<table>
<thead>
<tr>
<th>Title</th>
<th>On some arithmetical properties of Rogers-Ramanujan continued fraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Duverney, Daniel; Shiokawa, Iekata</td>
</tr>
<tr>
<td>Citation</td>
<td>Osaka Journal of Mathematics. 37(3) P.759-P.771</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2000</td>
</tr>
<tr>
<td>Text Version</td>
<td>publisher</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://doi.org/10.18910/4719">https://doi.org/10.18910/4719</a></td>
</tr>
<tr>
<td>DOI</td>
<td>10.18910/4719</td>
</tr>
<tr>
<td>rights</td>
<td></td>
</tr>
</tbody>
</table>
ON SOME ARITHMETICAL PROPERTIES OF ROGERS-RAMANUJAN CONTINUED FRACTION

DANIEL DUVERNEY and IEKATA SHIOKAWA

(Received July 14, 1998)

1. Introduction

Let \( R(z) \) be the Rogers-Ramanujan continued fraction defined by

\[
R(z) = 1 + \frac{z}{1 + \frac{z^2}{1 + \frac{z^3}{1 + \ldots}}} \quad (|z| < 1).
\]

For \( z = 1/q \) (\( q \in \mathbb{N} - \{0, 1\} \)), it is easy to transform \( R(1/q) \) into the regular continued fraction

\[
R(1/q) = 1 + \frac{1}{q + \frac{1}{q + \frac{1}{q^2 + \frac{1}{q^2 + q^3 + q^3 + \ldots}}}}
\]

(see e.g. [9; 2.3]). Since this expansion is not ultimately periodic, \( R(1/q) \) is not a quadratic number. More generally, as an application of a deep result of Nesterenko on modular functions [12], one can prove that \( R(z) \) is transcendental for every algebraic number \( z \) (\( 0 < |z| < 1 \)) [5]. In this paper, we want to focus on the fact that \( R(1/q) \) is not a quadratic number, and generalize this result in two directions.

First, we consider a more general Rogers-Ramanujan continued fraction

\[
R(z; x) = 1 + \frac{zx}{1 + \frac{z^2 x}{1 + \frac{z^3 x}{1 + \ldots}}} \quad (|z| < 1).
\]

Irrationality results on \( R(z; x) \) for rational \( x \) and \( z \) are given in [11], [13], [14]. We will prove the following

**Theorem 1.** Let \( x = a/b \in \mathbb{Q}^* \) and let \( z = 1/q \) with \( q \in \mathbb{Z} \), \( |q| \geq 2 \). Suppose that \( a^4 < |q| \). Then \( R(1/q; a/b) \) is not a quadratic number.

It should be noted that Lagrange’s theorem on regular continued fractions cannot be applied here, because

\[
R(1/q; a/b) = \frac{1}{q b/a + \frac{1}{q + \frac{1}{q^2 b/a + \frac{1}{q^2 + q^3 b/a + q^3 + \ldots}}}}
\]
is not a regular continued fraction if \( a \neq 1 \). Theorem 1 is a direct consequence of the following general result on continued fractions with rational coefficients, which should be compared to Lambert’s criterion on irrationality (see e.g. [10; p. 100]).

**Theorem 2.** Let \( c_1, c_2, c_3, \ldots \) be an infinite sequence of rational numbers satisfying the following conditions

1. \( |c_n| \geq 2 \) for every \( n \geq 1 \)
2. \( \sum_{n=1}^{+\infty} |c_n c_{n+1}|^{-1} < \infty \)
3. There exists an infinite sequence of rational integers \( d_n \) (\( n \geq 1 \)) such that \( d_n c_n \in \mathbb{Z} \) for every \( n \geq 1 \), and \( \liminf_{n \to +\infty} (d_1 d_2 \cdots d_n)^2/c_{n+1} = 0 \).

Then the continued fraction

\[
\alpha = 1 + \frac{1}{c_1} + \frac{1}{c_1 + c_2} + \cdots + \frac{1}{c_1 + c_2 + \cdots + c_n + \cdots}
\]

is convergent, and \( \alpha \) is not a quadratic number.

Note that, under the hypothesis of Theorem 2, Lambert’s criterion implies the irrationality of \( \alpha \).

For the second generalization, we will use Rogers-Ramanujan identities ([16; p. 36], or [8; p. 290], for example), and write

\[
R \left( \frac{1}{q} \right) = \frac{\alpha_q^*}{\beta_q^*}
\]

with

\[
\alpha_q^* = 1 + \sum_{n=1}^{+\infty} (-1)^n q^{-n(5n-1)/2} + \sum_{n=1}^{+\infty} (-1)^n q^{-n(5n+1)/2},
\]

\[
\beta_q^* = 1 + \sum_{n=1}^{+\infty} (-1)^n q^{-n(5n-3)/2} + \sum_{n=1}^{+\infty} (-1)^n q^{-n(5n+3)/2}.
\]

The numbers \( \alpha_q^* \) and \( \beta_q^* \) involve the sequences \((u_n)\) and \((v_n)\) defined by

\[
\begin{align*}
u_0 &= 0, \quad u_1 = 2, \quad u_2 = 3, \quad u_3 = 9, \quad u_4 = 11, \ldots, \\
u_{2n-1} &= \frac{n(5n - 1)}{2}, \quad u_{2n} = \frac{n(5n + 1)}{2}, \ldots, \\
u_0 &= 0, \quad v_1 = 1, \quad v_2 = 4, \quad v_3 = 7, \quad v_4 = 13, \ldots, \\
u_{2n-1} &= \frac{n(5n - 3)}{2}, \quad v_{2n} = \frac{n(5n + 3)}{2}, \ldots.
\end{align*}
\]
Indeed, one can write \( a^*_q = \sum_{n=0}^{\infty} a(n)q^{-n} \), where \( a(n) = \pm 1 \) if there exists \( k \in \mathbb{N} \) such that \( n = u_k \), \( a(n) = 0 \) otherwise. Similarly, we have \( \beta^*_q = \sum_{n=0}^{\infty} b(n)q^{-n} \), where \( b(n) = \pm 1 \) if there exists \( k \in \mathbb{N} \) such that \( n = v_k \), \( b(n) = 0 \) otherwise. Therefore, we can deduce that \( R(1/q) \) is not quadratic for \( q \in \mathbb{Z} \ (|q| \geq 2) \) from the following more general result.

**Theorem 3.** Let \( a(n) \) and \( b(n) \) be bounded sequences of rational integers, such that

\[
\begin{cases}
    a(n) \neq 0 & \text{if there exists } k \in \mathbb{N} \text{ such that } n = u_k, \\
    a(n) = 0 & \text{otherwise,} \\
    b(n) \neq 0 & \text{if there exists } k \in \mathbb{N} \text{ such that } n = v_k, \\
    b(n) = 0 & \text{otherwise.}
\end{cases}
\]

Let \( K \) be any quadratic field. Then, if \( q \in \mathbb{Z} \ (|q| \geq 2) \) the three numbers \( \alpha_q = \sum_{n=0}^{\infty} a(n)q^{-n}, \beta_q = \sum_{n=0}^{\infty} b(n)q^{-n}, \) and 1, are linearly independent over \( K \).

2. Proof of Theorem 2

We will need the following lemma.

**Lemma 1 ([14]).** Let \( c_1, c_2, c_3, \ldots \) be an infinite sequence of complex numbers satisfying (1) and (2). Let \( P_n = c_n P_{n-1} + P_{n-2}, \ Q_n = c_n Q_{n-1} + Q_{n-2} \ (n \geq 1) \) with \( P_0 = Q_0 = 0 \) and \( P_{-1} = Q_{-1} = 1 \). Then \( P_n/(c_2c_3 \cdots c_n) \) and \( Q_n/(c_1c_2 \cdots c_n) \) converge to non-zero limits \( \beta \) and \( \gamma \), and satisfy for every \( n \geq 1 \)

\[
A < \frac{|P_n|}{|c_2c_3 \cdots c_n|} < B, \quad A < \frac{|Q_n|}{|c_1c_2 \cdots c_n|} < B,
\]

where \( 0 < A = \prod_{n=1}^{\infty} (1 - 2/|c_nc_{n+1}|) < 1, \ B = \prod_{n=1}^{\infty} (1 + 2/|c_nc_{n+1}|) > 1 \). So the continued fraction \( 1 \overline{1} \cdots \) converges to the limit \( \alpha = \lim_{n \to +\infty} P_n/Q_n = \beta/(c_1\gamma), \) and

\[
\frac{A}{B} < \left| \frac{\beta}{\gamma} \right| < \frac{B}{A}.
\]

Proof. Since \( |c_n| \geq 2 \), we have \( |P_n| \geq 2|P_{n-1}| - |P_{n-2}| \). Hence \( |P_n| \geq |P_{n-1}| \) for every \( n \geq 1 \) by induction, and \( |P_n| \geq |P_1| = 1 \). Therefore \( P_n \neq 0 \) for every \( n \geq 1 \), and the same holds for \( Q_n \). We put \( u_n = c_n P_{n-1}/P_n, \ v_n = c_n Q_{n-1}/Q_n \) for \( n \geq 1 \), so that \( u_1 = 0, \ v_1 = 1 \). Then we have

\[
P_n = c_n \left(1 + \frac{u_{n-1}}{c_{n-1}c_n}\right) P_{n-1}, \quad Q_n = c_n \left(1 + \frac{v_{n-1}}{c_{n-1}c_n}\right) Q_{n-1},
\]
and so
\[
P_n = c_2 c_3 \cdots c_n \prod_{k=2}^{n-1} \left(1 + \frac{u_k}{c_{k-1} c_k}\right) \quad (n \geq 2),
\]
\[
Q_n = c_1 c_2 \cdots c_n \prod_{k=1}^{n-1} \left(1 + \frac{v_k}{c_{k-1} c_k}\right) \quad (n \geq 1).
\]

Since \( u_n = (1 + u_{n-1} / c_{n-1} c_n)^{-1} \) and \( v_n = (1 + v_{n-1} / c_{n-1} c_n)^{-1} \), we see by induction on \( n \) that \( |u_n| \leq 2, |v_n| \leq 2 \) for \( n \geq 1 \), which together with (1) and (2) ensures the convergence of the products \( \beta = \prod_{k=2}^{\infty} (1 + u_k / c_k c_{k+1}) \) and \( \gamma = \prod_{k=1}^{\infty} (1 + v_k / c_k c_{k+1}) \), and (1) and (2) follow immediately.

\[\square\]

**Lemma 2.** With the notations in Lemma 1, there exists \( n_0 \in \mathbb{N} \) such that \( |\alpha - P_n/Q_n| < 2/(|Q_n Q_{n+1}|) \leq 1 \) for every \( n \geq n_0 \).

**Proof.** Put \( \alpha_n = \frac{1}{c_n} + c_{n+1} + \cdots \) \((n \geq 1)\). We have
\[
\alpha = \alpha_1 = \frac{1}{c_1 + c_2 + \cdots + c_{n+1} + \alpha_{n+2}} = \frac{1}{c_1 + \cdots + c_{n+1} + \frac{\alpha_{n+2}}{1}} = \frac{P_{n+1} + \alpha_{n+2} P_n}{Q_{n+1} + \alpha_{n+2} Q_n},
\]
and we get the well-known formula
\[
\alpha - \frac{P_n}{Q_n} = \frac{(-1)^n}{Q_n Q_{n+1} (1 + \alpha_{n+2} Q_n / Q_{n+1})} \quad (n \geq 1).
\]
By (1), we have
\[
(3) \quad |Q_n/Q_{n+1}| \leq \frac{B}{A|c_{n+1}|}.
\]
By (2) with \( \alpha_{n+2} \) in place of \( \alpha = \alpha_1 \), we get \( |\alpha_{n+2}| \leq B/(A|c_{n+2}|) \). Hence \( \lim_{n \to +\infty} (1 + \alpha_{n+2} Q_n / Q_{n+1}) = 1 \) by (2), and Lemma 2 follows. \[\square\]

**Proof of Theorem 2.** Suppose that \( \alpha \) is a root of \( f(x) = ax^2 + bx + c, \ a, b, c \in \mathbb{Z}, \ \alpha \neq 0 \). It follows from the mean value theorem that \( -f(P_n/Q_n) = (\alpha - P_n/Q_n) f'(\theta) \), with \( \alpha - 1 \leq \theta \leq \alpha + 1 \). By Lemma 2 we get \( |f(P_n/Q_n)| \leq 2M/|Q_n Q_{n+1}| \) \((n \geq n_0)\) where \( M = \max(|f'(x)| | \alpha - 1 \leq x \leq \alpha + 1) \). Using (3) yields \( |Q_{n+1}^2 f(P_n/Q_n)| \leq 2MB/(A|c_{n+1}|) \) \((n \geq n_0)\).

We see by induction on \( n \) that \( d_1 d_2 \cdots d_n P_n \) and \( d_1 d_2 \cdots d_n Q_n \) are rational integers; the same holds for \( A_n = (d_1 d_2 \cdots d_n)^2 Q_n^2 f(P_n/Q_n) \) \((n \geq 1)\). Using (3), we get \( \liminf_{n \to +\infty} A_n = 0 \), and \( A_n = 0 \) for infinitely many \( n \), namely \( f(P_n/Q_n) = 0 \) for infinitely many \( n \). Hence \( f \) has infinitely many roots, and \( f = 0 \). The proof of Theorem 2 is complete. \[\square\]
3. Proof of Theorem 3

To prove Theorem 3, we essentially use the same method as in [2]. We put

\[
\alpha_q^2 = \sum_{n=0}^{+\infty} \left( \sum_{k=0}^{n} a(k) a(n-k) \right) q^{-n} = \sum_{n=0}^{+\infty} r'(n) q^{-n},
\]

\[
\beta_q^2 = \sum_{n=0}^{+\infty} \left( \sum_{k=0}^{n} b(k) b(n-k) \right) q^{-n} = \sum_{n=0}^{+\infty} s'(n) q^{-n},
\]

\[
\alpha_q \beta_q = \sum_{n=0}^{+\infty} \left( \sum_{k=0}^{n} a(k) b(n-k) \right) q^{-n} = \sum_{n=0}^{+\infty} t'(n) q^{-n}.
\]

As \(a(n)\) and \(b(n)\) are bounded sequences of rational integers, we see that there exists \(M > 0\) such that

\[
|s'(n)| \leq M r(n),
\]

\[
|A'(n)| \leq M s(n),
\]

\[
|t'(n)| \leq M t(n),
\]

where \(r(n), s(n), t(n)\) are the numbers of solutions \((k, l) \in \mathbb{N}^2\) of the equations \(u_k + u_l = n, v_k + v_l = n, u_k + v_l = n\), respectively.

As in [2], the numbers \(r(n), s(n)\) and \(t(n)\) can be connected to the number \(\rho(n)\) of solutions \((k, l) \in \mathbb{N}^2\) of the equation \(k^2 + l^2 = n\). This will be done in the paragraph 3.1, Lemmas 4 and 5. In the paragraph 3.2, we will recall an elementary criterion of irrationality from [1] (Theorem 4) and prove a modified version of [3; Lemma 2] (Theorem 5), concerning the gaps in the sequence \(r(n)\). The proof of Theorem 3 will be given in the paragraph 3.3.

3.1. Three technical lemmas

We prove some connections between \(r(n), s(n), t(n)\) and \(\rho(n)\).

**Lemma 3.** Suppose that \(n = 2^a \prod p^\beta \prod q^\gamma\), where \(p\) and \(q\) are primes congruent to 1 and 3 modulo 4, respectively. Then, if \(n\) is not a square,

\[
\rho(n) = \prod (\beta + 1) \prod \left( \frac{1 + (-1)^\gamma}{2} \right).
\]

Proof. Let \(\rho^*(n)\) be the number of decompositions of \(n\) as sum of squares of two rational integers. It is well known that the generating function of \(\rho^*(n)\) is

\[
g^*(x) = \left( \sum_{n=-\infty}^{+\infty} x^{n^2} \right)^2.
\]
while the generating function of \( \rho(n) \) is

\[
g(x) = \left( \sum_{n=0}^{+\infty} x^{n^2} \right)^2.
\]

Hence \( g^*(x) = \left( 2 \sum_{n=0}^{+\infty} x^{n^2} - 1 \right)^2 = 4g(x) - 4\sum_{n=0}^{+\infty} x^{n^2} + 1 \). Thus if \( n \) is not a square, \( \rho(n) = \rho^*(n)/4 \), and Lemma 1 follows directly from [8; (16–9–5) and Theorem 278].

**Lemma 4.** For every natural integer \( n \), we have

\[
(5) \quad r(n) = \rho(40n + 2),
\]
\[
(6) \quad s(n) = \rho(40n + 18).
\]

Proof. We prove (5). Let \((k, l)\) be a solution of the equation

\[
(7) \quad \frac{k(5k + u)}{2} + \frac{l(5l + v)}{2} = n
\]

with \( u^2 = 1, v^2 = 1 \). It is easy to verify that this equation is equivalent to

\[
(10k + u)^2 + (10l + v)^2 = 40n + 2.
\]

Thus every solution \((k, l)\) of (7) yields a solution \((k', l')\) of the equation

\[
(8) \quad k'^2 + l'^2 = 40n + 2.
\]

Conversely, let \((k', l')\) be a solution of (8). By reduction modulo 5, we obtain \( k' = 5k_1 + u \) and \( l' = 5l_1 + v \), with \( k_1 \in \mathbb{N}, l_1 \in \mathbb{N}, u^2 = 1, v^2 = 1 \). But \( k' \) and \( l' \) must be odd by (8), therefore \( k_1 \) and \( l_1 \) must be even, and \( k' = 10k + u, l' = 10l + v \). Thus \((k, l)\) is a solution of (7), and (5) is proved. The proof of (6) is similar.

The connection between \( t(n) \) and \( \rho(n) \) is a bit more difficult to handle, and we only prove:

**Lemma 5.** For every integer \( n \geq 0 \), we have

\[
(9) \quad t(n) = \frac{1}{2} \rho(40n + 10) \quad \text{if} \quad n \not\equiv 1 \pmod{5},
\]
\[
(10) \quad t(n) \leq \rho(40n + 10),
\]
\[
(11) \quad t(n) = 2 \quad \text{if} \quad \rho(40n + 10) = 4 \quad \text{and} \quad 8n + 2 \not\equiv 0 \pmod{5}.
\]
Proof. Let us prove first (16). The equation

\[ \frac{k(5k + u)}{2} + \frac{l(5l + v)}{2} = n \]

with \( u^2 = 1, v^2 = 9 \) is equivalent to

\[ (10k + u)^2 + (10l + v)^2 = 40n + 10. \]

Thus every solution \((k, l)\) of (12) yields one solution \((k', l')\) of the equation

\[ k'^2 + l'^2 = 40n + 10, \]

and (16) is proved.

Next we prove (15). Let \((k', l')\) be a solution of (13). It is easy to verify that only two cases can occur:

Case 1. \(k' \equiv u \) (mod 5) and \(l' \equiv v \) (mod 5), with \( u, v \in \{1, -1, 3, -3\}\). As \(k'\) and \(l'\) must be odd by (13), we obtain \(k' = 10k + u\) and \(l' = 10l + v\).

Case 2. \(k' \equiv 0 \) (mod 5) and \(l' \equiv 0 \) (mod 5).

Suppose that \(n \not\equiv 1 \) (mod 5). Then Case 2 cannot occur, because \(k' = 5k_1\) and \(l' = 5l_1\) implies \(8n + 2 = 5(k_1^2 + l_1^2)\) by (13), and reduction modulo 5 yields \(n \equiv 1 \) (mod 5). Hence we are in Case 1 and \(k' = 10k + u\), \(l' = 10l + v\), with \(u, v \in \{1, -1, 3, -3\}\). But this gives a solution of (12) only if \(u = 1\) or \(-1\) and \(v = 3\) or \(-3\). Therefore (15) is proved.

Finally (17) is an immediate consequence of (15).

3.2. Two theorems

The following theorem is proved in [1](see also [4] for a generalization).

**Theorem 4.** Let \(q \in \mathbb{Z} \ (|q| \geq 2)\). Let \(\tau(n)\) be a sequence of rational integers with the following properties (i), (ii), (iii):

(i) \(\tau(n) \neq 0\) for infinitely many \(n\).

(ii) When \(n\) is large enough, \(|\tau(n)| \leq \omega(n)\) with \(\omega(n) > 0\) and
\[
\limsup_{n \to +\infty} \omega(n + 1)/\omega(n) < |q|.
\]

(iii) There exists infinitely many \(k \in \mathbb{N}\) and integers \(n_k \in \mathbb{N}\) such that \(\tau(n_k + 1) = \tau(n_k + 2) = \cdots = \tau(n_k + k) = 0\) and \(\lim_{k \to +\infty} \omega(n_k + k + 1)/|q|^k = 0\).

Let \(x = \sum_{n=0}^{+\infty} \tau(n)q^{-n}\). Then if \(x = \alpha/\beta \in \mathbb{Q}\), we have

\[ \alpha q^{n_k} - \beta \sum_{n=0}^{n_k} \tau(n)q^{n_k-n} = 0 \]

for all sufficiently large \(k\).

One sees that Theorem 4 is a criterion of irrationality for gap series under some
conditions. The following result allows to show that $\rho(n), r(n), s(n), t(n)$ are gap series, and to apply Theorem 4 in order to prove Theorem 3.

**Theorem 5.** Let $\Omega_1$ and $\Omega_2$ be two natural integers, with $\Omega_1 \equiv 1 \pmod{4}$, $\Omega_2$ odd, $\gcd(\Omega_1, \Omega_2) = \Delta \equiv 1 \pmod{4}$, and let $\theta_1 \in \mathbb{N}, \theta_2 \in \mathbb{N} - \{0, 1\}, \delta \in \mathbb{N} - \{0\}, \varepsilon \in ]0, 1[$. Denote by $p_1 < p_2 < \cdots < p_n$ a sequence of consecutive rational primes congruent to 3 modulo 4 with the following properties:

\begin{equation}
\tag{14}
p_n \text{ does not divide } \Omega_2 \text{ for every } n \geq 1,
\end{equation}

Then there exists an integer $m_0 = m_0(\Omega_1, \Omega_2, \theta_1, \theta_2, \delta, \varepsilon)$ and a constant $L > 1$ (Linnik’s constant [7]) such that, for every $k = p_1 p_2 \cdots p_m$ with $m \geq m_0$, there exists $N_k \in \mathbb{N}$ such that

\begin{equation}
\tag{15}
\rho(N_k - \delta) = \cdots = \rho(N_k - 1) = \rho(N_k + 1) = \cdots = \rho(N_k + k) = 0,
\end{equation}

\begin{equation}
\tag{22}
N_k = 2^\theta \Delta p_k^2 h_k^2, \text{ where } p_k^\ast \text{ is a rational prime satisfying } p_k^\ast \equiv 1 \pmod{4}, \text{ and } h_k \text{ is an integer whose prime divisors are all distinct and congruent to 3 modulo 4,}
\end{equation}

\begin{equation}
\tag{23}
N_k \equiv 2^\theta \Omega_1 \pmod{2^{\theta_1+\theta_2} \Omega_2},
\end{equation}

\begin{equation}
\tag{24}
N_k \leq (2^{\theta_1+\theta_2} \Omega_2)^L \exp(4LP_{2\varepsilon}^2).
\end{equation}

**Proof of Theorem 5.** We follow the proof of [1; Lemma 2] until the fourth step. We modify the fifth step in the following way. Because of (14), we can choose $\eta \in \{0, 1, \ldots, 2^{\theta_1+\theta_2} \Omega_2 - 1\}$, such that

\begin{equation}
\tag{25}
\eta(p_1 p_2 \cdots p_{m+N-M})^4 + t_m \equiv 2^{\theta_1} \Omega_1 \pmod{2^{\theta_1+\theta_2} \Omega_2}.
\end{equation}

Then we put for $s \in \mathbb{N}$

\begin{equation}
\tag{26}
w_s = 2^{\theta_1+\theta_2} \Omega_2 (p_1 p_2 \cdots p_{m+N-M})^4 s + \eta(p_1 p_2 \cdots p_{m+N-M})^4 + t_m,
D = \gcd[2^{\theta_1+\theta_2} \Omega_2 (p_1 p_2 \cdots p_{m+N-M})^4, \eta(p_1 p_2 \cdots p_{m+N-M})^4 + t_m].
\end{equation}

Using (25) and [1; (30)], we see that

\begin{equation}
\tag{27}
D = 2^{\theta_1} \Delta \prod_{i=1}^{n+N-M} \pi_i^{\alpha_i}, \text{ with } \alpha_i = 0 \text{ or } 2.
\end{equation}

We write

\begin{equation}
w_s = D(\xi s + \chi), \text{ with } (\xi, \chi) \in \mathbb{N} \times \mathbb{N}.
\end{equation}
Because of [1; (31)], we have $\chi < \eta$ for large $m$. Then, by Linnik's theorem, there exists a prime number $p_k^*$ and a natural integer $\sigma$ such that

$$\omega_\sigma = Dp_k^* \leq D\left(\frac{2^{\beta_1+\beta_2}\Omega_2(p_1p_2\cdots p_{m+N+M})^4}{D}\right)^L.$$  

We put $N_k = \omega_\sigma$. By (28) with $L > 1$, we have

$$N_k \leq (2^{\beta_1+\beta_2}\Omega_2)^L(p_1p_2\cdots p_{m+N+M})^{4L},$$

which leads to (24) by following the sixth step of the proof of [1; Lemma 2].

Moreover, as $\Omega_1 \equiv 1 \pmod{4}$ and $\theta_2 \geq 2$, we have by using (25) $w_i \equiv 1 \pmod{4}$ $(s \in \mathbb{N})$. Thus, by (27) and (28)

$$\Delta \prod_{i=1}^{m+N+M} p_i^\sigma \cdot p_k^* \equiv 1 \pmod{4}.$$

As $\Delta \equiv 1 \pmod{4}$ and $\alpha_t = 0$ or 2, we get $p_k^* \equiv 1 \pmod{4}$, and $p_k^*$ is a sum of two squares. This proves (22), while (23) results from (26) and the definition of $N_k$. Finally, (15) is a direct consequence of [1; (35)]. The proof of Theorem 4 is complete.

### 3.3. Proof of Theorem 3

For the proof of Theorem 3, it is sufficient to show that the numbers $\alpha_q^2$, $\beta_q^2$, $\alpha_q\beta_q$, $\alpha_q$, $\beta_q$ and 1 are linearly independent over $\mathbb{Q}$, because $(a+b\sqrt{d})+(a'+b'\sqrt{d})\alpha_q+(a''+b''\sqrt{d})\beta_q = 0$ implies $(a+a'\alpha_q+a''\beta_q)^2 = d(b+b'\alpha_q+b''\beta_q)^2$. So suppose that, for rational integers $A, B, C, D, E, F$,

$$A\alpha_q^2 + B\beta_q^2 + C\alpha_q\beta_q + D\alpha_q + E\beta_q + F = 0.$$

Then, if

$$\tau(n) = Ar'(n) + Bs'(n) + Ct'(n) + Da(n) + Eb(n),$$

we have $\sum_{n=0}^{\infty} \tau(n)q^{-n} = -F$.

First step. Suppose first that $B \neq 0$. Let $\sigma \in \mathbb{N}$ such that $q^\sigma$ divides none of the numbers $2Bb(u)b(v)$ with $(u, v) \in \mathbb{N}^2$ and $b(u)b(v) \neq 0$; we can choose such a $\sigma$ because $b(u)$ and $b(v)$ are bounded. In Theorem 5, we put

$$\delta = 40\sigma + 16,$$

and choose $\varepsilon$ such that

$$32L - \frac{\log |q|}{320\varepsilon} < 0.$$
Also we put $\Omega_1 = 9$, $\Omega_2 = 5$, $\theta_1 = 1$, $\theta_2 = 2$ and then $N_k$ in (23) satisfies $N_k \equiv 18 \pmod{40}$. We put $n_k = (N_k - 18)/40$.

By using (15) and (22), and Lemma 3, 4, 5, we have

\begin{align*}
    s(n_k - \sigma) = \cdots = s(n_k - 1) = s(n_k + 1) = \cdots = s\left(n_k + \left\lfloor \frac{k}{40} \right\rfloor \right) &= 0, \\
    s(n_k) &= 2, \\
    r(n_k - \sigma) = \cdots = r(n_k - 1) = r(n_k) = \cdots = r\left(n_k + \left\lfloor \frac{k}{40} \right\rfloor \right) &= 0, \\
    t(n_k - \sigma) = \cdots = t(n_k - 1) = t(n_k) = \cdots = t\left(n_k + \left\lfloor \frac{k}{40} \right\rfloor \right) &= 0, \\
    a(n_k - \sigma) = \cdots = a(n_k - 1) = a(n_k) &= \cdots = a\left(n_k + \left\lfloor \frac{k}{40} \right\rfloor \right) = 0, \\
    b(n_k - \sigma) = \cdots = b(n_k - 1) = b(n_k) &= \cdots = b\left(n_k + \left\lfloor \frac{k}{40} \right\rfloor \right) = 0. \\
\end{align*}

For the proof of the relations (31) and (32), observe that $t(n) = 0$ implies $a(n) = b(n) = 0$; otherwise, since $u_0 = v_0 = 0$, the equation $u_p + v_m = n$ would have a solution. Thus, by using (2), (3), (4), (29), we get

\begin{align*}
    \tau(n_k - \sigma) &= \cdots = \tau(n_k - 1) = \tau(n_k + 1) = \cdots = \tau\left(n_k + \left\lfloor \frac{k}{40} \right\rfloor \right) = 0, \\
    \tau(n_k) &= 2Bb(u)b(v), \text{ with } (u, v) \in \mathbb{N}^2, \quad b(u)b(v) \neq 0. \\
\end{align*}

For the proof of the relation (34), by (29) one has $\tau(n_k) = Bs'(n_k) = 2Bb(u)b(v)$ for some $u = u_p$ and $v = v_m$ by (1), where $v_p + v_m = v_m + v_p = n_k$ comes from $s(n_k) = 2$.

But we know that

$$
    \rho(n) \leq d(n) \leq \exp\left(\frac{\log n}{\log \log n}\right)
$$

for large $n$ ([8; p. 262, Th. 317, and §18-7, p. 270]). Using (29), (2), (3), (4), and Lemmas 4 and 5, we get for large $n$

\begin{equation}
    \tau(n) \leq \exp\left(\frac{2 \log n}{\log \log n}\right) = \omega(n).
\end{equation}

Moreover, Theorem 5 and (24) yield

\begin{equation}
    n_k + \left[ \frac{k}{40} \right] + 1 \leq 40^{k-1} \exp(4LP_{2k}) + \left[ \frac{k}{40} \right] + 1.
\end{equation}

Using the prime number theorem in arithmetic progressions, we have for large $k$

\begin{equation}
    \frac{1}{4} \log p_{2k} \leq 2\varepsilon k \leq \frac{p_{2k}}{\log p_{2k}},
\end{equation}

where $p_{2k}$ is the $2k$-th prime number.
so that by (36)

\[ n_k + \left[ \frac{k}{40} \right] + 1 \leq \exp(8Lp_{2[e_k]}). \]

Hence we get by (35)

\[ \log \omega \left( n_k + \left[ \frac{k}{40} \right] + 1 \right) \leq \frac{16Lp_{2[e_k]}}{\log 8L + \log p_{2[e_k]}} \]

and so for large \( k \)

(38)

\[ \omega \left( n_k + \left[ \frac{k}{40} \right] + 1 \right) \leq \frac{32Lp_{2[e_k]}}{\log p_{2[e_k]}}. \]

We put \( h = p_{2[e_k]}/(\log p_{2[e_k]}) \). Then \( h \) tends to infinity as \( k \) does. By using (38) and (37), we get

\[ \frac{\omega(n_k + [k/40] + 1)}{|q|^{[k/40]}} \leq \frac{\exp 32L \cdot h}{|q|^{(h/320) - 1}}. \]

Therefore, by the choice of \( \varepsilon \) in (30), we have

\[ \lim_{k \to +\infty} \frac{\omega(n_k + [k/40] + 1)}{|q|^{[k/40]}} = 0. \]

Noting that \( \lim_{k \to +\infty} \omega(n + 1)/\omega(n) = 1 \), and recalling (29) and (33), we can apply Theorem 4 and obtain

\[ Fq^{n_1} + \sum_{n=0}^{n_k} \tau(n)q^{n_k-n} = 0. \]

By using (33) and (34), we now have for some \((u, v) \in \mathbb{N}^2\)

\[ Fq^{n_1} + 2Bb(u)b(v) + \sum_{n=0}^{n_k-\sigma-1} \tau(n)q^{n_k-n} = 0. \]

Thus \( q^{\sigma+1} \) divides \( 2Bb(u)b(v) \), and this contradiction proves that \( B = 0 \).

Second step. We now suppose that \( C \neq 0 \), and we choose \( \sigma \) such that \( q^\sigma \) does not divide any of the numbers \( 2Ca(u)b(v) \) for \((u, v) \in \mathbb{N}^2\) with \( a(u)b(v) \neq 0 \). In Theorem 5, we put

\[ \delta = 40\sigma + 16, \]
and choose $\varepsilon$ as in (30), $\Omega_1 = 5$, $\Omega_2 = 5$, $\theta_1 = 1$, $\theta_2 = 2$. Then $N_k$ in (23) satisfies $N_k \equiv 10 \pmod{40}$ and we put $n_k = (N_k - 10)/40$. By using (15), (22), and Lemmas 3, 4 and 5 (observe that $N_k = 40n_k + 10$, so that (17) in Lemma 5 applies), we get

$$t(n_k - \sigma) = \cdots = t(n_k - 1) = t(n_k + 1) = \cdots = t(n_k + \frac{k}{40}) = 0,$$

$$t(n_k) = 2,$$

$$r(n_k - \sigma) = \cdots = r(n_k - 1) = r(n_k) = \cdots = r(n_k + \frac{k}{40}) = 0,$$

$$s(n_k - \sigma) = \cdots = s(n_k - 1) = s(n_k) = \cdots = s(n_k + \frac{k}{40}) = 0,$$

$$a(n_k - \sigma) = \cdots = a(n_k - 1) = a(n_k) = \cdots = a(n_k + \frac{k}{40}) = 0,$$

$$b(n_k - \sigma) = \cdots = b(n_k - 1) = b(n_k) = \cdots = b(n_k + \frac{k}{40}) = 0.$$

By arguing exactly the same way as the first step, we obtain $C = 0$.

Third step. Suppose that $A \neq 0$, and choose $\sigma$ such that $q^\sigma$ does not divide any of the numbers $2Aa(u)a(v)$ for $(u, v) \in \mathbb{N}^2$ with $a(u)a(v) \neq 0$. Choose again $\delta = 40\sigma + 16$, $\varepsilon$ as in (30), $\Omega_1 = 1$, $\Omega_2 = 5$, $\theta_1 = 1$, $\theta_2 = 2$ in Theorem 5, and put $n_k = (N_k - 2)/40$. By going on exactly as in the first and second steps, one can prove that $A = 0$.

Fourth step. Thus we have $D\alpha_q + E\beta_q + F = 0$. It can be proved, by elementary means, this is impossible. Hence Theorem 3 is proved.

ACKNOWLEDGEMENT. This paper has been written at the occasion of two stays of the first-named author in Keio University, Yokohama, in June 1996 and 1997; the author thanks Professors Kumiko Nishioka and Iekata Shiokawa for their kind invitation and hospitality.

References


D. Duverney
24 Place du Concert
59800 LILLE, France
e-mail: duverney@gat.univ-lille1.fr

I. Shiokawa
Department of Mathematics
Keio University
Hiyoshi 3-14-1, Kohoku-ku
Yokohama 223-0061, Japan
e-mail: shiokawa@math.keio.ac.jp