Arithmétique moderne

Paul Zimmermann

INRIA Nancy - Grand Est, France

RAIM'09, Lyon, 28 octobre 2009

Modern Computer Arithmetic

Richard P. Brent and Paul Zimmermann

Version 0.3

Historique

Commencé en juillet 2003, presque terminé.

Téléchargeable depuis
`http://www.loria.fr/~zimmerma/mca/pub226.html`

La version actuelle (0.3) a 221 pages.

Version papier en 2010 ?

La version électronique restera accessible en ligne.

Un livre de plus ?

Certaines parties du volume 2 de Knuth TAOCP sont obsolètes : division récursive, multiplication de Schönhage-Strassen, algorithmes sur les flottants

La plupart des livres ne considèrent que le domaine quadratique ou le domaine de la FFT, pas les algorithmes intermédiaires (Karatsuba, Toom-Cook)

La plupart des livres ne considèrent que la multiplication rapide, quelques-uns parlent de division rapide, très peu d'autres algorithmes (racine carrée, conversion entre bases, pgcd, ...)

La plupart des références laissent au lecteur la gestion des retenues et erreurs d'arrondi, ...

Les algorithmes de « Modern Computer Arithmetic » peuvent être implantés « tels quels ».

Autres livres (1/2)

The Design and Analysis of Computer Algorithms, Aho, Hopcroft, Ullman, 1974, pgcd rapide de polynômes

The Art of Computer Programming, vol .2, Seminumerical Algorithms, D. E. Knuth, 3e édition, 1998, nombreux algorithmes

Fast Algorithms, A Multitape Turing Machine Implementation, Schönhage, Grotefeld, Vetter, 1994, quelques beaux algorithmes

Handbook of Applied Cryptography, chapitre 14, Menezes, van Oorschot, Vanstone, 1997 : traite uniquement du domaine quadratique

Autres livres (2/2)

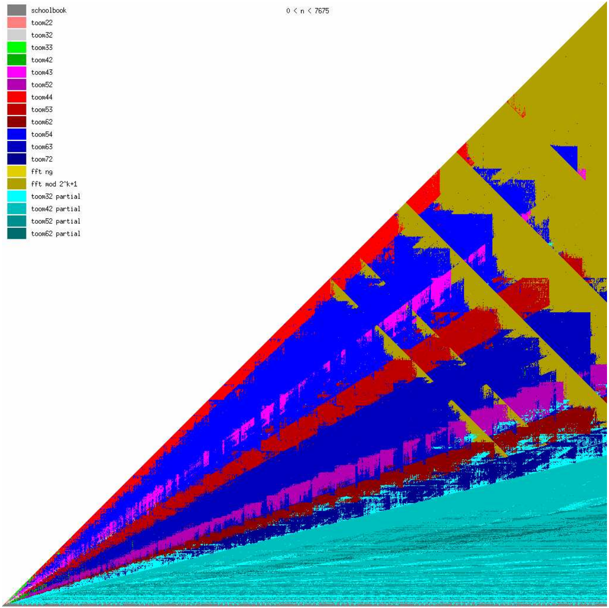
Modern Computer Algebra, von zur Gathen and Gerhard, 1999 : même principe pour polynômes et séries

Prime Numbers : A Computational Perspective, chapitre 9 (Fast Algorithms for Large-Integer Arithmetic), 2001

Handbook of Elliptic and Hyperelliptic Curve Cryptography, Cohen, Frey, Avanzi, Doche, Lange, Vercauteren, 2005 (chapitres 9, 10, 11, 12), traite principalement du domaine quadratique

Handbook of Floating-Point Arithmetic, Brisebarre, de Dinechin, Jeannerod, Lefèvre, Melquiond, Muller, Revol, Stehlé, Torres, Birkhäuser, 2009-2010, traite uniquement des algorithmes sur les nombres flottants

GNU MP Reference Manual, chapitre Algorithms, peu connu mais très bien fait



(copyright `gmplib.org`)

Contenu

Le livre comporte 4 chapitres :

1. Integer Arithmetic
2. The FFT and Modular Arithmetic
3. Floating-Point Arithmetic
4. Newton's Method and Function Evaluation

Dans chaque chapitre nous indiquons les principaux algorithmes.

(Les algorithmes trop techniques sont traités en exercice.)

Plan de l'exposé

- pgcd binaire
- division récursive
- division de Hensel et multiplication de Montgomery
- multiplication déséquilibrée
- division de Svoboda
- division bidirectionnelle
- symbole de Jacobi

Le pgcd 2-adique (avec Stehlé)

On peut calculer le pgcd de deux entiers de n bits en $O(M(n) \log n)$ avec l'algorithme de Knuth-Schönhage (proposé par Knuth en 1970 mais avec un coût $O(n \log^5 n \log \log n)$, amélioré par Schönhage en 1971 à $O(n \log^2 n \log \log n)$)

À cause des retenues, cet algorithme nécessite une « étape de correction », qui est difficile à implanter correctement (cf « On Schönhage's Algorithm and Subquadratic Integer GCD Computation », Niels Möller, Mathematics of Computation, 2008)

Or on sait diviser des entiers par les poids faibles (LSB).

Question (posée à Damien Stehlé en 2003) : peut-on avoir un pgcd asymptotiquement rapide par les poids faibles ?

	division	pgcd
classique	$O(M(n))$	$O(M(n)\log n)$
2-adique	$O(M(n))$	? ? ?

Pgcd rapide classique

Soient $a = 935$ et $b = 714$.

$$a_{i-1} = q_i a_i + a_{i+1}$$

$a_0 = 935$, $a_1 = 714$, $a_2 = 221$, $a_3 = 51$, $a_4 = 17$, $a_5 = 0$.

$$\begin{pmatrix} a_i \\ a_{i-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & q_i \end{pmatrix} \begin{pmatrix} a_{i+1} \\ a_i \end{pmatrix}$$

$$\begin{pmatrix} a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} a_5 \\ a_4 \end{pmatrix}$$

Astuce : calculer q_i à partir des bits de poids fort de a_i, et multiplier les matrices $\begin{pmatrix} 0 & 1 \\ 1 & q_i \end{pmatrix}$ avec une multiplication rapide (product tree)

Problème : déterminer correctement q_i malgré les retenues.

Pgcd rapide classique en base 2

935	1110100111
714	1011001010
221	0011011101
51	0000110011
17	0000010001
0	0000000000

Division binaire

Définition (division binaire)
Soient $a, b \in \mathbb{Z}$ avec $\nu_2(b) > \nu_2(a)$.
Soit $j = \nu_2(b) - \nu_2(a)$.
Il existe un unique $|q| < 2^j$ tel que $\nu_2(b) < \nu_2(r)$ et :

$$r = a + q2^{-j}b$$

q est le quotient binaire de a par b
r est le reste binaire de a par b

Soient $a' = a/2^{\nu_2(a)}$, $b' = b/2^{\nu_2(b)}$.
$\nu_2(a') = \nu_2(b') = 0$
On veut $\nu_2(a' + qb') > j$, donc $a' + qb' \equiv 0 \bmod 2^{j+1}$.

$$q \equiv -a'/b' \bmod 2^{j+1} \quad \text{(centré)}$$

Division binaire : un exemple

Soit $a = 935 = (1110100111)_2$ avec $\nu_2(a) = 0$.
Soit $b = 714 = (1011001010)_2$ avec $\nu_2(b) = 1 > \nu_2(a)$.

$$q \equiv -935/(714/2) \equiv 1 \bmod 2^2$$

$r = a + 1 \cdot b/2 = 1292 = (10100001100)_2$.

Attention : on garde les zéros dans les poids faibles !

Pgcd binaire

Itérer simplement la division binaire jusqu'à atteindre 0.

i	q_i	a_i	a_i (base 2)
0		935	1110100111
1	0	714	1011001010
2	1	1292	10100001100
3	1	1360	10101010000
4	1	1632	11001100000
5	1	2176	100010000000
6	-3	0	000000000000

Le pgcd de a, b est la partie impaire du dernier terme non nul.

Pgcd binaire : avantages et inconvénients

$\oplus$ les retenues vont vers les poids forts : plus de « correction »

$\oplus$ $q = a/b \bmod 2^j$ plus facile à calculer que $q = \lfloor a/b \rfloor$

$\oplus$ même complexité $O(M(n) \log n)$ pour la version « diviser pour régner » que pour le pgcd classique

$\ominus$ croissance des poids forts (environ 2.5% en moyenne). analysée précisément par Brigitte Vallée via *analyse dynamique*

Division récursive

Décrite dans le cadre de la multiplication de Karatsuba par Burnikel and Ziegler (1998), évoquée auparavant par Moenck et Borodin (1972) et Jebelean (1997).

Input: $A = \sum_0^{n+m-1} a_i\beta^i$, $B = \sum_0^{n-1} b_j\beta^j$, B normalisé, $n \geq m$
Output: quotient Q et reste R de A divisé par B.

```
if m < 2 then return BasecaseDivRem(A, B)
k ← ⌊m/2⌋, B_1 ← B div β^k, B_0 ← B mod β^k
(Q_1, R_1) ← RecursiveDivRem(A div β^{2k}, B_1)
A' ← R_1 β^{2k} + (A mod β^{2k}) − Q_1 B_0 β^k
while A' < 0 do Q_1 ← Q_1 − 1, A' ← A' + β^k B
(Q_0, R_0) ← RecursiveDivRem(A' div β^k, B_1)
A'' ← R_0 β^k + (A' mod β^k) − Q_0 B_0
while A'' < 0 do Q_0 ← Q_0 − 1, A'' ← A'' + B
return Q := Q_1 β^k + Q_0, R := A''.
```

Prêt à implanter, avec retenues

Division récursive : vue graphique

$$\boxed{\quad A_h \quad}\boxed{\quad A_\ell \quad} \ \text{div} \ \boxed{B_h}\boxed{B_\ell}$$

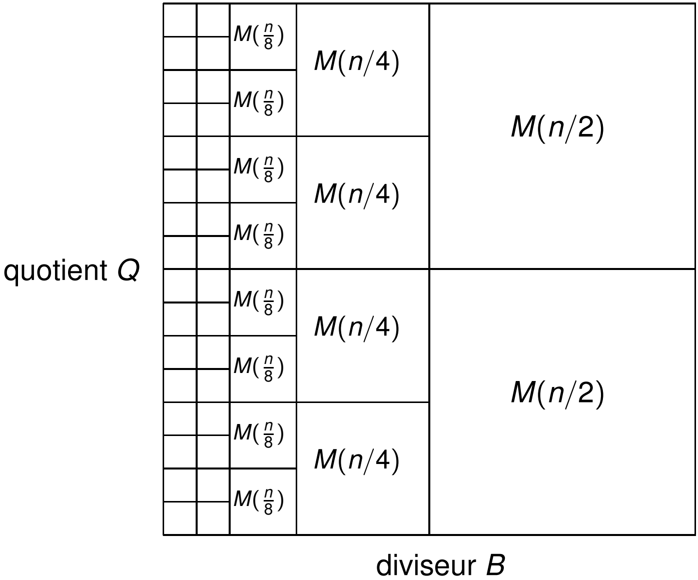
$$\boxed{\quad A_h \quad} = \boxed{Q_h}\boxed{B_h} + \boxed{R_h}$$

$$\boxed{R_h}\boxed{\quad A_\ell \quad} - \boxed{Q_h} \times \boxed{B_\ell}\boxed{0} = \boxed{\quad A'_h \quad}\boxed{A'_\ell}$$

$$\boxed{\quad A'_h \quad} = \boxed{Q_\ell}\boxed{B_h} + \boxed{R_\ell}$$

$$\boxed{R_\ell}\boxed{A'_\ell} - \boxed{Q_\ell} \times \boxed{B_\ell} = \boxed{\quad A''_\ell \quad}$$

Division récursive : autre vue graphique



Division récursive : complexité

$$D(n) = 2D(n/2) + 2M(n/2)$$

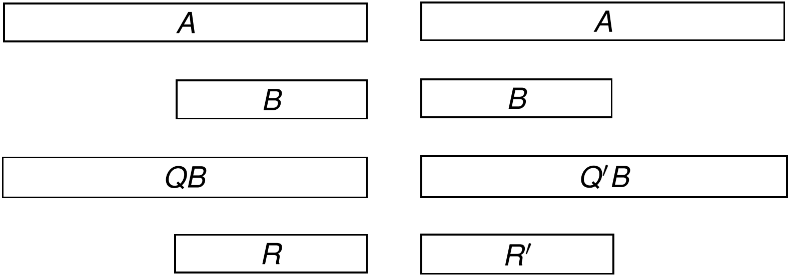
Domaine de Karatsuba : $D(n) = 2M(n)$ (on peut avoir $D(n) = M(n)$ avec un algorithme de van der Hoeven)

Domaine de Toom-Cook : $M(n) \approx n^{1.47}$: $D(n) \approx 2.63M(n)$

Domaine FFT : $D(n) = \Theta(M(n) \log n)$

C'est la division sous-quadratique implantée en GMP 4.3 (donc $M(n) \log n$) ! (La frontière avec la division quadratique est 27 mots sur Pentium M.)

Division classique et division de Hensel



division classique
(poids forts à gauche)

division de Hensel
(poids faibles à droite)

$$A = QB + R$$

$$A = Q'B + R'2^n$$

Division de Hensel vs multiplication de Montgomery

Division de Hensel vs multiplication de Montgomery

Division de Hensel :

$$A = QB + R2^n$$

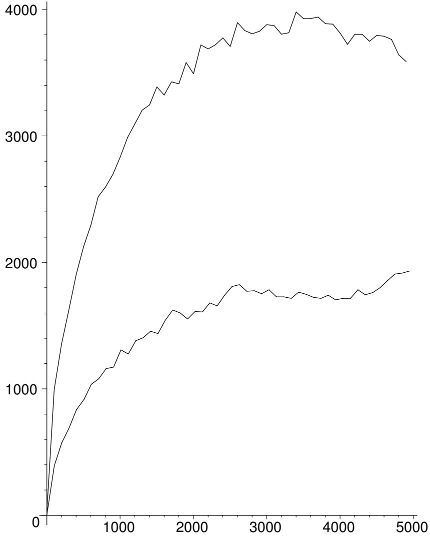
Le quotient est le quotient 2-adique :

$$Q = A/B \bmod 2^n$$

Le reste est le résultat de la multiplication REDC de Montgomery :

$$R = A/2^n \bmod B$$

Multiplication déséquilibrée (avec Hanrot)



Temps de multiplication $i \times (n - i)$ mots (en bas), et de division $n \div i$ mots (en haut) sur Pentium M, avec GMP 4.3.0.

Schéma de Karatsuba classique.

$$A = a_{2n-1}\beta^{2n-1} + \cdots + a_1\beta + a_0$$

Écrire $A = A_h\beta^n + A_\ell$, $B = B_h\beta^n + B_\ell$
Évaluer $C_h = A_hB_h$, $C_\ell = A_\ell B_\ell$, $C_m = (A_h + A_\ell)(B_h + B_\ell)$.
Interpoler :

$$A \cdot B = C_h\beta^{2n} + (C_m - C_h - C_\ell)\beta^n + C_\ell$$

Schéma de Karatsuba pair-impair.
Écrire $A = A_{\mathrm{odd}}(\beta^2)\beta + A_{\mathrm{even}}(\beta^2)$, $B = B_{\mathrm{odd}}(\beta^2)\beta + B_{\mathrm{even}}(\beta^2)$
Évaluer $C_{\mathrm{odd}} = A_{\mathrm{odd}}B_{\mathrm{odd}}$, $C_{\mathrm{even}} = A_{\mathrm{even}}B_{\mathrm{even}}$,
$C_m = (A_{\mathrm{odd}} + A_{\mathrm{even}})(B_{\mathrm{odd}} + B_{\mathrm{even}})$.
Interpoler :

$$A \cdot B = C_{\mathrm{odd}}(\beta^2)\cdot\beta^2 + (C_m - C_{\mathrm{odd}} - C_{\mathrm{even}})(\beta^2)\cdot\beta + C_{\mathrm{even}}(\beta^2)$$

Algorithme de Karatsuba déséquilibré

$$\underbrace{\boxed{\quad A_h \quad}\boxed{\quad A_\ell \quad}}_{m}$$

$$\underbrace{\boxed{\ B_h \ }\boxed{\quad B_\ell \quad}}_{n}$$

$$K(m, n) = K(m/2, n - m/2) + 2K(m/2)$$

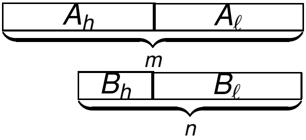
Mieux de « centrer » B ?

$$\underbrace{\boxed{\quad A_h \quad}\boxed{\quad A_\ell \quad}}_{m}$$

$$\underbrace{\boxed{\ B_h \ }\boxed{\ B_\ell \ }}_{n}$$

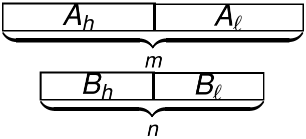
$$K(m, n) = 2K(m/2, n/2) + K(m/2)$$

Aligné aux poids faibles ou centré ?



$$K(5,3) = K(2,0) + K(3,3) + K(3,3) = 2 \cdot 7 = 14$$

$$K(3,3) = 2K(2,2) + K(1,1) = 7$$



$$K(5,3) = K(2,2) + K(3,1) + K(3,3) = 3 + 3 + 7 = 13$$

Pas toujours mieux : aligné pds faibles $K(6,4) = 17$, centré 19

Opérandes déséquilibrés avec pair-impair

$\boxed{a_4}\boxed{a_3}\boxed{a_2}\boxed{a_1}\boxed{a_0} \times \boxed{b_2}\boxed{b_1}\boxed{b_0}$

$\boxed{a_4}\boxed{a_2}\boxed{a_0} \times \boxed{b_2}\boxed{b_0}$

$\boxed{a_3}\boxed{a_1} \times \boxed{b_1}$

$\boxed{a_4}\boxed{a_3 + a_2}\boxed{a_1 + a_0} \times \boxed{b_2}\boxed{b_1 + b_0}$

$$K(m,n) = 2K(\lceil m/2 \rceil, \lceil n/2 \rceil) + K(\lfloor m/2 \rfloor, \lfloor n/2 \rfloor)$$

$$K(3,2) = 2K(2,1) + K(1,1) = 5$$

$$K(5,3) = 2K(3,2) + K(2,1) = 2 \times 5 + 2 = 12$$

On peut faire encore mieux !

Quand m et n sont impairs, ajouter 0 aux poids faibles de b :

$\boxed{a_4}\boxed{a_3}\boxed{a_2}\boxed{a_1}\boxed{a_0} \times \boxed{b_2}\boxed{b_1}\boxed{b_0}\boxed{0}$

$\boxed{a_4}\boxed{a_2}\boxed{a_0} \times \boxed{b_1}\boxed{0}$

$\boxed{a_3}\boxed{a_1} \times \boxed{b_2}\boxed{b_0}$

$\boxed{a_4}\boxed{a_3 + a_2}\boxed{a_1 + a_0} \times \boxed{b_2 + b_1}\boxed{b_0}$

$$K(m,n) = K(\lceil m/2 \rceil, \lfloor n/2 \rfloor) + K(\lfloor m/2 \rfloor, \lceil n/2 \rceil) + K(\lceil m/2 \rceil, \lceil n/2 \rceil)$$

$$K(3,2) = K(2,1) + K(1,1) + K(2,1) = 2 + 1 + 2 = 5$$

$$K(5,3) = K(3,1) + K(2,2) + K(3,2) = 3 + 3 + 5 = 11$$

Multiplication déséquilibrée

Deux stratégies :

- couper les opérandes en un même nombre de morceaux de tailles différentes (Karatsuba, Toom-Cook 3)
- couper les opérandes en des nombres différents de morceaux (Toom-Cook $(3, 2)$, Toom-Cook $(4, 3)$, $\ldots$)

Toom-Cook $(3,2)$ ou Toom-Cook 2.5

Introduit par Bodrato et Zanoni (ISSAC'07).

Multiplie $A = a_2x^2 + a_1x + a_0$ par $B = b_1x + b_0$

$A \cdot B = c_3x^3 + c_2x^2 + c_1x + c_0$

Nécessite 4 points d'évaluation, par exemple $0, 1, -1, \infty$

Exemple :

$$300 \times 200 \Longrightarrow 4 \text{ multiplications } 100 \times 100$$

Autre exemple : Toom-Cook $(5,3)$ vs Toom-Cook 4.

Multiplication de Montgomery

$$\text{Idée : } AB \bmod D \quad \Longrightarrow \quad \mathbf{REDC}(A, B) := AB\beta^{-n} \bmod D$$

$$A \quad \Longrightarrow \quad \widetilde{A} := A\beta^{n}$$

Multiplication de Montgomery

Idée : $AB \bmod D \quad \Longrightarrow \quad \mathbf{REDC}(A, B) := AB\beta^{-n} \bmod D$

$$A \quad \Longrightarrow \quad \widetilde{A} := A\beta^n$$

$$\boxed{\widetilde{A} = A\beta^n} \quad \boxed{\widetilde{B} = B\beta^n}$$

Multiplication de Montgomery

Idée : $AB \bmod D \quad \Longrightarrow \quad \mathbf{REDC}(A, B) := AB\beta^{-n} \bmod D$

$$A \quad \Longrightarrow \quad \widetilde{A} := A\beta^n$$

$$\boxed{\widetilde{A} = A\beta^n} \qquad \boxed{\widetilde{B} = B\beta^n}$$

$$\Downarrow \qquad M(n)$$

$$\boxed{\widetilde{A} \times \widetilde{B} = AB\beta^{2n}}$$

Multiplication de Montgomery

Idée : $AB \bmod D \quad \Longrightarrow \quad \mathbf{REDC}(A, B) := AB\beta^{-n} \bmod D$

$$A \quad \Longrightarrow \quad \widetilde{A} := A\beta^n$$

$$\boxed{\widetilde{A} = A\beta^n} \qquad \boxed{\widetilde{B} = B\beta^n}$$

$$\Downarrow \qquad M(n)$$

$$\boxed{\widetilde{A} \times \widetilde{B} = AB\beta^{2n}}$$

$$\Downarrow \qquad \widetilde{D}(n)$$

$$\boxed{\widetilde{A}\widetilde{B}\beta^{-n} = AB\beta^n = \widetilde{AB} \bmod D}$$

Multiplication de Montgomery (domaine quadratique)

Input : $C < D^2$, $\mu = -D^{-1} \bmod \beta$ (précalculé)
Output : $R = C\beta^{-n} \bmod D$
for i from 0 to $n-1$ do
  $q_i \leftarrow \mu c_i \bmod \beta$ (sélection du quotient)
  $C \leftarrow C + q_i D \beta^i$
$R \leftarrow C\beta^{-n}$
if $R \geq \beta^n$ then return $R - D$ else return R (correction)

Multiplication de Montgomery : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$.

$$C = 766\,970\,544\,842\,443\,844 \quad \Big| \quad D = 862\,664\,913$$

Multiplication de Montgomery : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$.

$$\begin{array}{r|r} C = 766\,970\,544\,842\,443\,{\color{red}844} & D = 862\,664\,{\color{red}913} \\ \hline & 412 \end{array}$$

Multiplication de Montgomery : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$.

$$
\begin{array}{r|l}
C = 766\,970\,544\,842\,443\,{\color{red}844} & D = 862\,664\,{\color{red}913} \\ \cline{2-2}
 & \hfill 412 \\
+\,\underline{355\,417\,944\,156} &
\end{array}
$$

Multiplication de Montgomery : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$.

$$\begin{array}{r|l}
C = 766\,970\,544\,842\,443\,{\color{red}844} & D = 862\,664\,{\color{red}913} \\ \cline{2-2}
 & \hfill 412 \\
+\ \underline{355\,417\,944\,156} & \\
766\,970\,900\,260\,{\color{red}388} &
\end{array}$$

Multiplication de Montgomery : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$.

$$
\begin{array}{r|r}
C = 766\,970\,544\,842\,443\,844 & D = 862\,664\,913 \\ \hline
 & 412 \\
+\ \underline{355\,417\,944\,156} & \\
766\,970\,900\,260\,388 & 924
\end{array}
$$

Multiplication de Montgomery : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$.

$$
\begin{array}{r|l}
C = 766\,970\,544\,842\,443\,844 & D = 862\,664\,913 \\ \hline
 & \hfill 412 \\
+\ \underline{355\,417\,944\,156} & \\
766\,970\,900\,260\,388\hphantom{\,000} & \hfill 924\hphantom{\,000} \\
+\ \underline{797\,102\,379\,612}\hphantom{\,000} &
\end{array}
$$

Multiplication de Montgomery : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$.

$$
\begin{array}{r|r}
C = 766\,970\,544\,842\,443\,{\color{red}844} & D = 862\,664\,{\color{red}913} \\
\hline
 & 412 \\
+\underline{355\,417\,944\,156} & \\
766\,970\,900\,260\,{\color{red}388} & 924 \\
+\underline{797\,102\,379\,612} & \\
767\,768\,002\,{\color{red}640} &
\end{array}
$$

Multiplication de Montgomery : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$.

$$
\begin{array}{r|r}
C = 766\,970\,544\,842\,443\,844 & D = 862\,664\,913 \\
\hline
 & 412 \\
+\underline{355\,417\,944\,156} & \\
766\,970\,900\,260\,388 & 924 \\
+\underline{797\,102\,379\,612} & \\
767\,768\,002\,640 & 720
\end{array}
$$

Multiplication de Montgomery : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$.

$$
\begin{array}{r|r}
C = 766\,970\,544\,842\,443\,\color{red}{844} & D = 862\,664\,\color{red}{913} \\
\hline
 & 412 \\
+\ \underline{355\,417\,944\,156} & \\
766\,970\,900\,260\,\color{red}{388} & 924 \\
+\ \underline{797\,102\,379\,612} & \\
767\,768\,002\,\color{red}{640} & 720 \\
+\ \underline{621\,118\,737\,360} &
\end{array}
$$

Multiplication de Montgomery : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$.

$$\begin{array}{r|r}
C = 766\,970\,544\,842\,443\,844 & D = 862\,664\,913 \\ \hline
 & 412 \\
+\ \underline{355\,417\,944\,156} & \\
766\,970\,900\,260\,388 & 924 \\
+\ \underline{797\,102\,379\,612} & \\
767\,768\,002\,640 & 720 \\
+\ \underline{621\,118\,737\,360} & \\
1\,388\,886\,740 &
\end{array}$$

Multiplication de Montgomery : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$.

$$
\begin{array}{r|l}
C = 766\,970\,544\,842\,443\,{\color{red}844} & D = 862\,664\,{\color{red}913} \\
\hline
 & \hphantom{D = 862\,664\,}412 \\
+\ \underline{355\,417\,944\,156} & \\
766\,970\,900\,260\,{\color{red}388}\hphantom{000\,} & \hphantom{D = 862\,}924 \\
+\ \underline{797\,102\,379\,612}\hphantom{000\,} & \\
767\,768\,002\,{\color{red}640}\hphantom{000\,000\,} & \hphantom{D = }720 \\
+\ \underline{621\,118\,737\,360}\hphantom{000\,000\,} & \\
1\,388\,886\,740\hphantom{000\,000\,000\,} & \\
-\ {\color{blue}\underline{862\,664\,913}}\hphantom{000\,000\,000\,} & {\color{blue}-1}
\end{array}
$$

Multiplication de Montgomery : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$.

$$
\begin{array}{r|r}
C = 766\,970\,544\,842\,443\,\color{red}{844} & D = 862\,664\,\color{red}{913} \\
\hline
 & 412 \\
+\underline{355\,417\,944\,156} & \\
766\,970\,900\,260\,\color{red}{388} & 924 \\
+\underline{797\,102\,379\,612} & \\
767\,768\,002\,\color{red}{640} & 720 \\
+\underline{621\,118\,737\,360} & \\
1\,388\,886\,740 & \\
-\color{blue}{\underline{862\,664\,913}} & \color{blue}{-1} \\
526\,221\,827 &
\end{array}
$$

Multiplication de Montgomery : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$.

$$
\begin{array}{r|l}
C = 766\,970\,544\,842\,443\,{\color{red}844} & D = 862\,664\,{\color{red}913} \\
\hline
 & 412 \\
+\,\underline{355\,417\,944\,156} & \\
766\,970\,900\,260\,{\color{red}388} & 924 \\
+\,\underline{797\,102\,379\,612} & \\
767\,768\,002\,{\color{red}640} & 720 \\
+\,\underline{621\,118\,737\,360} & \\
1\,388\,886\,740 & \\
{\color{blue}-\,\underline{862\,664\,913}} & {\color{blue}-1} \\
526\,221\,827 &
\end{array}
$$

$$C + 720924412 \times D = 10^9 \cdot 1388886740 = 10^9(D + 526221827)$$

Division classique vs Montgomery (domaine quadratique)

- la sélection du quotient est coûteuse (128 $\mathrm{bits} \div$ 64 bits)

  64 $\mathrm{bits} \times$ 64 bits mod 2^{64} : facile

Division classique vs Montgomery (domaine quadratique)

- la sélection du quotient est coûteuse (128 $\mathrm{bits} \div 64\ \mathrm{bits}$)

  64 $\mathrm{bits} \times 64\ \mathrm{bits}$ mod 2^{64} : facile

- jusqu'à $2n$ corrections par division

  au plus une correction finale

Division classique vs Montgomery (domaine quadratique)

- la sélection du quotient est coûteuse (128 bits $\div$ 64 bits)

  64 bits $\times$ 64 bits mod 2^{64} : facile

- jusqu'à $2n$ corrections par division

  au plus une correction finale

- prédiction de branche coûteuse

  pas de branche dans la boucle principale

Division classique vs Montgomery (domaine quadratique)

- la sélection du quotient est coûteuse (128 $\mathrm{bits} \div$ 64 bits)

  64 $\mathrm{bits} \times$ 64 bits mod 2^{64} : facile

- jusqu'à $2n$ corrections par division

  au plus une correction finale

- prédiction de branche coûteuse

  pas de branche dans la boucle principale

- dépendance entre correction et prochaine boucle : c_{n+j}, c_{n+j-1}

  même dépendance pour c_i

Division classique vs Montgomery (domaine quadratique)

- la sélection du quotient est coûteuse (128 $\mathrm{bits} \div$ 64 bits)

  64 $\mathrm{bits} \times$ 64 bits mod 2^{64} : facile

- jusqu'à $2n$ corrections par division

  au plus une correction finale

- prédiction de branche coûteuse

  pas de branche dans la boucle principale

- dépendance entre correction et prochaine boucle : c_{n+j}, c_{n+j-1}

  même dépendance pour c_i

- quadratique ...

  idem

Division de Svoboda

Avec $D = \overbrace{1,000}^{d_{n-1}}, \ldots$, la sélection du quotient est facile :

$$\lfloor \frac{c_{n+j}\beta + c_{n+j-1}}{d_{n-1}} \rfloor = c_{n+j}$$

Idée de Svoboda : imposer $d_{n-1} = \beta$!

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$766\,970\,544\,842\,443\,844 \;\Big|\; \underline{1000\,691\,299\,080}$$

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$\begin{array}{r|l} 766\,970\,544\,842\,443\,844 & 1000\,691\,299\,080 \\ \hline & 766 \end{array}$$

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$\begin{array}{rr|l} & 766\,970\,544\,842\,443\,844 & 1000\,691\,299\,080 \\ \cline{3-3} - & \underline{766\,529\,535\,095\,280} & 766 \end{array}$$

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$\begin{array}{rr|l} & 766\,970\,544\,842\,443\,844 & 1000\,691\,299\,080 \\ \cline{3-3} - & \underline{766\,529\,535\,095\,280} & 766 \\ & 441\,009\,747\,163\,844 & \end{array}$$

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$
\begin{array}{r|l}
766\,970\,544\,842\,443\,844 & 1000\,691\,299\,080 \\ \hline
-\ \underline{766\,529\,535\,095\,280} & 766 \\
441\,009\,747\,163\,844 & 441
\end{array}
$$

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$\begin{array}{r|l}
766\,970\,544\,842\,443\,844 & 1000\,691\,299\,080 \\ \cline{2-2}
-\ \underline{766\,529\,535\,095\,280} & 766 \\
441\,009\,747\,163\,844 & 441 \\
-\ \underline{441\,304\,862\,894\,280} &
\end{array}$$

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$
\begin{array}{r|l}
766\,970\,544\,842\,443\,844 & 1000\,691\,299\,080 \\ \cline{2-2}
-\ \underline{766\,529\,535\,095\,280} & 766 \\
441\,009\,747\,163\,844 & 441 \\
-\ \underline{441\,304\,862\,894\,280} & \\
-\ 295\,115\,730\,436 &
\end{array}
$$

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$
\begin{array}{rr|l}
 & 766\,970\,544\,842\,443\,844 & 1000\,691\,299\,080 \\ \cline{3-3}
- & \underline{766\,529\,535\,095\,280} & 766 \\
 & 441\,009\,747\,163\,844 & \,441 \\
- & \underline{441\,304\,862\,894\,280} & \\
 & -\,295\,115\,730\,436 & \\
+ & \underline{1000\,691\,299\,080} & \,-1 \\ \hline
\end{array}
$$

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$
\begin{array}{r|l}
766\,970\,544\,842\,443\,844 & 1000\,691\,299\,080 \\
\hline
-\,\underline{766\,529\,535\,095\,280} & 766 \\
441\,009\,747\,163\,844 & 441 \\
-\,\underline{441\,304\,862\,894\,280} & \\
-\,295\,115\,730\,436 & \\
+\,\underline{1000\,691\,299\,080} & -1 \\
\hline
705\,575\,568\,644 &
\end{array}
$$

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$\begin{array}{r|l}
766\,970\,544\,842\,443\,844 & 1000\,691\,299\,080 \\ \cline{2-2}
-\ \underline{766\,529\,535\,095\,280} & 766 \\
441\,009\,747\,163\,844 & 441 \\
-\ \underline{441\,304\,862\,894\,280} & \\
-\ 295\,115\,730\,436 & \\
+\ \underline{1000\,691\,299\,080} & {-1} \\ \hline
705\,575\,568\,644 & 818
\end{array}$$

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$
\begin{array}{r|l}
766\,970\,544\,842\,443\,844 & 1000\,691\,299\,080 \\ \cline{2-2}
-\ \underline{766\,529\,535\,095\,280} & 766 \\
441\,009\,747\,163\,844 & \quad 441 \\
-\ \underline{441\,304\,862\,894\,280} & \\
-\ 295\,115\,730\,436 & \\
+\ \underline{1000\,691\,299\,080} & \quad -1 \\ \hline
705\,575\,568\,644 & \qquad 818 \\
-\ \underline{705\,659\,898\,834} &
\end{array}
$$

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$\begin{array}{r|l}
766\,970\,544\,842\,443\,844 & 1000\,691\,299\,080 \\ \cline{2-2}
-\ \underline{766\,529\,535\,095\,280} & 766 \\
441\,009\,747\,163\,844 & 441 \\
-\ \underline{441\,304\,862\,894\,280} & \\
-\ 295\,115\,730\,436 & \\
+\ \underline{1000\,691\,299\,080} & -1 \\ \hline
705\,575\,568\,644 & 818 \\
-\ \underline{705\,659\,898\,834} & \\
-\ 084\,330\,190 &
\end{array}$$

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$
\begin{array}{r|l}
766\,970\,544\,842\,443\,844 & 1000\,691\,299\,080 \\
\cline{2-2}
-\underline{766\,529\,535\,095\,280} & 766 \\
441\,009\,747\,163\,844 & 441 \\
-\underline{441\,304\,862\,894\,280} & \\
-295\,115\,730\,436 & \\
+\underline{1000\,691\,299\,080} & {-1} \\
\hline
705\,575\,568\,644 & 818 \\
-\underline{705\,659\,898\,834} & \\
-084\,330\,190 & \\
+\underline{862\,664\,913} & {-1}
\end{array}
$$

Division de Svoboda : un exemple

Précalculer $D' = 1160 \cdot D = 1000\,691\,299\,080$

$$
\begin{array}{r|l}
766\,970\,544\,842\,443\,844 & 1000\,691\,299\,080 \\ \cline{2-2}
-\,\underline{766\,529\,535\,095\,280} & 766 \\
441\,009\,747\,163\,844 & \quad 441 \\
-\,\underline{441\,304\,862\,894\,280} & \\
-\,295\,115\,730\,436 & \\
+\,\underline{1000\,691\,299\,080} & \quad -1 \\ \hline
705\,575\,568\,644 & \qquad 818 \\
-\,\underline{705\,659\,898\,834} & \\
-\,084\,330\,190 & \\
+\,\underline{862\,664\,913} & \qquad -1 \\
778\,334\,723 &
\end{array}
$$

$$C = (766440 \times 1160 + 817)D + 778334723$$

Division de Svoboda :

$$C = Q(kD) + qD + R$$

- la sélection du quotient devient triviale (sauf dernière étape)
- la probabilité de correction diminue, car d_{n-1} augmente
- intéressante surtout quand seul le reste est calculé

Comment utiliser la division de Svoboda ?

- si possible, choisir D tel que $d_{n-1} = \beta$
- ou travailler modulo kD, avec $n + 1$ mots
- ou faire une dernière étape de division classique

Division Montgomery-Svoboda

Réduction de Montgomery :
Input : $C < D^2$, $\mu = -D^{-1} \bmod \beta$ (précalculé)
Output : $R = C\beta^{-n} \bmod D$
for i from 0 to $n - 1$ do
  $q_i \leftarrow \mu c_i \bmod \beta$ (sélection du quotient)
  $C \leftarrow C + q_i D \beta^i$
$R \leftarrow C\beta^{-n}$
if $R \geq \beta^n$ then return $R - D$ else return R

Division Montgomery-Svoboda

Réduction de Montgomery :
Input : $C < D^2$, $\mu = -D^{-1} \bmod \beta$ (précalculé)
Output : $R = C\beta^{-n} \bmod D$
for i from 0 to $n-1$ do
  $q_i \leftarrow \mu c_i \bmod \beta$ (sélection du quotient)
  $C \leftarrow C + q_i D \beta^i$
$R \leftarrow C\beta^{-n}$
if $R \geq \beta^n$ then return $R - D$ else return R

Réduction Montgomery-Svoboda :
Input : $C < D^2$, $\mu = -D^{-1} \bmod \beta$ (précalculé), μD
Output : $R = C\beta^{-n} \bmod D$
for i from 0 to $n-2$ do
  $q_i \leftarrow c_i \bmod \beta$ (sélection du quotient triviale)
  $C \leftarrow C + q_i(\mu D)\beta^i$
$q_{n-1} \leftarrow \mu c_{n-1} \bmod \beta$
$C \leftarrow C + q_{n-1} D \beta^{n-1}$
$R \leftarrow C\beta^{-n}$
if $R \geq \beta^n$ then return $R - D$ else return R

Montgomery-Svoboda : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$ et $D' = \mu D$.

$$C = 766\,970\,544\,842\,443\,844 \;\Big|\; D' = 19\,841\,292\,999$$

Montgomery-Svoboda : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$ et $D' = \mu D$.

$$\begin{array}{r|r} C = 766\,970\,544\,842\,443\,{\color{purple}844} & D' = 19\,841\,292\,{\color{purple}999} \\ \hline & 844 \end{array}$$

Montgomery-Svoboda : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$ et $D' = \mu D$.

$$
\begin{array}{r|r}
C = 766\,970\,544\,842\,443\,{\color{purple}844} & D' = 19\,841\,292\,{\color{purple}999} \\
\hline
+\ \underline{16\,746\,051\,291\,156} & 844
\end{array}
$$

Montgomery-Svoboda : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$ et $D' = \mu D$.

$$
\begin{array}{rr|l}
C = & 766\,970\,544\,842\,443\,844 & D' = 19\,841\,292\,999 \\
\cline{3-3}
+ & \underline{16\,746\,051\,291\,156} & \hfill 844 \\
 & 766\,987\,290\,893\,735 &
\end{array}
$$

Montgomery-Svoboda : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$ et $D' = \mu D$.

$$
\begin{array}{rr|r}
C = & 766\,970\,544\,842\,443\,844 & D' = 19\,841\,292\,999 \\
\cline{3-3}
+ & \underline{16\,746\,051\,291\,156} & 844 \\
 & 766\,987\,290\,893\,735 & 735
\end{array}
$$

Montgomery-Svoboda : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$ et $D' = \mu D$.

$$
\begin{array}{r|r}
C = 766\,970\,544\,842\,443\,844 & D' = 19\,841\,292\,999 \\
\hline
+\ \underline{16\,746\,051\,291\,156} & 844 \\
766\,987\,290\,893\,735 & 735 \\
+\ \underline{14\,583\,350\,354\,265} & \\
\hline
\end{array}
$$

Montgomery-Svoboda : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$ et $D' = \mu D$.

$$
\begin{array}{r|l}
C = 766\,970\,544\,842\,443\,844 & D' = 19\,841\,292\,999 \\ \cline{2-2}
+\underline{16\,746\,051\,291\,156} & \hphantom{D' = 19\,841\,292\,}844 \\
766\,987\,290\,893\,735\hphantom{\,000} & \hphantom{D' = 19\,841\,}735 \\
+\underline{14\,583\,350\,354\,265}\hphantom{\,000} & \\ \hline
781\,570\,641\,248\hphantom{\,000\,000} &
\end{array}
$$

Montgomery-Svoboda : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$ et $D' = \mu D$.

$$
\begin{array}{r|r}
C = 766\,970\,544\,842\,443\,\textcolor{purple}{844} & D' = 19\,841\,292\,\textcolor{purple}{999} \\
\cline{2-2}
+\ \underline{16\,746\,051\,291\,156} & 844 \\
766\,987\,290\,893\,\textcolor{purple}{735} & 735 \\
+\ \underline{14\,583\,350\,354\,265} & \\
\hline
781\,570\,641\,\textcolor{red}{248} & 704
\end{array}
$$

Montgomery-Svoboda : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$ et $D' = \mu D$.

$$\begin{array}{r|r}
C = 766\,970\,544\,842\,443\,844 & D' = 19\,841\,292\,999 \\ \cline{2-2}
+\ \underline{16\,746\,051\,291\,156} & 844 \\
766\,987\,290\,893\,735 & 735 \\
+\ \underline{14\,583\,350\,354\,265} & \\ \hline
781\,570\,641\,248 & 704 \\
+\ \underline{607\,316\,098\,752} &
\end{array}$$

Montgomery-Svoboda : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$ et $D' = \mu D$.

$$\begin{array}{r|r}
C = 766\,970\,544\,842\,443\,844 & D' = 19\,841\,292\,999 \\ \cline{2-2}
+\ \underline{16\,746\,051\,291\,156} & 844 \\
766\,987\,290\,893\,735 & 735 \\
+\ \underline{14\,583\,350\,354\,265} & \\ \hline
781\,570\,641\,248 & 704 \\
+\ \underline{607\,316\,098\,752} & \\
1\,388\,886\,740 &
\end{array}$$

Montgomery-Svoboda : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$ et $D' = \mu D$.

$$
\begin{array}{r|r}
C = 766\,970\,544\,842\,443\,844 & D' = 19\,841\,292\,999 \\
\hline
+\underline{16\,746\,051\,291\,156} & 844 \\
766\,987\,290\,893\,735 & 735 \\
+\underline{14\,583\,350\,354\,265} & \\
\hline
781\,570\,641\,248 & 704 \\
+\underline{607\,316\,098\,752} & \\
1\,388\,886\,740 & \\
-\underline{862\,664\,913} & -1
\end{array}
$$

Montgomery-Svoboda : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$ et $D' = \mu D$.

$C = 766\,970\,544\,842\,443\,844$	$D' = 19\,841\,292\,999$
$+\,\underline{16\,746\,051\,291\,156}$	844
$766\,987\,290\,893\,735$	735
$+\,\underline{14\,583\,350\,354\,265}$	
$781\,570\,641\,248$	704
$+\,\underline{607\,316\,098\,752}$	
$1\,388\,886\,740$	
$-\,\underline{862\,664\,913}$	-1
$526\,221\,827$	

Montgomery-Svoboda : un exemple

Précalculer $\mu = -1/913 \bmod 1000 = 23$ et $D' = \mu D$.

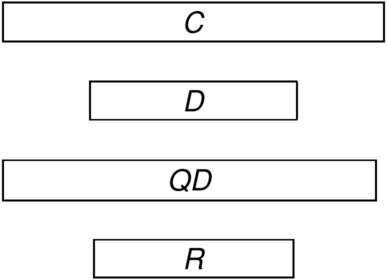
$$
\begin{array}{rr|r}
C = & 766\,970\,544\,842\,443\,\color{purple}{844} & D' = 19\,841\,292\,\color{purple}{999} \\ \cline{3-3}
 & + \underline{16\,746\,051\,291\,156} & 844 \\
 & 766\,987\,290\,893\,\color{purple}{735} & 735 \\
 & + \underline{14\,583\,350\,354\,265} & \\ \hline
 & 781\,570\,641\,\color{red}{248} & 704 \\
 & + \underline{607\,316\,098\,752} & \\
 & 1\,388\,886\,740 & \\
 & - \underline{\color{blue}{862\,664\,913}} & \color{blue}{-1} \\
 & 526\,221\,827 &
\end{array}
$$

$$C + (23 \times 735844 + 704000000)D = 10^9(D + 526221827)$$

Division bidirectionnelle

Bipartite Modular Multiplication Method, Kaihara and Takagi, IEEE TC, 2008.

Idée : réduire de $n/2$ par les poids forts (division classique), de $n/2$ par les poids faibles (réduction de Montgomery).



$$C = QD + R\beta^{n/2}$$

Division bidirectionnelle : un exemple

Diviser $868, 323, 539, 104, 235, 651, 444, 705$ par $D = 996, 417, 214, 181$

$\boxed{868, 323, 539, 104, 235, 651, 444, 705}$

Division bidirectionnelle : un exemple

Diviser $868, 323, 539, 104, 235, 651, 444, 705$ par
$D = 996, 417, 214, 181$

$$\boxed{868, 323, 539, 104, 235, 651, 444, 705} - (871 \cdot 10^9) \cdot D$$

Division bidirectionnelle : un exemple

Diviser $868, 323, 539, 104, 235, 651, 444, 705$ par
$D = 996, 417, 214, 181$

$\boxed{868, 323, 539, 104, 235, 651, 444, 705} - (871 \cdot 10^9) \cdot D$

$\boxed{\color{red}{000}, 444, 145, 552, 584, 651, 444, 705}$

Division bidirectionnelle : un exemple

Diviser $868,323,539,104,235,651,444,705$ par
$D = 996,417,214,181$

$\boxed{868,323,539,104,235,651,444,705}$ $-(871 \cdot 10^9) \cdot D$

$\boxed{000,444,145,552,584,651,444,705}$ $+195 \cdot D$

Division bidirectionnelle : un exemple

Diviser $868, 323, 539, 104, 235, 651, 444, 705$ par
$D = 996, 417, 214, 181$

$\boxed{868, 323, 539, 104, 235, 651, 444, 705}$ $-(871 \cdot 10^9) \cdot D$

$\boxed{{\color{red}000}, 444, 145, 552, 584, 651, 444, 705}$ $+195 \cdot D$

$\boxed{{\color{red}000}, 444, 145, 746, 886, 008, 210, {\color{red}000}}$

Division bidirectionnelle : un exemple

Diviser $868,323,539,104,235,651,444,705$ par $D = 996,417,214,181$

$\boxed{868,323,539,104,235,651,444,705}$ $-(871 \cdot 10^9) \cdot D$

$\boxed{000,444,145,552,584,651,444,705}$ $+195 \cdot D$

$\boxed{000,444,145,746,886,008,210,000}$ $-(445 \cdot 10^6) \cdot D$

Division bidirectionnelle : un exemple

Diviser $868, 323, 539, 104, 235, 651, 444, 705$ par $D = 996, 417, 214, 181$

$$\boxed{868, 323, 539, 104, 235, 651, 444, 705} \; -(871 \cdot 10^9) \cdot D$$

$$\boxed{{\color{red}000}, 444, 145, 552, 584, 651, 444, 705} \; +195 \cdot D$$

$$\boxed{{\color{red}000}, 444, 145, 746, 886, 008, 210, {\color{red}000}} \; -(445 \cdot 10^6) \cdot D$$

$$\boxed{{\color{red}000, 000}, 740, 086, 575, 463, 210, {\color{red}000}}$$

Division bidirectionnelle : un exemple

Diviser $868,323,539,104,235,651,444,705$ par $D = 996,417,214,181$

$\boxed{868,323,539,104,235,651,444,705} - (871 \cdot 10^9) \cdot D$

$\boxed{{\color{red}000},444,145,552,584,651,444,705} + 195 \cdot D$

$\boxed{{\color{red}000},444,145,746,886,008,210,{\color{red}000}} - (445 \cdot 10^6) \cdot D$

$\boxed{{\color{red}000,000},740,086,575,463,210,{\color{red}000}} + (590 \cdot 10^3) \cdot D$

Division bidirectionnelle : un exemple

Diviser $868, 323, 539, 104, 235, 651, 444, 705$ par $D = 996, 417, 214, 181$

$\boxed{868, 323, 539, 104, 235, 651, 444, 705}$ $-(871 \cdot 10^9) \cdot D$

$\boxed{000, 444, 145, 552, 584, 651, 444, 705}$ $+195 \cdot D$

$\boxed{000, 444, 145, 746, 886, 008, 210, 000}$ $-(445 \cdot 10^6) \cdot D$

$\boxed{000, 000, 740, 086, 575, 463, 210, 000}$ $+(590 \cdot 10^3) \cdot D$

$\boxed{000, 001, 327, 972, 731, 830, 000, 000}$

Division bidirectionnelle : un exemple

Diviser $868, 323, 539, 104, 235, 651, 444, 705$ par $D = 996, 417, 214, 181$

$\boxed{868, 323, 539, 104, 235, 651, 444, 705}$ $-(871 \cdot 10^9) \cdot D$

$\boxed{000, 444, 145, 552, 584, 651, 444, 705}$ $+195 \cdot D$

$\boxed{000, 444, 145, 746, 886, 008, 210, 000}$ $-(445 \cdot 10^6) \cdot D$

$\boxed{000, 000, 740, 086, 575, 463, 210, 000}$ $+(590 \cdot 10^3) \cdot D$

$\boxed{000, 001, 327, 972, 731, 830, 000, 000}$ $-D \cdot 10^6$

Division bidirectionnelle : un exemple

Diviser $868, 323, 539, 104, 235, 651, 444, 705$ par
$D = 996, 417, 214, 181$

$\boxed{868, 323, 539, 104, 235, 651, 444, 705}$ $-(871 \cdot 10^9) \cdot D$

$\boxed{000, 444, 145, 552, 584, 651, 444, 705}$ $+195 \cdot D$

$\boxed{000, 444, 145, 746, 886, 008, 210, 000}$ $-(445 \cdot 10^6) \cdot D$

$\boxed{000, 000, 740, 086, 575, 463, 210, 000}$ $+(590 \cdot 10^3) \cdot D$

$\boxed{000, 001, 327, 972, 731, 830, 000, 000}$ $-D \cdot 10^6$

$\boxed{000, 000, 331, 555, 517, 649, 000, 000}$

Division bidirectionnelle : un exemple

Diviser $868,323,539,104,235,651,444,705$ par $D = 996,417,214,181$

$$\boxed{868,323,539,104,235,651,444,705} \; -(871 \cdot 10^9) \cdot D$$

$$\boxed{000,444,145,552,584,651,444,705} \; +195 \cdot D$$

$$\boxed{000,444,145,746,886,008,210,000} \; -(445 \cdot 10^6) \cdot D$$

$$\boxed{000,000,740,086,575,463,210,000} \; +(590 \cdot 10^3) \cdot D$$

$$\boxed{000,001,327,972,731,830,000,000} \; -D \cdot 10^6$$

$$\boxed{000,000,331,555,517,649,000,000}$$

$$\frac{868323539104235651444705}{10^6} \equiv 331,555,517,649 \bmod D$$

Les deux réductions peuvent être faites indépendamment !

Les deux réductions peuvent être faites indépendamment !

Étape 1a : calculer le quotient classique à partir des n mots de poids fort

$868, 323, 539, 104, 235, 651, 444, 705 \div (10^6 D) = 871, 445$

Les deux réductions peuvent être faites indépendamment !

Étape 1a : calculer le quotient classique à partir des n mots de poids fort
$868, 323, 539, 104, 235, 651, 444, 705 \div (10^6 D) = 871, 445$

Étape 1b : calculer le quotient de Hensel à partir des $n/2$ mots de poids faible
$868, 323, 539, 104, 235, 651, 444, 705 \cdot \mu \equiv 590, 195 \bmod 10^6$
$(\mu = -1/D \bmod 10^6)$

Les deux réductions peuvent être faites indépendamment !

Étape 1a : calculer le quotient classique à partir des n mots de poids fort
$868, 323, 539, 104, 235, 651, 444, 705 \div (10^6 D) = 871, 445$

Étape 1b : calculer le quotient de Hensel à partir des $n/2$ mots de poids faible
$868, 323, 539, 104, 235, 651, 444, 705 \cdot \mu \equiv 590, 195 \bmod 10^6$
$(\mu = -1/D \bmod 10^6)$

Étape 2 : appliquer le quotient classique
$868, 323, 539, 104, 235, 651, 444, 705 - (871, 445 \cdot 10^6)D =$
$739, 892, 274, 106, 444, 705$

Les deux réductions peuvent être faites indépendamment !

Étape 1a : calculer le quotient classique à partir des n mots de poids fort
$868, 323, 539, 104, 235, 651, 444, 705 \div (10^6 D) = 871, 445$

Étape 1b : calculer le quotient de Hensel à partir des $n/2$ mots de poids faible
$868, 323, 539, 104, 235, 651, 444, 705 \cdot \mu \equiv 590, 195 \bmod 10^6$
$(\mu = -1/D \bmod 10^6)$

Étape 2 : appliquer le quotient classique
$868, 323, 539, 104, 235, 651, 444, 705 - (871, 445 \cdot 10^6)D =$
$739, 892, 274, 106, 444, 705$

Étape 3 : appliquer le quotient de Hensel
$739, 892, 274, 106, 444, 705 + 590, 195 \cdot D =$
$1, 327, 972, 731, 830, 000, 000$

Étape 4 : correction si nécessaire.

Remarque : les étapes 1a et 2 peuvent être fusionnées

Symbole de Jacobi

Soit $a \in \mathbb{Z}$, $n \in \mathbb{N}$ impair :
Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}$$

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a = 0 \bmod p \\ 1 & \text{si } a \neq 0 \bmod p \text{ et } a = x^2 \bmod p \\ -1 & \text{sinon} \end{cases}$$

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right) \text{ si } a = b \bmod n$$

$$\left(\frac{a}{n}\right) = 0 \text{ si } \gcd(a, n) \neq 1, \text{ -1 ou 1 sinon}$$

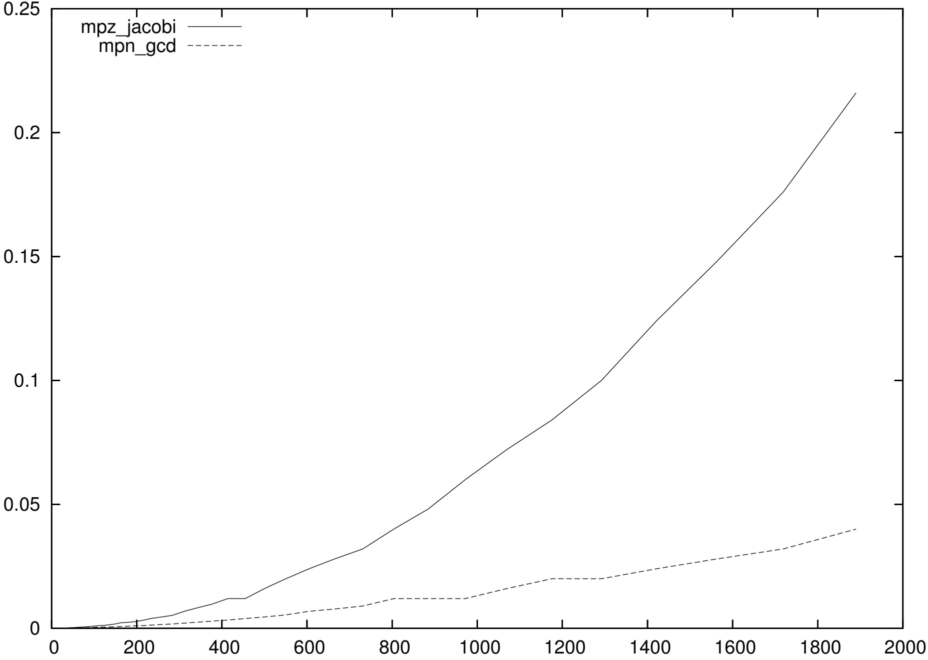
$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}, \left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$$

Symbole de Jacobi

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

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

Steven Galbraith : peut-on calculer le symbole de Jacobi de deux entiers de n bits en $O(M(n) \log n)$ comme pour le pgcd ?


mpz_jacobi
mpn_gcd
0.25
0.2
0.15
0.1
0.05
0
0
200
400
600
800
1000
1200
1400
1600
1800
2000

Symbole de Jacobi en $O(M(n)\log n)$?

Pgcd sous-quadratique par les poids forts : ne marche pas car on a besoin de a mod 4, b mod 4.

Pgcd sous-quadratique par les poids faibles : ne marche pas tel quel car a, b peuvent devenir négatifs.

Pgcd sous-quadratique par les poids faibles avec division binaire modifiée :

$$a, b \rightarrow b, a + q\frac{b}{2^j}$$

où

$$q = -a/(b/2^j) \bmod 2^{j+1}$$

Croissance plus grande des termes (33% expérimentalement) mais a, b restent positifs, et comportement sous-quadratique.

```
bash-3.00$ ./hjacobi 5000
mpz_jacobi took 1524ms
mpz_bjacobi took 652ms

bash-3.00$ ./hjacobi 10000
mpz_jacobi took 6752ms
mpz_bjacobi took 1476ms

bash-3.00$ ./hjacobi 20000
mpz_jacobi took 28121ms
mpz_bjacobi took 3516ms

bash-3.00$ ./hjacobi 50000
mpz_jacobi took 177431ms
mpz_bjacobi took 10940ms

bash-3.00$ ./hjacobi 100000
mpz_jacobi took 711956ms
mpz_bjacobi took 25722ms
```

`http://www.loria.fr/~zimmerma/mca/pub226.html`

(merci de nous signaler toute erreur)