FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

High Speed Modulo Calculation Algorithm with Radix-2^k SD Number

Masaaki Niimura
Shinshu University
Nagano

Yasushi Fuwa
Shinshu University
Nagano

Summary. In RSA Cryptograms, many modulo calculations are used, but modulo calculation is based on many subtractions and it takes long a time to calculate it. In this article, we explain a new modulo calculation algorithm using a table. And we prove that upper 3 digits of Radix-2^k SD numbers are enough to specify the answer.

In the first section, we present some useful theorems for operations of Radix-2^k SD Number. In the second section, we define Upper 3 Digits of Radix-2^k SD number and prove that property. In the third section, we prove some property connected with the minimum digits of Radix-2^k SD number. In the fourth section, we identify the range of modulo arithmetic result and prove that the Upper 3 Digits indicate two possible answers. And in the last section, we define a function to select true answer from the results of Upper 3 Digits.

MML Identifier: `RADIX_6`.

The articles [8], [10], [9], [1], [7], [4], [2], [3], [11], [5], and [6] provide the terminology and notation for this paper.

1. Some Useful Theorems

The following two propositions are true:

(1) Let n be a natural number. Suppose $n \geqslant 1$. Let m, k be natural numbers. If $m \geqslant 1$ and $k \geqslant 2$, then $\mathrm{SDDec\,Fmin}(m+n, m, k) = \mathrm{SDDec\,Fmin}(m, m, k)$.

(2) For all natural numbers m, k such that $m \geqslant 1$ and $k \geqslant 2$ holds $\mathrm{SDDec\,Fmin}(m, m, k) > 0$.

ISSN 1426–2630

2. Definitions of Upper 3 Digits of Radix-2^k SD Number and Its Property

Let i, m, k be natural numbers and let r be a $m+2$-tuple of k −SD. Let us assume that $i \in \mathrm{Seg}(m+2)$. The functor $\mathrm{M0Digit}(r, i)$ yielding an element of k −SD is defined as follows:

(Def. 1) $\mathrm{M0Digit}(r, i) = \begin{cases} r(i), & \text{if } i \geqslant m, \\ 0, & \text{if } i < m. \end{cases}$

Let m, k be natural numbers and let r be a $m+2$-tuple of k −SD. The functor $\mathrm{M0}(r)$ yielding a $m+2$-tuple of k −SD is defined as follows:

(Def. 2) For every natural number i such that $i \in \mathrm{Seg}(m+2)$ holds $\mathrm{DigA}(\mathrm{M0}(r), i) = \mathrm{M0Digit}(r, i)$.

Let i, m, k be natural numbers and let r be a $m+2$-tuple of k −SD. Let us assume that $k \geqslant 2$ and $i \in \mathrm{Seg}(m+2)$. The functor $\mathrm{MmaxDigit}(r, i)$ yielding an element of k −SD is defined as follows:

(Def. 3) $\mathrm{MmaxDigit}(r, i) = \begin{cases} r(i), & \text{if } i \geqslant m, \\ \mathrm{Radix}\, k - 1, & \text{if } i < m. \end{cases}$

Let m, k be natural numbers and let r be a $m+2$-tuple of k −SD. The functor $\mathrm{Mmax}(r)$ yields a $m+2$-tuple of k −SD and is defined as follows:

(Def. 4) For every natural number i such that $i \in \mathrm{Seg}(m+2)$ holds $\mathrm{DigA}(\mathrm{Mmax}(r), i) = \mathrm{MmaxDigit}(r, i)$.

Let i, m, k be natural numbers and let r be a $m+2$-tuple of k −SD. Let us assume that $k \geqslant 2$ and $i \in \mathrm{Seg}(m+2)$. The functor $\mathrm{MminDigit}(r, i)$ yields an element of k −SD and is defined by:

(Def. 5) $\mathrm{MminDigit}(r, i) = \begin{cases} r(i), & \text{if } i \geqslant m, \\ -\mathrm{Radix}\, k + 1, & \text{if } i < m. \end{cases}$

Let m, k be natural numbers and let r be a $m+2$-tuple of k −SD. The functor $\mathrm{Mmin}(r)$ yielding a $m+2$-tuple of k −SD is defined by:

(Def. 6) For every natural number i such that $i \in \mathrm{Seg}(m+2)$ holds $\mathrm{DigA}(\mathrm{Mmin}(r), i) = \mathrm{MminDigit}(r, i)$.

One can prove the following two propositions:

(3) For all natural numbers m, k such that $m \geqslant 1$ and $k \geqslant 2$ and for every $m+2$-tuple r of k −SD holds $\mathrm{SDDec}\, \mathrm{Mmax}(r) \geqslant \mathrm{SDDec}\, r$.

(4) For all natural numbers m, k such that $m \geqslant 1$ and $k \geqslant 2$ and for every $m+2$-tuple r of k −SD holds $\mathrm{SDDec}\, r \geqslant \mathrm{SDDec}\, \mathrm{Mmin}(r)$.

3. Properties of Minimum Digits of Radix-2^k SD Number

Let n, k be natural numbers and let x be an integer. We say that x needs digits of n, k if and only if:

(Def. 7) $x < (\mathrm{Radix}\,k)^n$ and $x \geqslant (\mathrm{Radix}\,k)^{n-'1}$.

One can prove the following three propositions:

(5) For all natural numbers x, n, k, i such that $i \in \mathrm{Seg}\,n$ holds $\mathrm{DigA}(\mathrm{DecSD}(x, n, k), i) \geqslant 0$.

(6) For all natural numbers n, k, x such that $n \geqslant 1$ and $k \geqslant 2$ and x needs digits of n, k holds $\mathrm{DigA}(\mathrm{DecSD}(x, n, k), n) > 0$.

(7) For all natural numbers f, m, k such that $m \geqslant 1$ and $k \geqslant 2$ and f needs digits of m, k holds $f \geqslant \mathrm{SDDec}\,\mathrm{Fmin}(m + 2, m, k)$.

4. Modulo Calculation Algorithm Using Upper 3 Digits of Radix-2^k SD Number

Next we state several propositions:

(8) For all integers m_1, m_2, f such that $m_2 < m_1 + f$ and $f > 0$ there exists an integer s such that $-f < m_1 - s \cdot f$ and $m_2 - s \cdot f < f$.

(9) Let m, k be natural numbers. Suppose $m \geqslant 1$ and $k \geqslant 2$. Let r be a m+2-tuple of k –SD. Then $\mathrm{SDDec}\,\mathrm{Mmax}(r) + \mathrm{SDDec}\,\mathrm{DecSD}(0, m+2, k) = \mathrm{SDDec}\,\mathrm{M0}(r) + \mathrm{SDDec}\,\mathrm{SDMax}(m + 2, m, k)$.

(10) For all natural numbers m, k such that $m \geqslant 1$ and $k \geqslant 2$ and for every $m + 2$-tuple r of k –SD holds $\mathrm{SDDec}\,\mathrm{Mmax}(r) < \mathrm{SDDec}\,\mathrm{M0}(r) + \mathrm{SDDec}\,\mathrm{Fmin}(m + 2, m, k)$.

(11) Let m, k be natural numbers. Suppose $m \geqslant 1$ and $k \geqslant 2$. Let r be a m+2-tuple of k –SD. Then $\mathrm{SDDec}\,\mathrm{Mmin}(r) + \mathrm{SDDec}\,\mathrm{DecSD}(0, m+2, k) = \mathrm{SDDec}\,\mathrm{M0}(r) + \mathrm{SDDec}\,\mathrm{SDMin}(m + 2, m, k)$.

(12) Let m, k be natural numbers and r be a $m + 2$-tuple of k –SD. If $m \geqslant 1$ and $k \geqslant 2$, then $\mathrm{SDDec}\,\mathrm{M0}(r) + \mathrm{SDDec}\,\mathrm{DecSD}(0, m + 2, k) = \mathrm{SDDec}\,\mathrm{Mmin}(r) + \mathrm{SDDec}\,\mathrm{SDMax}(m + 2, m, k)$.

(13) For all natural numbers m, k such that $m \geqslant 1$ and $k \geqslant 2$ and for every $m + 2$-tuple r of k –SD holds $\mathrm{SDDec}\,\mathrm{M0}(r) < \mathrm{SDDec}\,\mathrm{Mmin}(r) + \mathrm{SDDec}\,\mathrm{Fmin}(m + 2, m, k)$.

(14) Let m, k, f be natural numbers and r be a m+2-tuple of k –SD. Suppose $m \geqslant 1$ and $k \geqslant 2$ and f needs digits of m, k. Then there exists an integer s such that $-f < \mathrm{SDDec}\,\mathrm{M0}(r) - s \cdot f$ and $\mathrm{SDDec}\,\mathrm{Mmax}(r) - s \cdot f < f$.

(15) Let m, k, f be natural numbers and r be a m+2-tuple of k –SD. Suppose $m \geqslant 1$ and $k \geqslant 2$ and f needs digits of m, k. Then there exists an integer s such that $-f < \mathrm{SDDec}\,\mathrm{Mmin}(r) - s \cdot f$ and $\mathrm{SDDec}\,\mathrm{M0}(r) - s \cdot f < f$.

(16) Let m, k be natural numbers and r be a $m + 2$-tuple of k –SD. If $m \geqslant 1$ and $k \geqslant 2$, then $\mathrm{SDDec}\,\mathrm{M0}(r) \leqslant \mathrm{SDDec}\,r$ and $\mathrm{SDDec}\,r \leqslant \mathrm{SDDec}\,\mathrm{Mmax}(r)$ or $\mathrm{SDDec}\,\mathrm{Mmin}(r) \leqslant \mathrm{SDDec}\,r$ and $\mathrm{SDDec}\,r < \mathrm{SDDec}\,\mathrm{M0}(r)$.

5. How to Identify the Range of Modulo Arithmetic Result

Let i, m, k be natural numbers and let r be a $m+2$-tuple of k −SD. Let us assume that $i \in \mathrm{Seg}(m+2)$. The functor $\mathrm{MmaskDigit}(r, i)$ yielding an element of k −SD is defined by:

(Def. 8) $$\mathrm{MmaskDigit}(r, i) = \begin{cases} r(i), & \text{if } i < m, \\ 0, & \text{if } i \geqslant m. \end{cases}$$

Let m, k be natural numbers and let r be a $m+2$-tuple of k −SD. The functor $\mathrm{Mmask}(r)$ yields a $m+2$-tuple of k −SD and is defined by:

(Def. 9) For every natural number i such that $i \in \mathrm{Seg}(m+2)$ holds $\mathrm{DigA}(\mathrm{Mmask}(r), i) = \mathrm{MmaskDigit}(r, i)$.

One can prove the following two propositions:

(17) For all natural numbers m, k and for every $m+2$-tuple r of k −SD such that $m \geqslant 1$ and $k \geqslant 2$ holds $\mathrm{SDDec}\,\mathrm{M0}(r) + \mathrm{SDDec}\,\mathrm{Mmask}(r) = \mathrm{SDDec}\,r + \mathrm{SDDec}\,\mathrm{DecSD}(0, m+2, k)$.

(18) For all natural numbers m, k and for every $m+2$-tuple r of k −SD such that $m \geqslant 1$ and $k \geqslant 2$ holds if $\mathrm{SDDec}\,\mathrm{Mmask}(r) > 0$, then $\mathrm{SDDec}\,r > \mathrm{SDDec}\,\mathrm{M0}(r)$.

Let i, m, k be natural numbers. Let us assume that $k \geqslant 2$. The functor $\mathrm{FSDMinDigit}(m, k, i)$ yields an element of k −SD and is defined as follows:

(Def. 10) $$\mathrm{FSDMinDigit}(m, k, i) = \begin{cases} 0, & \text{if } i > m, \\ 1, & \text{if } i = m, \\ -\mathrm{Radix}\,k + 1, & \text{otherwise}. \end{cases}$$

Let n, m, k be natural numbers. The functor $\mathrm{FSDMin}(n, m, k)$ yields a n-tuple of k −SD and is defined as follows:

(Def. 11) For every natural number i such that $i \in \mathrm{Seg}\,n$ holds $\mathrm{DigA}(\mathrm{FSDMin}(n, m, k), i) = \mathrm{FSDMinDigit}(m, k, i)$.

One can prove the following proposition

(19) For every natural number n such that $n \geqslant 1$ and for all natural numbers m, k such that $m \in \mathrm{Seg}\,n$ and $k \geqslant 2$ holds $\mathrm{SDDec}\,\mathrm{FSDMin}(n, m, k) = 1$.

Let n, m, k be natural numbers and let r be a $m+2$-tuple of k −SD. We say that r is zero over n if and only if:

(Def. 12) For every natural number i such that $i > n$ holds $\mathrm{DigA}(r, i) = 0$.

We now state the proposition

(20) Let m be a natural number. Suppose $m \geqslant 1$. Let n, k be natural numbers and r be a $m+2$-tuple of k −SD. If $k \geqslant 2$ and $n \in \mathrm{Seg}(m+2)$ and $\mathrm{Mmask}(r)$ is zero over n and $\mathrm{DigA}(\mathrm{Mmask}(r), n) > 0$, then $\mathrm{SDDec}\,\mathrm{Mmask}(r) > 0$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[4] Yoshinori Fujisawa and Yasushi Fuwa. Definitions of radix-2^k signed-digit number and its adder algorithm. *Formalized Mathematics*, 9(**1**):71–75, 2001.

[5] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.

[6] Masaaki Niimura and Yasushi Fuwa. Magnitude relation properties of radix-2^k SD number. *Formalized Mathematics*, 12(**1**):5–8, 2004.

[7] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

[8] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[9] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[10] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[11] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received November 7, 2003