Modular Arithmetic

Paul Zimmermann


INRIA Nancy - Grand Est

8th Central European Conference on Cryptography, Graz,
July 4th, 2008

October 7-9, Nancy, France Workshop on Integer Factorization

`cado.gforge.inria.fr`

October 7-9, Nancy, France
Workshop on Integer Factorization

`cado.gforge.inria.fr`

October 10-15, Nancy, France
Sage Days 10

`sagemath.org`

Plan of the talk

- Applications, Notations

Plan of the talk

- Applications, Notations
- Classical Algorithms

Plan of the talk

- Applications, Notations
- Classical Algorithms
- Unknown and New Algorithms

References

Modern Computer Arithmetic, with Richard Brent:

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

Version 0.2, June 2008:

Chapter 1: Integer Arithmetic

Chapter 2: The FFT and Modular Arithmetic

Chapter 3: Floating-Point Arithmetic

Chapter 4: Newton's Method and Function Evaluation

References

Modern Computer Arithmetic, with Richard Brent:

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

Version 0.2, June 2008:

Chapter 1: Integer Arithmetic

Chapter 2: The FFT and Modular Arithmetic

Chapter 3: Floating-Point Arithmetic

Chapter 4: Newton's Method and Function Evaluation

Chapter 14 of *Handbook of Applied Cryptography* by Menezes, van Oorschot and Vanstone, 1997.

References

Modern Computer Arithmetic, with Richard Brent:

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

Version 0.2, June 2008:

Chapter 1: Integer Arithmetic

Chapter 2: The FFT and Modular Arithmetic

Chapter 3: Floating-Point Arithmetic

Chapter 4: Newton's Method and Function Evaluation

Chapter 14 of *Handbook of Applied Cryptography* by Menezes, van Oorschot and Vanstone, 1997.

Chapter 10 of *Handbook of Elliptic and Hyperelliptic Curve Cryptography* by Cohen, Frey, Avanzi, Doche, Lange, Nguyen and Vercauteren, 2005.

Outline

Applications

Cryptography: RSA encryption and signature (m^e mod N), Diffie-Hellman key-exchange (g^a mod p), elliptic curve cryptography (group addition $\longrightarrow$ multiplication modulo p).

Applications

Cryptography: RSA encryption and signature (m^e mod N), Diffie-Hellman key-exchange (g^a mod p), elliptic curve cryptography (group addition $\longrightarrow$ multiplication modulo p).

Integer factorization: Pollard's rho, Pollard's P-1, Williams P+1, Lenstra's elliptic curve method (ECM).
Complexity $O(L(p)M(\log N))$.

Outline

Notations

Word **radix** β, say $\beta = 2^{64}$.

Notations

Word **radix** β, say $\beta = 2^{64}$.

D is the (invariant) **divisor**: $\beta^{n-1} \leq D < \beta^n$

Notations

Word **radix** β, say $\beta = 2^{64}$.

D is the (invariant) **divisor**: $\beta^{n-1} \leq D < \beta^n$

$a, b, \ldots$: word-size numbers

Notations

Word **radix** β, say $\beta = 2^{64}$.

D is the (invariant) **divisor**: $\beta^{n-1} \leq D < \beta^n$

$a, b, \ldots$: word-size numbers

$A, B, \ldots$: multiple-precision numbers (n or $2n$ words)

Notations

Word **radix** β, say $\beta = 2^{64}$.

D is the (invariant) **divisor**: $\beta^{n-1} \leq D < \beta^n$

$a, b, \ldots$: word-size numbers

$A, B, \ldots$: multiple-precision numbers (n or $2n$ words)

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

Notations

Word **radix** β, say $\beta = 2^{64}$.

D is the (invariant) **divisor**: $\beta^{n-1} \leq D < \beta^n$

$a, b, \ldots$: word-size numbers

$A, B, \ldots$: multiple-precision numbers (n or $2n$ words)

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

Sometimes D has to be **normalized**: $\beta^n/2 \leq D < \beta^n$

Basic Low-level Routines

- to multiply 2 words:

$$a, b \Longrightarrow h, \ell \quad \text{such that} \quad h\beta + \ell = a \times b$$

Basic Low-level Routines

- to multiply 2 words:

$$a, b \Longrightarrow h, \ell \quad \text{such that} \quad h\beta + \ell = a \times b$$

- to divide 2 words by 1 word:

$$a, b, d \text{ with } a < d \Longrightarrow q, r \quad \text{such that} \quad a\beta + b = qd + r$$

Basic Low-level Routines

- to multiply 2 words:

$$a, b \Longrightarrow h, \ell \quad \text{such that} \quad h\beta + \ell = a \times b$$

- to divide 2 words by 1 word:

$$a, b, d \text{ with } a < d \Longrightarrow q, r \quad \text{such that} \quad a\beta + b = qd + r$$

- to multiply 2 multiple-precision numbers:

$$A, B \Longrightarrow A \times B$$

In GMP: `umul_ppmm`, `udiv_qrnnd`, `mpn_mul`.

Outline

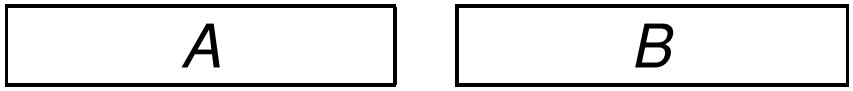
Classical Multiply-and-Divide Reduction

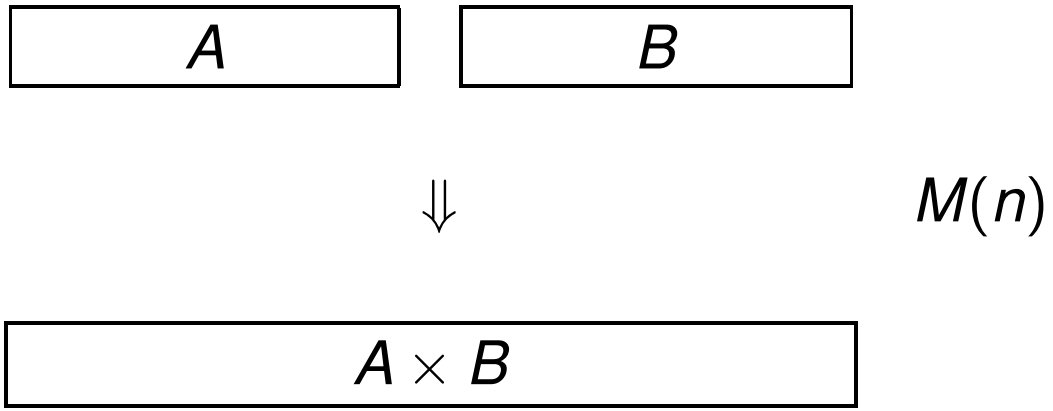
Input: $0 \leq A, B < D$

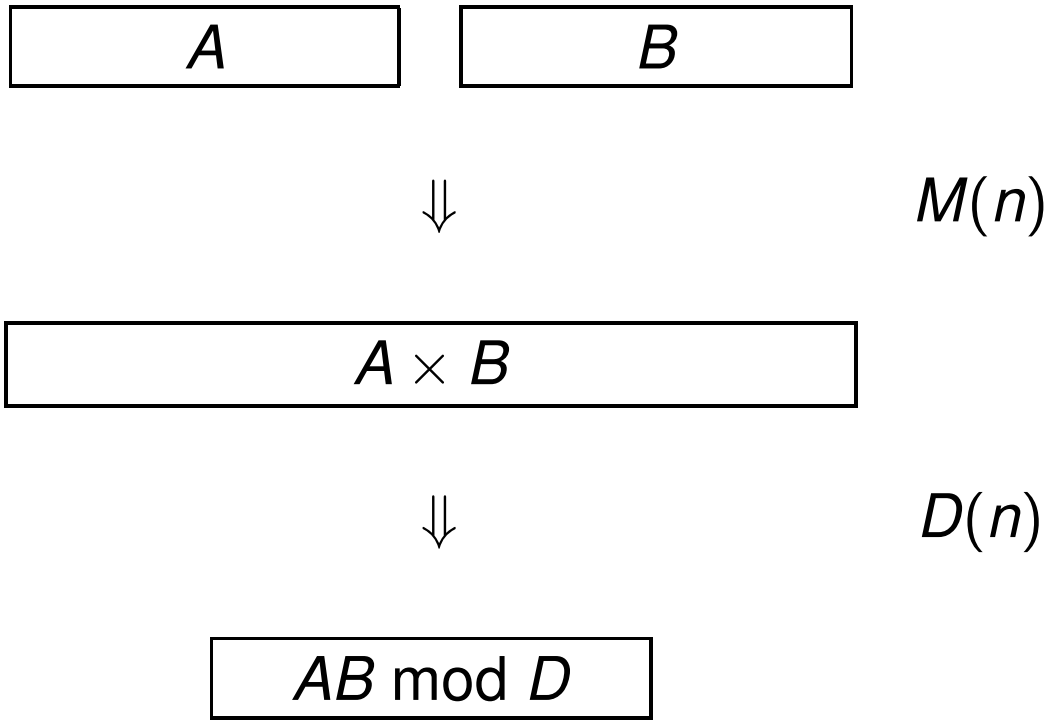
Output: $AB \bmod D$

1. Compute $C = AB$
2. Compute $R = C \bmod D$

Total cost $M(n) + D(n)$.


A
B


A
B
⇓
M(n)
A × B


A
B
⇓
M(n)
A × B
⇓
D(n)
AB mod D

Quadratic Division (Knuth vol2)

Input: $C < D^2$, D normalized
Output: quotient Q, remainder R
for j from $n-1$ downto 0 do
    $q_j \leftarrow \min(\lfloor (c_{n+j}\beta + c_{n+j-1})/d_{n-1} \rfloor, \beta - 1)$ (quotient selection)
    $C \leftarrow C - q_j D \beta^j$
    while $C < 0$ do
        $q_j \leftarrow q_j - 1$
        $C \leftarrow C + \beta^j D$
Return $Q = \sum_0^{n-1} q_j \beta^j$, $R = C$

Quadratic Division: An Example

$$766\,970\,544\,842\,443\,844 \mid 862\,664\,913$$

Quadratic Division: An Example

$$\begin{array}{r|l} 766\,970\,544\,842\,443\,844 & 862\,664\,913 \\ \hline 889 & \end{array}$$

Quadratic Division: An Example

$$
\begin{array}{rl|l}
 & 766\,970\,544\,842\,443\,844 & 862\,664\,913 \\
\cline{3-3}
 & & 889 \\
- & \underline{766\,909\,107\,657} & \\
 & &
\end{array}
$$

Quadratic Division: An Example

$$
\begin{array}{rl|l}
 & 766\,970\,544\,842\,443\,844 & 862\,664\,913 \\
 & & \overline{} \\
- & \underline{766\,909\,107\,657} & 889 \\
 & 061\,437\,185\,443 &
\end{array}
$$

Quadratic Division: An Example

$$
\begin{array}{rl|l}
 & 766\,970\,544\,842\,443\,844 & 862\,664\,913 \\
\cline{3-3}
 & & 889 \\
- & \underline{766\,909\,107\,657} & \\
 & 061\,437\,185\,443 & 071
\end{array}
$$

Quadratic Division: An Example

$$
\begin{array}{rl|l}
 & 766\,970\,544\,842\,443\,844 & 862\,664\,913 \\
\hline
 & & 889 \\
 & & \\
- & \underline{766\,909\,107\,657} & \\
 & 061\,437\,185\,443 & \quad 071 \\
- & \underline{061\,249\,208\,823} & \\
 & & \\
\end{array}
$$

Quadratic Division: An Example

$$
\begin{array}{rl|l}
766\,970\,544\,842\,443\,844 & & 862\,664\,913 \\
\cline{3-3}
 & & 889 \\
-\ \underline{766\,909\,107\,657} & & \\
\quad 061\,437\,185\,443 & & \quad 071 \\
\quad -\ \underline{061\,249\,208\,823} & & \\
\quad\quad 187\,976\,620\,844 & &
\end{array}
$$

Quadratic Division: An Example

$$
\begin{array}{rl|l}
 & 766\,970\,544\,842\,443\,844 & 862\,664\,913 \\
\cline{3-3}
 & & 889 \\
- & \underline{766\,909\,107\,657} & \\
 & \quad 061\,437\,185\,443 & \quad 071 \\
- & \quad \underline{061\,249\,208\,823} & \\
 & \quad\quad 187\,976\,620\,844 & \quad\quad 218
\end{array}
$$

Quadratic Division: An Example

$$
\begin{array}{rl|l}
 & 766\,970\,544\,842\,443\,844 & 862\,664\,913 \\
\hline
 & & 889 \\
- & \underline{766\,909\,107\,657} & \\
 & 061\,437\,185\,443 & \quad 071 \\
- & \underline{061\,249\,208\,823} & \\
 & 187\,976\,620\,844 & \quad\quad 218 \\
- & \underline{188\,060\,951\,034} &
\end{array}
$$

Quadratic Division: An Example

$$
\begin{array}{rl|l}
766\,970\,544\,842\,443\,844 & & 862\,664\,913 \\
\cline{3-3}
 & & 889 \\
-\ \underline{766\,909\,107\,657} & & \\
\quad 061\,437\,185\,443 & & \quad 071 \\
\quad -\ \underline{061\,249\,208\,823} & & \\
\quad\quad 187\,976\,620\,844 & & \quad\quad 218 \\
\quad\quad -\ \underline{188\,060\,951\,034} & & \\
\quad\quad\quad -\ 084\,330\,190 & &
\end{array}
$$

Quadratic Division: An Example

$$
\begin{array}{rl|l}
766\,970\,544\,842\,443\,844 & & 862\,664\,913 \\
\hline
 & & 889 \\
-\ 766\,909\,107\,657 & & \\
\underline{} & & \\
\quad 061\,437\,185\,443 & & \quad 071 \\
\quad -\ 061\,249\,208\,823 & & \\
\quad \underline{} & & \\
\quad\quad 187\,976\,620\,844 & & \quad\quad 218 \\
\quad\quad -\ 188\,060\,951\,034 & & \\
\quad\quad \underline{} & & \\
\quad\quad\quad -\ 084\,330\,190 & & \\
\quad\quad\quad +\ 862\,664\,913 & & \quad\quad -1 \\
\quad\quad\quad \underline{} & &
\end{array}
$$

Quadratic Division: An Example

$$
\begin{array}{rl|l}
766\,970\,544\,842\,443\,844 & & 862\,664\,913 \\
\cline{3-3}
 & & 889 \\
-\ 766\,909\,107\,657 & & \\
\cline{1-1}
\quad 061\,437\,185\,443 & & \quad 071 \\
-\ 061\,249\,208\,823 & & \\
\cline{1-1}
\quad 187\,976\,620\,844 & & \quad 218 \\
-\ 188\,060\,951\,034 & & \\
\cline{1-1}
-\ 084\,330\,190 & & \\
+\ 862\,664\,913 & & -1 \\
\cline{1-1}
778\,334\,723 & &
\end{array}
$$

Quadratic Division: An Example

$$
\begin{array}{rl|l}
766\,970\,544\,842\,443\,844 & & 862\,664\,913 \\
\cline{3-3}
 & & 889 \\
-\ 766\,909\,107\,657 & & \\
\cline{1-1}
\quad 061\,437\,185\,443 & & \quad 071 \\
-\ 061\,249\,208\,823 & & \\
\cline{1-1}
\quad 187\,976\,620\,844 & & \quad 218 \\
-\ 188\,060\,951\,034 & & \\
\cline{1-1}
-\ 084\,330\,190 & & \\
+\ 862\,664\,913 & & -1 \\
\cline{1-1}
\quad 778\,334\,723 & &
\end{array}
$$

$$C = 889071217 \times D + 778334723$$

Quadratic Division: Drawbacks

- quotient selection is expensive (128 bits $\div$ 64 bits)

Quadratic Division: Drawbacks

- quotient selection is expensive (128 bits $\div$ 64 bits)
- up to $2n$ repair steps per division

Quadratic Division: Drawbacks

- quotient selection is expensive (128 bits $\div$ 64 bits)
- up to $2n$ repair steps per division
- difficult branch prediction

Quadratic Division: Drawbacks

- quotient selection is expensive (128 bits $\div$ 64 bits)
- up to $2n$ repair steps per division
- difficult branch prediction
- dependency between repair step and next loop: c_{n+j}, c_{n+j-1}

Quadratic Division: Drawbacks

- quotient selection is expensive (128 bits $\div$ 64 bits)
- up to $2n$ repair steps per division
- difficult branch prediction
- dependency between repair step and next loop: c_{n+j}, c_{n+j-1}
- and it is quadratic ...

Outline

Montgomery's Multiplication

Montgomery's Multiplication

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

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

Montgomery's Multiplication

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

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

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

Montgomery's Multiplication

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

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

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

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

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

Montgomery's Multiplication

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

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

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

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

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

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

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

Montgomery's Multiplication

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

Montgomery's Multiplication: An Example

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

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

Montgomery's Multiplication: An Example

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

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

412

Montgomery's Multiplication: An Example

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

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

Montgomery's Multiplication: An Example

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

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

Montgomery's Multiplication: An Example

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

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

Montgomery's Multiplication: An Example

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

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

Montgomery's Multiplication: An Example

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

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

Montgomery's Multiplication: An Example

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

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

Montgomery's Multiplication: An Example

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

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

Montgomery's Multiplication: An Example

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

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

Montgomery's Multiplication: An Example

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

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

Montgomery's Multiplication: An Example

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

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

Montgomery's Multiplication: An Example

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

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

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

Classical vs Montgomery Quadratic Division

- quotient selection is expensive (128 bits $\div$ 64 bits)

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

Classical vs Montgomery Quadratic Division

- quotient selection is expensive (128 bits $\div$ 64 bits)

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

- up to $2n$ repair steps per division

  at most one final repair step

Classical vs Montgomery Quadratic Division

- quotient selection is expensive (128 bits $\div$ 64 bits)

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

- up to $2n$ repair steps per division

  at most one final repair step

- difficult branch prediction

  no branch inside loop

Classical vs Montgomery Quadratic Division

- quotient selection is expensive (128 bits $\div$ 64 bits)
  64 bits $\times$ 64 bits mod 2^{64}: cheap
- up to $2n$ repair steps per division
  at most one final repair step
- difficult branch prediction
  no branch inside loop
- dependency between repair step and next loop: c_{n+j}, c_{n+j-1}
  still holds for c_i

Classical vs Montgomery Quadratic Division

- quotient selection is expensive (128 bits $\div$ 64 bits)
  64 bits $\times$ 64 bits mod 2^{64}: cheap
- up to $2n$ repair steps per division
  at most one final repair step
- difficult branch prediction
  no branch inside loop
- dependency between repair step and next loop: c_{n+j}, c_{n+j-1}
  still holds for c_i
- and it is quadratic ...
  still holds

Outline

Barrett's Algorithm

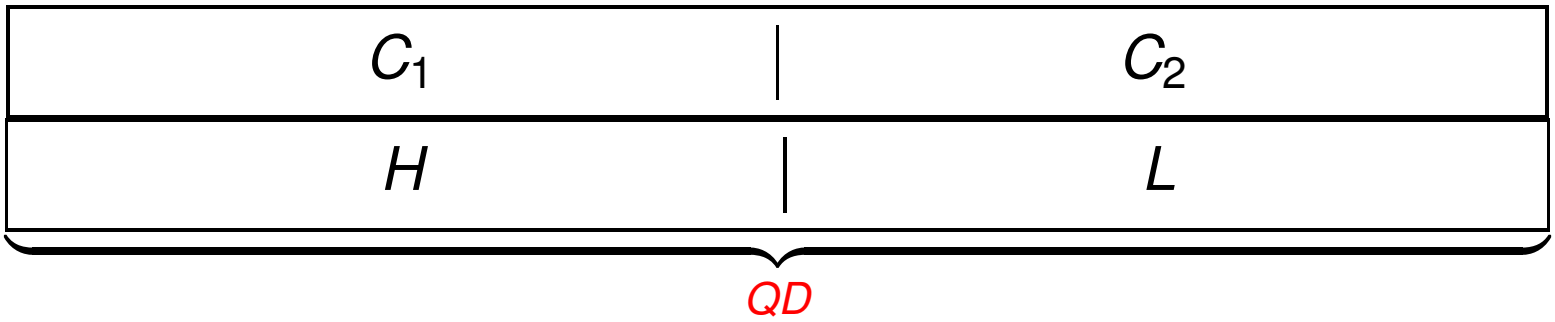
Input: $0 \leq C < D^2$, $\beta/2 < D < \beta$
Output: quotient Q, remainder R
$\mu \leftarrow \lfloor \beta^2/D \rfloor$ [precomputation]
Write $C = C_1\beta + C_0$
$Q \leftarrow \lfloor C_1\mu/\beta \rfloor$
$R \leftarrow C - QD$
while $R \geq D$ do
    $(Q, R) \leftarrow (Q + 1, R - D)$ [at most 3 times]
Return (Q, R)

Replace β by β^n.

Complexity of Barrett's Algorithm

$C_1\,\mu$: cost $M(n)$

Wrap-around trick for QD:



FFT mod $2^n \pm 1$ yields $L \mp H$, from which we get L: cost $\frac{1}{2}M(n)$.

Transforms of μ and D are precomputed: total cost $M(n)$ for reduction, $2M(n)$ for $A \times B$ mod D.

Montgomery-Barrett

Simply make $n = 1$ in the quadratic version!

Input: $C < D^2$, $\mu = -D^{-1} \bmod \beta$ (precomputed)
Output: $R = C\beta^{-1} \bmod D$
Write $C = C_1\beta + C_0$
$Q \leftarrow \mu C_0 \bmod \beta$
$R \leftarrow (C + QD)\beta^{-1}$
if $R \geq D$ do
    $R \leftarrow R - D$

Now replace β by β^n.

Outline

MSB vs LSB Algorithms

MSB algorithms: working from most significant bits to least significant bits.

Most MSB algorithms admit an LSB variant.

Hensel Division

Hensel Division

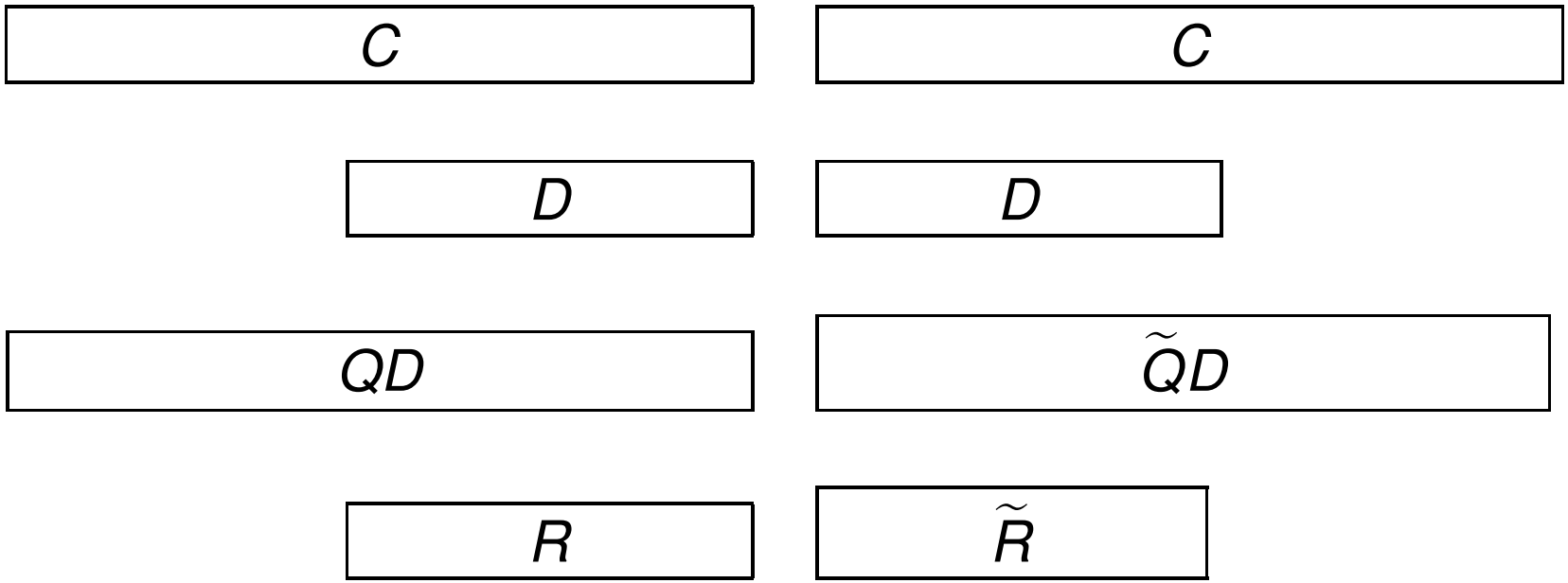
Fast Implementations of RSA Cryptography, Shand and Vuillemin, ARITH'11, 1993.

Euclidean division:

$$C = QD + R$$

Hensel division:

$$C = \widetilde{Q}D + \widetilde{R}\beta^n$$



Euclidean division

Hensel division

Hensel division:

$$C = QD + R\beta^n$$

Hensel division:

$$C = QD + R\beta^n$$

Quotient only:

$$Q = C/D \bmod \beta^n$$

This is the 2-adic division.

Hensel division:

$$C = QD + R\beta^n$$

Quotient only:

$$Q = C/D \bmod \beta^n$$

This is the 2-adic division.

Remainder only:

$$R = C/\beta^n \bmod D$$

This is Montgomery's reduction!

Outline

Antonin Svoboda (1907-1980)

Born in Prague, Czechoslovakia
Studied Theoretical and Experimental Physics
1938: Math. Prof., Czech Institute Technology
1939: forced to emigrate to the USA
1943-1946: stay at MIT
1946: back to Czechoslovakia
Dream: build a "mathematical machines" industry
1964: back to USA (Prof. at UCLA)

Svoboda Division

When dividing by $D = \overbrace{1,000}^{d_{n-1}}, \ldots$, quotient selection is easy:

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

Svoboda's idea: force $d_{n-1} = \beta$!

Svoboda Division: An Example

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

$$766\,970\,544\,842\,443\,844 \;\big|\; 1000\,691\,299\,080$$

Svoboda Division: An Example

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

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

Svoboda Division: An Example

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

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

Svoboda Division: An Example

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

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

Svoboda Division: An Example

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

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

Svoboda Division: An Example

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

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

Svoboda Division: An Example

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

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

Svoboda Division: An Example

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

$766\,970\,544\,842\,443\,844$	$1000\,691\,299\,080$
$-\ 766\,529\,535\,095\,280$	766
$441\,009\,747\,163\,844$	441
$-\ 441\,304\,862\,894\,280$	
$-\ 295\,115\,730\,436$	
$+\ 1000\,691\,299\,080$	-1

Svoboda Division: An Example

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

$766\,970\,544\,842\,443\,844$	$1000\,691\,299\,080$
$-\ 766\,529\,535\,095\,280$	766
$441\,009\,747\,163\,844$	441
$-\ 441\,304\,862\,894\,280$	
$-\ 295\,115\,730\,436$	
$+\ 1000\,691\,299\,080$	-1
$705\,575\,568\,644$	

Svoboda Division: An Example

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

$766\,970\,544\,842\,443\,844$	$1000\,691\,299\,080$
$-\ 766\,529\,535\,095\,280$	766
$441\,009\,747\,163\,844$	441
$-\ 441\,304\,862\,894\,280$	
$-\ 295\,115\,730\,436$	
$+\ 1000\,691\,299\,080$	-1
$705\,575\,568\,644$	818

Svoboda Division: An Example

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

$766\,970\,544\,842\,443\,844$	$1000\,691\,299\,080$
$-\ 766\,529\,535\,095\,280$	766
$441\,009\,747\,163\,844$	441
$-\ 441\,304\,862\,894\,280$	
$-\ 295\,115\,730\,436$	
$+\ 1000\,691\,299\,080$	-1
$705\,575\,568\,644$	818
$-\ 705\,659\,898\,834$	

Svoboda Division: An Example

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

$766\,970\,544\,842\,443\,844$	$1000\,691\,299\,080$
$-\ 766\,529\,535\,095\,280$	766
$441\,009\,747\,163\,844$	441
$-\ 441\,304\,862\,894\,280$	
$-\ 295\,115\,730\,436$	
$+\ 1000\,691\,299\,080$	-1
$705\,575\,568\,644$	818
$-\ 705\,659\,898\,834$	
$-\ 084\,330\,190$	

Svoboda Division: An Example

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

$766\,970\,544\,842\,443\,844$	$1000\,691\,299\,080$
$-\ 766\,529\,535\,095\,280$	766
$441\,009\,747\,163\,844$	441
$-\ 441\,304\,862\,894\,280$	
$-\ 295\,115\,730\,436$	
$+\ 1000\,691\,299\,080$	-1
$705\,575\,568\,644$	818
$-\ 705\,659\,898\,834$	
$-\ 084\,330\,190$	
$+\ 862\,664\,913$	-1

Svoboda Division: An Example

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

$766\,970\,544\,842\,443\,844$	$1000\,691\,299\,080$
$-\ 766\,529\,535\,095\,280$	766
$441\,009\,747\,163\,844$	441
$-\ 441\,304\,862\,894\,280$	
$-\ 295\,115\,730\,436$	
$+\ 1000\,691\,299\,080$	-1
$705\,575\,568\,644$	818
$-\ 705\,659\,898\,834$	
$-\ 084\,330\,190$	
$+\ 862\,664\,913$	-1
$778\,334\,723$	

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

Svoboda Division:

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

- quotient selection becomes trivial (except last step)
- smaller repair probability, since d_{n-1} larger
- very interesting when quotient is not needed

How to Use Svoboda Division?

- either choose D such that $d_{n-1} = \beta$
- or work modulo kD of $n + 1$ words
- or perform a last ordinary division step

Montgomery-Svoboda Division:

Remember $\mu = -D^{-1} \bmod \beta$.

- compute $D' = \mu D$, then $D' \equiv -1 \bmod \beta$ (D': $n+1$ words)

Montgomery-Svoboda Division:

Remember $\mu = -D^{-1} \bmod \beta$.

- compute $D' = \mu D$, then $D' \equiv -1 \bmod \beta$ (D': $n+1$ words)
- $R' = C/\beta^{n-1} \bmod D'$ ($\mu' = -1/D' = 1 \bmod \beta$)

$$C = Q(kD) + R'\beta^{n-1}$$

Montgomery-Svoboda Division:

Remember $\mu = -D^{-1} \bmod \beta$.

- compute $D' = \mu D$, then $D' \equiv -1 \bmod \beta$ (D': $n+1$ words)
- $R' = C/\beta^{n-1} \bmod D'$ ($\mu' = -1/D' = 1 \bmod \beta$)

$$C = Q(kD) + R'\beta^{n-1}$$

- $R = R'/\beta \bmod D$ (classical Montgomery)

$$R' = qD + R\beta$$

Montgomery-Svoboda Division:

Remember $\mu = -D^{-1} \bmod \beta$.

- compute $D' = \mu D$, then $D' \equiv -1 \bmod \beta$ (D': $n+1$ words)
- $R' = C/\beta^{n-1} \bmod D'$ ($\mu' = -1/D' = 1 \bmod \beta$)

$$C = Q(kD) + R'\beta^{n-1}$$

- $R = R'/\beta \bmod D$ (classical Montgomery)

$$R' = qD + R\beta$$

$$C = (kQ + q\beta^{n-1})D + R\beta^n$$

Montgomery-Svoboda: An Example

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

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

Montgomery-Svoboda: An Example

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

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

Montgomery-Svoboda: An Example

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

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

Montgomery-Svoboda: An Example

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

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

Montgomery-Svoboda: An Example

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

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

$$\begin{array}{r} 844 \\ 735 \end{array}$$

Montgomery-Svoboda: An Example

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

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

Montgomery-Svoboda: An Example

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

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

Montgomery-Svoboda: An Example

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

$C = 766\,970\,544\,842\,443\,844$	$D' = 19\,841\,292\,999$
$+\ \underline{16\,746\,051\,291\,156}$	844
$766\,987\,290\,893\,735$	735
$+\ \underline{14\,583\,350\,354\,265}$	
$781\,570\,641\,248$	704

Montgomery-Svoboda: An Example

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

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

Montgomery-Svoboda: An Example

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

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

Montgomery-Svoboda: An Example

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

$C = 766\,970\,544\,842\,443\,844$	$D' = 19\,841\,292\,999$
$+\ \underline{16\,746\,051\,291\,156}$	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

Montgomery-Svoboda: An Example

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

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

Montgomery-Svoboda: An Example

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

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

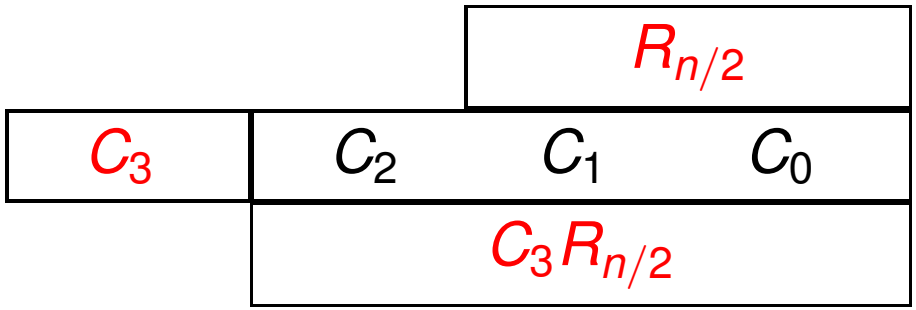
$$C + (23 \times 735844 + 704000000)D = 10^9(D + 526221827)$$

Subquadratic Svoboda Division

Svoboda Division: $kD = beta^{n+1} + R$, $0 \leq R < D < \beta^n$.
Could also choose $kD = beta^{n+1} - R$:

$$\beta^{n+1} \equiv R \bmod D$$

Generalization: $\beta^{n+i} \equiv R_i \bmod D$
Take $i = n/2$: reduce from $2n$ to $\frac{3}{2}n$ words in $M(n, n/2)$:



Hasenplaugh, Gaubatz, Gopal, *Fast Modular Reduction*, ARITH'18, 2007.

Outline

Generalized Montgomery Multiplication

Montgomery Multiplication:

$$AB\beta^{-n} \bmod D$$

Generalized Montgomery Multiplication:

$$ABX^{-1} \bmod D$$

Philip McLaughlin, Math. of Comp., 2004.
Rephrased by Mihailescu, Math. of Comp., 2008.

McLaughlin's Algorithm

$X = 2^k - 1 > D$, $Y = 2^k + 1$, $\mu = 1/D \bmod X$

(1) $m = AB\mu \bmod X$
(2) $S = (AB + mD) \bmod Y$
(3) $w = -S \bmod Y$
(4) If $2 \| w$, then $s \leftarrow w/2$ else $s \leftarrow (w + Y)/2$
(5) If $AB + mD \equiv s \bmod 2$ then $t \leftarrow s$ else $t \leftarrow s + Y$
(6) If $t < D$ then return t else return $t - D$

(1) costs $\frac{5}{6}M(n)$: $\frac{3}{6}$ for AB, $\frac{2}{6}$ for $(AB)\mu$
(2) costs $\frac{4}{6}M(n)$: forward transforms $\frac{3}{6}$, backward $\frac{1}{6}$

Total cost $1.5M(n)$!

Summary

Raw Barrett: $3M(n)$

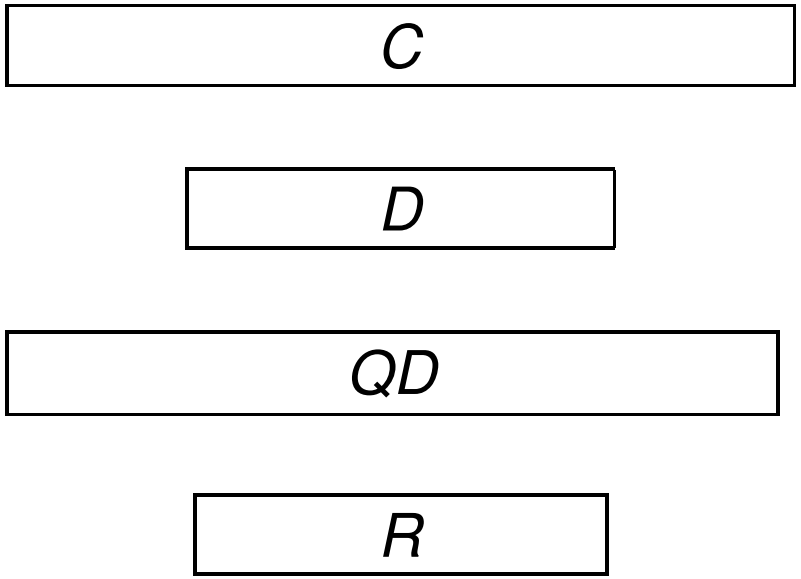
Optimized Barrett (cached FFTs, wrap-around trick): $2M(n)$

McLaughlin: $1.5M(n)$

Can we do better?

$D = 2^n \pm 1$: $0.5M(n)$

A New Algorithm?



bidirectional division

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