FORMALIZED MATHEMATICS
Vol. **27**, No. **1**, Pages 79–83, **2019**
DOI: 10.2478/forma-2019-0009

sciendo
https://www.sciendo.com/

Maximum Number of Steps Taken by Modular Exponentiation and Euclidean Algorithm

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Koich Nagao
Kanto Gakuin University
Kanagawa, Japan

Yuichi Futa
Tokyo University of Technology
Tokyo, Japan

Summary. In this article we formalize in Mizar [3], [4] the maximum number of steps taken by some number theoretical algorithms, "right–to–left binary algorithm" for modular exponentiation and "Euclidean algorithm" [8]. For any natural numbers a, b, n, "right–to–left binary algorithm" can calculate the natural number $\texttt{ALGO\_BPOW}(a, n, m) := a^b \bmod n$ and for any integers a, b, "Euclidean algorithm" can calculate the non negative integer $gcd(a, b)$. We have not formalized computational complexity of algorithms yet, though we had already formalize the "Euclidean algorithm" in [12].

For "right-to-left binary algorithm", we formalize the theorem, which says that the required number of the modular squares and modular products in this algorithms are $1 + \lfloor \log_2 n \rfloor$ and for "Euclidean algorithm", we formalize the Lamé's theorem [9], which says the required number of the divisions in this algorithm is at most $5 \log_{10} \min(|a|, |b|)$. Our aim is to support the implementation of number theoretic tools and evaluating computational complexities of algorithms to prove the security of cryptographic systems.

MSC: 68W40 11A05 11A15 03B35

Keywords: algorithms; power residues; Euclidean algorithm

MML identifier: NTALGO_2, version: 8.1.09 5.54.1344

1. Right–to–Left Binary Algorithm for Modular Exponentiation

Let F be an element of *Boolean** and x be an object. Let us note that the functor $F(x)$ yields a natural number. Let n, m be natural numbers. Let us note that the functor n^m yields a natural number. Let a, b be objects and c be a natural number. The functor $\mathrm{BinBranch}(a, b, c)$ is defined by the term

$$\text{(Def. 1)} \quad \begin{cases} a, & \textbf{if } c = 0, \\ b, & \textbf{otherwise}. \end{cases}$$

Let a, b, c be natural numbers. Let us note that the functor $\mathrm{BinBranch}(a, b, c)$ yields a natural number. Let a, n, m be elements of $\mathbb{N}$. The functor $\text{ALGO-BPOW}(a, n, m)$ yielding an element of $\mathbb{N}$ is defined by

(Def. 2) there exist sequences A, B of $\mathbb{N}$ such that $it = B(\mathrm{LenBinSeq}(n))$ and $A(0) = a \bmod m$ and $B(0) = 1$ and for every natural number i, $A(i + 1) = A(i) \cdot A(i) \bmod m$ and $B(i + 1) = \mathrm{BinBranch}(B(i), B(i) \cdot A(i) \bmod m, (\mathrm{Nat2BinLen})(n)(i + 1))$.

Now we state the propositions:

(1) Let us consider natural numbers a, m, i, and a sequence A of $\mathbb{N}$. Suppose $A(0) = a \bmod m$ and for every natural number j, $A(j + 1) = A(j) \cdot A(j) \bmod m$. Then $A(i) = a^{2^i} \bmod m$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv A(\$_1) = a^{2^{\$_1}} \bmod m$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i + 1]$ by [15, (11)], [14, (27)]. For every natural number i, $\mathcal{P}[i]$ from [1, Sch. 2]. □

(2) $\mathrm{LenBinSeq}(0) = 1$.

(3) $\mathrm{LenBinSeq}(1) = 1$.

(4) Let us consider a natural number x. If $2 \leqslant x$, then $1 < \mathrm{LenBinSeq}(x)$.

(5) Let us consider a natural number n. Suppose $0 < n$. Then $\mathrm{LenBinSeq}(n) = \lfloor \log_2 n \rfloor + 1$.

(6) $(\mathrm{Nat2BinLen})(0) = \langle 0 \rangle$.

(7) $(\mathrm{Nat2BinLen})(1) = \langle 1 \rangle$. The theorem is a consequence of (3).

(8) Let us consider an element n of $\mathbb{N}$. If $0 < n$, then $(\mathrm{Nat2BinLen})(n)(\mathrm{LenBinSeq}(n))$ = 1.

Proof: Reconsider $x = (\mathrm{Nat2BinLen})(n)$ as an element of *Boolean**. $x \notin \{y$, where y is an element of *Boolean** : $y(\mathrm{len}\, y) = 1\}$ by [17, (153)]. □

(9) $(\mathrm{Nat2BinLen})(2) = \langle 0, 1 \rangle$. The theorem is a consequence of (5).

(10) $(\mathrm{Nat2BinLen})(3) = \langle 1, 1 \rangle$. The theorem is a consequence of (5).

(11) $(\mathrm{Nat2BinLen})(4) = \langle 0, 0, 1 \rangle$. The theorem is a consequence of (5).

(12) Let us consider a natural number n. Then $(\mathrm{Nat2BinLen})(2^n) = \langle\underbrace{0,\ldots,0}_{n}\rangle^\frown \langle 1\rangle$. The theorem is a consequence of (5).

(13) Let us consider an element m of $\mathbb{N}$. Then ALGO-BPOW$(0, 0, m) = 1$. The theorem is a consequence of (6).

(14) Let us consider elements n, m of $\mathbb{N}$. If $0 < n$, then ALGO-BPOW$(0, n, m) = 0$. The theorem is a consequence of (1) and (8).

Let us consider elements a, n, m of $\mathbb{N}$. Now we state the propositions:

(15) If $0 < n$ and $m \leqslant 1$, then ALGO-BPOW$(a, n, m) = 0$. The theorem is a consequence of (8).

(16) If $a \neq 0$ and $1 < m$, then ALGO-BPOW$(a, n, m) = a^n \bmod m$.
Proof: Consider A, B being sequences of $\mathbb{N}$ such that ALGO-BPOW$(a, n, m) = B(\mathrm{LenBinSeq}(n))$ and $A(0) = a \bmod m$ and $B(0) = 1$ and for every natural number i, $A(i + 1) = A(i) \cdot A(i) \bmod m$ and $B(i + 1) = \mathrm{BinBranch}(B(i), B(i) \cdot A(i) \bmod m, (\mathrm{Nat2BinLen})(n)(i+1))$. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 < \mathrm{LenBinSeq}(n)$, then there exists a $(\$_1 + 1)$-tuple S of *Boolean* such that $S = (\mathrm{Nat2BinLen})(n){\restriction}(\$_1 + 1)$ and $B(\$_1 + 1) = a^{\mathrm{AbsVal}(S)} \bmod m$. $\mathcal{P}[0]$ by [5, (20)], [6, (5)], [11, (14), (16), (15)]. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i + 1]$ by [16, (7)], [1, (11)], [2, (89)], [17, (153)]. For every natural number i, $\mathcal{P}[i]$ from [1, Sch. 2]. Reconsider $f = \mathrm{LenBinSeq}(n) - 1$ as a natural number. Consider F_1 being an $(f + 1)$-tuple of *Boolean* such that $F_1 = (\mathrm{Nat2BinLen})(n){\restriction}(f + 1)$ and $B(f + 1) = a^{\mathrm{AbsVal}(F_1)} \bmod m$. □

2. Lamé's Theorem

Now we state the propositions:

(17) $\mathrm{Fib}(5) = 5$.

(18) $1 < \tau$.

(19) $\tau < 2$.

(20) $\log_\tau 10 < 5$. The theorem is a consequence of (17) and (18).

(21) Let us consider a natural number n. If $3 \leqslant n$, then $\tau^{n-2} < \mathrm{Fib}(n)$.
Proof: Define $\mathcal{P}$[natural number] $\equiv \tau^{\$_1 - 2} < \mathrm{Fib}(\$_1)$. For every natural number k such that $k \geqslant 3$ holds if for every natural number i such that $i \geqslant 3$ holds if $i < k$, then $\mathcal{P}[i]$, then $\mathcal{P}[k]$ by [1, (9)], [7, (22)], (19), [18, (9)]. For every natural number k such that $k \geqslant 3$ holds $\mathcal{P}[k]$ from [1, Sch. 9]. □

(22) Let us consider elements a, b of $\mathbb{Z}$. Suppose $|a| > |b|$ and $b > 1$. Then there exist sequences A, B of $\mathbb{N}$ and there exists a sequence C of real

numbers and there exists an element n of $\mathbb{N}$ such that $A(0) = |a|$ and $B(0) = |b|$ and for every natural number i, $A(i+1) = B(i)$ and $B(i+1) = A(i) \bmod B(i)$ and $n = \min^*\{i$, where i is a natural number : $B(i) = 0\}$ and $\gcd(a,b) = A(n)$ and $\mathrm{Fib}(n+1) \leqslant |b|$ and $n \leqslant 5 \cdot \lceil \log_{10} |b| \rceil$ and $n \leqslant C(|b|)$ and C is polynomially bounded.

Proof: Consider A, B being sequences of $\mathbb{N}$ such that $A(0) = |a|$ and $B(0) = |b|$ and for every natural number i, $A(i+1) = B(i)$ and $B(i+1) = A(i) \bmod B(i)$ and $\mathrm{ALGO}_{\mathrm{GCD}}(a,b) = A(\min^*\{i$, where i is a natural number : $B(i) = 0\})$. Consider n being an element of $\mathbb{N}$ such that $n = \min^*\{i$, where i is a natural number : $B(i) = 0\}$ and $\mathrm{ALGO}_{\mathrm{GCD}}(a,b) = A(n)$. For every elements a, b of $\mathbb{Z}$ and for every sequences A, B of $\mathbb{N}$ such that $A(0) = |a|$ and $B(0) = |b|$ and for every natural number i, $A(i+1) = B(i)$ and $B(i+1) = A(i) \bmod B(i)$ holds $\{i$, where i is a natural number : $B(i) = 0\}$ is a non empty subset of $\mathbb{N}$ by [1, (13)], [16, (58)], [1, (14)]. $B(n-1) \neq 0$. For every natural number i such that $i < n$ holds $B(i) > 0$. For every natural number i such that $i < n$ holds $B(i+1) \leqslant B(i) - 1$ by [1, (13)], [16, (58)]. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \leqslant n$, then $B(\$_1) \leqslant B(0) - \$_1$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by [1, (16)]. For every natural number i, $\mathcal{P}[i]$ from [1, Sch. 2]. $n \leqslant B(0)$. For every natural number j such that $j < n$ holds $A(j+1) < A(j)$ by [16, (7), (5)], [1, (13)]. If $1 < n$, then $\mathrm{Fib}(3) \leqslant A(n-1)$ by [1, (20)], [16, (7)], [7, (22)]. For every natural number i such that $0 < i < n$ holds $A(i+2) + A(i+1) \leqslant A(i)$ by [10, (13)]. For every natural number i such that $i < n$ holds $\mathrm{Fib}(i+2) \leqslant A(n-i)$ by [16, (7)], [1, (13), (22), (23)]. $n \leqslant 5 \cdot \lceil \log_{10} |b| \rceil$ by [1, (22)], [13, (4)], [14, (57), (51)]. □

Acknowledgement: This study was supported in part by JSPS KAKENHI Grant Numbers JP17K00182 and JP15K00183. The authors would also like to express our gratitude to Prof. Yasunari Shidama for his support and encouragement.

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] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[4] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[5] Czesław Byliński. Some properties of restrictions of finite sequences. *Formalized Mathematics*, 5(**2**):241–245, 1996.

[6] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Euler's Theorem and small Fermat's Theorem. *Formalized Mathematics*, 7(**1**):123–126, 1998.

[7] Magdalena Jastrzębska and Adam Grabowski. Some properties of Fibonacci numbers. *Formalized Mathematics*, 12(**3**):307–313, 2004.

[8] Donald E. Knuth. *Art of Computer Programming.* Volume 2: Seminumerical Algorithms, 3rd Edition, Addison-Wesley Professional, 1997.

[9] Gabriel Lamé. Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers. *Comptes Rendus Acad. Sci.*, 19:867–870, 1844.

[10] Robert Milewski. Natural numbers. *Formalized Mathematics*, 7(**1**):19–22, 1998.

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

[12] Hiroyuki Okazaki, Yosiki Aoki, and Yasunari Shidama. Extended Euclidean algorithm and CRT algorithm. *Formalized Mathematics*, 20(**2**):175–179, 2012. doi:10.2478/v10037-012-0020-2.

[13] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.

[14] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.

[15] Marco Riccardi. Pocklington's theorem and Bertrand's postulate. *Formalized Mathematics*, 14(**2**):47–52, 2006. doi:10.2478/v10037-006-0007-y.

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

[17] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

[18] Piotr Wojtecki and Adam Grabowski. Lucas numbers and generalized Fibonacci numbers. *Formalized Mathematics*, 12(**3**):329–333, 2004.

Accepted March 11, 2019