PACIFIC JOURNAL OF MATHEMATICS
Vol. 78, No. 1, 1978

INTEGER MULTIPLES OF PERIODIC CONTINUED FRACTIONS

T. W. CUSICK

This paper contains much simpler proofs of the results of Henri Cohen (Acta Arithmetica 26 (1974–75), 129–148) on the period length of the continued fraction for $N\alpha$, where N is a positive integer and α is a quadratic irrational.

1. Introduction. We let $[a_0, a_1, \cdots]$ denote the simple continued fraction whose partial quotients are the integers a_i ($a_i > 0$ for $i > 0$). If α is a quadratic irrational, so that α has a periodic continued fraction, then we put

$$\alpha = [b_0, b_1, \cdots, b_m, \overline{a_1, \cdots, a_n}] ,$$

where $b_0, b_1, \cdots, b_m$ is the nonperiodic part of the continued fraction and $a_1, \cdots, a_n$ is the period. We let $P(\alpha) = n$ denote the length of the period of the expansion of α.

H. Cohen [2] defined the functions

$$S(N, n) = \sup_{P(\alpha)=n} P(N\alpha)$$

for each pair of integers $N > 1$, $n \geqq 1$. The fact that $S(N, n)$ is always finite was already known (see Schinzel [4]).

Let A denote the set of all real quadratic irrationals. Cohen defined the function

$$R(N) = \sup_{n \geqq 1} (S(N, n)/n) = \sup_{\alpha \in A} (P(N\alpha)/P(\alpha))$$

for each integer $N > 1$, and proved that $R(N)$ is always finite. The paper of Cohen [2] is devoted to proving various results about $S(N, n)$ and $R(N)$. In particular, Cohen [2, pp. 141–147] obtained the exact value of $R(N)$ for infinitely many N and gave a conjecture for the value of $R(N)$ in all the remaining cases.

Cohen made use of an algorithm given by Mendès France [3] for computing the continued fraction expansion of $N\alpha$ from the expansion of α, where α is any real number. Cohen [2, §§3 and 4, pp. 132–137] devotes considerable space to showing that if one wants to use the algorithm of Mendès France [3] in order to study $P(N\alpha)$ for quadratic irrationals α, then one needs various facts about 2 by 2 matrices with integer entries taken mod N.

It turns out that the algorithm of Mendès France [3] was already given by A. Châtelet [1] in a different but equivalent form. The

Châtelet formulation of the algorithm has a great advantage as far as the application to the problems considered by Cohen is concerned; namely, in the Châtelet version the algorithm is defined in terms of 2 by 2 matrices with integer entries, so the relevance of these matrices is immediately apparent. We show below that the results of Cohen concerning the functions $S(N, n)$ and $R(N)$ can all be obtained much more simply by using the approach of Châtelet [1].

2. **The Chatelet algorithm.** For the convenience of the reader, we give an exposition of the algorithm of Châtelet [1]. Proofs (all of which are elementary) are omitted; they are given by Châtelet [1].

We suppose that $\alpha = [a_0, a_1, a_2, \cdots]$ is a real number and that $N > 1$ is an integer. We wish to determine the partial quotients of the continued fraction for $N\alpha$. We suppose for simplicity that infinitely many of the a_i are $> N$ (Châtelet [1, p. 12] considers only this situation). We may make this supposition with no loss of generality because $S(N, n)$ depends only on the a_i taken mod N (this is easily verified; see Cohen [2, p. 132]).

We first need the following lemma of Châtelet [1, p. 7] on matrix factorization. We use the abbreviated notation (a) defined for each integer $a \geqq 0$ by

$$(a) = \begin{bmatrix} a & 1 \\ 1 & 0 \end{bmatrix};$$

this notation was also employed by Châtelet.

LEMMA 1. *Any matrix*

$$\begin{bmatrix} P & Q \\ R & S \end{bmatrix}, \qquad PS - QR = \pm 1$$

with nonnegative integer entries at least three of which are positive can be written in one of the four forms

$$A\,, \qquad (0)A\,, \qquad A(0)\,, \qquad (0)A(0)$$

where the matrix A is given by

$$A = \prod_{i=1}^{n} (u_i)\,, \qquad u_i \geqq 1 \quad \textit{for} \quad 1 \leqq i \leqq n\,.$$

If $P > Q > S$ and $P > R > S$, then the integers u_i in the factorization of Lemma 1 are just the successive partial quotients in the continued fraction for P/R (we need only take care that the

number of partial quotients is even or odd, as required, by letting the last partial quotient be 1 if necessary). For example,

$$\begin{bmatrix} 27 & 19 \\ 10 & 7 \end{bmatrix} = (2)(1)(2)(2)(1) .$$

The same kind of calculation applies if $P > Q > S$ and $P > R > S$ do not both hold.

Before continuing, we need the following lemma of Châtelet [1, pp. 12-15].

LEMMA 2. *Suppose δ and d are any positive integers such that $\delta d = N$, and suppose k is any integer such that $0 \leqq k < d$. Given any matrix*

$$\begin{bmatrix} P & Q \\ R & S \end{bmatrix}, \qquad PS - QR = \pm 1 , \qquad \frac{P}{R} \geqq N - 1 , \qquad \frac{Q}{S} \geqq N - 1$$

with nonnegative integer entries, there exist unique nonnegative integers A, B, C, D, δ_1 and d_1 with $\delta_1 d_1 = N$ and a unique integer k_1 with $0 \leqq k_1 < d_1$, such that the following matrix identity holds:

$$\begin{bmatrix} \delta & -k \\ 0 & d \end{bmatrix} \begin{bmatrix} P & Q \\ R & S \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} \delta_1 & -k_1 \\ 0 & d_1 \end{bmatrix} . \tag{1}$$

The integers A, B, C, D are determined by

$$A = \delta_1^{-1}(\delta P - kR) , \qquad B = N^{-1}((\delta P - kR)k_1 + (\delta Q - kS)\delta_1) ,$$
$$C = dR\delta_1^{-1} , \qquad D = dN^{-1}(k_1 R + \delta_1 S) .$$

The integers δ_1, d_1 and k_1 are determined by the conditions $\delta_1 d_1 = N$, $0 \leqq k_1 < d_1$ and

$$\delta_1 = (\delta P - kR, d\mu) \quad \text{where} \quad \mu = (\delta, R) ,$$
$$k_1 R + \delta_1 S \equiv 0 \mod \delta ,$$
$$k_1(\delta P - kR) + \delta_1(\delta Q - kS) \equiv 0 \mod N .$$

Later on we shall mainly be interested in the following corollary, which is proved by taking $P = a$, $Q = R = 1$, $S = 0$ in Lemma 2.

COROLLARY. *Suppose δ and d are any positive integers such that $\delta d = N$, and suppose k is any integer such that $0 \leqq k < d$. Given any integer $a \geqq N - 1$, there exist unique nonnegative integers A, B, C, D, δ_1 and d_1 with $\delta_1 d_1 = N$ and a unique integer k_1 with $0 \leqq k_1 < d_1$ such that the following matrix identity holds:*

$$\begin{bmatrix} \delta & -k \\ 0 & d \end{bmatrix}\begin{bmatrix} a & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix}\begin{bmatrix} \delta_1 & -k_1 \\ 0 & d_1 \end{bmatrix}.$$

The integers A, B, C, D are determined by

$$A = \delta_1^{-1}(\delta a - k), \qquad B = N^{-1}((\delta a - k)k_1 + \delta\delta_1),$$
$$C = d\delta_1^{-1}, \qquad D = dN^{-1}k_1.$$

The integers δ_1, d_1 and k_1 are determined by the conditions $\delta_1 d_1 = N$, $0 \leqq k_1 < d_1$ and

$$\delta_1 = (\delta a - k, d)$$
$$k_1 \equiv 0 \mod \delta$$
$$-\frac{k_1}{\delta}\left(\frac{\delta a - k}{\delta_1}\right) \equiv 1 \mod \left(\frac{N}{\delta\delta_1}\right).$$

Now we can describe the algorithm for finding the partial quotients of $N\alpha$, as follows: We divide the partial quotients $a_0, a_1, \cdots$ of α into blocks, each of which begins with an $a_i > N$ followed by other a_i's which are $\leqq N$ (we can assume $a_0 > N$ without loss of generality). We denote the ith block by

$$b_1^{(i)}, b_2^{(i)}, \cdots, b_{n(i)}^{(i)}, \quad \text{so} \quad b_1^{(i)} > N \quad \text{and} \quad b_j^{(i)} \leqq N \quad \text{for} \quad 2 \leqq j \leqq n(i).$$

For each block, we compute the matrix product $(b_1^{(i)})(b_2^{(i)}) \cdots (b_{n(i)}^{(i)})$ and define

$$(b_1^{(i)})(b_2^{(i)}) \cdots (b_{n(i)}^{(i)}) = \begin{bmatrix} P_i & Q_i \\ R_i & S_i \end{bmatrix} \qquad (i = 1, 2, \cdots).$$

Starting with $\delta = N$, $d = 1$, $k = 0$ in Lemma 2, we use (1) to define successively integers A_i, B_i, C_i, D_i, δ_i, d_i and k_i $(i = 1, 2, \cdots)$, as follows:

$$(2)\qquad \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} P_1 & Q_1 \\ R_1 & S_1 \end{bmatrix} = \begin{bmatrix} A_1 & B_1 \\ C_1 & D_1 \end{bmatrix}\begin{bmatrix} \delta_1 & -k_1 \\ 0 & d_1 \end{bmatrix}$$
$$\begin{bmatrix} \delta_1 & -k_1 \\ 0 & d_1 \end{bmatrix}\begin{bmatrix} P_2 & Q_2 \\ R_2 & S_2 \end{bmatrix} = \begin{bmatrix} A_2 & B_2 \\ C_2 & D_2 \end{bmatrix}\begin{bmatrix} \delta_2 & -k_2 \\ 0 & d_2 \end{bmatrix}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\begin{bmatrix} \delta_{i-1} & -k_{i-1} \\ 0 & d_{i-1} \end{bmatrix}\begin{bmatrix} P_i & Q_i \\ R_i & S_i \end{bmatrix} = \begin{bmatrix} A_i & B_i \\ C_i & D_i \end{bmatrix}\begin{bmatrix} \delta_i & -k_i \\ 0 & d_i \end{bmatrix}.$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

In this way we obtain a sequence of matrices M_i with entries A_i, B_i, C_i, D_i. By Lemma 1, we can factor each of these matrices M_i as follows:

$$(3)\quad M_i = (u_1^{(i)})(u_2^{(i)}) \cdots (u_{n(i)}^{(i)}), \quad u_j^{(i)} \geqq 0, \quad u_j^{(i)} > 0 \quad \text{if} \quad 1 < j < n(i).$$

Thus we obtain a sequence of nonnegative integers

$$(4) \qquad u_1^{(1)}, \cdots, u_{n(1)}^{(1)}, u_1^{(2)}, \cdots, u_{n(2)}^{(2)}, \cdots, u_1^{(i)}, \cdots, u_{n(i)}^{(i)}, \cdots .$$

We modify this sequence, if necessary, by replacing every triple a, 0, b by the single integer $a + b$, and repeating this until a sequence of only positive integers is obtained. This new sequence is precisely the sequence of partial quotients for $N\alpha$.

REMARK. In the discussion of this algorithm given by Mendès France [3], the sequence corresponding to (4) may contain some members equal to -1 in addition to some members equal to 0. This is because Mendès France does not make the simplifying assumption that infinitely many of the partial quotients a_i of α are $>N$, as we did at the beginning of this section.

From now on, it will be convenient to make the following even stronger

ASSUMPTION. Suppose that all of the partial quotients of $\alpha = [a_0, a_1, \cdots]$ satisfy $a_i \geqq 2N$.

As we remarked earlier, this assumption can be made with no loss of generality in the study of the functions $S(N, n)$ and $R(N)$.

The assumption means that the blocks of partial quotients mentioned above are all of length one, so in (2) we have $P_i = a_{i-1}$, $Q_i = R_i = 1$, $S_i = 0$ for $i = 1, 2, \cdots$. Also, by Lemma 2 Corollary, the integers δ_i, d_i, k_i in (2) are determined recursively as follows:

$$(5) \qquad \delta_0 = N, \qquad d_0 = 1, \qquad k_0 = 0;$$

$$(6) \qquad \delta_i = (\delta_{i-1}a_{i-1} - k_{i-1}, d_{i-1}) \quad \text{for} \quad i \geqq 1;$$

$$(7) \qquad k_i \equiv 0 \mod \delta_{i-1} \quad \text{for} \quad i \geqq 1;$$

$$(8) \qquad -\frac{k_i}{\delta_{i-1}}\left(\frac{\delta_{i-1}a_{i-1} - k_{i-1}}{\delta_i}\right) \equiv 1 \mod \frac{N}{\delta_{i-1}\delta_i} \quad \text{for} \quad i \geqq 1.$$

In view of (7), we can define integers t_i ($i = 1, 2, \cdots$) by

$$(9) \qquad k_i = \delta_{i-1}t_i .$$

Under our assumption, it is a simple matter to verify that the algorithm described by Cohen [2, §2] is the same as the Châtelet algorithm described above. The formulas (5), (6), (7), (8) above correspond to Cohen [2, formulas (1), p. 130]. Cohen's δ_i corresponds to δ_{i+1} above, Cohen's d_i corresponds to d_i above, Cohen's c_i corresponds to $\delta_i a_i - k_i$ and Cohen's $(c_i/\delta_i)^{-1}$ corresponds to $-t_{i+1}$ defined in (9).

We close this section with the following lemma, which we need later on.

LEMMA 3. *In the sequence of identities* (2), *we have* $(\delta_{i-1}, \delta_i) = 1$ *for each* $i = 1, 2, \cdots$.

Proof. Suppose that for some i, a prime p divides (δ_{i-1}, δ_i). Then by (6) p divides $\delta_{i-1}a_{i-1} - k_{i-1}$, so p divides $k_{i-1} = \delta_{i-2}t_{i-1}$. Hence either p divides δ_{i-2} or p divides t_{i-1}. But in the latter case we have p divides $N\delta_{i-1}^{-1} = d_{i-1}$ (from (6)) and $(t_{i-1}, N(\delta_{i-1}\delta_{i-2})^{-1}) = 1$ (from (8) and (9)), so that p divides δ_{i-2} also. Hence if p divides (δ_{i-1}, δ_i), then p divides δ_j for every $j \leqq i$; but this is a contradiction, since $\delta_1 = 1$ by (5) and (6).

3. **Upper bounds for $S(N, n)$ and $R(N)$.** In this section we use our previous work to give a much simpler proof of certain upper bounds on $S(N, n)$ and $R(N)$ given by Cohen [2, Theorem 4.3, p. 136].

For each rational number $x = [a_0, a_1, \cdots, a_n]$, $a_n \geqq 2$, we use Cohen's [2, p. 129] notation $L(x)$ to denote the number of partial quotients in that continued fraction expansion of x which has an *odd* number of partial quotients; thus $L(x) = n + 1$ if n is even and $L(x) = n + 2$ if n is odd.

Now suppose $N > 1$ is a given integer and

$$\alpha = [b_0, b_1, \cdots, b_m, \overline{c_1, \cdots, c_n}] = [a_0, a_1, a_2, \cdots] \tag{10}$$

is a given quadratic irrational for which the Assumption of §2 holds. It is easily verified that the Assumption implies that $A_i > B_i > D_i$ and $A_i > C_i > D_i$ for each matrix M_i $(i = 1, 2, \cdots)$ in (2). Hence (see the remarks after Lemma 1) in the factorization (3) of M_i each $u_j^{(i)}$ is positive, so the unmodified sequence (4) is the sequence of partial quotients of $N\alpha$. In fact, the sequence (4) is just the sequences of partial quotients of the rational numbers A_i/C_i $(i = 1, 2, \cdots)$ taken in order, where the continued fraction expansion used for each A_i/C_i is the one with an odd number of partial quotients (this is because the determinant of each M_i is -1, so the corresponding factorization given by Lemma 1 has an odd number of matrices).

In is clear from the work of §2 that the sequence of triples (a_i, k_i, d_i) $(i = 0, 1, 2, \cdots)$ is eventually periodic, and thus the sequence of rational numbers A_i/C_i $(i=1, 2, \cdots)$ is also eventually periodic. Say $A_{m+1}/C_{m+1}, \cdots, A_{m+r}/C_{m+r}$ is the period of the latter; then the length of the period of $N\alpha$ is given by

$$P(N\alpha) = \sum_{i=1}^{r} L(A_{m+i}/C_{m+i}) . \tag{11}$$

Our next lemma shows that $P(N\alpha)$ can also be expressed in terms of $L(k_i/d_i)$.

LEMMA 4. *Suppose p and q are two relatively prime positive integers. Define p^*, $0 < p^* < q$, by $pp^* \equiv -1 \bmod q$. Then $L(p/q) = L(p^*/q)$.*

Proof. We assume $p < q$ with no loss of generality. Let $p/q = [0, f_1, \cdots, f_n]$, $f_n \geqq 2$, and define $p_i/q_i = [0, f_1, \cdots, f_i]$ for $1 \leqq i \leqq n$. First suppose that $p/q < 1/2$. We have $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$, so $pq_{n-1} \equiv (-1)^{n-1} \bmod q$. Thus if n is even, then $q_{n-1} = p^*$. But

$$\frac{q_{n-1}}{q} = [0, f_n, f_{n-1}, \cdots, f_1] \tag{12}$$

so $L(p/q) = L(p^*/q)$ if n is even.

Now define p', $0 < p' < q$, by $pp' \equiv 1 \bmod q$ (so $p' + p^* = q$). It is easy to see that $p'/q < 1/2$ if and only if n is odd. Thus when n is odd we have $p' = q_{n-1}$, so by (12)

$$\frac{p^*}{q} = 1 - \frac{q_{n-1}}{q} = [0, 1, f_n - 1, f_{n-1}, \cdots, f_1] .$$

Hence $L(p/q) = L(p^*/q) = n + 2$. Similar arguments take care of the case $p/q > 1/2$, so the lemma is proved.

COROLLARY. *For each $i = 1, 2, \cdots$, $L(A_i/C_i) = L(k_i/d_i)$.*

Proof. We take $p = (\delta_{i-1} a_{i-1} - k_{i-1})\delta_i^{-1} = A_i$ and $q = N(\delta_{i-1}\delta_i)^{-1} = C_i$. Then $p^* = k_i \delta_{i-1}^{-1}$ by (8) and $p^*/q = k_i/d_i$, so the corollary follows from the lemma.

It follows from Lemma 4 Corollary and (11) that

$$P(N\alpha) = \sum_{i=1}^{r} L(k_{m+i}/d_{m+i}) . \tag{13}$$

We have from (8) and (9)

$$\frac{k_i}{d_i} = \frac{\delta_{i-1} t_i}{N/\delta_i} = \frac{t_i}{N(\delta_{i-1}\delta_i)^{-1}} \quad \text{where} \quad \left(t_i, \frac{N}{\delta_{i-1}\delta_i}\right) = 1 . \tag{14}$$

Thus if we define sets $T(m)$ for each positive integer m by $T(m) = \{(m_1, m_2)$: m_1, m_2 positive integers such that $(m_1, m_2) = 1$ and $m_1 m_2 = m\}$ (so that if m has $k \geqq 0$ distinct prime divisors, then $T(m)$ has 2^k members), then (using Lemma 3 and (14)) we see that all possible

values of k_i/d_i, one for each of the different pairs k_i, d_i, are contained in the set

$$C_1(N) = \left\{ \frac{t}{N(ab)^{-1}} < 1 : ab = m \text{ divides } N, (a, b) \in T(m), \left(t, \frac{N}{ab}\right) = 1 \right\}.$$

Note that $C_1(N)$ will contain repeated elements.

LEMMA 5. *The set $C_1(N)$ has $f(N) = N \prod (1 + p^{-1})$ elements, where the product is taken over all distinct primes p which divide N.*

Proof. Define $W(m)$ for positive integers m by $W(1) = 1$, $W(\prod_{i=1}^{k} p_i^{\alpha_i}) = 2^k$, where the p_i's are distinct primes and the α_i's are positive integers. It follows from the principle of inclusion and exclusion that

$$\sum_{a=1}^{N} W((a, N)) = N \prod (1 + p^{-1}),$$

and the left-hand side is just the number of elements in $C_1(N)$.

It turns out that the set $C_1(N)$ is the same as the set

$$C_2(N) = \left\{ \frac{a'}{N/c} : c \text{ divides } N,\ 0 \leqq a' < N/c,\ a' \equiv a \bmod (N/c), \right.$$
$$\left. \text{where } a \text{ lies exactly once in each residue class mod } (N/c) \text{ such that } (a, c) = 1 \text{ is possible} \right\}.$$

LEMMA 6. *The sets $C_1(N)$ and $C_2(N)$ are identical for each $N > 1$.*

Proof. Cohen [2, Proposition 3.4, p. 134] proved that the number of elements in $C_2(N)$ is the number $f(N)$ of Lemma 5. It is easily seen that the map from $C_2(N) \to C_1(N)$ given by

$$\frac{a'}{N/c} \longrightarrow \frac{a'/(a', N/c)}{N(c(a', N/c))^{-1}} \quad \text{where} \quad \begin{matrix} t = a'/(a', N/c) \\ ab = c(a', N/c) \end{matrix}$$

is *into* and *one-to-one*. Since $C_1(N)$ and $C_2(N)$ have the same number of elements, this proves the lemma.

THEOREM 1. *For each $n \geqq 1$ and each $N > 1$, we have*

$$S(N, n) \leqq n \sum_{u \in C_1(N)} L(u), \qquad R(N) \leqq \sum_{u \in C_1(N)} L(u). \tag{15}$$

If $N = p^s$, $s \geqq 1$, for a prime p, then the latter estimate becomes

$$R(p^s) \leqq \sum_{i=0}^{p^{s-1}} L\left(\frac{i}{p^s}\right) + \sum_{i=0}^{p^{s-1}-1} L\left(\frac{i}{p^{s-1}}\right). \tag{16}$$

Proof. We consider the number α, with a period of length n, given by (10). We have already seen that the periodicity of the sequence of triples (a_i, k_i, d_i) $(i = 1, 2, \cdots)$ leads to the formulas (11) and (13) for $P(N\alpha)$. Evidently the period of the (a_i, k_i, d_i) is as long as possible if each of the n $a_i'^s$ in the period of α occurs with each of the possible different pairs k_i, d_i; thus by Lemma 5 the longest possible period length for the (a_i, k_i, d_i) is $nf(N)$. This fact and (13) lead at once to the estimates (15). The estimate (16) follows because it is easy to see that the set $C_1(p^s)$ is made up of the $p^s + p^{s-1}$ numbers i/p^s $(0 \leqq i < p^s)$ and i/p^{s-1} $(0 \leqq i < p^{s-1})$.

Theorem 1 is the same as Cohen's Theorem 4.3 and Corollary 4.4 [2, pp. 136-137]; but the states his estimates in terms of $C_2(N)$ instead of $C_1(N)$.

4. **Periodicity properties of matrices.** For each integer $N > 1$, we define a multiplicative group $\Gamma(N)$ of 2 by 2 unimodular matrices with integer entries by

$$\Gamma(N) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = \pm 1,\ b \equiv c \equiv a - d \equiv 0 \bmod N\right\}.$$

The same notation is used by Cohen [2, p. 132]; for any 2 by 2 unimodular matrix M, he also defined [2, p. 135] $\lambda_0(N, M)$ to be the smallest positive integer such that $M^{\lambda_0(N,M)}$ belongs to $\Gamma(N)$.

We can associate a unimodular matrix M with the quadratic irrational α given in (10) as follows:

$$M = (c_1)(c_2)\cdots(c_n) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad \text{say}. \tag{17}$$

We call M the *matrix of* α or the *matrix of the period* $c_1, \cdots, c_n$ or the *matrix of the continued fraction* $[a_1, \cdots, a_n]$. We have

$$\frac{a}{c} = [a_1, \cdots, a_n] \quad \text{and} \quad \frac{b}{d} = [a_1, \cdots, a_{n-1}] \tag{18}$$

(here $b = 1$, $d = 0$ if $n = 1$). In view of (18), we see that this definition of the matrix of α is the same as the one given by Cohen [2, p. 129].

Cohen showed the relevance of $\lambda_0(N, M)$ to the study of $S(N, n)$ and $R(N)$. The role of $\lambda_0(N, M)$ is made really clear by the use of the Châtelet algorithm of §2. Before exploring this further, we need the following lemmas.

LEMMA 6. *Let*

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a(M) & b(M) \\ c(M) & d(M) \end{bmatrix}, \qquad ad - bc = (-1)^n = \varepsilon, \quad say, \tag{19}$$

be a unimodular matrix with integer entries. Define sequences $r(i)$ *and* $s(i)$ *by*

$$r(1) = 1,\ r(2) = a + d,\ \cdots,\ r(i) = (a + d)r(i - 1) - \varepsilon r(i - 2) \quad (i \geqq 3)$$

and

$$s(1) = 1/2(a + d),\ s(2) = 1/2(a + d)^2 - \varepsilon,\ \cdots,$$
$$s(i) = (a + d)s(i - 1) - \varepsilon s(i - 2) \quad (i \geqq 3).$$

Then for each positive integer k

$$a(M^k) = s(k) + 1/2(a - d)r(k), \qquad b(M^k) = br(k),$$
$$c(M^k) = cr(k), \qquad d(M^k) = s(k) - 1/2(a - d)r(k).$$

Proof. This is Lemma 5.4 of Cohen [2, p. 139].

LEMMA 7. *Let* p *be a prime and suppose* M *is given by* (19). *Define*

$$D = D(M) = (a - d)^2 + 4bc = (a + d)^2 - 4\varepsilon = (a + d)^2 + 4(-1)^{n-1}.$$

Then M^λ *belongs to* $\Gamma(N)$ (i.e., $\lambda_0(p^s, M)$ *divides* λ) *for the value of* λ *given in the following tables, where* (D/p) *is a Jacobi symbol*:

(a) *if* $p > 2$

	$\left(\frac{D}{p}\right) = +1$	$\left(\frac{D}{p}\right) = 0$	$\left(\frac{D}{p}\right) = -1$
$1/2n(p-1)$ odd	$p^{s-1}(p-1)$	impossible	$p^{s-1}(p+1)$
$1/2n(p-1)$ even	$1/2p^{s-1}(p-1)$	p^s	$1/2p^{s-1}(p+1)$

(b) *if* $p = 2$

$$\left(\frac{D}{p}\right) = -1 \qquad \text{(i.e., } D \equiv 5 \bmod 8\text{)}$$

	$s = 1$	$s = 2$	$s \geqq 3$
n odd	3	6	$3 \cdot 2^{s-2}$
n even	3	3	$3 \cdot 2^{s-3}$

$\left(\frac{D}{p}\right) = 0$:

if $D \equiv 0 \bmod 8$, $\quad \lambda = 2^s$

if $D \equiv 4 \bmod 8$, $\quad \lambda = 2$ *for* $s = 1$, $\lambda = 2^{s-1}$ *for* $s \geqq 2$.

Proof. This is Theorem 5.3 of Cohen [2, pp. 137-138].

Our next lemma shows how $\lambda_0(p, M)$, where p is prime and M is defined by (17), is related to periodicity properties of the algorithm (2). We here confine ourselves to the case $N = p$, p prime, because the results are simplest in that case.

LEMMA 8. *Suppose M is given by* (19), *and let p be a prime which does not divide the entry c in M. Define*

$$\Delta = \left\{ \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -k \\ 0 & p \end{bmatrix} \quad (0 \leqq k \leqq p-1) \right\}.$$

Suppose

$$\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} M^n = \begin{bmatrix} A & B \\ C & D \end{bmatrix} P \tag{20}$$

for some n and some P in Δ. Then M^n is in $\Gamma(p)$ if and only if $P = \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}$.

Proof. Suppose M^n is in $\Gamma(p)$, but P does not have the form asserted in the lemma, i.e.,

$$P = \begin{bmatrix} 1 & -k \\ 0 & p \end{bmatrix} \quad \text{for some} \quad k .$$

Then (20) gives

$$\begin{bmatrix} pa(M^n) & pb(M^n) \\ c(M^n) & d(M^n) \end{bmatrix} = \begin{bmatrix} A & -kA + pB \\ C & -kC + pD \end{bmatrix},$$

so $c(M^n) = C$, whence p divides C, since p divides $c(M^n)$ because M^n is in $\Gamma(p)$. But this means p also divides $d(M^n) = -kC + pD$, which contradicts

$$a(M^n)d(M^n) - b(M^n)c(M^n) = \pm 1 \equiv a(M^n)d(M^n) \bmod p .$$

Now suppose P does have the form asserted in the lemma. Then (20) gives

$$\begin{bmatrix} pa(M^n) & pb(M^n) \\ c(M^n) & d(M^n) \end{bmatrix} = \begin{bmatrix} pA & B \\ pC & D \end{bmatrix},$$

so $c(M^n) = pC$, whence p divides $c(M^n)$. By Lemma 6, $b(M^n) = br(n)$ and $c(M^n) = cr(n)$; now p divides $r(n)$ since p does not divide c, so also p divides $b(M^n)$. It also follows from Lemma 6 that p divides $a(M^n) - d(M^n)$. Hence P is in $\Gamma(p)$, and the proof of Lemma 8 is complete.

Now we are in a position to give the exact value for $R(p)$, p prime. We use the abbreviated notation

$$F(m) = \sum_{i=0}^{m-1} L\left(\frac{i}{m}\right)$$

of Cohen [2, p. 141].

THEOREM 2. *We have* $R(2) = F(2) + 1 = 5$. *If* p *is an odd prime, then*

$$R(p) = F(p) + 1 \quad \text{if} \quad p \equiv 3 \mod 4, \tag{21}$$

$$R(p) = F(p) \quad \text{if} \quad p \equiv 1 \mod 4. \tag{22}$$

Proof. Suppose the Assumption of §2 holds and suppose α is a quadratic irrational with period length n and continued fraction expansion given by (10). We saw in §2 that under these conditions the sequence of identities (2) holds with the matrices M_i there equal to (a_{i-1}) $(i = 1, 2, \cdots)$. We saw in §3 that the sequence of triples (a_i, k_i, d_i) $(i = 0, 1, 2, \cdots)$ is eventually periodic. Let us suppose that α, with period length n, has been chosen so that the period length of the sequence of triples (a_i, k_i, d_i) is maximal, say equal to r. Since each c_i in the period of α given in (10) can be associated with at most $p + 1$ different pairs k_i, d_i (namely, those corresponding to the $p + 1$ matrices in the set Δ of Lemma 8), we have $r \leqq n(p + 1)$.

Suppose $r = n(p + 1)$ does occur, and that the sequence of r identities

$$\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}(a_I) = \begin{bmatrix} A_{I+1} & B_{I+1} \\ C_{I+1} & D_{I+1} \end{bmatrix}\begin{bmatrix} \delta_{I+1} & -k_{I+1} \\ 0 & d_{I+1} \end{bmatrix}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \tag{23}$$

$$\begin{bmatrix} \delta_{I+r-1} & -k_{I+r-1} \\ 0 & d_{I+r-1} \end{bmatrix}(a_{I+r-1}) = \begin{bmatrix} A_{I+r} & B_{I+r} \\ C_{I+r} & D_{I+r} \end{bmatrix}\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}$$

is a typical periodic part of the sequence (2) (of course, this means $\delta_{I+r} = p$, $k_{I+r} = 0$, $d_{I+r} = 1$, as indicated in (23)). If we multiply on

the right in the first equation of (23) by $(a_{I+1}), (a_{I+2}), \cdots, (a_{I+r-1})$ in order, and after the ith such multiplication use equation $i+1$ of (23) for $1 \leqq i \leqq r-1$, we obtain

$$\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} M^{p+1} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}$$

for some A, B, C, D, with

$$M = (a_I)(a_{I+1}) \cdots (a_{I+n-1}) . \tag{24}$$

It follows from Lemma 8 that M^{p+1} is in $\Gamma(p)$, so $r = n(p+1)$ is possible if and only if there exists a matrix M of form (24) such that $\lambda_0(p, M) = p+1$. By Lemma 7, $\lambda_0(p, M) = p+1$ is possible for $p = 2$ and for any $p \equiv 3 \bmod 4$, but not for $p \equiv 1 \bmod 4$. An easy calculation shows that $\lambda_0(2, M) = 3$ for $M = (3)^n$ $(n = 1, 2, \cdots)$. Thus, by (13), $S(2, n) = 5n$ for all n and $R(2) = 5$. For any $p \equiv 3 \bmod 4$, it is also possible to find M such that $\lambda_0(p, M) = p+1$, but only when n is odd (by Lemma 7). In fact, if n is odd we can take $M = (a)(2p) \cdots (2p)$ ($n-1$ factors $(2p)$), where a is defined by $a \equiv z + \bar{z} \bmod p$; here $z = u + vi$ is any generator of the group of numbers $x + iy$, x and y integers, with norm $\pm 1 \bmod p$ (this group has $2(p+1)$ elements and $\phi(2(p+1))$ generators, where ϕ is Euler's function). A proof that this choice of M satisfies $\lambda_0(p, M) = p+1$ was given by Cohen [2, pp. 142-143] (note that there is an incorrect factor of 1/2 in the congruence defining a [2, p. 142]). Thus, by (13), we have $S(p, n) = (F(p)+1)n$ whenever $p \equiv 3 \bmod 4$ and n is odd. Since always $S(p, n) \leqq (F(p)+1)n$ by Theorem 1, this proves (21).

If $p \equiv 1 \bmod 4$, then by Lemma 7 the largest possible value of r is np, and this attained if and only if p divides $D(M)$. Hence $S(p, n) \leqq nF(p)$; equality actually holds here for n even because $r = np$ when $M = (a)(2p) \cdots (2p)$ $(n-1$ factors $(2p))$, where a satisfies $a^2 + 4 \equiv \bmod p$. This is stated without proof by Cohen [2, p. 145]. A proof using (13) can easily be given by considering the sequence of triples (a_i, k_i, d_i) which arises from (2) for this choice of M. It turns out that each of the $p-1$ pairs $(k_i, d_i) = (k, p)$ with $1 \leqq k \leqq p-1$ occurs n times among the triples (a_i, k_i, d_i) in a period, and the remaining p triples in the period have the form $(2p, 0, 1)$ or $(2p, 0, p)$, except for one triple $(1, 0, p)$. Thus we have (22), and this completes the proof of Theorem 2.

REMARK. Theorem 2 shows that the estimate (16) of Theorem 1 holds with equality when $s = 1$ and $p = 2$ or $p \equiv 3 \bmod 4$. As Cohen [2, Corollary 6.5, p. 144] remarked, the only other cases in which (16) holds with equality are those in the following theorem.

THEOREM 3. *Let p be a prime such that $p \equiv 3 \bmod 4$. Then for each $s \geqq 1$ we have*

$$R(p^s) = F(p^s) + F(p^{s-1}) . \tag{25}$$

If $p \equiv 7 \bmod 12$, then also

$$R(2p^s) = F(2p^s) + F(2p^{s-1}) + F(p^s) + F(p^{s-1}) . \tag{26}$$

We also have $R(4) = 14$ and $R(6) = 28$.

Proof. First suppose $p \equiv 3 \bmod 4$. By a generalization of the argument used in the proof of Theorem 1 to establish (21), we see that (25) holds if, for each odd n, we can find a matrix M of form (24) such that $\lambda_0(p^s, M) = p^{s-1}(p+1)$. In fact, the matrix M used for the case $s = 1$ in the proof of (21) also suffices for any $s > 1$ (see Cohen [2, pp. 142-143]).

Now suppose $p \equiv 7 \bmod 12$. In this case we see that (26) holds if, for each odd n, we can find a matrix M of form (24) such that $\lambda_0(2p^s, M) = 3p^{s-1}(p+1)$. It is easy to deduce the existence of such a matrix (see Cohen [2, p. 144]) from the existence of M with $\lambda_0(p^s, M) = p^{s-1}(p+1)$.

Finally, we evaluate $R(4)$ and $R(6)$ by special arguments similar to the one used to show $R(2) = 5$ in the proof of Theorem 1.

5. **Concluding remarks.** In the final part of his paper, Cohen [2, §§7 and 8, pp. 144-147] gave several conjectures, including conjectures for the exact values of $S(N, n)$ when n is even and N is arbitrary, and for the exact values of $R(N)$ when N is arbitrary. These conjectures can certainly be approached via the Châtelet algorithm as described above, but it seems that considerable calculation might be necessary in order to make progress. We do not go into these questions here.

REFERENCES

1. A. Châtelet, *Contribution a la théorie des fractions continues arithmétiques*, Bull. Soc. Math. France, **40** (1912), 1-25.

2. H. Cohen, *Multiplication par un entier d'une fraction continue périodique*, Acta Arith., **26** (1974-75), 129-148.

3. M. Mendès France, *Sur les fractions continues limitées*, Acta Arith., **23** (1973), 207-215.

4. A. Schinzel, *On some problems of the arithmetical theory of continued fractions, I*, Acta. Arith., **6** (1961), 394-413; II, Ibid. **7** (1962), 288-298.

Received October 8, 1977.

STATE UNIVERSITY OF NEW YORK AT BUFFALO
BUFFALO, NY 14214