SIAM J. COMPUT.
Vol. 32, No. 2, pp. 548–556

ACCELERATION OF EUCLIDEAN ALGORITHM AND RATIONAL NUMBER RECONSTRUCTION*

XINMAO WANG† AND VICTOR Y. PAN‡

Abstract. We accelerate the known algorithms for computing a selected entry of the extended Euclidean algorithm for integers and, consequently, for the modular and numerical rational number reconstruction problems. The acceleration is from quadratic to nearly linear time, matching the known complexity bound for the integer gcd, which our algorithm computes as a special case.

Key words. extended Euclidean algorithm, rational number reconstruction

AMS subject classifications. 68W40, 68W30, 68Q25

PII. S0097539702408636

1. Introduction.

A customary approach in computer algebra is to perform computations with rational numbers modulo a large integer q (a prime, prime power, or product of several selected primes) and then to reconstruct the rational output from its value modulo q [GG99]. In particular, the *modular rational number reconstruction* is the final stage of the solution of a nonsingular linear system of n equations by means of p-adic lifting [MC79], [D82], [P02] (see [GG99], [S86], [UP83], [Z93], [HW60] for other important applications).

PROBLEM 1.1 (modular rational number reconstruction). *Compute a pair of integers (η, δ) from three positive integers m, n, k such that*

$$|\eta| < k < m, \quad 1 \le \delta \le m/k, \quad \eta = n\delta \bmod m. \tag{1.1}$$

PROBLEM 1.1a. *Compute all coprime solutions (η, δ) to Problem* 1.1.

There always exists a solution to Problem 1.1. There are at most two solutions to Problem 1.1a, and at most one of them satisfies $|\eta| < k/2$ [GG99, Theorem 5.26]. To ensure unique correct reconstruction of η and δ, having some upper bounds on $|\eta|$ and δ (e.g., Hadamard's bound applies to the coordinates of the rational solution to a linear system of equations), we may double the available bound k on $|\eta|$, compute one solution to (1.1), and either output it if $|\eta| < k/2$ or otherwise compute and output the other solution.

A related problem of *numerical rational number reconstruction* or *rational roundoff* is the problem of computing the best rational approximation s/t to a given rational n/m such that $1 \le t \le k$.

PROBLEM 1.2 (rational roundoff). *Compute all rational numbers s/t from three positive integers m, n, k such that*

$$1 \le t \le k, \quad |s/t - n/m| \text{ is minimal.} \tag{1.2}$$

*Received by the editors June 3, 2002; accepted for publication (in revised form) October 17, 2002; published electronically February 20, 2003. Some results of this paper were presented at ISSAC 2002; we are grateful to the ACM for the permission to reuse them.

http://www.siam.org/journals/sicomp/32-2/40863.html

†Ph.D. Program in Mathematics, Graduate School of CUNY, New York, NY 10016 (xwang2@gc.cuny.edu).

‡Department of Mathematics and Computer Science, Lehman College of CUNY, Bronx, NY 10468 (vpan@lehman.cuny.edu). This author's research was supported by NSF grant CCR 9732206 and PSC CUNY award 66383-0032.

Problem 1.2 is closely related to computing *Diophantine approximations* to a real number [HW60], [H82], [GG99] and extends the following problem.

Problem 1.2a (see [UP83]). *Given a rational number $\alpha = m/n$ and a natural number k, find a rational number p/q such that $1 \le q \le k$ and $|\alpha - p/q| < 1/(2k^2)$.*

Problem 1.2a may have no solution, but the solution is unique if it exists. In section 5, we show that the solution to Problem 1.2 is also unique.

Dirichlet [D1842] showed that, for any real numbers α and $0 < \epsilon \le 1$, there exist integers p and q such that $|\alpha - p/q| < \epsilon/q$ and $1 \le q \le \epsilon^{-1}$. In particular, let p_i/q_i be the ith *convergent* of α (i.e., the ith term in the continued fraction approximation for α); then $|\alpha - p_i/q_i| \le 1/(q_i q_{i+1}) < 1/q_i^2$ [HW60], [H82]. Furthermore, Hurwitz [H1891] showed that at least one of the two consecutive convergents of α satisfies $|\alpha - p/q| < 1/(2q^2)$, and at least one of the three consecutive convergents of α satisfies $|\alpha - p/q| < 1/(\sqrt{5}q^2)$. On the other hand, Legendre [L1798] showed that if $|\alpha - p/q| < 1/(2q^2)$, then p/q is a convergent of α. Therefore, Problems 1.2 and 1.2a are reduced to computing the convergents of α.

The common approach to the solution of the problems of modular and numerical rational number reconstruction is by applying the extended Euclidean algorithm to m and n [HW60]. Hereafter, we refer to this algorithm as the *EEA* and we seek faster solution algorithms based on accelerating the EEA. The algorithm produces a sequence of triples (r_j, s_j, t_j), $j = 1, \dots, l$ (notation used in [GG99]; see our Remark 2.10). In our case, we need only the triples $(r_{j-1}, s_{j-1}, t_{j-1})$ and (r_j, s_j, t_j) for a specially selected j. Extension from computing these triples to the solution to Problems 1.1 and 1.1a is shown in full detail in [GG99, Theorem 5.26]. We show an alternative approach, which is more directly related to our modification of the EEA. We also extend the known reduction of the Diophantine approximation to the EEA to solve Problem 1.2. Our main result, however, is the acceleration of the EEA and consequently the solution of all the listed problems. The known algorithms compute the desired pair of the EEA triples and thus solve Problems 1.1, 1.1a, 1.2, and 1.2a by using

$$f(d) = O(d^2)$$

bit operations, where $d = \lfloor \log_2 m \rfloor$, $m \ge n$. We speed up the computation by the factor of almost d; that is, we decrease the above bit cost bound to the level

$$\rho(d) = O(\mu(d) \log d), \tag{1.3}$$

provided that $\mu(d)$ bit operations are sufficient to multiply two integers modulo $2^d + 1$, and (see [SS71]) we have

$$\mu(d) = O((d \log d) \log \log d). \tag{1.4}$$

A similar acceleration is known for the Euclidean algorithm applied to polynomials [M73], [AHU74], [BGY80], but in the integer case a well-known additional difficulty is due to the carries. Among the known methods, only the Knuth–Schönhage algorithm [S71] has settled the problem for integers but only in the special case in which $j = l$ and the triple (r_l, s_l, t_l) terminates the Euclidean algorithm, that is, where r_l is the gcd. In our work, we were motivated by the following excerpt from [GG99, p. 305] on the EEA for integers:

> *The method also works for integers, although there are some complications due to the carries,*

and by the recent comments of expert Joachim von zur Gathen on the state of the art which he sent by email to one of the present authors:

> *Yes, I suppose rational number reconstruction can be done in time $O(m(n)\log n)$ for n-bit numbers and a given upper bound on the denominator. This is alluded to in* [GG99], *as you observed. But we do not give a proof, and I do not know any rigorous proof in the literature. I can imagine roughly what needs to be done, but it will be quite messy.*

In the next sections, we clear the cited mess and come out with a desired algorithm, which solves the gcd problem as a special case (see Remark 4.3(ii)). Our construction relies on computing a matrix sequence $\{Q_i,\ i = 0, 1, \dots\}$, which represents the quotients and cofactors computed in the EEA, rather than on computing just the remainder sequence $\{r_i,\ i = 0, 1, \dots\}$. This enables a simpler control over the growth of the magnitude of the entries of the Q_i than we would have had over the decrease of the r_i.

We organize our paper as follows. After some preliminaries in the next section, we prove our technical results on the EEA in section 3. In section 4, we present our main algorithm. In section 5, we apply it to accelerate the modular and numerical rational number reconstruction. Our proof of our main result is substantially simpler than in the proceedings version [PW02].

2. Some basic results. Hereafter, we write log to replace $\log_2$ unless specified otherwise.

DEFINITION 2.1. *$\mathbb{Z}$ is the ring of integers. $\lfloor x\rfloor$ and $\lceil x\rceil$ are two integers closest to a real number x such that $\lfloor x\rfloor \le x \le \lceil x\rceil$. $\{x\} = x - \lfloor x\rfloor$. $|A| = \max_{i,j}|a_{i,j}|$ for any real matrix $A = (a_{i,j})_{i,j}$. $m \bmod n$ is defined to be $m - n\lfloor m/n\rfloor$ for $m, n \in \mathbb{Z}$, and $n > 0$.*

ALGORITHM 2.2 (Euclidean algorithm).

INPUT: *A pair of natural numbers (m, n), $m \ge n$.*

OUTPUT: $\gcd(m, n)$.

COMPUTATION: *Write $r_0 = m$, $r_1 = n$. Compute*

$$r_{i+1} = r_{i-1} \bmod r_i$$

for $i = 1, 2, \dots, l$ until $r_{l+1} = 0$. Output r_l.

DEFINITION 2.3. *Let $\binom{r_{i-1}}{r_i} = P_i\binom{r_i}{r_{i+1}}$, where*

$$P_i = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}, \quad q_i = \lfloor r_{i-1}/r_i\rfloor, \quad i = 1, 2, \dots, l, \tag{2.1}$$

$$Q_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} = P_1P_2\cdots P_i, \quad i = 1, 2, \dots, l, \tag{2.2}$$

$$Q_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad Q_{l+1} = \begin{pmatrix} \infty & \infty \\ \infty & \infty \end{pmatrix}.$$

The sequence $\{r_i\}_{i=0}^{l}$ is called the remainder sequence*, and the sequence $\{Q_i\}_{i=0}^{l}$ is called the* matrix sequence*. The* extended Euclidean algorithm (EEA) *outputs both sequences $\{r_i\}_{i=0}^{l}$ and $\{Q_i\}_{i=0}^{l}$ (see Remark* 2.10*).*

For a given pair (m, n) and the sequence $\{Q_i\}$, we can immediately compute the sequence $\{r_i\}$ because

$$\det P_i = -1, \quad \det Q_i = (-1)^i, \tag{2.3}$$

$$\begin{pmatrix} m \\ n \end{pmatrix} = Q_i \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}, \quad Q_i^{-1} = (-1)^i \begin{pmatrix} d_i & -b_i \\ -c_i & a_i \end{pmatrix} \tag{2.4}$$

for all $i = 1, 2, \ldots, l$.

Our main task is to solve the following problem.

Problem 2.4 (selected output of the EEA).

Input: *Integers* m, n, h *such that* $m \geq n \geq 1$, $h \geq 0$.

Output: *The unique* Q_i *such that* $|Q_i| \leq 2^h < |Q_{i+1}|$.

In the remaining part of this section, we state some simple auxiliary properties of the remainders r_i and the matrices Q_i.

Theorem 2.5. $r_i > r_{i+1} > 0$, $r_i \geq r_{i+1} + r_{i+2}$ *for* $i = 0, 1, \ldots, l-1$.

Theorem 2.6 (cf. Definition 2.3 for a_i, b_i, c_i, q_i).

(i) $b_i = a_{i-1}$, $d_i = c_{i-1}$ *for* $i = 1, 2, \ldots, l$.

(ii) $a_i = a_{i-1}q_i + a_{i-2} > a_{i-1}$, $c_i = c_{i-1}q_i + c_{i-2} > c_{i-1}$ *for* $i = 2, 3, \ldots, l$.

(iii) $a_{i-2} = a_i \bmod a_{i-1}$, $c_{i-2} = c_i \bmod c_{i-1}$ *for* $i = 3, 4, \ldots, l$.

(iv) $a_0 > c_0$, $a_1 \geq c_1$, $a_i > c_i$ *for* $i = 2, 3, \ldots, l$.

Corollary 2.7. Q_{i-1} *can be computed from* Q_i *by Theorem* 2.6 (i), (iii).

Corollary 2.8.

(i) $|Q_i| = a_i$ *for* $i = 0, 1, \ldots, l$.

(ii) $|Q_i| \geq |Q_{i-1}| + |Q_{i-2}|$ *for* $i = 2, 3, \ldots, l$.

Corollary 2.9. $m/2 < r_i|Q_i| \leq m$ *for* $i = 0, 1, \ldots, l$.

Remark 2.10. Note an equivalent customary representation of the EEA's output by the sequences $\{r_i\}$, $\{s_i\}$, $\{t_i\}$ (with the notation in [GG99]), where $s_i = (-1)^i d_i$, $t_i = (-1)^{i-1} b_i$.

Remark 2.11. By Corollary 2.9, we have $|Q_i| \leq m$ for $i \leq l$, so it is sufficient to consider Problem 2.4 for $h \leq d+1$, $d = \lfloor \log m \rfloor$.

Remark 2.12. The remainder r_i defined by (2.4) for the solution Q_i of Problem 2.4 equals the gcd of m and n if and only if $Q_{i+1} = \left(\begin{smallmatrix} \infty & \infty \\ \infty & \infty \end{smallmatrix}\right)$, which is always the case for $h = d+1$.

3. The EEA for a modified input. To accelerate the solution of Problem 2.4, we apply the divide-and-conquer techniques. Roughly, the idea is to solve Problem 2.4 in two steps. In each step, Problem 2.4 is solved for h replaced by $\lfloor h/2 \rfloor$, and the output of the first step is used as the input of the second step. We are going to show that

(i) this leads to the same desired output, and

(ii) the computational cost of the reduction to the pair of half-size problems is small.

A basic observation is that the matrix sequence $\{Q_i\}$ depends only on the quotient m/n. That is, for another input values m^* and n^* such that $m^*/n^* = m/n$, the Euclidean algorithm computes the same matrices $Q_i^* = Q_i$ for all i. A relatively small perturbation of the quotient m/n should not affect the first several terms of the sequence $\{Q_i\}$, using which is enough to solve the problem for smaller h. That is, we may replace m and n by smaller integers m^* and n^* provided that $m^*/n^* \approx m/n$. For the input values m^* and n^*, we denote by $\{r_i^*\}$ the remainder sequence and by $\{Q_i^*\}$ the matrix sequence. Next, we specify some bounds on the allowed perturbations of m/n for which $Q_i = Q_i^*$ and then state our main theorem.

THEOREM 3.1. *Suppose $m^* = \lfloor m/\lambda \rfloor$ and $n^* = \lfloor n/\lambda \rfloor$ for a positive integer λ. For any given integer i, if*

$$r^*_{i+2} \geq |Q^*_{i+1}| \quad \text{or} \quad r_{i+2} \geq \lambda |Q_{i+1}|,$$

then $Q_i = Q^*_i$.

Proof. (i) Suppose $r^*_{i+2} \geq |Q^*_{i+1}|$. Write $\binom{u_j}{v_j} = Q^{*\,-1}_j \binom{m}{n}$ for $j = 0, 1, \dots, i+1$. Then we have

$$\begin{pmatrix} u_{j+1} \\ v_{j+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q^*_{j+1} \end{pmatrix} \begin{pmatrix} u_j \\ v_j \end{pmatrix}.$$

Therefore, $u_{j+1} = v_j$ for $j = 0, 1, \dots, i$. Furthermore, extending (2.4) to (m^*, n^*), we obtain that

$$\begin{pmatrix} r^*_j \\ r^*_{j+1} \end{pmatrix} = Q^{*\,-1}_j \begin{pmatrix} m^* \\ n^* \end{pmatrix},$$

$$\begin{pmatrix} u_j \\ v_j \end{pmatrix} = \begin{pmatrix} r^*_j \\ r^*_{j+1} \end{pmatrix} \lambda + Q^{*\,-1}_j \begin{pmatrix} m - m^*\lambda \\ n - n^*\lambda \end{pmatrix}.$$

By (2.4) we also know that, in each row of $Q^{*\,-1}_j$, one of the entries is nonnegative, and another is nonpositive, and their absolute values are bounded by $|Q^*_{j-1}|$ in the first row and by $|Q^*_j|$ in the second row. Therefore, we have

$$v_j > (r^*_{j+1} - |Q^*_j|)\lambda$$

and

$$u_j - v_j > (r^*_j - |Q^*_{j-1}|)\lambda - (r^*_{j+1} + |Q^*_j|)\lambda \geq (r^*_{j+2} - |Q^*_{j+1}|)\lambda.$$

So, by assumption, $u_j > v_j > 0$ for $j = 1, 2, \dots, i$. Now we have $u_0 = m$, $u_1 = n$, $u_{j+1} = u_{j-1} \bmod u_j$ for $j = 1, 2, \dots, i$. So $u_j = r_j$ and $Q_j = Q^*_j$ for $j = 0, 1, \dots, i$.

(ii) Suppose $r_{i+2} \geq \lambda |Q_{i+1}|$. Write $\binom{x_j}{y_j} = Q^{-1}_j \binom{m^*}{n^*}$ for $j = 0, 1, \dots, i+1$. Then we have

$$\begin{pmatrix} x_{j+1} \\ y_{j+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{j+1} \end{pmatrix} \begin{pmatrix} x_j \\ y_j \end{pmatrix}.$$

Therefore, $x_{j+1} = y_j$ for $j = 0, 1, \dots, i$. Furthermore, by (2.4), we extend the above expression for x_j and y_j as follows:

$$\begin{pmatrix} x_j \\ y_j \end{pmatrix} = \begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix} \lambda^{-1} - Q^{-1}_j \begin{pmatrix} m/\lambda - m^* \\ n/\lambda - n^* \end{pmatrix}.$$

Now, similarly as in part (i), we deduce that $y_j > r_{j+1}\lambda^{-1} - |Q_j|$ and $x_j - y_j > (r_j\lambda^{-1} - |Q_{j-1}|) - (r_{j+1}\lambda^{-1} + |Q_j|) \geq (r_{j+2}\lambda^{-1} - |Q_{j+1}|)$. So, by assumption, $x_j > y_j > 0$ for $j = 1, 2, \dots, i$. Now we have $x_0 = m^*$, $x_1 = n^*$, $x_{j+1} = x_{j-1} \bmod x_j$ for $j = 1, 2, \dots, i$. So $x_j = r^*_j$ and $Q_j = Q^*_j$ for $j = 0, 1, \dots, i$. $\square$

COROLLARY 3.2. *Suppose $m^* = \lfloor m/\lambda \rfloor$, $n^* = \lfloor n/\lambda \rfloor$ for a positive integer λ. For any given integer i, if*

$$m^* \geq 2|Q^*_{i+2}| \cdot |Q^*_{i+1}| \quad \text{or} \quad m \geq 2\lambda |Q_{i+2}| \cdot |Q_{i+1}|,$$

then $Q_i = Q_i^*$.

Proof. Combine the assumed bound on m^* and m with the first inequality of Corollary 2.9 extended also to m^*, r_i^*, Q_i^*, and arrive at the bounds on r_{i+2}^* and r_{i+2} in Theorem 3.1. ∎

THEOREM 3.3 (main theorem). *Suppose* $m^* = \lfloor m/\lambda \rfloor$, $n^* = \lfloor n/\lambda \rfloor$ *for a positive integer* λ, *and* K *is a given positive integer such that* $m^* \geq 2K^2$. *If* $|Q_i^*| \leq K < |Q_{i+1}^*|$, *then* $Q_j = Q_j^*$ *for all* $j \leq i-2$ *and* $|Q_j| \leq K < |Q_{j+1}|$ *for some* j *such that* $i-2 \leq j \leq i+2$.

Proof. By Corollary 3.2, we have $Q_j = Q_j^*$ for $j \leq i-2$. If $|Q_{i+3}| > K$, then we are done. Otherwise, we have $m \geq \lambda m^* \geq 2\lambda K^2 \geq 2\lambda |Q_{i+3}|^2$. By applying Corollary 3.2 again, we obtain $Q_{i+1} = Q_{i+1}^*$, $Q_i = Q_i$. ∎

4. Our main algorithm.

ALGORITHM 4.1 (selected output of the EEA).

INPUT: *A triple of integers* (m, n, h) *such that* $m \geq n > 0, h \geq 0$.

OUTPUT: *The unique matrix* Q_k *such that* $|Q_k| \leq 2^h < |Q_{k+1}|$.

COMPUTATION: *Let* $d = \lfloor \log m \rfloor$.

1. *When* $h \leq \lfloor d/2 \rfloor - 1$, *let* $\lambda = 2^{d-2h-1}$, $m^* = \lfloor m/\lambda \rfloor$, *and* $n^* = \lfloor n/\lambda \rfloor$; *then* $2^{2h+1} \leq m^* \leq m/2$. *We first apply the algorithm to the input* (m^*, n^*, h) *and have the output* Q_i^*. *Theorem* 3.3 *for* $K = 2^h$ *implies that* $Q_{i-2} = Q_{i-2}^*$ *and* $|Q_k| \leq 2^h < |Q_{k+1}|$ *for some* $i-2 \leq k \leq i+2$. *We may compute* $Q_{i-2} = Q_{i-2}^*$ *from* Q_i^* *(cf. Corollary* 2.7*) and then find* Q_k *in a few Euclidean steps.*
2. *When* $\lfloor d/2 \rfloor \leq h \leq d-1$, *we first apply the algorithm to find* $|Q_i| \leq 2^{\lfloor h/2 \rfloor} < |Q_{i+1}|$. *Next we apply the algorithm again for the input* $(r_i, r_{i+1}, \lfloor h/2 \rfloor)$ *and have the output* $\tilde{Q}_j$. *Now we have* $Q_{i+j} = Q_i \tilde{Q}_j$, $|Q_{i+j}| < 2^{h+1}$, *and* $|Q_{i+j+2}| > 2^{h-1}$. *Then* $|Q_k| \leq 2^h < |Q_{k+1}|$ *for some* $i+j-2 \leq k \leq i+j+2$, *and we may find* Q_k *in a few Euclidean steps.*
3. *When* $h \geq d$, *we first apply the algorithm to find* $|Q_i| \leq 2^{d-1} < |Q_{i+1}|$. *Then* $|Q_k| \leq 2^h < |Q_{k+1}|$ *for some* $i \leq k \leq i+4$, *and we may find* Q_k *in a few Euclidean steps.*

THEOREM 4.2. *Let* $f(d, h)$ *be the bit cost of performing Algorithm* 4.1 *for the input* (m, n, h), *where* $d = \lfloor \log m \rfloor$. *Then we have*

$$f(d, h) = O(\mu(d) \log h)$$

for μ *in* (1.4).

Proof. By inspection of the algorithm, we have

$$f(d,h) = \begin{cases} f(2h+1, h) + O(\mu(d)) & \text{if } h \leq \lfloor \frac{d}{2} \rfloor - 1, \\ f(d, \lfloor \frac{h}{2} \rfloor) + f(d - \lfloor \frac{h}{2} \rfloor, \lfloor \frac{h}{2} \rfloor) + O(\mu(d)) & \\ & \text{if } \lfloor \frac{d}{2} \rfloor \leq h \leq d-1, \\ f(d, d-1) + O(\mu(d)) & \text{if } h \geq d. \end{cases}$$

Let us write $F(h) = f(2h+1, h)$. Then

$$F(h) = 2F(\lfloor h/2 \rfloor) + O(\mu(2h)),$$

and we obtain that

$$F(h) = O(\mu(2h) \log h).$$

By recursively combining this bound with the above expressions for $f(d,h)$, we obtain

$$f(d,h) = \sum_{i=1}^{1+\lfloor \log h \rfloor} (F(\lfloor h/2^i \rfloor) + O(\mu(d))) = O(\mu(d)\log h). \qquad \square$$

Remark 4.3.

(i) We may easily extend Algorithm 4.1 to compute the matrix Q_i (at the bit cost $O(\mu(d)\log\log K)$), such that $|Q_i| \le K < |Q_{i+1}|$ for any real $K \ge 1$, not just for $K = 2^h$.

(ii) Due to Remark 2.12, we may also easily extend Algorithm 4.1 to find the remainder r_i (at the bit cost $O(\mu(d)\log\log(m/K))$, such that $r_i \ge K > r_{i+1}$ for any real $1 \le K \le m$. By choosing $K = 1$, we compute $r_i = \gcd(m,n)$.

5. Applications to rational number reconstruction. Let us next extend Algorithm 4.1 to solve Problems 1.1, 1.1a, 1.2, and 1.2a of rational number reconstruction.

Solution of Problems 1.1 *and* 1.1a. Note that (cf. (2.4))

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = Q_i^{-1} \begin{pmatrix} m \\ n \end{pmatrix} = (-1)^i \begin{pmatrix} d_i & -b_i \\ -c_i & a_i \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}.$$

Therefore,

$$(-1)^i r_{i+1} = n a_i \bmod m \text{ for all } i.$$

Let i be such that $a_i \le m/k < a_{i+1}$.

1. Since $a_i \le m/k$ and $r_{i+1} \le \frac{m}{a_{i+1}} < k$, we obtain a solution $\big((-1)^i r_{i+1},\ a_i\big)$ to Problem 1.1.
2. Suppose Problem 1.1a has a solution (η,δ) such that $\eta/\delta = (-1)^i r_{i+1}/a_i$; then $(\eta,\delta) = \big((-1)^i r_{i+1},\ a_i\big)$ and $\gcd(r_{i+1}, a_i) = 1$. Indeed, a_i divides δ because $\frac{n\delta-\eta}{m} = \frac{c_i\delta}{a_i} \in \mathbb{Z}$ and $\gcd(a_i, c_i) = 1$.
3. Suppose Problem 1.1a has a solution such that $\eta/\delta \ne (-1)^i r_{i+1}/a_i$. Then the solution is unique. (Indeed, it follows from $a_i\eta - (-1)^i r_{i+1}\delta = 0 \bmod m$ that $a_i(-1)^{i-1}\eta + r_{i+1}\delta = m$ and $(-1)^{i-1}\eta \ge 0$. Furthermore, if there are two such solutions (η_1,δ_1) and (η_2,δ_2), then $\eta_1\delta_2 - \eta_2\delta_1 = 0 \bmod m$. So $\eta_1\delta_2 - \delta_1\eta_2$ equals $0, m$, or $-m$. Combine $(-1)^{i-1}\eta_1 \ge 0$ and $(-1)^{i-1}\eta_2 \ge 0$ to deduce that only $\eta_1\delta_2 - \eta_2\delta_1 = 0$ can hold.) Since $m = a_i r_i + r_{i+1} a_{i-1}$ by (2.4), we have $((-1)^{i-1}\eta - r_i)a_i = (a_{i-1} - \delta) r_{i+1}$. Therefore, $(\eta,\delta) = \big((-1)^{i-1}(r_i - t r_{i+1}),\ a_{i-1} + t a_i\big)$ for a real t. Note that $a_{i-1} + t a_i \in \mathbb{Z}$, $\frac{n\delta-\eta}{m} = c_{i-1} + t c_i \in \mathbb{Z}$, and $\gcd(a_i, c_i) = 1$, and so $t \in \mathbb{Z}$. If $r_i < k$, then $(\eta,\delta) = \big((-1)^{i-1} r_i,\ a_{i-1}\big)$ defines the unique solution. If $r_i \ge k$, then by applying the inequalities $|\eta| < k$ and $\delta \le m/k$, we obtain $\frac{r_i - k}{r_{i+1}} < t \le \frac{m/k - a_{i-1}}{a_i}$. Therefore, the unique solution must be defined by the unique integer t in the interval $\big(\frac{r_i-k}{r_{i+1}}, \frac{m/k - a_{i-1}}{a_i}\big]$. $\square$

COROLLARY 5.1. *Problems* 1.1 *and* 1.1a *of modular rational number reconstruction can be solved by using $\rho(d)$ bit operations for ρ in* (1.3).

Solution of Problems 1.2 *and* 1.2a. Recall that c_i/a_i is the ith continued fraction approximation of n/m, and $|\frac{c_i}{a_i} - \frac{n}{m}| < |\frac{s}{t} - \frac{n}{m}|$ for all i, s, t, where $1 \le t < a_i$ (see [HW60, Theorem 181]). In particular, $|\frac{c_i}{a_i} - \frac{n}{m}| < |\frac{c_{i-1}}{a_{i-1}} - \frac{n}{m}|$ for all i. Let i be such that $a_i \le k < a_{i+1}$. Suppose

$$|\tfrac{s}{t} - \tfrac{n}{m}| \le |\tfrac{c_i}{a_i} - \tfrac{n}{m}|, \quad a_i < t \le k.$$

Then

$$\begin{aligned} & |\tfrac{c_i}{a_i} - \tfrac{s}{t}| \le 2|\tfrac{c_i}{a_i} - \tfrac{n}{m}| = \tfrac{2r_{i+1}}{a_i m} < \tfrac{2}{a_i k} \\ \Longrightarrow\quad & |c_i t - a_i s| < \tfrac{2t}{k} \le 2 \\ \Longrightarrow\quad & |c_i t - a_i s| = 1 = |c_i a_{i-1} - a_i c_{i-1}| \\ \Longrightarrow\quad & (s,t) = (c_i,\ a_i)\tau \pm (c_{i-1},\ a_{i-1}) \end{aligned}$$

for a real τ. Since $t > a_i > a_{i-1}$ and $tc_{i-1} - sa_{i-1} = (a_i c_{i-1} - c_i a_{i-1})\tau = (-1)^i \tau$, τ is a positive integer. Furthermore, observe that $\frac{c_i}{a_i} - \frac{n}{m} = \frac{(-1)^{i+1} r_{i+1}}{a_i m}$ and $\frac{c_{i-1}}{a_{i-1}} - \frac{n}{m} = \frac{(-1)^i r_i}{a_{i-1} m}$ have opposite signs, and recall that $|\frac{s}{t} - \frac{n}{m}| \le |\frac{c_i}{a_i} - \frac{n}{m}| < |\frac{c_{i-1}}{a_{i-1}} - \frac{n}{m}|$, so $(s,t) = \tau(c_i,\ a_i) + (c_{i-1},\ a_{i-1})$. Therefore, (s,t) is the unique solution to Problem 1.2 for $\tau = \lfloor \frac{k - a_{i-1}}{a_i} \rfloor$. □

COROLLARY 5.2. *Problems* 1.2 *and* 1.2a *of rational roundoff can be solved by using* $\rho(d)$ *bit operations for* ρ *in* (1.3).

Acknowledgment. We are grateful to Joachim von zur Gathen for his expert advice on the state of the art of the bit complexity of rational number reconstruction and for his helpful comments on the original draft of our paper.

REFERENCES

[AHU74] A. V. AHO, J. E. HOPCROFT, AND J. D. ULLMAN, *The Design and Analysis of Computer Algorithms*, Addison–Wesley, Reading, MA, 1974.

[BGY80] R. P. BRENT, F. G. GUSTAVSON, AND D. Y. Y. YUN, *Fast solution of Toeplitz systems of equations and computation of Padé approximations*, J. Algorithms, 1 (1980), pp. 259–295.

[D1842] G. LEJEUNE DIRICHLET, *Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen*, in Bericht über die zur Bekanntmachung geeigneten Verhandlungen der Königlich Preussischen Akademie der Wissenschaften zu Berlin, 1842, pp. 93–95 (reprinted in *G. Lejeune Dirichlet's Werke, Vol.* I, L. Kronecher, ed., G. Reimer, Berlin, 1889, pp. 635–638 (reprinted: Chelsea, New York, 1969)).

[D82] J. D. DIXON, *Exact solution of linear equations using p-adic expansions*, Numer. Math., 40 (1982), pp. 137–141.

[GG99] J. VON ZUR GATHEN AND J. GERHARD, *Modern Computer Algebra*, Cambridge University Press, Cambridge, UK, 1999.

[H82] L. K. HUA, *Introduction to Number Theory*, Springer-Verlag, Berlin, 1982.

[H1891] A. HURWITZ, *Ueber die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche*, Math. Ann., 39 (1891), pp. 279–284 (reprinted in Mathematische Werke von Adolf Hurwitz, Zweiter Band, Birkhäuser, Basel, 1963, pp. 122–128).

[HW60] G. H. HARDY AND E. M. WRIGHT, *An Introduction to the Theory of Numbers*, 4th ed., Clarendon Press, Oxford, UK, 1960.

[L1798] A. M. LEGENDRE, *Essai sur la théorie des nombres*, J. B. M. Duprat, Paris, 1798 (4th edition reprinted: *Théorie des nombres*, A. Blanchard, Paris, 1979).

[M73] R. MOENCK, *Fast computation of GCDs*, in Proceedings of 5th ACM Annual Symposium on Theory of Computing, ACM, New York, 1973, pp. 142–171.

[MC79] R. T. MOENCK AND J. H. CARTER, *Approximate algorithms to derive exact solutions to systems of linear equations*, in Proceedings of EUROSAM, Lecture Notes in Comput. Sci. 72, Springer-Verlag, Berlin, 1979, pp. 63–73.

[P02] V. Y. PAN, *Can we optimize Toeplitz/Hankel computations?*, in Proceedings of the Fifth International Workshop on Computer Algebra in Scientific Computing (CASC 2002, Yalta, Ukraine), V. G. Ganzha, E. W. Mayr, and E. V. Vorozhzov, eds., Institut fuer Informatik, Technische Universitaet Muenchen, Garching, Germany, 2002, pp. 253–264.

[PW02] V. Y. PAN AND X. WANG, *Acceleration of Euclidean algorithm and extensions*, in Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, T. Mora, ed., ACM, New York, 2002, pp. 207–213.

[S71] A. Schönhage, *Schnelle Berechnung von Kettenbruchentwicklungen*, Acta Inform., 1 (1971), pp. 139–144.

[S86] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley, New York, 1986.

[SS71] A. Schönhage and V. Strassen, *Schnelle Multiplikation grosse Zahlen*, Computing, 7 (1971), pp. 281–292.

[UP83] S. Ursic and C. Patarra, *Exact solution of systems of linear equations with iterative methods*, SIAM J. Algebraic Discrete Methods, 4 (1983), pp. 111–115.

[Z93] R. E. Zippel, *Effective Polynomial Computation*, Kluwer Academic Publishers, Norwell, MA, 1993.