Multiplication rapide de polynômes sur les corps finis

David Harvey
UNSW, Sydney

Joris van der Hoeven
Grégoire Lecerf
CNRS

Robin Larrieu
École polytechnique

RAIM, Gif-sur-Yvette

13 novembre 2018

Le problème

p : nombre premier

$q = p^\lambda$

$\mathbb{F}_q[x]_n = \{P \in \mathbb{F}_q[x] : \deg P < n\}$

$\lg k = \lceil \log_2 \max(k, 1) \rceil$

Le problème

p : nombre premier

$q = p^\lambda$

$\mathbb{F}_q[x]_n = \{P \in \mathbb{F}_q[x] : \deg P < n\}$

$\lg k = \lceil \log_2 \max(k, 1) \rceil$

Problème

Étant donnés $P, Q \in \mathbb{F}_q[x]_n$, calculer $R = PQ \in \mathbb{F}_q[x]_{2n}$.

Le problème

p : nombre premier

$q = p^\lambda$

$\mathbb{F}_q[x]_n = \{P \in \mathbb{F}_q[x] : \deg P < n\}$

$\lg k = \lceil \log_2 \max(k, 1) \rceil$

Problème

Étant donnés $P, Q \in \mathbb{F}_q[x]_n$, calculer $R = PQ \in \mathbb{F}_q[x]_{2n}$.

Quelle est la complexité $\mathsf{M}_q(n)$ de cette opération en fonction de $n \lg q$?

Kronecker

Théorème

Si $\mathsf{M}_{\mathbb{Z}}(n)$ *désigne la complexité pour multiplier deux entiers de* n *bits, alors*

$$\mathsf{M}_p(n) \lesssim \mathsf{M}_{\mathbb{Z}}(n\,(2\lg p + \lg n))$$

Théorème

Si $\mathsf{M}_{\mathbb{Z}}(n)$ *désigne la complexité pour multiplier deux entiers de* n *bits, alors*

$$\mathsf{M}_p(n) \lesssim \mathsf{M}_{\mathbb{Z}}(n\,(2\lg p + \lg n))$$

$P = (3 \bmod 7)\,x^2 + (2 \bmod 7)\,x + (5 \bmod 7)$

$Q = (2 \bmod 7)\,x^2 + (1 \bmod 7)\,x + (4 \bmod 7)$

Théorème

Si $\mathsf{M}_{\mathbb{Z}}(n)$ *désigne la complexité pour multiplier deux entiers de* n *bits, alors*

$$\mathsf{M}_p(n) \lesssim \mathsf{M}_{\mathbb{Z}}(n\,(2\lg p + \lg n))$$

$P = (3 \bmod 7)\,x^2 + (2 \bmod 7)\,x + (5 \bmod 7)$

$Q = (2 \bmod 7)\,x^2 + (1 \bmod 7)\,x + (4 \bmod 7)$

$$\hat{P} = 3\,x^2 + 2\,x + 5$$

$$\hat{Q} = 2\,x^2 + 1\,x + 4$$

Théorème

Si $\mathsf{M}_{\mathbb{Z}}(n)$ désigne la complexité pour multiplier deux entiers de n bits, alors

$$\mathsf{M}_p(n) \lesssim \mathsf{M}_{\mathbb{Z}}(n\,(2\lg p + \lg n))$$

$P = (3 \bmod 7)\,x^2 + (2 \bmod 7)\,x + (5 \bmod 7)$

$Q = (2 \bmod 7)\,x^2 + (1 \bmod 7)\,x + (4 \bmod 7)$

$$\hat{P} = 3\,x^2 + 2\,x + 5$$

$$\hat{Q} = 2\,x^2 + 1\,x + 4$$

$$\hat{P}(2^8) = 110000001000000101$$

$$\hat{Q}(2^8) = 1000000000100000100$$

Théorème

Si $\mathsf{M}_{\mathbb{Z}}(n)$ *désigne la complexité pour multiplier deux entiers de* n *bits, alors*

$$\mathsf{M}_p(n) \lesssim \mathsf{M}_{\mathbb{Z}}(n\,(2\lg p + \lg n))$$

$P = (3 \bmod 7)\,x^2 + (2 \bmod 7)\,x + (5 \bmod 7)$ $\qquad$ $Q = (2 \bmod 7)\,x^2 + (1 \bmod 7)\,x + (4 \bmod 7)$

$$\hat{P} = 3\,x^2 + 2\,x + 5 \qquad \hat{Q} = 2\,x^2 + 1\,x + 4$$

$$\hat{P}(2^8) = 11000000100000101 \qquad \hat{Q}(2^8) = 10000000010000000100$$

$$(\hat{P}\,\hat{Q})(2^8) = 11000000111000110000000110100010100$$

Théorème

Si $\mathsf{M}_{\mathbb{Z}}(n)$ *désigne la complexité pour multiplier deux entiers de* n *bits, alors*

$$\mathsf{M}_p(n) \lesssim \mathsf{M}_{\mathbb{Z}}(n\,(2\lg p + \lg n))$$

$P = (3 \bmod 7)\,x^2 + (2 \bmod 7)\,x + (5 \bmod 7)$ $\qquad$ $Q = (2 \bmod 7)\,x^2 + (1 \bmod 7)\,x + (4 \bmod 7)$

$\hat{P} = 3\,x^2 + 2\,x + 5$ $\qquad$ $\hat{Q} = 2\,x^2 + 1\,x + 4$

$\hat{P}(2^8) = 11000000100000101$ $\qquad$ $\hat{Q}(2^8) = 1000000001000000100$

$$(\hat{P}\,\hat{Q})\,(2^8) = 110000001110001100000000110100010100$$

$$\hat{R} = \hat{P}\,\hat{Q} = 6\,x^4 + 7\,x^3 + 24\,x^2 + 13\,x + 20$$

Kronecker

Théorème

Si $\mathsf{M}_{\mathbb{Z}}(n)$ *désigne la complexité pour multiplier deux entiers de* n *bits, alors*

$$\mathsf{M}_p(n) \lesssim \mathsf{M}_{\mathbb{Z}}(n\,(2\lg p + \lg n))$$

$P = (3 \bmod 7)\,x^2 + (2 \bmod 7)\,x + (5 \bmod 7)$

$Q = (2 \bmod 7)\,x^2 + (1 \bmod 7)\,x + (4 \bmod 7)$

$$\hat{P} = 3\,x^2 + 2\,x + 5 \qquad \hat{Q} = 2\,x^2 + 1\,x + 4$$

$$\hat{P}(2^8) = 11000000100000101 \qquad \hat{Q}(2^8) = 10000000010000000100$$

$$(\hat{P}\,\hat{Q})(2^8) = 1100000011100011000000001101000100 10100$$

$$\hat{R} = \hat{P}\,\hat{Q} = 6\,x^4 + 7\,x^3 + 24\,x^2 + 13\,x + 20$$

$$R = (6 \bmod 7)\,x^4 + (0 \bmod 7)\,x^3 + (3 \bmod 7)\,x^2 + (6 \bmod 7)\,x + (6 \bmod 7)$$

Kronecker

Théorème

Si $\mathsf{M}_{\mathbb{Z}}(n)$ *désigne la complexité pour multiplier deux entiers de* n *bits, alors*

$$\mathsf{M}_p(n) \lesssim \mathsf{M}_{\mathbb{Z}}(n\,(2\lg p + \lg n))$$

- En général : $2^b \geqslant p^2 n \implies b \sim 2\lg p + \lg n$
- Corollaire : si $n = p^{O(1)}$, alors $\mathsf{M}_p(n) = O(\mathsf{M}_{\mathbb{Z}}(n \lg p))$

Kronecker

Théorème

Si $\mathsf{M}_{\mathbb{Z}}(n)$ *désigne la complexité pour multiplier deux entiers de* n *bits, alors*

$$\mathsf{M}_p(n) \lesssim \mathsf{M}_{\mathbb{Z}}(n\,(2\lg p + \lg n))$$

- En général : $2^b \geqslant p^2 n \implies b \sim 2\lg p + \lg n$
- Corollaire : si $n = p^{O(1)}$, alors $\mathsf{M}_p(n) = O(\mathsf{M}_{\mathbb{Z}}(n \lg p))$

Théorème (Harvey–vdH, ANTS 2018)

$$\begin{aligned} \mathsf{M}_{\mathbb{Z}}(n) &= O(n \lg n\, 4^{\log^* n}) \\ \log^* n &= \min\{n \in \mathbb{N} : \log \circ \overset{\ell\times}{\cdots} \circ \log n \leqslant 1\} \end{aligned}$$

Encore Kronecker

$$\mathbb{F}_q \;=\; \mathbb{F}_p[t]\,/\,(\mu(t)) \;\hookrightarrow\; \mathbb{F}_p[t]_{2\lambda} \qquad\qquad (q = p^\lambda)$$

Encore Kronecker

$$\mathbb{F}_q \;=\; \mathbb{F}_p[t]\,/\,(\mu(t)) \hookrightarrow \mathbb{F}_p[t]_{2\lambda} \qquad (q = p^\lambda)$$

$$\mathbb{F}_q[x]_n \hookrightarrow \mathbb{F}_p[t]_{2\lambda}[x]_n \xhookrightarrow{x=t^{2\lambda}} \mathbb{F}_p[t]_{2\lambda n}$$

$$\mathbb{F}_q = \mathbb{F}_p[t]/(\mu(t)) \hookrightarrow \mathbb{F}_p[t]_{2\lambda} \qquad (q = p^\lambda)$$

$$\mathbb{F}_q[x]_n \hookrightarrow \mathbb{F}_p[t]_{2\lambda}[x]_n \xhookrightarrow{x=t^{2\lambda}} \mathbb{F}_p[t]_{2\lambda n}$$

Théorème

$$\mathsf{M}_q(n) \leqslant \mathsf{M}_p(2\lambda n) + O(\mathsf{M}_p(\lambda)\, n)$$

Encore Kronecker

$$\mathbb{F}_q \;=\; \mathbb{F}_p[t]/(\mu(t)) \hookrightarrow \mathbb{F}_p[t]_{2\lambda} \qquad (q=p^\lambda)$$

$$\mathbb{F}_q[x]_n \hookrightarrow \mathbb{F}_p[t]_{2\lambda}[x]_n \xhookrightarrow{x=t^{2\lambda}} \mathbb{F}_p[t]_{2\lambda n}$$

Théorème

$$\mathsf{M}_q(n) \leqslant \mathsf{M}_p(2\lambda n) + O(\mathsf{M}_p(\lambda)\, n)$$

$$\mathbb{F}_p[t]_{\lambda n} \xhookrightarrow{x=t^{\lambda/2}} \mathbb{F}_p[t]_{\lambda/2}[x]_{2n} \hookrightarrow \mathbb{F}_q[x]_{2n}$$

Encore Kronecker

$$\mathbb{F}_q = \mathbb{F}_p[t]/(\mu(t)) \hookrightarrow \mathbb{F}_p[t]_{2\lambda} \qquad (q = p^\lambda)$$

$$\mathbb{F}_q[x]_n \hookrightarrow \mathbb{F}_p[t]_{2\lambda}[x]_n \xhookrightarrow{x=t^{2\lambda}} \mathbb{F}_p[t]_{2\lambda n}$$

Théorème

$$\mathsf{M}_q(n) \leqslant \mathsf{M}_p(2\lambda n) + O(\mathsf{M}_p(\lambda)\, n)$$

$$\mathbb{F}_p[t]_{\lambda n} \xhookrightarrow{x=t^{\lambda/2}} \mathbb{F}_p[t]_{\lambda/2}[x]_{2n} \hookrightarrow \mathbb{F}_q[x]_{2n}$$

Théorème

$$\mathsf{M}_p(\lambda n) \leqslant \mathsf{M}_q(2n) + O(n \lg q)$$

Multiplication par FFT

$\mathcal{R}$: anneau

$\omega \in \mathcal{R}$: racine principale n-ième d'unité $\longrightarrow \sum_{j=0}^{n-1} \omega^{ij} = 0$ pour $i = 1, \ldots, n-1$

Multiplication par FFT

$\mathscr{R}$: anneau

$\omega \in \mathscr{R}$: racine principale n-ième d'unité $\longrightarrow \sum_{j=0}^{n-1} \omega^{ij} = 0$ pour $i = 1, \ldots, n-1$

$$x^n - 1 \quad = \quad (x-1)(x-\omega)\cdots(x-\omega^{n-1})$$

Multiplication par FFT

$\mathcal{R}$: anneau

$\omega \in \mathcal{R}$: racine principale n-ième d'unité $\longrightarrow \sum_{j=0}^{n-1} \omega^{ij} = 0$ pour $i = 1, \ldots, n-1$

$$\mathcal{R}[x]/(x^n - 1) \quad \cong \quad \prod_{0 \leqslant i < n} \mathcal{R}[x]/(x - \omega^i) \quad \cong \quad \mathcal{R}^n$$

Multiplication par FFT

$\mathcal{R}$: anneau

$\omega \in \mathcal{R}$: racine principale n-ième d'unité $\longrightarrow \sum_{j=0}^{n-1} \omega^{ij} = 0$ pour $i = 1, \ldots, n-1$

$$\begin{array}{ccccc} \mathcal{R}[x]/(x^n - 1) & \cong & \prod_{0 \leqslant i < n} \mathcal{R}[x]/(x - \omega^i) & \cong & \mathcal{R}^n \\ P = P_0 + \cdots + P_{n-1} x^{n-1} & \xmapsto{\mathrm{DFT}_\omega} & (P(1), P(\omega), \ldots, P(\omega^{n-1})) & & \end{array}$$

Multiplication par FFT

$\mathcal{R}$: anneau

$\omega \in \mathcal{R}$: racine principale n-ième d'unité $\longrightarrow \sum_{j=0}^{n-1} \omega^{ij} = 0$ pour $i = 1, \ldots, n-1$

$$\begin{array}{ccccc} \mathcal{R}[x]/(x^n - 1) & \cong & \prod_{0 \leqslant i < n} \mathcal{R}[x]/(x - \omega^i) & \cong & \mathcal{R}^n \\ P = P_0 + \cdots + P_{n-1} x^{n-1} & \xmapsto{\mathrm{DFT}_\omega} & (P(1), P(\omega), \ldots, P(\omega^{n-1})) & & \\ Q = Q_0 + \cdots + Q_{n-1} x^{n-1} & \xmapsto{\mathrm{DFT}_\omega} & (Q(1), Q(\omega), \ldots, Q(\omega^{n-1})) & & \end{array}$$

Multiplication par FFT

$\mathcal{R}$: anneau

$\omega \in \mathcal{R}$: racine principale n-ième d'unité $\longrightarrow \sum_{j=0}^{n-1} \omega^{ij} = 0$ pour $i = 1, \ldots, n-1$

$$\begin{array}{rcl}
\mathcal{R}[x]/(x^n - 1) & \cong & \prod_{0 \leqslant i < n} \mathcal{R}[x]/(x - \omega^i) \quad \cong \quad \mathcal{R}^n \\
P = P_0 + \cdots + P_{n-1} x^{n-1} & \xmapsto{\mathrm{DFT}_\omega} & (P(1), P(\omega), \ldots, P(\omega^{n-1})) \\
Q = Q_0 + \cdots + Q_{n-1} x^{n-1} & \xmapsto{\mathrm{DFT}_\omega} & (Q(1), Q(\omega), \ldots, Q(\omega^{n-1})) \\
R = P\,Q & \xleftarrow{\mathrm{DFT}_\omega^{-1}} & (P(1)\,Q(1), P(\omega)\,Q(\omega), \ldots, P(\omega^{n-1})\,Q(\omega^{n-1}))
\end{array}$$

Multiplication par FFT

$\mathcal{R}$: anneau

$\omega \in \mathcal{R}$: racine principale n-ième d'unité $\longrightarrow \sum_{j=0}^{n-1} \omega^{ij} = 0$ pour $i = 1, \dots, n-1$

$$\mathcal{R}[x]/(x^n - 1) \quad \cong \quad \prod_{0 \leqslant i < n} \mathcal{R}[x]/(x - \omega^i) \quad \cong \quad \mathcal{R}^n$$

$$P = P_0 + \cdots + P_{n-1} x^{n-1} \xrightarrow{\mathrm{DFT}_\omega} (P(1), P(\omega), \dots, P(\omega^{n-1}))$$

$$Q = Q_0 + \cdots + Q_{n-1} x^{n-1} \xrightarrow{\mathrm{DFT}_\omega} (Q(1), Q(\omega), \dots, Q(\omega^{n-1}))$$

$$R = PQ \xleftarrow{\mathrm{DFT}_\omega^{-1}} (P(1)\,Q(1), P(\omega)\,Q(\omega), \dots, P(\omega^{n-1})\,Q(\omega^{n-1}))$$

$$\boxed{PQ \;=\; \mathrm{DFT}_\omega^{-1}(\mathrm{DFT}_\omega(P), \mathrm{DFT}_\omega(Q)) \;=\; \frac{1}{n} \mathrm{DFT}_{\omega^{-1}}(\mathrm{DFT}_\omega(P), \mathrm{DFT}_\omega(Q))}$$

Cooley–Tukey

$n = n_1 n_2, \qquad n_1, n_2 > 1, \qquad i = i_1 n_2 + i_2, \qquad 0 \leqslant i_1 < n_1, \qquad 0 \leqslant i_2 < n_2$

Cooley–Tukey

$$n = n_1 n_2, \qquad n_1, n_2 > 1, \qquad i = i_1 n_2 + i_2, \qquad 0 \leqslant i_1 < n_1, \qquad 0 \leqslant i_2 < n_2$$

$$\begin{aligned}
\hat{P}_i = P(\omega^i) &= \sum_{0 \leqslant k < n} P_k \omega^{ki} \\
&= \sum_{0 \leqslant k_1 < n_1} \sum_{0 \leqslant k_2 < n_2} P_{k_2 n_1 + k_1} \omega^{(k_2 n_1 + k_1)(i_1 n_2 + i_2)} \\
&= \sum_{0 \leqslant k_1 < n_1} \omega^{k_1 i_2} \left(\sum_{0 \leqslant k_2 < n_2} P_{k_2 n_1 + k_1} (\omega^{n_1})^{k_2 i_2} \right) (\omega^{n_2})^{k_1 i_1}
\end{aligned}$$

Cooley–Tukey

$$n = n_1 n_2, \qquad n_1, n_2 > 1, \qquad i = i_1 n_2 + i_2, \qquad 0 \leqslant i_1 < n_1, \qquad 0 \leqslant i_2 < n_2$$

$$\begin{aligned}
\hat{P}_i = P(\omega^i) &= \sum_{0 \leqslant k < n} P_k \omega^{ki} \\
&= \sum_{0 \leqslant k_1 < n_1} \sum_{0 \leqslant k_2 < n_2} P_{k_2 n_1 + k_1} \omega^{(k_2 n_1 + k_1)(i_1 n_2 + i_2)} \\
&= \sum_{0 \leqslant k_1 < n_1} \omega^{k_1 i_2} \left(\sum_{0 \leqslant k_2 < n_2} P_{k_2 n_1 + k_1} (\omega^{n_1})^{k_2 i_2} \right) (\omega^{n_2})^{k_1 i_1}
\end{aligned}$$

Cooley–Tukey

$$n = n_1 n_2, \qquad n_1, n_2 > 1, \qquad i = i_1 n_2 + i_2, \qquad 0 \leqslant i_1 < n_1, \qquad 0 \leqslant i_2 < n_2$$

$$\begin{aligned}
\hat{P}_i = P(\omega^i) &= \sum_{0 \leqslant k < n} P_k \, \omega^{ki} \\
&= \sum_{0 \leqslant k_1 < n_1} \; \sum_{0 \leqslant k_2 < n_2} P_{k_2 n_1 + k_1} \, \omega^{(k_2 n_1 + k_1)(i_1 n_2 + i_2)} \\
&= \sum_{0 \leqslant k_1 < n_1} \omega^{k_1 i_2} \left(\sum_{0 \leqslant k_2 < n_2} P_{k_2 n_1 + k_1} \, (\omega^{n_1})^{k_2 i_2} \right) (\omega^{n_2})^{k_1 i_1}
\end{aligned}$$

$\mathsf{F}_{\mathscr{R}}(n)$: coût DFT, $\qquad$ $\mathsf{m}_{\mathscr{R}}$: coût multiplication ω^i, $\qquad$ $\mathsf{s}_{\mathscr{R}}$: espace élément

$$\boxed{\mathsf{F}_{\mathscr{R}}(n_1 n_2) \leqslant n_2 \, \mathsf{F}_{\mathscr{R}}(n_1) + n_1 \, \mathsf{F}_{\mathscr{R}}(n_2) + n \, \mathsf{m}_{\mathscr{R}} + O(\mathsf{s}_{\mathscr{R}} \, n \log \min(n_1, n_2))}$$

Cooley–Tukey récursif

$n = n_1 \cdots n_\ell$

Théorème

$$\mathsf{F}_{\mathscr{R}}(n) \leqslant n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{\mathscr{R}}(n_i)}{n_i} + \ell\, n\, \mathsf{m}_{\mathscr{R}} + O(\mathsf{s}_{\mathscr{R}}\, n \log n).$$

Cooley–Tukey récursif

$n = n_1 \cdots n_\ell$

Théorème

$$\mathsf{F}_{\mathscr{R}}(n) \leqslant n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{\mathscr{R}}(n_i)}{n_i} + \ell\, n\, \mathsf{m}_{\mathscr{R}} + O(\mathsf{s}_{\mathscr{R}}\, n \log n).$$

$n = 2^\ell, \quad n_1 = \cdots = n_\ell = 2$

Corollaire

$$\mathsf{F}_{\mathscr{R}}(n) = O(\mathsf{m}_{\mathscr{R}}\, n \log n).$$

Schönhage-Straßen

$\mathbb{K}$: corps de caractéristique $\neq 2$

$n = 2^\ell$

$\mathcal{R} = \mathbb{K}[t]/(t^{n/2}+1)$

$\omega = t$

$\mathsf{m}_{\mathcal{R}} = O(\mathsf{s}_{\mathcal{R}})$

$\mathbb{K}$: corps de caractéristique $\neq 2$

$n = 2^\ell$

$\mathcal{R} = \mathbb{K}[t]/(t^{n/2}+1)$

$\omega = t$

$\mathsf{m}_{\mathcal{R}} = O(\mathsf{s}_{\mathcal{R}})$

$$\boxed{\mathsf{F}_{\mathcal{R}}(n) = O(\mathsf{s}_{\mathcal{R}}\, n \log n)}$$

Schönhage-Straßen

$\mathbb{K}$: corps de caractéristique $\neq 2$

$n = 2^\ell$

$\mathcal{R} = \mathbb{K}[t]/(t^{n/2}+1)$

$\omega = t$

$\mathsf{m}_{\mathcal{R}} = O(\mathsf{s}_{\mathcal{R}})$

$$\boxed{\mathsf{F}_{\mathcal{R}}(n) = O(\mathsf{s}_{\mathcal{R}}\, n \log n)}$$

$$\boxed{\mathsf{M}_{\mathbb{K}}(n^2) = 2n\,\mathsf{M}_{\mathbb{K}}(n) + O(\mathsf{s}_{\mathbb{K}}\, n^2 \log n)}$$

Schönhage-Straßen

$\mathbb{K}$: corps de caractéristique $\neq 2$

$n = 2^\ell$

$\mathcal{R} = \mathbb{K}[t]/(t^{n/2}+1)$

$\omega = t$

$\mathsf{m}_\mathcal{R} = O(\mathsf{s}_\mathcal{R})$

$$\boxed{\mathsf{F}_\mathcal{R}(n) = O(\mathsf{s}_\mathcal{R}\, n \log n)}$$

$$\boxed{\mathsf{M}_\mathbb{K}(n^2) = 2n\,\mathsf{M}_\mathbb{K}(n) + O(\mathsf{s}_\mathbb{K}\, n^2 \log n)}$$

Théorème

$$\mathsf{M}_\mathbb{K}(n) = O(\mathsf{s}_\mathbb{K}\, n \log n \log\log n + \mathsf{M}_\mathbb{K}(1)\, n \log n)$$

Retour aux corps finis

$\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{p^\lambda}, \qquad n = n_1 \cdots n_\ell, \qquad n \mid (q-1)$

Retour aux corps finis

$\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{p^\lambda}$, $\quad n = n_1 \cdots n_\ell$, $\quad n \mid (q-1)$

$$\mathsf{F}_{\mathbb{K}}(n) \leqslant n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{\mathbb{K}}(n_i)}{n_i} + \ell\, n\, \mathsf{m}_{\mathbb{K}} + O(\mathsf{s}_{\mathbb{K}}\, n \log n)$$

Retour aux corps finis

$\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{p^\lambda}, \qquad n = n_1 \cdots n_\ell, \qquad n \mid (q-1)$

$$\mathsf{F}_{\mathbb{K}}(n) \leqslant n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{\mathbb{K}}(n_i)}{n_i} + \ell\, n\, \mathsf{m}_{\mathbb{K}} + O(\mathsf{s}_{\mathbb{K}}\, n \log n)$$

$n_1, \ldots, n_\ell$ petits

Retour aux corps finis

$\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{p^\lambda}, \qquad n = n_1 \cdots n_\ell, \qquad n \mid (q-1)$

$$\mathsf{F}_{\mathbb{K}}(n) \leqslant n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{\mathbb{K}}(n_i)}{n_i} + \ell\, n\, \mathsf{m}_{\mathbb{K}} + O(\mathsf{s}_{\mathbb{K}}\, n \log n)$$

$n_1, \ldots, n_\ell$ petits

$\ell \ll \log n$

Exemple

$$2^{60}-1=3^2\cdot 5^2\cdot 7\cdot 11\cdot 13\cdot 31\cdot 41\cdot 61\cdot 151\cdot 331\cdot 1321$$

Exemple

$$2^{60}-1 = 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$$

Motif plus général

λ friable $\implies$ $p^{\lambda}-1$ admet un grand facteur friable

Exemple

$$2^{60}-1=3^2\cdot 5^2\cdot 7\cdot 11\cdot 13\cdot 31\cdot 41\cdot 61\cdot 151\cdot 331\cdot 1321$$

Motif plus général

λ friable $\implies$ $p^{\lambda}-1$ admet un grand facteur friable

$r\neq p$ premier, $(r-1)\,|\,\lambda \implies r\,|\,(p^{\lambda}-1)$

Énonce rigoureux

$$H_\lambda := \prod_{q \text{ prime}, \ (q-1) \mid \lambda} q.$$

Théorème (Adleman–Pomerance–Rumely, 1983)

Il existe $c_5 > c_4 > 0$ tels que pour tout $k > 100$, on a

$$(\log k)^{c_4 \log\log\log k} < \min\{\lambda \in \mathbb{N} : H_\lambda \geqslant \sqrt{k}\} < (\log k)^{c_5 \log\log\log k}$$

Théorème

Il existe $c_3 > c_2 > 0$ et $n_0 \in \mathbb{N}$ tels que pour tout p premier et $n \geqslant n_0$, il existe λ avec

$$(\lg n)^{c_2 \lg\lg\lg n} < \lambda < (\lg n)^{c_3 \lg\lg\lg n},$$

et un entier $(\lambda+1)$-friable $M \geqslant n$ avec $M \mid (p^\lambda - 1)$.

$n_1, \ldots, n_\ell$ petits, mais pas trop petits…

$$2^{60} - 1 = 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$$

$n_1, \ldots, n_\ell$ petits, mais pas trop petits...

$$2^{60} - 1 = 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$$

$$100 \quad < \quad 225 \qquad 1001 \qquad 1271 \qquad 9211 \qquad 331 \qquad 1321 \quad < \quad 10000$$

$n_1, \ldots, n_\ell$ petits, mais pas trop petits…

$$2^{60}-1 = 3^2\cdot 5^2 \cdot 7\cdot 11\cdot 13 \cdot 31\cdot 41 \cdot 61\cdot 151 \cdot 331 \cdot 1321$$

$$100 \quad < \quad 225 \quad 1001 \quad 1271 \quad 9211 \quad 331 \quad 1321 \quad < \quad 10000$$

Théorème

Avec p, n, λ, M *comme* $\uparrow$, *soient* $L, S \in \mathbb{N}$ *tels que* $\lambda < S < L < M$. *Alors il existe (et on peut rapidement calculer) des entiers* $(\lambda+1)$*-friables* $N_1, \ldots, N_d$ *tels que :*

a) $N := N_1 \cdots N_d$ *divise* M *(et donc divise* $p^\lambda - 1$*).*

b) $L \leqslant N \leqslant (\lambda+1)\,L$.

c) $S \leqslant N_i \leqslant S^3$ *pour* $i = 1, \ldots, d$.

Choix des paramètres

$\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{p^\lambda}, \qquad n = n_1 \cdots n_\ell, \qquad n \mid (q-1), \qquad n \gg p$

$$\mathsf{F}_{\mathbb{K}}(n) \leqslant n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{\mathbb{K}}(n_i)}{n_i} + O(\ell\, n\, \mathsf{m}_{\mathbb{K}} + \mathsf{s}_{\mathbb{K}}\, n \log n)$$

Choix des paramètres

$\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{p^\lambda}, \qquad n = n_1 \cdots n_\ell, \qquad n \mid (q-1), \qquad n \gg p$

$$\mathsf{F}_{\mathbb{K}}(n) \leqslant n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{\mathbb{K}}(n_i)}{n_i} + O(n \lg q\, (\ell \lg \lg q \lg \lg \lg q + \lg n))$$

Choix des paramètres

$$\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{p^\lambda}, \qquad n = n_1 \cdots n_\ell, \qquad n \mid (q-1), \qquad n \gg p$$

$$\mathsf{F}_{\mathbb{K}}(n) \leqslant n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{\mathbb{K}}(n_i)}{n_i} + O(n \lg q\, (\ell \lg \lg q \lg \lg \lg q + \lg n))$$

$$(\lg n)^{c_2 \lg \lg \lg n} < \lambda < (\lg n)^{c_3 \lg \lg \lg n}, \qquad \ell \approx \frac{\lg n}{(\lg \lg n)^3 \lg \lg \lg n}, \qquad n_i \approx \sqrt[\ell]{n}$$

Choix des paramètres

$$\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{p^\lambda}, \qquad n = n_1 \cdots n_\ell, \qquad n \mid (q-1), \qquad n \gg p$$

$$\mathsf{F}_{\mathbb{K}}(n) \leqslant n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{\mathbb{K}}(n_i)}{n_i} + O(n \lg q \, (\ell \lg \lg q \lg \lg \lg q + \lg n))$$

$$(\lg n)^{c_2 \lg \lg \lg n} < \lambda < (\lg n)^{c_3 \lg \lg \lg n}, \qquad \ell \approx \frac{\lg n}{(\lg \lg n)^3 \lg \lg \lg n}, \qquad n_i \approx \sqrt[\ell]{n}$$

$$\mathsf{F}_{\mathbb{K}}(n) \leqslant n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{\mathbb{K}}(n_i)}{n_i} + O(n \lg q \lg n)$$

Réduction de Bluestein

$\omega = \eta^2$: racine n-ième principale dans $\mathbb{K}$ avec n pair

Réduction de Bluestein

$\omega = \eta^2$: racine n-ième principale dans $\mathbb{K}$ avec n pair

$$f_i := \eta^{i^2}, \qquad g_i := \eta^{-i^2}$$

Réduction de Bluestein

$\omega = \eta^2$: racine n-ième principale dans $\mathbb{K}$ avec n pair

$$f_i := \eta^{i^2}, \qquad g_i := \eta^{-i^2}$$

$$\omega^{ij} = \eta^{2ij} = \eta^{i^2+j^2-(i-j)^2} = f_i \, f_j \, g_{i-j}$$

Réduction de Bluestein

$\omega = \eta^2$: racine n-ième principale dans $\mathbb{K}$ avec n pair

$$f_i := \eta^{i^2}, \qquad g_i := \eta^{-i^2}$$

$$\omega^{ij} = \eta^{2ij} = \eta^{i^2+j^2-(i-j)^2} = f_i\, f_j\, g_{i-j}$$

$$g_{i+n} = \eta^{-(i+n)^2} = \eta^{-i^2-n^2-2ni} = \eta^{-i^2}\,\omega^{-\left(\frac{n}{2}+i\right)n} = g_i$$

Réduction de Bluestein

$\omega = \eta^2$: racine n-ième principale dans $\mathbb{K}$ avec n pair

$$f_i := \eta^{i^2}, \qquad g_i := \eta^{-i^2}$$

$$\omega^{ij} = \eta^{2ij} = \eta^{i^2+j^2-(i-j)^2} = f_i\, f_j\, g_{i-j}$$

$$g_{i+n} = \eta^{-(i+n)^2} = \eta^{-i^2-n^2-2ni} = \eta^{-i^2}\,\omega^{-(\frac{n}{2}+i)n} = g_i$$

Pour tout $P = P_0 + \cdots + P_{n-1}\, x^{n-1} \in \mathbb{K}[x]/(x^n - 1)$, on a

$$\hat{P}_i = \sum_{j=0}^{n-1} P_j \omega^{ij} = f_i \sum_{j=0}^{n-1} (P_j\, f_j)\, g_{i-j} \longrightarrow f_i\,(F\,G)_i$$

Réduction de Bluestein

$\omega = \eta^2$: racine n-ième principale dans $\mathbb{K}$ avec n pair

$$f_i := \eta^{i^2}, \qquad g_i := \eta^{-i^2}$$

Pour tout $P = P_0 + \cdots + P_{n-1} x^{n-1} \in \mathbb{K}[x]/(x^n - 1)$, on a

$$\hat{P}_i = \sum_{j=0}^{n-1} P_j \omega^{ij} = f_i \sum_{j=0}^{n-1} (P_j f_j)\, g_{i-j} \longrightarrow f_i (F G)_i$$

$$\boxed{\mathsf{F}_{\mathbb{K}}(n) \leqslant \mathsf{M}_{\mathbb{K}}(n) + O(\mathsf{M}_{\mathbb{K}}(1)\, n)}$$

Résumé

$$\mathsf{M}_p(\lambda n) \preccurlyeq \mathsf{M}_{p^\lambda}(n) \preccurlyeq \mathsf{F}_{p^\lambda}(n) + n\,\mathsf{M}_{p^\lambda}(1) \preccurlyeq n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{p^\lambda}(n_i)}{n_i} + O(n \lg n \lg q)$$

Résumé

$$\mathsf{M}_p(\lambda n) \preccurlyeq \mathsf{M}_{p^\lambda}(n) \preccurlyeq \mathsf{F}_{p^\lambda}(n) + n\,\mathsf{M}_{p^\lambda}(1) \preccurlyeq n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{p^\lambda}(n_i)}{n_i} + O(n \lg n \lg q)$$

$$\sum_{i=1}^{\ell} \frac{\mathsf{F}_{p^\lambda}(n_i)}{n_i} \preccurlyeq \sum_{i=1}^{\ell} \frac{\mathsf{M}_{p^\lambda}(n_i)}{n_i} + O(\lg n \lg q) \preccurlyeq \sum_{i=1}^{\ell} \frac{\mathsf{M}_p(\lambda n_i)}{n_i} + O(\lg n \lg q)$$

Résumé

$$\mathsf{M}_p(\lambda n) \preccurlyeq \mathsf{M}_{p^\lambda}(n) \preccurlyeq \mathsf{F}_{p^\lambda}(n) + n\,\mathsf{M}_{p^\lambda}(1) \preccurlyeq n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{p^\lambda}(n_i)}{n_i} + O(n \lg n \lg q)$$

$$\sum_{i=1}^{\ell} \frac{\mathsf{F}_{p^\lambda}(n_i)}{n_i} \preccurlyeq \sum_{i=1}^{\ell} \frac{\mathsf{M}_{p^\lambda}(n_i)}{n_i} + O(\lg n \lg q) \preccurlyeq \sum_{i=1}^{\ell} \frac{\mathsf{M}_p(\lambda n_i)}{n_i} + O(\lg n \lg q)$$

$$\frac{\mathsf{M}_p(\lambda n)}{\lambda n \cdot \lg(\lambda n) \cdot \lg q} \leqslant K \max_{1 \leqslant i \leqslant \ell} \frac{\mathsf{M}_p(\lambda n_i)}{\lambda n_i \cdot \lg(\lambda n_i) \cdot \lg q} + O(1)$$

Résumé

$$\mathsf{M}_p(\lambda n) \preccurlyeq \mathsf{M}_{p^\lambda}(n) \preccurlyeq \mathsf{F}_{p^\lambda}(n) + n\,\mathsf{M}_{p^\lambda}(1) \preccurlyeq n\sum_{i=1}^{\ell} \frac{\mathsf{F}_{p^\lambda}(n_i)}{n_i} + O(n \lg n \lg q)$$

$$\sum_{i=1}^{\ell} \frac{\mathsf{F}_{p^\lambda}(n_i)}{n_i} \preccurlyeq \sum_{i=1}^{\ell} \frac{\mathsf{M}_{p^\lambda}(n_i)}{n_i} + O(\lg n \lg q) \preccurlyeq \sum_{i=1}^{\ell} \frac{\mathsf{M}_p(\lambda n_i)}{n_i} + O(\lg n \lg q)$$

$$\frac{\mathsf{M}_p(\lambda n)}{\lambda n \cdot \lg(\lambda n) \cdot \lg q} \leqslant K \max_{1 \leqslant i \leqslant \ell} \frac{\mathsf{M}_p(\lambda n_i)}{\lambda n_i \cdot \lg(\lambda n_i) \cdot \lg q} + O(1)$$

Théorème (Harvey–vdH–Lecerf, JACM 2017)

$$\mathsf{M}_p(n) = O(n \lg p \cdot \lg(n \lg p) \cdot K^{\log^*(n \lg p)})$$

Résumé

$$\mathsf{M}_p(\lambda n) \preccurlyeq \mathsf{M}_{p^\lambda}(n) \preccurlyeq \mathsf{F}_{p^\lambda}(n) + n\,\mathsf{M}_{p^\lambda}(1) \preccurlyeq n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{p^\lambda}(n_i)}{n_i} + O(n \lg n \lg q)$$

$$\sum_{i=1}^{\ell} \frac{\mathsf{F}_{p^\lambda}(n_i)}{n_i} \preccurlyeq \sum_{i=1}^{\ell} \frac{\mathsf{M}_{p^\lambda}(n_i)}{n_i} + O(\lg n \lg q) \preccurlyeq \sum_{i=1}^{\ell} \frac{\mathsf{M}_p(\lambda n_i)}{n_i} + O(\lg n \lg q)$$

$$\frac{\mathsf{M}_p(\lambda n)}{\lambda n \cdot \lg(\lambda n) \cdot \lg q} \leqslant K \max_{1 \leqslant i \leqslant \ell} \frac{\mathsf{M}_p(\lambda n_i)}{\lambda n_i \cdot \lg(\lambda n_i) \cdot \lg q} + O(1)$$

Théorème (Harvey–vdH–Lecerf, JACM 2017)

$$\mathsf{M}_p(n) = O(n \lg p \cdot \lg(n \lg p) \cdot 8^{\log^*(n \lg p)})$$

Résumé

$$\mathsf{M}_p(\lambda n) \preccurlyeq \mathsf{M}_{p^\lambda}(n) \preccurlyeq \mathsf{F}_{p^\lambda}(n) + n\,\mathsf{M}_{p^\lambda}(1) \preccurlyeq n \sum_{i=1}^{\ell} \frac{\mathsf{F}_{p^\lambda}(n_i)}{n_i} + O(n \lg n \lg q)$$

$$\sum_{i=1}^{\ell} \frac{\mathsf{F}_{p^\lambda}(n_i)}{n_i} \preccurlyeq \sum_{i=1}^{\ell} \frac{\mathsf{M}_{p^\lambda}(n_i)}{n_i} + O(\lg n \lg q) \preccurlyeq \sum_{i=1}^{\ell} \frac{\mathsf{M}_p(\lambda n_i)}{n_i} + O(\lg n \lg q)$$

$$\frac{\mathsf{M}_p(\lambda n)}{\lambda n \cdot \lg(\lambda n) \cdot \lg q} \leqslant K \max_{1 \leqslant i \leqslant \ell} \frac{\mathsf{M}_p(\lambda n_i)}{\lambda n_i \cdot \lg(\lambda n_i) \cdot \lg q} + O(1)$$

Théorème (Harvey–vdH, 2017, soumis)

$$\mathsf{M}_p(n) = O(n \lg p \cdot \lg(n \lg p) \cdot 4^{\log^*(n \lg p)})$$

Frobenius–FFT

Pour passage $\mathbb{F}_p \to \mathbb{F}_q$, directement plonger $\mathbb{F}_p[x] \subseteq \mathbb{F}_q[x]$

Comment regagner le facteur λ ?

Frobenius–FFT

Pour passage $\mathbb{F}_p \to \mathbb{F}_q$, directement plonger $\mathbb{F}_p[x] \subseteq \mathbb{F}_q[x]$

Comment regagner le facteur λ ?

Idée

$$P(\omega^p) = P(\omega)^p$$

Frobenius–FFT

Pour passage $\mathbb{F}_p \to \mathbb{F}_q$, directement plonger $\mathbb{F}_p[x] \subseteq \mathbb{F}_q[x]$

Comment regagner le facteur λ ?

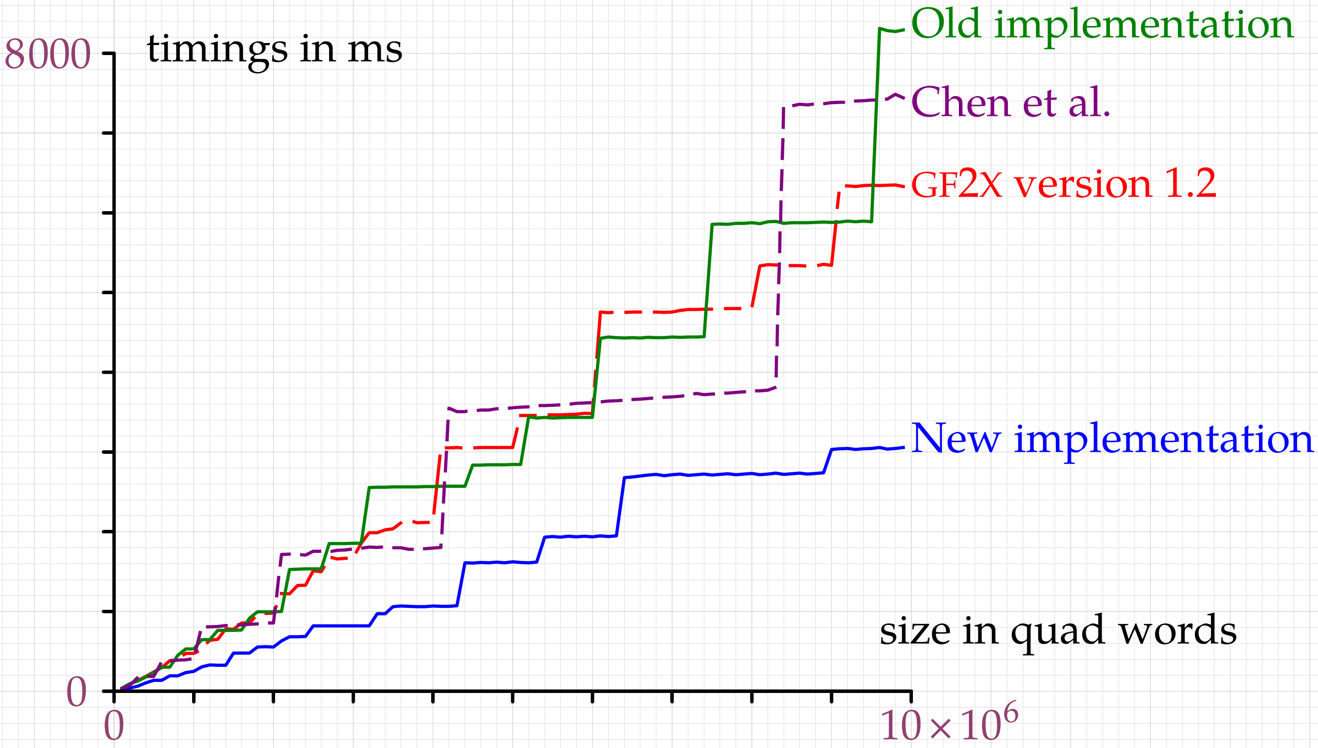
Idée

$$P(\omega^p) = P(\omega)^p$$

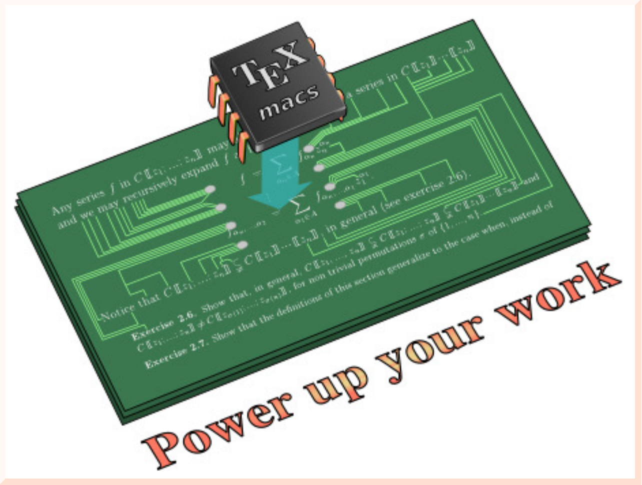
Corps Babylonien $\mathbb{F}_{2^{60}}$

- $60 = 64 - \epsilon$
- $(t^{61} - 1) / (t - 1)$ est irréductible $\Longrightarrow$ plongement $\mathbb{F}_{2^{60}} \subseteq \mathbb{F}_2[x] / (x^{61} - 1)$
- Pour DFT d'ordre 61, racine primitive ω d'ordre 60 pour Frobenius

Implantation dans MATHEMAGIX



Merci !



http://www.TeXmacs.org