corrects dans le résultat. Après les calculs, on obtient

**1, 1, 513, 512, 0, 512, 513, 1, 897, 897, 385.**

**513 = 1,000000001; 512 = 0,000000001; 897 = 1,000000111; 385 = 1,00000011**

Il y a au moins **7** bits corrects : on a perdu uniquement **3** bits.

## Et c'est plus qu'un miracle...

Plusieurs tests, différents polynômes modulo différents premiers.

Rappel :  $F = X^d + A_1 X^{d-1} + \dots + A_d$ .

$p = 2$  : on perd au plus 0 bit pour  $A_1$ , 1 bit pour  $A_2$  et  $A_3$ , 2 bits pour  $A_4, A_5, A_6$  et  $A_7, \dots$  ; on obtient la suite

$$0, 1, 1, 2, 2, 2, 2, 3, 3, 3, \dots \simeq (\lfloor \log_2(i) \rfloor)_{i \geq 1}$$

$p = 3$  : on perd au plus 0 bits pour  $A_1$  et  $A_2$ , 1 bits pour  $A_3, \dots, A_8, \dots$  ; on obtient la suite

$$0, 0, 1, 1, 1, 1, 1, 1, 2, 2, \dots \simeq (\lfloor \log_3(i) \rfloor)_{i \geq 1}$$

$p > 3$  : même type de résultats.

## Une meilleure borne

On considère :

- $\mathbb{Z}_p$  (et  $\mathbb{Q}_p$ ) l'anneau (le corps) des entiers (nombres)  $p$ -adiques ;
- $w : \mathbb{N}^* \rightarrow \mathbb{N}$ ,  $w(i) = \lfloor \log_p(i) \rfloor$ , nombre de chiffres de  $i$  en base  $p$ .

**Théorème (BGPS'05).** Soit  $P$  dans  $\mathbb{Z}_p[X]$  et  $Q$  dans  $\mathbb{Q}_p[X]$ , où

$$P = X^d + A_1 X^{d-1} + \dots + A_d, \quad Q = X^d + B_1 X^{d-1} + \dots + B_d.$$

Soit  $(S_i)_{i \geq 1}$  et  $(T_i)_{i \geq 1}$  les sommes de Newton de  $P$  et  $Q$ .

On suppose que  $v(S_i - T_i) \geq \alpha$  pour tout  $i \geq 1$ . Alors :

- $v(A_i - B_i) \geq \alpha - w(i)$  pour tout  $i \geq 1$  ;
- Si  $\alpha \geq w(d) + 1$ , alors  $P \in \mathbb{Z}_p[X]$ .

## Quelque mots sur la preuve

Par récurrence, il suffit de prouver :

**Théorème.** Soient  $P$  et  $Q$  dans  $\mathbb{Z}_p[\mathbf{X}]$  et  $i \in \{1, \dots, d\}$  tels que :

- $v(S_i - T_i) \geq \alpha$  ;
- $v(A_j - B_j) \geq \alpha - w(j)$ , pour tout  $1 \leq j < i$ .

Alors  $v(A_i - B_i) \geq \alpha - w(i)$ .

**Reformulation** (inutile) en termes de norme  $p$ -adique  $\left(\|x\| = \frac{1}{p^{v(x)}}\right)$

$$\|P - Q\| \leq d \times \|S - T\|$$

## Quelques mots sur la preuve, suite

1. (Girard 1629, Waring 1762, Rouché 1862, Carlitz 1978) :

$$\frac{S_i}{i} = \sum_{i=\mu_1+2\mu_2+3\mu_3+\dots} (-1)^{\mu_1+\dots+\mu_i} \frac{(\mu_1 + \dots + \mu_i - 1)!}{\mu_1! \dots \mu_i!} A_1^{\mu_1} \dots A_i^{\mu_i}.$$

## Quelques mots sur la preuve, suite

1. (Girard 1629, Waring 1762, Rouché 1862, Carlitz 1978) :

$$\frac{S_i}{i} = \sum_{i=\mu_1+2\mu_2+3\mu_3+\dots} (-1)^{\mu_1+\dots+\mu_i} \frac{(\mu_1 + \dots + \mu_i - 1)!}{\mu_1! \dots \mu_i!} A_1^{\mu_1} \dots A_i^{\mu_i}.$$

C'est une généralisation de l'identité bien connue (Waring) :

$$x^n + y^n = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{n}{n-k} \binom{n-k}{k} (x+y)^{n-2k} (xy)^k.$$

## Quelques mots sur la preuve, suite

1. (Girard 1629, Waring 1762, Rouché 1862, Carlitz 1978) :

$$\frac{S_i}{i} = \sum_{i=\mu_1+2\mu_2+3\mu_3+\dots} (-1)^{\mu_1+\dots+\mu_i} \frac{(\mu_1 + \dots + \mu_i - 1)!}{\mu_1! \dots \mu_i!} A_1^{\mu_1} \dots A_i^{\mu_i}.$$

C'est une généralisation de l'identité bien connue (Waring) :

$$x^n + y^n = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{n}{n-k} \binom{n-k}{k} (x+y)^{n-2k} (xy)^k.$$

Preuve : “Je suis l'exponentielle de mon logarithme” (Flajolet).

## Quelques mots sur la preuve, suite

1. (Girard 1629, Waring 1762, Rouché 1862, Carlitz 1978) :

$$\frac{S_i}{i} = \sum_{i=\mu_1+2\mu_2+3\mu_3+\dots} (-1)^{\mu_1+\dots+\mu_i} \frac{(\mu_1 + \dots + \mu_i - 1)!}{\mu_1! \dots \mu_i!} A_1^{\mu_1} \dots A_i^{\mu_i}.$$

C'est une généralisation de l'identité bien connue (Waring) :

$$x^n + y^n = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{n}{n-k} \binom{n-k}{k} (x+y)^{n-2k} (xy)^k.$$

Preuve : “Je suis l'exponentielle de mon logarithme” (Flajolet).

2. Écrire l'analogie pour  $T$ , soustraire et isoler le terme  $A_i - B_i$ .

## Quelques mots sur la preuve, suite

1. (Girard 1629, Waring 1762, Rouché 1862, Carlitz 1978) :

$$\frac{S_i}{i} = \sum_{i=\mu_1+2\mu_2+3\mu_3+\dots} (-1)^{\mu_1+\dots+\mu_i} \frac{(\mu_1 + \dots + \mu_i - 1)!}{\mu_1! \dots \mu_i!} A_1^{\mu_1} \dots A_i^{\mu_i}.$$

C'est une généralisation de l'identité bien connue (Waring) :

$$x^n + y^n = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{n}{n-k} \binom{n-k}{k} (x+y)^{n-2k} (xy)^k.$$

Preuve : “Je suis l'exponentielle de mon logarithme” (Flajolet).

2. Écrire l'analogue pour  $T$ , soustraire et isoler le terme  $A_i - B_i$ .
3. Les autres termes  $A_1^{\mu_1} \dots A_{i-1}^{\mu_{i-1}} - B_1^{\mu_1} \dots B_{i-1}^{\mu_{i-1}}$  s'écrivent

$$\sum_{j < i} \ell_j (A_j - B_j), \quad \text{avec } \ell_j \in \mathbb{Z}_p.$$

## Quelques mots sur la preuve, suite

4. En mettant tout ensemble :

$$A_i - B_i = \frac{T_i - S_i}{i} + \sum_{j < i} \gamma_j (A_j - B_j),$$

pour certains  $\gamma_j$  (qui vivent dans  $\mathbb{Q}_p$ ).

## Quelques mots sur la preuve, suite

4. En mettant tout ensemble :

$$A_i - B_i = \frac{T_i - S_i}{i} + \sum_{j < i} \gamma_j (A_j - B_j),$$

pour certains  $\gamma_j$  (qui vivent dans  $\mathbb{Q}_p$ ).

5. Chaque  $\gamma_j$  apparaissant dans la somme est une somme ( $c = c_\gamma \in \mathbb{Z}_p$ )

$$\gamma = c \frac{(\mu_1 + \cdots + \mu_i - 1)!}{\mu_1! \cdots \mu_i!} = \frac{c \times \text{multinomial}}{\mu_j}, \quad \text{avec } j\mu_j \leq i.$$

## Quelques mots sur la preuve, suite

4. En mettant tout ensemble :

$$A_i - B_i = \frac{T_i - S_i}{i} + \sum_{j < i} \gamma_j (A_j - B_j),$$

pour certains  $\gamma_j$  (qui vivent dans  $\mathbb{Q}_p$ ).

5. Chaque  $\gamma_j$  apparaissant dans la somme est une somme ( $c = c_\gamma \in \mathbb{Z}_p$ )

$$\gamma = c \frac{(\mu_1 + \cdots + \mu_i - 1)!}{\mu_1! \cdots \mu_i!} = \frac{c \times \text{multinomial}}{\mu_j}, \quad \text{avec } j\mu_j \leq i.$$

Ces  $\gamma$  ont donc une **petite** valuation  $p$ -adique :  $v(\gamma) \geq w(j) - w(i)$ .

Ainsi,  $v(\gamma(A_j - B_j)) \geq \alpha - w(i)$ .

## Quelques mots sur la preuve, suite

4. En mettant tout ensemble :

$$A_i - B_i = \frac{T_i - S_i}{i} + \sum_{j < i} \gamma_j (A_j - B_j),$$

pour certains  $\gamma_j$  (qui vivent dans  $\mathbb{Q}_p$ ).

5. Chaque  $\gamma_j$  apparaissant dans la somme est une somme ( $c = c_\gamma \in \mathbb{Z}_p$ )

$$\gamma = c \frac{(\mu_1 + \cdots + \mu_i - 1)!}{\mu_1! \cdots \mu_i!} = \frac{c \times \text{multinomial}}{\mu_j}, \quad \text{avec } j\mu_j \leq i.$$

Ces  $\gamma$  ont donc une **petite** valuation  $p$ -adique :  $v(\gamma) \geq w(j) - w(i)$ .

Ainsi,  $v(\gamma(A_j - B_j)) \geq \alpha - w(i)$ .

6. Par l'hypothèse, on a aussi  $v((T_i - S_i)/i) \geq \alpha - w(i)$ , et comme tout triangle est isocèle, on a fini. □

## Conséquences algorithmiques

**Corollaire.** Soit  $F$  dans  $\mathbb{F}_p[X]$ ,  $d = \deg F$ , et  $N > \lfloor \log_p(d) \rfloor$ .

Soit  $\bar{F}$  une remontée arbitraire de  $F$  à  $\mathbb{Z}/\mathfrak{p}^N\mathbb{Z}[X]$ .

Données les  $d$  premières sommes de Newton de  $\bar{F}$ , on peut calculer les coefficients de  $F$  :

- en  $\mathcal{O}(d^2)$  opérations  $(+, -, \times)$  et  $d$  divisions dans  $\mathbb{Z}/\mathfrak{p}^N\mathbb{Z}$  par les relations de Newton.
- en  $\mathcal{O}(M(d))$  opérations  $(+, -, \times)$  et  $d$  divisions dans  $\mathbb{Z}/\mathfrak{p}^N\mathbb{Z}$  par exponentiation rapide.

## Preuve (esquisse, pour l'algorithme quadratique)

Soit  $F = X^d + a_1 X^{d-1} + \dots + a_d$ , et supposons des approximations  $\bar{a}_1, \dots, \bar{a}_i \in \mathbb{Z}/p^N \mathbb{Z}$  déjà construites :  $v(a_j - \bar{a}_j) \geq N - w(j)$  si  $j \leq i$ .

On veut construire  $\overline{a_{i+1}}$  tel que  $v(a_{i+1} - \overline{a_{i+1}}) \geq N - w(i+1)$ .

- (1) On choisit  $A_1, \dots, A_{i+1}$  et  $\bar{A}_1, \dots, \bar{A}_i$ , remontées arbitraires à  $\mathbb{Z}_p$ .
- (2) On calcule  $\bar{A}_{i+1} \in \mathbb{Q}_p$  par les relations de Newton.
- (3)  $\bar{A}_{i+1}$  appartient à  $\mathbb{Z}_p$ , et on définit  $\overline{a_{i+1}} := \bar{A}_{i+1} \bmod p^N$ .

Point délicat : montrer qu'en fait  $\bar{A}_{i+1} \in \mathbb{Z}_p$  ; appliquer le Th. à

$$X^{i+1} + A_1 X^i + \dots + A_{i+1} \quad \text{et} \quad X^{i+1} + \bar{A}_1 X^i + \dots + \bar{A}_{i+1},$$

dont les sommes de Newton sont proches par construction. □

## Complexité binaire

Soit  $\mathbf{M}_{\text{int}}(n)$  la complexité binaire du produit d'entiers de taille bit  $n$ .

FFT  $\implies \mathbf{M}_{\text{int}}(n) \in \mathcal{O}(n \log n \log \log n)$ .

**Proposition.** Soit  $M \in \mathbb{N}$  et  $\mathbf{R} = \mathbb{Z}/M\mathbb{Z}$ . Alors :

- Chaque opération  $(+, -, \times)$  dans  $\mathbf{R}$  s'exécute en  $\mathcal{O}(\mathbf{M}_{\text{int}}(\log M))$  opérations binaires.
- Les divisions exactes dans  $\mathbf{R}$  se font en  $\mathcal{O}(\mathbf{M}_{\text{int}}(\log M) \log \log M)$  opérations binaires.

**Corollaire.** La complexité binaire de notre algorithme rapide est en

$$\mathcal{O}((\mathbf{M}(d) + d \log \log d) \mathbf{M}_{\text{int}}(\log d)).$$

## Application : calculs avec des nombres algébriques

Soit  $F, G$  dans  $k[X]$ , et soit

$$F = \prod_i (X - f_i), \quad G = \prod_i (X - g_i)$$

dans une clôture algébrique de  $k$ .

Leur **produit composé** est le polynôme

$$F \otimes G = \prod_{i,j} (X - f_i g_j).$$

C'est un polynôme à coefficients dans  $k$ , de degré  $D = \deg(F) \deg(G)$ .

## Résultats de complexité existants

Supposons pour simplifier que  $\deg(F) = \deg(G) = \sqrt{D}$ .

**Dvornicich-Traverso.** Sommes de Newton en car. 0,  $\mathcal{O}(D^2)$  ops.

**Brawley-Carlitz.** Résultants (toute caractéristique),  $\mathcal{O}(D^{1.5})$  ops.

**Bostan-Flajolet-Salvy-Schost.** Arithmétique rapide,

- $\mathcal{O}(M(D))$  ops en car  $\mathbf{0}$  et
- $\mathcal{O}(M(D) + p M(D/p) \log(D/p))$  en car  $\mathbf{p}$

Applications (crypto) : produits composés sur des corps finis, degré de l'entrée entre **500** et **1000**, donc  $D > \mathbf{200000}$  peut être atteint.

## En passant par les sommes de Newton

Soit  $S_i, T_i$  et  $U_i$  sommes de Newton de  $F, G$  et  $F \otimes G$ . Alors :

$$U_i = S_i T_i \quad \text{pour } i \geq 1.$$

**En caractéristique 0 :**

1. Calculer les sommes de Newton  $F, G$  de 1 à  $D = \deg(F) \deg(G)$  ;
2. Les multiplier terme à terme ;
3. Retrouver  $F \otimes G$ .

**Dans  $\mathbb{F}_p$  :**

- Même algorithme, mais tous les calculs sont faits dans  $\mathbb{Z}/p^N\mathbb{Z}$ , où  $N = \lfloor \log_p(D) + 1 \rfloor$ .

## Résultat de complexité

**Théorème (BGPS'05).** Soit  $k = \mathbb{F}_p$ . Le produit composé  $F \otimes G$  peut être calculé en  $\mathcal{O}((M(D) + D \log \log D)M_{\text{int}}(\log D))$  ops binaires.

Une comparaison rapide avec Bostan-Flajolet-Salvy-Schost.

On suppose FFT pour la multiplication des polynômes et des entiers :

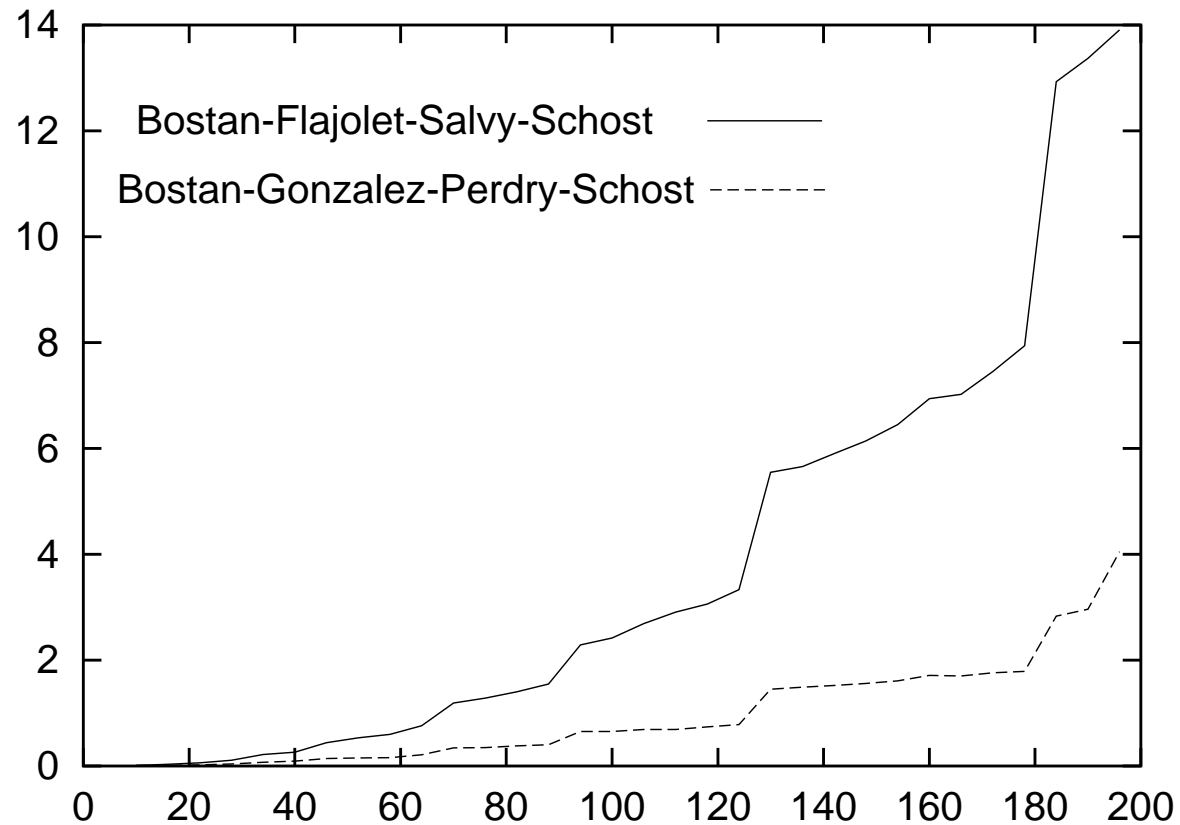
- Si  $p \simeq \text{constant}$ , on perd un facteur  $\log \log D$ .
- Si  $p = D^\beta$ , avec  $0 < \beta_0 \leq \beta \leq \beta_1 < 1$ , on gagne un facteur  $\log D$ .
- Si  $p \simeq D$ , les complexités asymptotiques coïncident.

## Résultats expérimentaux

Tous les tests utilisent la librairie C++ NTL écrite par Shoup.

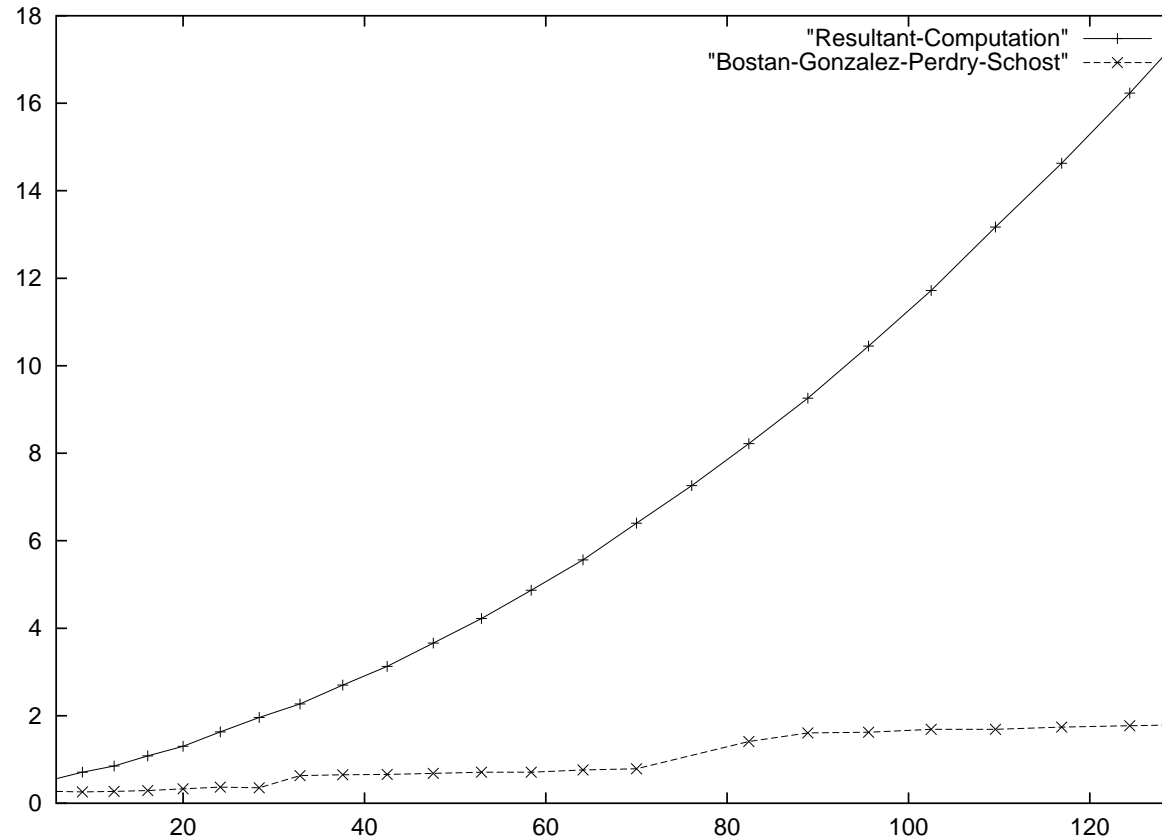
- multiplication des polynômes par FFT, complexité  $\mathcal{O}(d \log d)$  ;
- algorithme de type demi-pgcd pour les approximants de Padé ;
- entiers GMP (mais pas dans la taille où la FFT est utilisée) ;
- itérations de Newton accélérées par des produits médians (Hanrot-Quercia-Zimmermann, Bostan-Lecerf-Schost).

## Temps de calcul



- Axe horizontal :  $\deg(F) = \deg(G) \simeq p$   
( $\implies D$  monte jusqu'à 40000).
- Axe vertical : temps en secondes (2GHz Pentium 4).

# Temps de calcul



- Axe horizontal :  $\deg(F) = \deg(G) \simeq p$   
( $\implies D$  monte jusqu'à 14400).
- Axe vertical : temps en secondes (2GHz Pentium 4).