Modular multiplication and division algorithms based on continued fraction expansion

Mourad Gouicem
UPMC Univ Paris 06 and CNRS UMR 7606, LIP6,
4 place Jussieu, F-75252, Paris cedex 05, France
Contact: gouicem.mourad@gmail.com

***Abstract*—In this paper, we provide new methods to generate a class of algorithms computing modular multiplication and division. All these algorithms rely on sequences derived from the Euclidean algorithm for a well chosen input. We then use these sequences as number scales of the Ostrowski number system to construct the result of either the modular multiplication or division.**

I. Introduction

Continued fractions are commonly used to provide best rational approximations of an irrational number. This sequence of best rational approximations $(p_i/q_i)_{i\in\mathbb{N}}$ is called the convergents' sequence. In the beginning of the 20^{th} century, Ostrowski introduced number systems derived from the continued fraction expansion of any irrational α [1]. He proved that the sequence $(q_i)_{i\in\mathbb{N}}$ of the denominators of the convergents of any irrational α forms a number scale, and any integer can be uniquely written in this basis. In the same way, the sequence $(q_i\alpha - p_i)_{i\in\mathbb{N}}$ also forms a number scale.

In this paper, we show how such number systems based on continued fraction expansions can be used to perform modular arithmetic, and more particularly modular multiplication and modular division. The presented algorithms are of quadratic complexity like many of the existing implemented algorithms [2, Chap. 2.4]. Furthermore, they present the advantage of being only based on the extended Euclidean algorithm, and to integrate the reduction step.

In the following, we will first introduce notations and some properties of the number systems based on continued fraction expansions in Section II. Then we describe the new algorithms in Section III. Finally, we give elements of complexity analysis of these algorithms in Section IV, and perspectives in Section VI.

II. Number systems and continued fractions

A. Notations

First, we give some notations on the continued fraction expansion of an irrational α with $0 < \alpha < 1$ [3]. We call the *tails* of the continued fraction expansion of α the real sequence $(r_i)_{i\in\mathbb{N}}$ defined by

$$\begin{aligned} r_0 &= \alpha, \\ r_i &= 1/r_{i-1} - \lfloor 1/r_{i-1} \rfloor. \end{aligned}$$

We denote $(k_i)_{i\in\mathbb{N}}$ the integer sequence of the partial quotients of the continued fraction expansion of α. They are computed as $k_i = \lfloor 1/r_{i-1} \rfloor$. We have

$$\alpha = \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{\ddots + \cfrac{1}{k_i + r_i}}}} := [0; k_1, k_2, \ldots, k_i + r_i].$$

We write p_i/q_i the i^{th} convergent of α. The sequences $(p_i)_{i\in\mathbb{N}}$ and $(q_i)_{i\in\mathbb{N}}$ are integer valued and positive,

$$\frac{p_i}{q_i} = [0; k_1, k_2, \ldots, k_i].$$

We will also write $(\theta_i)_{i\in\mathbb{N}}$ the positive real sequence of $(-1)^i(q_i\alpha - p_i)$ which we call the sequence of the *partial remainders* as they are related to the tails by $r_i = \theta_i/\theta_{i-1}$. Hereafter, we recall the recurrence relations to compute these sequences,

$$\begin{array}{lll} p_{-1} = 1 & p_0 = 0 & p_i = p_{i-2} + k_i p_{i-1}, \\ q_{-1} = 0 & q_0 = 1 & q_i = q_{i-2} + k_i q_{i-1}, \\ \theta_{-1} = 1 & \theta_0 = \alpha & \theta_i = \theta_{i-2} - k_i \theta_{i-1}. \end{array}$$

We also write $\eta_i = q_i\alpha - p_i$ the sequence of the *signed partial remainders*, which elements are of sign $(-1)^i$. The sequence $(\eta_i)_{i\in\mathbb{N}}$ of the signed partial remainders can be computed as $((-1)^i\theta_i)_{i\in\mathbb{N}}$.

1063-6889/15 $31.00 © 2015 IEEE
DOI 10.1109/ARITH.2015.21

B. Related number systems over irrational numbers

In this section, we present two number systems based on the sequences of the signed partial remainders $(\eta_i)_{i\in\mathbb{N}}$ and the denominators of the convergents $(q_i)_{i\in\mathbb{N}}$ of an irrational α. They have been extensively studied during the second part of the 20^{th} century [1], [4].

Property II.1 ([1, Proposition 1]). *Given $(q_i)_{i\in\mathbb{N}}$ the denominators of the convergents of any irrational $0 < \alpha < 1$, every positive integer N can be uniquely written as*

$$N = 1 + \sum_{i=1}^{m} n_i q_{i-1}$$

where the following "Markovian" conditions are verified:

$$\begin{cases} 0 \leq n_1 \leq k_1 - 1, 0 \leq n_i \leq k_i, \text{ for } i \geq 2, \\ n_i = 0 \text{ if } n_{i+1} = k_{i+1} \end{cases}$$

This number system associated to the $(q_i)_{i\in\mathbb{N}}$ is named the Ostrowski number system. To write an integer in this number system, we use a classical greedy decomposition algorithm (Algorithm 1). The rank m is chosen such that $q_m > N$.

Algorithm 1: Integer decomposition in Ostrowski number system.

input : $N \in \mathbb{N}$, $(q_i)_{i<m}$

output: n_i such that $N = 1 + \sum_{i=1}^{m} n_i q_{i-1}$

```
tmp ← N − 1;
i ← m;
while i ≥ 1 do
    n_i ← ⌊tmp/q_{i−1}⌋;
    tmp ← tmp − n_i q_{i−1};
    i ← i − 1;
```

Property II.2 ([1, Proposition 2]). *Given $(\eta_i)_{i\in\mathbb{N}}$ the sequence of the signed partial remainders of any irrational $0 < \alpha < 1$, every real β, with $0 \leq \beta < 1$ can be uniquely written as*

$$\beta = \alpha + \sum_{i=1}^{+\infty} b_i \eta_{i-1}$$

where the following "Markovian" conditions are verified:

$$\begin{cases} 0 \leq b_1 \leq k_1 - 1, 0 \leq b_i \leq k_i, \text{ for } i \geq 2, \\ b_i = 0 \text{ if } b_{i+1} = k_{i+1}. \end{cases}$$

There also exists two other number systems that are dual to these two. One decomposes integers in the basis $((-1)^i q_i)_{i\in\mathbb{N}}$ and the other decomposes reals in the basis of the unsigned partial remainders $(\theta_i)_{i\in\mathbb{N}}$ [1]. The second Markovian condition then becomes $b_{i+1} = 0$ if $b_i = k_i$. An algorithm to write real numbers in the $(\theta_i)_{i\in\mathbb{N}}$ number scale has been proposed by Ito [5]. It proceeds by iterating the mapping $T_1 : (\alpha, \beta) \to (1/\alpha - \lfloor 1/\alpha \rfloor, \beta/\alpha - \lfloor \beta/\alpha \rfloor)$.

C. Related number systems over rational numbers

In this subsection, we consider $\alpha = p/q$ rational. We recall that the continued fraction expansion of a rational is finite. We denote

$$\frac{p}{q} = [0; k_1, k_2, \ldots, k_n]$$

the continued fraction expansion of p/q, and recall $p_n = p$ and $q_n = q$.

We can still write any integer N using the finite sequence $(q_i)_{i\leq n}$ and a greedy algorithm. However, the first quotient N/q_n will not respect the Markovian conditions for $N \geq q_n$, as the condition is not defined for this quotient (there is no k_{n+1}). Nevertheless, the Markovian conditions will still hold for integers $N < q_n$, since the keypoint in the Ostrowski number system is that there exists q_m such that $q_m > N$ [4].

The $(\eta_i)_{i<n}$ number system also still holds under one supplemental condition: β must be rational with precision at most q (i.e. the denominator of β must be less or equal than q).

III. Modular arithmetic and continued fraction

In this section, we consider $\alpha = a/d$. We highlight that the same decomposition $(b_1, \ldots, b_{n+1})$ can be interpreted in two ways depending on the number system used. In the Ostrowski number system, we obtain an integer N whereas in the number scale $(\eta_i)_{i\in\mathbb{N}}$, we obtain the reduced value of $N\alpha \mod 1$ [1]. Hence, we will use the fact that studying an integer a modulo d is similar to considering the rational a/d modulo 1. This enables us to use properties II.1 and II.2 to compute modular multiplication and division.

A. Modular arithmetic and continued fraction

First, we briefly recall how continued fraction expansion and the Euclidean algorithm are linked. We write $(\theta'_i)_{i\in\mathbb{N}}$ the integer sequence of remainders when computing $\gcd(a, d)$. This sequence is composed of decreasing values less than d. We also write $(\eta'_i)_{i\in\mathbb{N}}$

the sequence $((-1)^i\theta'_i)_{i\in\mathbb{N}}$. We obtain the following recurrence relation, and recall the recurrence relation over the $(\theta_i)_{i\in\mathbb{N}}$ sequence of partial remainders of the continued fraction expansion of a/d :

$$\begin{array}{llll}\theta'_{-1}=d & \theta'_0=a & & \theta'_i=\theta'_{i-2}-\lfloor\theta'_{i-2}/\theta'_{i-1}\rfloor\theta'_{i-1}\\ \theta_{-1}=1 & \theta_0=a/d & & \theta_i=\theta_{i-2}-\lfloor\theta_{i-2}/\theta_{i-1}\rfloor\theta_{i-1}.\end{array}$$

It has to be noticed that $\theta'_i = d\theta_i$ as the extended Euclidean algorithm compute the relations $\theta'_i = (-1)^i(q_i a - p_i d)$ and $\theta_i = (-1)^i(q_i\frac{a}{d} - p_i)$. In particular, this implies that the same partial quotients, noted k_i, are obtained when computing both sequences.

Finally, we notice that the extended Euclidean algorithm gives the Bezout's identity with $\theta'_{n-1} = (-1)^{n-1}(q_{n-1}a - p_{n-1}d) = \gcd(a,d)$, and q_{n-1} the inverse of a if a is invertible modulo d ($\gcd(a,d)=1$).

B. Modular multiplication

Now, given $a, b \in \mathbb{Z}/d\mathbb{Z}$, we write $c = a\cdot b \mod d$ the integer $0 \le c < d$ such that $ab - \lfloor ab/d\rfloor \cdot d = c$.

We can observe that the decompositions presented in properties II.1 and II.2 are both unique and both need the same "Markovian" condition over their coefficients. Hence, we can interpret the same decomposition in both basis.

Theorem III.1. *Given $a, b \in \mathbb{Z}/d\mathbb{Z}$, and $(q_i)_{i\le n}$, $(\eta'_i)_{i\le n}$ from Euclidean algorithm on a and d, if we write b in the $(q_i)_{i\le n}$ number scale as*

$$b = 1 + \sum_{i=1}^{n+1} b_i q_{i-1},$$

then

$$a\cdot b \mod d = a + \sum_{i=1}^{n+1} b_i\eta'_{i-1}.$$

Proof: First, we consider $b < q_n$, it can be written in the Ostrowski number system as

$$b = 1 + \sum_{i=1}^{n} b_i q_{i-1},$$

and the coefficients b_i respect the "Markovian" condition of the Ostrowski number system. Hence,

$$\alpha\cdot b = \alpha + \sum_{i=1}^{n} b_i q_{i-1}\alpha.$$

By definition, $\eta_i = q_i\alpha - p_i$, thus

$$\alpha\cdot b = \alpha + \sum_{i=1}^{n} b_i\eta_{i-1} + \sum_{i=1}^{n} b_i p_{i-1}.$$

i	θ'_i	k_i	q_i	bi	b_{rem}
-1	45		0		
0	17		1		
1	11	2	2	0	0
2	6	1	3	1	2
3	5	1	5	0	2
4	1	1	8	1	7
5	0	5	45	2	24
6				0	30

Table I
EXECUTION OF THE PROPOSED MODULAR MULTIPLICATION ALGORITHM WITH $d = 45$, $a = 17$ AND $b = 30$.

As the coefficients b_i's verify the "Markovian" condition, the uniqueness of the decomposition in property II.2 gives $0 \le \alpha + \sum_{i=1}^{n} b_i\eta_{i-1} < 1$ and $\sum_{i=1}^{n} b_i p_{i-1} \in \mathbb{N}$. Hence,

$$\alpha\cdot b \mod 1 = \alpha + \sum_{i=1}^{n} b_i\eta_{i-1}.$$

By multiplying this inequality by d, as $\alpha = a/d$ and $\eta'_i = \eta_i d$, we obtain

$$a\cdot b \mod d = a + \sum_{i=1}^{n} b_i\eta'_{i-1}.$$

which finalizes the proof of the theorem for $b < q_n$.

Now if $b \ge q_n$ and $b = b_{n+1}q_n + b'$ with $b' < q_n$ the remainder of the division of b by q_n, b' can be uniquely written in the Ostrowski number system. Furthermore, as $\eta'_n = 0$, $b_{n+1}\eta'_n = 0$, which finishes the proof. ■

Example III.1. We give in Table I the sequences involved in theorem III.2 with $d = 45$, $a = 17$ and $b = 24$. We denote $(b_{rem})_{i\in\mathbb{N}}$ the sequence of remainders generated by the greedy decomposition of b in the $(q_i)_{i\in\mathbb{N}}$ number scale. One can notice that $b = 1 + 2*8 + 1*5 + 0*3 + 1*2 + 0*1$, and that

$$\begin{aligned} b\cdot a = 24\cdot 17 = 3 \mod d \\ = 17 + 2\cdot 1 - 1\cdot 5 + 0\cdot 6 - 1\cdot 11 + 0\cdot 17\end{aligned}$$

C. Modular division

Inversely, given $a, b \in \mathbb{Z}/d\mathbb{Z}$, with a invertible modulo d ($\gcd(a,d) = 1$) we can efficiently compute $a^{-1}\cdot b \mod d$.

Theorem III.2. *Given $a, b \in \mathbb{Z}/d\mathbb{Z}$ with $\gcd(a,d) = 1$, and $(q_i)_{i\le n}$, $(\theta'_i)_{i\le n}$ from Euclidean algorithm on a and*

d, if we write b in the $(\theta'_i)_{i<n}$ number scale as

$$b = \sum_{i=1}^{n+1} b_i \theta'_{i-1},$$

then if we denote $c = \sum_{i=1}^{n+1} b_i (-1)^{i-1} q_{i-1}$,

$$a^{-1} \cdot b \mod d \in \{c, d+c\}.$$

Proof: The proof of correctness is similar to the one of theorem III.1, using the facts that $\theta'_i = \theta_i d$ and that $\theta_i = (-1)^i (q_i \alpha - p_i)$.

Now, the greatest integer c is clearly the one associated to the decomposition $(k_1, 0, k_3, 0, \ldots, k_n)$ when n is odd. However, $k_i q_{i-1} = q_i - q_{i-2}$ by definition, which implies

$$\sum_{i=0}^{(n-1)/2} k_{2i+1} q_{2i} = q_n.$$

The smallest integer that can be returned is clearly the one associated to the decomposition $(0, k_2, 0, k_4, \ldots, k_n)$ when n is even. Once again, as $k_i q_{i-1} = q_i - q_{i-2}$, we get

$$-\sum_{i=1}^{n/2} k_{2i} q_{2i-1} = 1 - q_n.$$

Hence, $-d < \sum_{i=1}^{n+1} b_i (-1)^{i-1} q_{i-1} < d$, that is to say, the result needs at most a correction by an addition by d. ∎

Example III.2. We give in Table II the sequences involved in theorem III.2 with $d = 45$, $a = 17$ and $b = 30$. We here notice that $b = 1*17+1*11+0*6+0*5+2*1$, and that

$$\begin{aligned} b \cdot a^{-1} &= 30 \cdot 8 = 15 \mod d \\ &= 2 \cdot 8 - 0 \cdot 5 + 0 \cdot 3 - 1 \cdot 2 + 1 \cdot 1 \end{aligned}$$

We mention that we also tried to decompose b in the $(\eta'_i)_{i \leq n}$ signed remainders number scale and evaluate this same decomposition in the $(q_i)_{i \leq n}$ number scale to compute modular division. We used Ito T_2 transform [5] $T_2 : (\alpha, \beta) \rightarrow (1/\alpha - \lfloor 1/\alpha \rfloor, \lceil \beta/\alpha \rceil - \beta/\alpha)$. In practice, it returns the right result without the need of any correction. However, as the decomposition computed by Ito T_2 transform does not verify the same "Markovian" conditions as in the Ostrowski number system, we were not able to give a theoretical proof that it always returns the reduced result of the modular division.

i	θ'_i	k_i	q_i	bi	b_{rem}
-1	45		0		
0	17		1		30
1	11	2	2	1	13
2	6	1	3	1	2
3	5	1	5	0	2
4	1	1	8	0	2
5	0	5	45	2	0
6				0	0

Table II
EXECUTION OF THE PROPOSED MODULAR DIVISION ALGORITHM WITH $d = 45$, $a = 17$ AND $b = 30$.

IV. ELEMENTS OF COMPLEXITY ANALYSIS

In this section, we introduce elements of complexity analysis of the proposed modular multiplication algorithm based on theorem III.1. The same analysis holds for the division. This analysis is highly eased by previous works on the Euclidean algorithm complexity [].

A. Worst-case complexity

The introduced algorithms compute $(q_i)_{i \leq n}$ and $(\eta'_i)_{i \leq n}$. This can be computed using the classical extended Euclidean algorithm in $O(\log(d)^2)$ binary operations.

Second, the binary complexity of the decomposition in $(q_i)_{i \leq n}$ as in algorithm 1 is bounded by the complexity of computing the sequence $(q_i)_{i \leq n}$ since the same number of quotients are computed, with values of similar size, and the quotients b_i are bounded by the quotients k_i (Markovian condition). Hence, the greedy decomposition has complexity in $O(\log(d)^2)$.

To finish the worst-case complexity analysis, evaluating the sum to return the final result can also be done in $O(\log(d)^2)$.

B. Average number of quotients k_i

The average number of quotients k_i computed by the Euclidean algorithm has been extensively studied [6], [7], [8]. In particular, Porter [9] showed that it is bounded by

$$\frac{12 \ln(2)}{\pi^2} \ln(d) + (4P + 2, 5) + O(d^{-1/6+\epsilon}) \quad (1)$$

for every $\epsilon > 0$ and P Porter's constant ($P \approx 1.47$ and $12 \ln(2)/\pi^2 \approx 0.84$ [10]).

C. Average value of quotients k_i and b_i

The average value of the quotients k_i is equal to Khinchin's constant (approximately 2.69) [3, p. 93]. Furthermore, big quotients are very unlikely to occur as

the quotients of any continued fraction follow the Gauss-Kuzmin distribution [3, p. 83] [7, p. 352],

$$\mathbb{P}(k_i = k) = -\log_2\left(1 - \frac{1}{(k+1)^2}\right).$$

This typically means that most of the divisions computed in the Euclidean algorithm can be computed by subtraction efficiently.

By the same arguments, the coefficients b_i of the decomposition in $(q_i)_{i\leq n}$ can be computed by subtraction as they are also likely small (as they are bounded by the k_i due to the Markovian conditions).

In the modular multiplication algorithm, the only quotient not following the Gauss-Kuzmin distribution is the coefficient b_{n+1} when $gcd(a,d) \neq 1$, as it corresponds to the quotient $\lfloor b/q_n \rfloor$. Here, we prove the folowing theorem, showing that b_{n+1} is still likely to be very small.

Theorem IV.1. *Let a, d, b and N integers. If a and d are uniformly chosen in $[1, N]$ and b is uniformly chosen in $[1, d]$, then when N tends to infinity, $\mathbb{P}(b_{n+1} \leq k)$ tends to*

$$\zeta(2)^{-1}\left[\sum_{i=1}^{k+1}\frac{i-(k+1)}{i^3} + (k+1)\zeta(3)\right].$$

with $\zeta(s) = \sum_{i=1}^{+\infty}\frac{1}{i^s}$ the Riemann zeta function.

Proof: Let U_1, U_2 and U_3 be three independent uniform distributions over $[0,1]$. We write $a = \lceil U_1 N \rceil$, $d = \lceil U_2 N \rceil$ and $b = \lceil U_3 d \rceil$. We denote $A = \{b < (k+1)q_n\}$, $B = \{\gcd(a,d) \leq k+1\}$, $\bar{B} = \{\gcd(a,d) > k+1\}$ and $B_i = \{\gcd(a,d) = i\}$. Hence using the law of total probability we have

$$\begin{aligned}
A &= (A \cap B) \bigsqcup (A \cap \bar{B}),\\
&= \left(\bigsqcup_{i\leq k+1}(A \cap B_i)\right) \bigsqcup \left(\bigsqcup_{i>k+1}(A \cap B_i)\right),\\
&= \left(\bigsqcup_{i\leq k+1}\mathbb{P}(A|B_i)\cdot\mathbb{P}(B_i)\right) \bigsqcup \left(\bigsqcup_{i>k+1}\mathbb{P}(A|B_i)\cdot\mathbb{P}(B_i)\right).
\end{aligned}$$

As the B_i are disjoint events, we have

$$\mathbb{P}(A) = \sum_{i=1}^{k+1}\mathbb{P}(A|B_i)\cdot\mathbb{P}(B_i) + \sum_{i=k+2}^{+\infty}\mathbb{P}(A|B_i)\cdot\mathbb{P}(B_i).$$

First, $\mathbb{P}(A|B_i) = 1$ for $i \leq k+1$ as $b < d = \gcd(a,d)\cdot q_n \leq (k+1)\cdot q_n$. Hence,

$$\mathbb{P}(A) = \sum_{i=1}^{k+1}\mathbb{P}(B_i) + \sum_{i=k+2}^{+\infty}\mathbb{P}(A|B_i)\cdot\mathbb{P}(B_i).$$

Now we want to determine $\mathbb{P}(A|B_i)$ for $i \geq k+2$. Hereafter, to simplify equations, we write $\mathbb{Q}_i(\cdot) = \mathbb{P}(\cdot|B_i)$ and $C = \{a = l\} \cap \{d = m\}$.

$$\begin{aligned}
\mathbb{P}(A|B_i) &= \mathbb{Q}_i(A),\\
&= \sum_{l=1}^{N}\sum_{m=1}^{N}\mathbb{Q}_i(C)\cdot\mathbb{Q}_i(A \mid C).
\end{aligned}$$

However,

$$\mathbb{Q}_i(A \mid C) = \frac{k+1}{i}$$

as b is uniformly distributed between 1 and $d = iq_n$. If we consider the segment of length d and slice it in i segments of length q_n, it can be interpreted as the probability that b is in the first $k+1$ slices. Hence

$$\begin{aligned}
\mathbb{P}(A|B_i) &= \sum_{l=1}^{N}\sum_{m=1}^{N}\mathbb{Q}_i(\{a=l\}\cap\{d=m\})\cdot\frac{k+1}{i},\\
&= \frac{k+1}{i}\cdot\sum_{l=1}^{N}\sum_{m=1}^{N}\mathbb{Q}_i(\{a=l\}\cap\{d=m\}).
\end{aligned}$$

As $\{a = l\}$ and $\{d = m\}$ are independent by hypothesis (U_1 and U_2 are independent),

$$\mathbb{Q}_i(\{a=l\}\cap\{d=m\}) = \mathbb{Q}_i(\{a=l\})\cdot\mathbb{Q}_i(\{d=m\}),$$

and

$$\mathbb{P}(A|B_i) = \frac{k+1}{i}\cdot\sum_{l=1}^{N}\mathbb{Q}_i(\{a=l\})\cdot\sum_{m=1}^{N}\mathbb{Q}_i(\{d=m\}).$$

Now, we use the fact that the sum of the probabilities over the whole sample space always sum to 1 to obtain

$$\mathbb{P}(A|B_i) = \frac{k+1}{i}.$$

If we recapitulate,

$$\mathbb{P}(A) = \sum_{i=1}^{k+1}\mathbb{P}(B_i) + \sum_{i=k+2}^{+\infty}\frac{k+1}{i}\cdot\mathbb{P}(B_i).$$

Finally, it is widely known that $\mathbb{P}(B_i)$ tends to $\frac{\zeta(2)^{-1}}{i^2}$ when N tends to infinity [11, p. 353]. Hence, we get

$$\begin{aligned}
\lim_{N\to+\infty}\mathbb{P}(A) &= \sum_{i=1}^{k+1}\frac{\zeta(2)^{-1}}{i^2} + \sum_{i=k+2}^{\infty}\frac{k+1}{i}\cdot\frac{\zeta(2)^{-1}}{i^2},\\
&= \zeta(2)^{-1}\left[\sum_{i=1}^{k+1}\frac{1}{i^2} + (k+1)\sum_{i=k+2}^{+\infty}\frac{1}{i^3}\right],
\end{aligned}$$

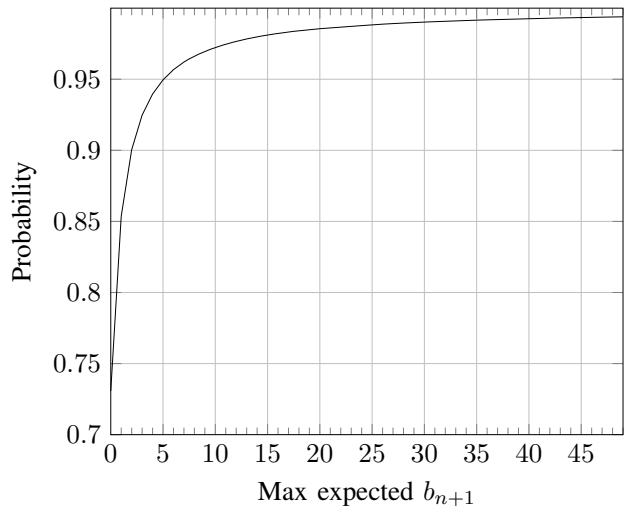

Figure 1. Cumulative distribution function of the coefficient b_{n+1}.

which equals to

$$\zeta(2)^{-1}\left[\sum_{i=1}^{k+1}\frac{1}{i^2}+(k+1)\left(\sum_{i=1}^{+\infty}\frac{1}{i^3}-\sum_{i=1}^{k+1}\frac{1}{i^3}\right)\right],$$
$$=\zeta(2)^{-1}\left[\sum_{i=1}^{k+1}\frac{i-(k+1)}{i^3}+(k+1)\left(\sum_{i=1}^{+\infty}\frac{1}{i^3}\right)\right].$$

Hence, using Riemann zeta function definition, we get the following simplification, which is more convenient for computation and has been used to generate Fig. 1,

$$\lim_{N\to+\infty}\mathbb{P}(A)=\zeta(2)^{-1}\left[\sum_{i=1}^{k+1}\frac{i-(k+1)}{i^3}+(k+1)\cdot\zeta(3)\right].$$

■

Figure 1 shows the probability distribution of $\mathbb{P}(b_{n+1} \leq k)$. In particular, we obtain $\mathbb{P}(b_{n+1} \leq 3) \approx 92.5\%$.

V. Comments on a practical use of these algorithms

Existing algorithms for modular multiplication are of two kinds. They either integrate the reduction, making it possible to do all the computations with the input precision (Blakley [12] and Takagi [13]) , or they rely on an efficient multiplication of the arguments, and then efficiently reduce their product – which size is the sum of the arguments' size – (Barrett [14] and Montgomery [15]). All these algorithms are usually used in different contexts, whether we compute many multiplications by the same large values (Montgomery [15]) or small values (Takagi[13]), or whether we compute few multiplications by small values (Blakley [12]) or large values (Barrett [14]).

The proposed algorithms are of the first kind – with integrated reduction – and do not need conversion or pre-computation. They clearly target contexts where few multiplications of small values (because of the quadratic complexity) are computed.

The proposed modular multiplication seems to be of little interest in practice in its current form, as its memory consumption might be high – the sequences $(\theta'_i)_{i\in\mathbb{N}}$ and $(q_i)_{i\in\mathbb{N}}$ have to be stored entirely to decompose b and recompose the result– even if it is of same complexity as competing methods (Blakley[12] and Takagi[13]).

Concerning the modular division, to our knowledge, all existing algorithms require to multiply by an inverse – which need to be computed. In the proposed modular division, the modular multiplication is integrated to the computation of the inverse. This enables to partially cover the latency of the inverse computation. Moreover, its memory footprint is low since the computed sequences do not need to be stored. First experiments with a straightforward 64-bit implementation show an encouraging speedup of 2.44x against GMP [16] low-level functions (`mpn_gcd_ext`, `mpn_mul` and `mpn_tdiv_qr`).

These arguments make it suitable in some context like Gaussian elimination on a small dimension matrix with coefficients in a finite field. For each row, several values are divided by the same pivot. The proposed modular division helps covering the latency of computing an inverse, seems adapted to decompose several inputs at the same time (like any greedy algorithm) and can be easily vectorized (if a vectorized integer division instruction is available).

VI. Perspectives

In this paper, we presented an algorithm for modular multiplication and an algorithm for modular division. Both are based on the extended Euclidean algorithm and are of quadratic complexity in the size of the modulus,and do not require pre-computation or changing the inputs representation.

They present a theoretical interest since it it the first use of Ostrowski number systems to this purpose. Even though the proposed modular multiplication algorithm in its actual form is not relevant in practice, the modular division seems to be efficient as it integrate the multiplication to the computation of the inverse.

Further investigations have to be led to find optimal decomposition algorithms, that minimize the number of coefficients of the produced decomposition and their

size. Also, a supplemental effort is necessary to provide efficient software implementation of the modular division algorithm.

VII. Aknowledgement

This work was supported by the TaMaDi project of the french ANR (grant ANR 2010 BLAN 0203 01). This work has also been greatly supported and improved by many helpful proof readings and discussions with Jean-Claude Bajard, Valérie Berthé, Pierre Fortin, Stef Graillat and Emmanuel Prouff.

References

[1] V. Berthé and L. Imbert, "Diophantine approximation, Ostrowski numeration and the double-base number system," *Discrete Mathematics & Theoretical Computer Science*, vol. 11, no. 1, pp. 153–172, 2009.

[2] R. Brent and P. Zimmermann, *Modern computer arithmetic*, vol. 18. Cambridge University Press, 2010.

[3] A. Y. Khinchin, *Continued fractions*. Dover, 1997.

[4] A. Vershik and N. Sidorov, "Arithmetic expansions associated with a rotation of the circle and with continued fractions," *Saint Petersburg Mathematical Journal*, vol. 5, no. 6, pp. 1121—-1136, 1994.

[5] S. Ito, "Some skew product transformations associated with continued fractions and their invariant measures," *Tokyo Journal of Mathematics*, vol. 9, no. 1, pp. 115–133, 1986.

[6] B. Vallée, "Euclideans dynamics," *Discrete and Continuous Dynamical Systems series S*, pp. 281–352, 2006.

[7] D. E. Knuth, *The Art of Computer Programming*, vol. 2 (Seminumerical Algorithms). Addison-Wesley, second ed., 1981.

[8] L. Lhote and B. Vallée, "Gaussian laws for the main parameters of the Euclid algorithms," *Algorithmica*, vol. 50, no. 4, pp. 497–554, 2008.

[9] J. W. Porter, "On a theorem of Heilbronn," *Mathematika*, vol. 22, no. 01, pp. 20–28, 1975.

[10] D. E. Knuth, "Evaluation of Porter's constant," *Computers & Mathematics with Applications*, vol. 2, no. 2, pp. 137–139, 1976.

[11] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*. Oxford University Press, 6^{th} ed., 2008.

[12] G. Blakley, "A computer algorithm for calculating the product ab modulo m," *IEEE Transactions on Computers*, vol. 32, no. 5, pp. 497–500, 1983.

[13] N. Takagi, "A radix-4 modular multiplication hardware algorithm for modular exponentiation," *Computers, IEEE Transactions on*, vol. 41, no. 8, pp. 949–956, 1992.

[14] P. Barrett, "Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor," in *Advances in cryptology—CRYPTO'86*, pp. 311–323, Springer, 1987.

[15] P. L. Montgomery, "Modular multiplication without trial division," *Mathematics of computation*, vol. 44, no. 170, pp. 519–521, 1985.

[16] T. Granlund and the GMP development team, *GNU MP*, 4.3.2 ed., January 2010.