

STICHTING  
MATHEMATISCH CENTRUM  
2e BOERHAAVESTRAAT 49  
AMSTERDAM

ZW 1953-232

Prime factors of the elements of certain  
sequences of integers

C.G. Lekkerkerker

Reprinted from  
Proceedings of the KNAW, Series A, 56(1953)  
Indagationes Mathematicae, 15(1953), p 265-280



MATHEMATICS

53.232

PRIME FACTORS OF THE ELEMENTS OF CERTAIN SEQUENCES  
 OF INTEGERS

I

BY

C. G. LEKKERKERKER

(Communicated by Prof. J. F. KOKSMA at the meeting of March 28, 1953)

1. *Introduction*

Very recently by VAN DER POL our attention was drawn to the following property of recurring sequences <sup>1)</sup>).

If  $\omega$ ,  $\bar{\omega}$  are two coprime rational integers, different in absolute value and not equal to zero, and if

$$(1.1) \quad u_n = \frac{\omega^n - \bar{\omega}^n}{\omega - \bar{\omega}} \quad (n = 0, 1, 2, \dots),$$

then each element  $u_n$ , with a finite number of exceptions, contains a prime factor  $q$ , which does not divide any of the elements  $u_1, u_2, \dots, u_{n-1}$ .

One may ask whether this result may be generalized. In the following we shall show that this is possible indeed. The restriction, imposed on  $\omega$ ,  $\bar{\omega}$ , to be coprime can be removed completely. Moreover it turns out that the result remains valid if for  $\omega$  we take a real quadratic integer and for  $\bar{\omega}$  its conjugate. So we obtain the following theorem a proof of which is the main object of this paper.

**Theorem.** Let  $a$ ,  $b$  be two non-vanishing rational integers with

$$(1.2) \quad a^2 + 4b > 0$$

and let  $\omega$ ,  $\bar{\omega}$  be the roots of the equation

$$(1.3) \quad x^2 - ax - b = 0.$$

Then the sequence of rational integers

$$(1.4) \quad u_n = \frac{\omega^n - \bar{\omega}^n}{\omega - \bar{\omega}} \quad (n = 0, 1, 2, \dots)$$

has the property, that for each positive integer  $n$ , with a finite number of exceptions, there exists a prime  $q$  with

$$q \mid u_n, \quad q \nmid u_m \quad \text{for } m = 1, 2, \dots, n-1.$$

**Preliminary remarks.** In view of  $a \neq 0$  and  $a^2 + 4b > 0$ , the numbers  $\omega$  and  $\bar{\omega}$  evidently are real and different in absolute value. Since inter-

<sup>1)</sup> Cf. L. E. DICKSON, History of the theory of numbers, (New York, 1934) Vol. I, especially the results of A. S. BANG (p. 385) and of G. D. BIRKHOFF-H. S. VANDIVER (p. 388).

changing  $\omega$  and  $\tilde{\omega}$  does not affect the assertion of the theorem, we may suppose without loss of generality

$$(1.5) \quad |\omega| > |\tilde{\omega}|.$$

From (1.3) it follows that  $\omega$ ,  $\tilde{\omega}$  satisfy the relations

$$(1.6) \quad \omega^2 = a\omega + b, \quad \tilde{\omega}^2 = a\tilde{\omega} + b.$$

Using (1.6) we deduce from (1.1) that the integers  $u_n$  satisfy the following relations

$$(1.7) \quad u_0 = 0, \quad u_1 = 1, \quad u_{n+2} = au_{n+1} + bu_n \quad (n = 0, 1, 2, \dots).$$

The sequence  $\{u_n\}$  is determined uniquely by (1.7), so by (1.1) and (1.7) the same sequence is defined.

By means of the relations (1.7) the following formulae can easily be proved by induction

$$(1.8) \quad \omega^n = u_n \omega + bu_{n-1}, \quad \tilde{\omega}^n = u_n \tilde{\omega} + bu_{n-1} \quad (n = 1, 2, \dots).$$

With the aid of the last relations a certain kind of addition formula can be deduced. Let  $\mu$  be a positive integer,  $\nu$  a non-negative integer. From  $\omega^{\mu+\nu} = \omega^\mu \cdot \omega^\nu$  it follows by repeated application of (1.8) for  $\nu > 0$

$$\begin{aligned} u_{\mu+\nu} \omega + bu_{\mu+\nu-1} &= (u_\mu \omega + bu_{\mu-1}) (u_\nu \omega + bu_{\nu-1}) \\ &= u_\mu u_\nu \omega^2 + b(u_\mu u_{\nu-1} + u_{\mu-1} u_\nu) \omega + b^2 u_{\mu-1} u_{\nu-1}, \end{aligned}$$

hence by (1.6) and (1.7)

$$\begin{aligned} u_{\mu+\nu} \omega + bu_{\mu+\nu-1} &= (au_\mu u_\nu + bu_\mu u_{\nu-1} + bu_{\mu-1} u_\nu) \omega + \\ &+ b(u_\mu u_\nu + bu_{\mu-1} u_{\nu-1}) \\ &= (u_\mu u_{\nu+1} + bu_{\mu-1} u_\nu) \omega + b(u_\mu u_\nu + bu_{\mu-1} u_{\nu-1}). \end{aligned}$$

The same relation holds with  $\omega$  replaced by  $\tilde{\omega}$ . Hence by (1.5) we may conclude

$$(1.9) \quad u_{\mu+\nu} = u_\mu u_{\nu+1} + bu_{\mu-1} u_\nu.$$

Since this relation also holds if  $\nu = 0$ , (1.9) is valid for  $\mu > 0$ ,  $\nu \geq 0$ .

## 2. Some lemma's

Elsewhere<sup>2)</sup> periodicity properties, modulo an arbitrary positive integer  $m$ , for the sequence defined by (1.7) are studied extensively. These properties partially coincide with some of our lemma's; for the sake of completeness however we shall give a proof of all our assertions in section 3.

*Lemma 1.* Let  $q$  be a prime. If  $q \nmid b$ , then there exists for each positive integer  $t$  a positive integer  $c = c(q^t)$ , such that

$$(2.1) \quad q^t \mid u_n \text{ if and only if } c(q^t) \mid n.$$

If  $q \mid b$ ,  $q \nmid a$ , then  $q \mid u_n$  only if  $n = 0$ .

<sup>2)</sup> H. J. A. DUPARC-W. PEREMANS, Reduced sequences of integers and pseudo-random numbers II, Rapport Z. W. 1952-013, Mathematisch Centrum, Amsterdam (dutch).

Before stating the other lemma's we introduce the following symbols which will appear to be useful.

If  $q$  is a prime and  $f$  an arbitrary positive integer, then

$$(2.2) \quad A(q, f)$$

denotes the number of factors  $q$  which are contained in  $f$  (possibly 0). Furthermore, if  $q \nmid b$  and  $n$  is a positive multiple of  $c(q)$ , we write

$$(2.3) \quad \eta(q, n) = A\left(q, \frac{n}{c(q)}\right),$$

so  $\eta(q, n)$  denotes the difference in the number of factors  $q$ , contained respectively in  $n$  and the smallest positive integer  $c$  with  $q \mid u_c$ .

*Lemma 2.* Let  $q$  be a prime with  $q \nmid b$ . Then there exists a positive integer  $k = k(q)$  with the following properties

$$(2.4) \quad A(q, u_n) = 0 \text{ if } c(q) \nmid n$$

$$(2.5) \quad A(q, u_n) = k + \eta(q, n) \text{ if } c(q) \mid n,$$

except when we have simultaneously

$$q = 2, A(2, u_{c(2)}) = 1, \eta(2, n) = 0;$$

in this case the right hand member of (2.5) must be replaced by 1.

*Lemma 3.* Let  $q$  be a prime with  $q \mid b$ ,  $q \nmid a$ . Let  $\alpha, \beta$  be the positive integers

$$(2.6) \quad \alpha = A(q, a), \beta = A(q, b).$$

If  $2\alpha < \beta$ , then

$$(2.7) \quad A(q, u_n) = (n-1)\alpha \quad (n = 1, 2, \dots).$$

If  $2\alpha \geq \beta$ , then there exist a positive integer  $d = d(q)$  and a monotonously increasing function  $\varphi_q(x) = \varphi_q(a, b; x)$ , defined on the set of non negative integers  $x$ , depending on  $q, a, b$  and assuming integral values only, with the following properties

$$(2.8) \quad A(q, u_n) = \frac{n-1}{2} \beta \text{ if } d \nmid n$$

$$(2.9) \quad A(q, u_n) = \frac{n}{2} \beta + \varphi_q\left(A\left(q, \frac{n}{d}\right)\right) \text{ if } d \mid n \quad \left. \vphantom{\begin{matrix} (2.8) \\ (2.9) \end{matrix}} \right\} (n = 1, 2, \dots).$$

Although generally spoken no definite statement can be made about the values of  $\varphi_q(0)$  and  $\varphi_q(1)$ , the following formula holds in each case:

$$(2.10) \quad \varphi_q(x) = x - 1 + \varphi_q(1) \quad (x = 1, 2, \dots).$$

*Lemma 4.* Suppose  $g = (a, b)$  and put

$$(2.11) \quad g = q_1^{l_1} q_2^{l_2} \dots q_\sigma^{l_\sigma},$$

where  $q_1, q_2, \dots, q_\sigma$  are different primes and  $l_1, l_2, \dots, l_\sigma$  are positive integers. Let  $n$  be an integer  $> 1$  and put

$$(2.12) \quad n = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s},$$

where  $p_1, p_2, \dots, p_s$  are different primes and  $r_1, r_2, \dots, r_s$  are positive integers. Put

$$(2.13) \quad v_m = \prod_{j=1}^{\sigma} q_j^{A(q_j, u_m)} \quad (m = 1, 2, \dots),$$

$$(2.14) \quad v(i_1, i_2, \dots, i_k) = v_m,$$

where  $i_1, i_2, \dots, i_k$  are positive integers with  $1 \leq i_1 < i_2 < \dots < i_k \leq s$  ( $1 \leq k \leq s$ ) and  $m = \frac{n}{p_{i_1} p_{i_2} \dots p_{i_k}}$ ,

$$(2.15) \quad \gamma_j = \min(A(q_j, a), \frac{1}{2}A(q_j, b)),$$

$$(2.16) \quad \varepsilon_k = (-1)^k \quad (k = 1, 2, \dots, s).$$

Then we have

$$(2.17) \quad \left\{ \begin{aligned} & v_n [\prod^{(1)} v(i_1)]^{\varepsilon_1} \cdot [\prod^{(2)} v(i_1, i_2)]^{\varepsilon_2} \dots [\prod^{(k)} v(i_1, i_2, \dots, i_k)]^{\varepsilon_k} \dots \\ & \dots [v(1, 2, \dots, s)]^{\varepsilon_s} \leq K \cdot (q_1^{\gamma_1} q_2^{\gamma_2} \dots q_s^{\gamma_s})^{\varphi(n)}, \end{aligned} \right.$$

where the product  $\prod^{(k)}$  is extended over the sets  $(i_1, i_2, \dots, i_k)$  with  $1 \leq i_1 < i_2 < \dots < i_k \leq s$  and where  $K = K(a, b)$  is a constant not depending on  $n$ , whereas  $\varphi(n)$  denotes Euler's  $\varphi$ -function.

*Lemma 5.* Given a finite number of non vanishing integers  $x_1, x_2, \dots, x_w$ , we have the following formula

$$(2.18) \quad \left\{ \begin{aligned} & \{x_1, x_2, \dots, x_w\} = [\prod^{(1)} x_{i_1}]^{-\varepsilon_1} \cdot [\prod^{(2)} (x_{i_1}, x_{i_2})]^{-\varepsilon_2} \dots \\ & \dots [\prod^{(k)} (x_{i_1}, x_{i_2}, \dots, x_{i_k})]^{-\varepsilon_k} \dots [(x_1, x_2, \dots, x_w)]^{-\varepsilon_w}, \end{aligned} \right.$$

where the product  $\prod^{(k)}$  is extended over the sets  $(i_1, i_2, \dots, i_k)$  with  $1 \leq i_1 < i_2 < \dots < i_k \leq w$ ,  $\varepsilon_k$  is defined by (2.16) and  $\{a_1, a_2, \dots, a_n\}$  and  $(a_1, a_2, \dots, a_n)$  denote the least common multiple and the greatest common divisor of  $a_1, a_2, \dots, a_n$  respectively.

### 3. Proof of the lemma's

*Proof of lemma 1.* Suppose  $q \nmid b$ . We can find two positive integers,  $n$  and  $n+h > n$  say, with

$$(3.1) \quad u_{n+h} \equiv u_n \pmod{q^t}, \quad u_{n+h-1} \equiv u_{n-1} \pmod{q^t},$$

since the number of pairs of classes of residues modulo  $q^t$  is evidently finite. If  $n > 1$ , then from (3.1) and the recurrence relations (1.7) we deduce  $bu_{n+h-2} \equiv bu_{n-2} \pmod{q^t}$ , which by assumption implies  $u_{n+h-2} \equiv u_{n-2} \pmod{q^t}$ . Using this relation and the second part of (3.1) we can proceed in this way, until we find  $u_h \equiv u_0 \equiv 0 \pmod{q^t}$ . So the existence of a positive integer  $h$  with  $q^t \mid u_h$  is secured. Let  $c$  be the smallest positive integer with that property.

Using the above argument reversed we see  $u_{2c} \equiv u_c \pmod{q^t}$ , etc. .... So we have

$$q^t \mid u_{hc} \text{ for } h = 1, 2, \dots$$

If on the other hand  $q^t \mid u_n$  for a certain positive integer  $n$ , then put

$n = hc + r$ , where  $0 \leq r < c$  and  $h$  is a positive integer. Then by (1.9) we have  $u_n = u_{hc}u_{r+1} + bu_{hc-1}u_r$ , hence  $q^t \mid bu_{hc-1}u_r$ .

If  $q$  was a divisor of  $u_{hc-1}$ , then from  $bu_{hc-2} = u_{hc} - au_{hc-1}$  and  $q \nmid b$ , we would obtain  $q \mid u_{hc-2}$ , hence also  $q \mid u_{hc-3}, \dots, q \mid u_1$ ; this is a contradiction, since  $u_1 = 1$ . Hence we have  $q \nmid u_{hc-1}$ . From  $q^t \mid bu_{hc-1}u_r$ ,  $q \nmid b$ ,  $q \nmid u_{hc-1}$  it follows that we have  $q^t \mid u_r$ . Hence, by the definition of  $c$ , we have  $r = 0$ . So the first part of the lemma is proved.

Now let  $q \mid b$ ,  $q \nmid a$ .

First we have  $q \nmid u_1$ . Secondly, if  $q \nmid u_n$ , then  $q \nmid u_{n+1}$  ( $n = 1, 2, \dots$ ), since from  $q \mid u_{n+1}$  and  $q \mid b \mid bu_{n-1} = u_{n+1} - au_n$  would follow  $q \mid au_n$ , hence  $q \mid u_n$  in view of  $q \nmid a$ . This proves the second part of the lemma.

*Proof of lemma 2.* The relation (2.4) is a restatement of the part of (2.1), implied by the words "only if".

We now prove, that if  $q$  is an odd prime (2.5) is valid, when we take

$$k = k(q) = A(q, u_{c(q)}).$$

Let  $n$  be a positive integer with  $c(q) \mid n$ , i.e.  $q \mid u_n$ . Put  $h = A(q, u_n)$ . Then  $u_n = eq^h$  with  $q \nmid e$ ,  $h \geq 1$ . Applying (1.8) we find

$$(3.2) \quad \begin{cases} u_{qn}\omega + bu_{qn-1} = \omega^n = (u_n\omega + bu_{n-1})^q \\ = b^q u_{n-1}^q + eb^{q-1} u_{n-1}^{q-1} q^{h+1} \omega + \dots + e^q q^{qh} \omega^q. \end{cases}$$

In the last member for  $j = 2, \dots, q$  replace  $\omega^j$  by  $u_j\omega + bu_{j-1}$ . Since for a prime  $q > 2$  the coefficient of  $\omega^j$  in the right hand member of (3.2) contains at least the factor  $q^{2h+1}$  for  $j = 2, \dots, q$ , we obtain

$$(3.3) \quad u_{qn}\omega + bu_{qn-1} = a_1\omega + a_2,$$

where  $a_1, a_2$  are two rational integers with

$$a_1 \equiv eb^{q-1} u_{n-1}^{q-1} q^{h+1} \pmod{q^{h+2}}.$$

The relation (3.3) remains true if we replace  $\omega$  by  $\bar{\omega}$ . Hence we have

$$(3.4) \quad u_{qn} \equiv eb^{q-1} u_{n-1}^{q-1} q^{h+1} \pmod{q^{h+2}}.$$

In view of  $q \nmid e$ ,  $q \nmid b$ ,  $q \nmid u_{n-1}$  we may conclude

$$(3.5) \quad A(q, u_{qn}) = h + 1 \text{ if } A(q, u_n) = h > 0.$$

In particular we have  $A(q, u_{qc(q)}) = k + 1$ . If  $n$  is a positive integer with  $c(q) \mid n$ , then by the first part of lemma 1, we have  $A(q, u_n) \geq k$ . If moreover  $\eta(q, n) = 0$ , then we do not have  $A(q, u_n) \geq k + 1$ . For from  $A(q, u_{qc(q)}) = k + 1$ ,  $A(q, u_n) \geq k + 1$  and the first part of lemma 1 would follow  $A(q, u_{c(q)}) = k + 1$ , which is a contradiction. This proves (2.5) in the case  $\eta(q, n) = 0$ . The validity of (2.5) for other values of  $\eta(q, n)$  now is an immediate consequence of (3.5).

We note, that for positive integers  $t$ , on account of the first part of lemma 1 and the relations (2.4) and (2.5), we have the following formula

$$(3.6) \quad c(q^t) = q^{\max(0, t-k)} c(q).$$

If  $q = 2$ , then again (3. 2) is valid; it has the form

$$u_{2n}\omega + bu_{2n-1} = b^2 u_{n-1}^2 + ebu_{n-1} 2^{h+1}\omega + e^2 2^{2h}\omega^2.$$

Hence we have for  $c(2) \mid n$

$$(3. 4a) \quad u_{2n} = ebu_{n-1} 2^{h+1} + e^2 a 2^{2h} \quad (h = A(2, u_{c(2)}).$$

Since  $2h > h + 1$  only if  $h \geq 2$ , the deduction of (3. 5) remains valid only if  $h \geq 2$ . Thus in the case  $q = 2$ ,  $A(2, u_{c(2)}) \geq 2$  the formula (2. 5) can be proved with  $k = A(2, u_{c(2)})$  by the same argument as before.

Finally suppose  $q = 2$ ,  $A(2, u_{c(2)}) = 1$ . Then put

$$k = k(2) = A(2, u_{2c(2)}) - 1.$$

At any rate by (3. 4a) we have  $4 \mid u_{2c(2)}$ , hence  $k \geq 1$ . If  $2c(2) \mid n$  and moreover  $4c(2) \nmid n$ , i.e.  $\eta(2, n) = 1$ , then by the same argument as before we may conclude  $A(2, u_n) = A(2, u_{2c(2)}) = k + 1$ . From the last relation and (3. 5) we infer the truth of (2. 5) in the case  $\eta(2, n) \geq 1$ . If  $\eta(2, n) = 0$ , then  $A(2, u_n) = A(2, u_{c(2)}) = 1$ .

*Proof of lemma 3.* If  $2\alpha < \beta$ , then from  $u_2 = a$ ,  $u_3 = a^2 + b$  it follows that (2. 7) holds for  $n = 2, 3$ . If  $A(q, u_n) = (n - 1)\alpha$ ,  $A(q, u_{n+1}) = n\alpha$ , then we have  $A(q, u_{n+2}) = (n + 1)\alpha$  on account of

$$\begin{aligned} u_{n+2} &= au_{n+1} + bu_n, \quad A(q, au_{n+1}) = (n + 1)\alpha, \\ A(q, bu_n) &= \beta + (n - 1)\alpha > (n + 1)\alpha. \end{aligned}$$

Hence, by induction on  $n$ , we see that (2. 7) is true for  $n = 1, 2, \dots$

Now suppose  $2\alpha = \beta$ . Using the same argument as above we see, by induction on  $n$ ,

$$(3. 7) \quad A(q, u_n) \geq (n - 1)\alpha = \frac{n-1}{2}\beta \quad (n = 1, 2, \dots);$$

however it can not be decided by that argument whether in (3. 7) the equality sign holds. We put

$$a^* = \frac{a}{q^\alpha}, b^* = \frac{b}{q^{2\alpha}}, u_0^* = 0, u_n^* = \frac{u_n}{q^{(n-1)\alpha}} \quad (n = 1, 2, \dots).$$

Then  $a^*$ ,  $b^*$ ,  $u_n^*$  are integers satisfying

$$q \nmid a^*, q \nmid b^*, u_0^* = 0, u_1^* = 1, u_{n+2}^* = a^* u_{n+1}^* + b^* u_n^*.$$

Hence on the sequence  $\{u_n^*\}$  lemma 2 can be applied. So there exist two positive integers  $c^* = c^*(q)$  and  $k^* = k^*(q)$ , such that

$$\begin{aligned} A(q, u_n^*) &= 0 \text{ if } c^* \nmid n \\ A(q, u_n^*) &= k^* + A\left(q, \frac{n}{c^*}\right) \text{ if } c^* \mid n, \end{aligned}$$

with the exception that  $A(q, u_n^*)$  is always equal to 1, in the case  $q = 2$ ,  $A(2, u_{c^*(2)}^*) = 1$ , if  $n$  has a value with  $c^* \mid n$ ,  $2c^* \nmid n$ . From these facts follow (2. 8), (2. 9), (2. 10) if we take

$$\left. \begin{aligned} \varphi_q(0) &= -\frac{1}{2}\beta + k^*(q) \text{ or } -\frac{1}{2}\beta + 1 \\ \varphi_q(1) &= -\frac{1}{2}\beta + k^*(q) + 1 \\ \varphi_q(x) &= x - 1 + \varphi_q(1) \end{aligned} \right\} \quad (x = 1, 2, \dots).$$

It should be noted that  $\frac{1}{2}\beta$  is integral, in view of the assumption  $2\alpha = \beta$ .

Finally we treat the case  $2\alpha > \beta$ . First we prove, by induction on  $n$ , the following formulae

$$\left. \begin{aligned} (3.8) \quad A(q, u_n) &= \frac{n-1}{2} \beta \text{ if } n \text{ is odd} \\ (3.9) \quad A(q, u_n) &\geq \alpha + \frac{n-2}{2} \beta \text{ if } n \text{ is even} \end{aligned} \right\} \quad (n = 1, 2, \dots).$$

If  $n = 1$  or  $2$ , (3.8) and (3.9) respectively are trivially true. If  $m$  is a positive integer and (3.8), (3.9) hold for  $n = 2m - 1$  and for  $n = 2m$  respectively, we deduce

$$A(q, u_{2m+1}) = A(q, au_{2m} + bu_{2m-1}) = A(q, bu_{2m-1}) = m\beta,$$

since we have

$$A(q, au_{2m}) = \alpha + A(q, u_{2m}) \geq 2\alpha + (m-1)\beta > m\beta = A(q, bu_{2m-1});$$

and

$$A(q, u_{2m+2}) = A(q, au_{2m+1} + bu_{2m}) \geq \alpha + m\beta.$$

So (3.8) and (3.9) are proved.

In order to determine exactly the value of  $A(q, u_n)$  if  $n$  is even, we now deduce a recurrence relation for the numbers  $u_{2m}$  ( $m = 0, 1, 2, \dots$ ), analogous to the relations (1.7) for the numbers  $u_n$ . Using (1.7) with  $n = 2m, 2m+1, 2m+2$  and eliminating  $u_{2m+1}, u_{2m+3}$ , we obtain

$$u_{2m+4} = bu_{2m+2} + a(au_{2m+2} + bu_{2m+1}) = (a^2 + 2b)u_{2m+2} - b^2u_{2m}.$$

In view of  $a \mid u_0, a \mid u_2$  we have  $a \mid u_{2m}$  for all  $m$ .

We put

$$(3.10) \quad a^* = \frac{a^2+2b}{q^\beta}, b^* = -\frac{b^2}{q^{2\beta}}, u_0^* = 0, u_m^* = \frac{u_{2m}}{aq^{(m-1)\beta}} \quad (m = 1, 2, \dots).$$

By the last remark and (3.9) the numbers  $a^*, b^*, u_m^*$  are integers. Furthermore we have  $u_0^* = 0, u_1^* = 1$ ,

$$(3.11) \quad \begin{cases} a^*u_{m+1}^* + b^*u_m^* = \frac{(a^2+2b)u_{2m+2}}{q^\beta \cdot aq^{m\beta}} - \frac{b^2u_{2m}}{q^{2\beta} \cdot aq^{(m-1)\beta}} \\ = \frac{(a^2+2b)u_{2m+2} - b^2u_{2m}}{aq^{(m+1)\beta}} = \frac{u_{2m+4}}{aq^{(m+1)\beta}} = u_{m+2}^*. \end{cases}$$

From (3.10) follows  $q \nmid b^*$ . So lemma 2 can be applied on the sequence  $\{u_m^*\}$ , i.e. there exist positive integers  $c^* = c^*(q)$  and  $k^* = k^*(q)$  such that

$$\begin{aligned} A(q, u_m^*) &= 0 \text{ if } c^* \nmid m, \\ A(q, u_m^*) &= k^* + A\left(q, \frac{m}{c^*}\right) \text{ if } c^* \mid m; \end{aligned}$$

in the case  $q = 2, 2\alpha > \beta, A(2, u_{c^*(2)}^*) = 1$  however we have  $A(q, u_m^*) = 1$  if  $c^* \mid m, 2c^* \nmid m$ .

A further property of the sequence  $\{u_m^*\}$  is the fact, that the numbers  $c^*, k^*$  can be determined exactly (except for the number  $k^*$  in the case



$q = 2$ ). By repeated application of (1. 8) we find in the case  $q > 2$

$$\begin{aligned} u_{2q}\omega + u_{2q-1} &= \omega^{2q} = (a\omega + b)^q \\ &= \sum_{n=0}^q \binom{q}{n} a^n \omega^n b^{q-n} = \sum_{n=1}^q \binom{q}{n} a^n (u_n \omega + bu_{n-1}) b^{q-n} + b^q, \\ u_{2q} &= \sum_{n=1}^q \binom{q}{n} a^n b^{q-n} u_n = \sum_{n=1}^q X_n, \text{ say.} \end{aligned}$$

By (3. 8) and (3. 9) we have

$$\begin{aligned} A(q, X_1) &= A(q, qab^{q-1}) = 1 + \alpha + (q-1)\beta, \quad A(q, X_q) = q\alpha + \frac{q-1}{2}\beta, \\ A(q, X_n) &= 1 + n\alpha + (q-n)\beta + \frac{n-1}{2}\beta = 1 + n\alpha + \left(q-1 - \frac{n-1}{2}\right)\beta \\ &\quad \text{if } n \text{ is odd and } 2 \leq n \leq q-1 \\ A(q, X_n) &\geq 1 + n\alpha + (q-n)\beta + \alpha + \frac{n-2}{2}\beta \\ &= 1 + (n+1)\alpha + \left(q-1 - \frac{n}{2}\right)\beta \text{ if } n \text{ is even and } 2 \leq n \leq q-1. \end{aligned}$$

Hence in view of  $\alpha > \frac{1}{2}\beta$  we find

$$A(q, X_n) > A(q, X_1) \text{ for } n = 2, \dots, q,$$

so

$$A(q, u_{2q}) = A(q, X_1) = 1 + \alpha + (q-1)\beta,$$

hence  $A(q, u_q^*) = 1$ . Since  $q$  is a prime, from this relation and lemma 2 follows  $q \nmid u_m^*$  for  $1 \leq m \leq q-1$ . This shows that we have  $c^* = q$ ,  $k^* = 1$  in the case  $q > 2$ . For arbitrary  $m$  we now have

$$(3. 12) \quad A(q, u_m^*) = A(q, m).$$

In the case  $q = 2$  however, we have  $u_2^* = a^* = \frac{a^2+2b}{q\beta}$ , which only implies  $A(2, u_2^*) \geq 1$ . Hence we only may conclude  $c^*(2) = 2$ . For even  $m$  we get

$$(3. 12a) \quad A(2, u_m^*) = A\left(2, \frac{m}{2}\right) + k^*(2).$$

Taking  $d(q) = 2$ ,  $\varphi_q(0) = \alpha - \beta$ ,  $\varphi_q(x) = x + \varphi_q(0)$  if  $q > 2$ ,

$$d(2) = 2, \quad \varphi_2(0) = \alpha - \beta, \quad \varphi_2(1) = \alpha - \beta + k^*(2),$$

$$\varphi_2(x) = x - 1 + \varphi_2(1) \quad (x = 1, 2, \dots),$$

the relations (2. 8), (2. 9), (2. 10) follow from (3. 8), (3. 10), (3. 12), (3. 12a). This completes the proof of the lemma.

*Proof of lemma 4.* Let the left hand member of (2. 17) be denoted by  $M_1$  and let  $q$  be one of the prime factors  $q_1, q_2, \dots, q_\sigma$  of  $g$ . Let  $\alpha$  and  $\beta$  be given by (2. 6). In the case  $2\alpha \geq \beta$  let  $d$  and  $\varphi_q(x)$  be determined by lemma 3. In order to evaluate  $A(q, M_1)$  we distinguish the following five cases according to the values of  $\alpha$ ,  $\beta$ ,  $n$

- I.  $2\alpha < \beta$
- II.  $2\alpha \geq \beta$  and  $d \nmid n$
- III.  $2\alpha \geq \beta$ ;  $d \mid \frac{n}{p_i}$  if and only if  $i = 1, 2, \dots, s_1$  where  $s_1$  is an integer with  $1 \leq s_1 \leq s$ ;  $q \neq p_1, p_2, \dots, p_{s_1}$
- IV.  $2\alpha \geq \beta$ ;  $q = p_1$ ;  $d \mid \frac{n}{p_i}$  if and only if  $i = 1, 2, \dots, s_1$  where  $s_1$  is an integer with  $2 \leq s_1 \leq s$
- V.  $2\alpha \geq \beta$ ;  $q = p_1$ ;  $d \mid n$ ;  
 $\frac{n}{d} = q^t$  where  $t$  is a non negative integer.

It is obvious that in each case, after having arranged the prime factors of  $n$  in (2.12) in a suitable way, (exactly) one of the cases I–V occurs. In the sequel  $i_1, i_2, \dots, i_k$  are always supposed to form a set of unequal positive integers with increasing order.

*Case I.* By (2.7) and (2.13) we have  $A(q, v_n) = A(q, u_n) = (n-1)\alpha$ . Using also (2.14) we further have for each admissible set  $(i_1, i_2, \dots, i_k)$

$$A(q, v(i_1, i_2, \dots, i_k)) = A(q, u(i_1, i_2, \dots, i_k)) = \left( \frac{n}{p_{i_1} p_{i_2} \dots p_{i_k}} - 1 \right) \alpha.$$

In view of the form of  $M_1$  this yields

$$\begin{aligned} A(q, M_1) &= A(q, u_n) - \sum^{(1)} A(q, u(i_1)) + \sum^{(2)} A(q, u(i_1, i_2)) - \dots \\ &\dots + (-1)^k \sum^{(k)} A(q, u(i_1, i_2, \dots, i_k)) + \dots + (-1)^s A(q, u(1, 2, \dots, s)) \\ &= n\alpha \cdot \left[ 1 - \sum^{(1)} \frac{1}{p_{i_1}} + \sum^{(2)} \frac{1}{p_{i_1} p_{i_2}} - \dots + (-1)^s \frac{1}{p_1 p_2 \dots p_s} \right] \\ &- \alpha \cdot \left[ 1 - \binom{s}{1} + \binom{s}{2} - \dots + (-1)^s \right], \end{aligned}$$

the superscript  $(k)$  denoting summation over all admissible sets  $(i_1, i_2, \dots, i_k)$ , hence in view of  $s \geq 1$  and a wellknown formula for  $\varphi(n)$

$$A(q, M_1) = \alpha \varphi(n).$$

*Case II.* By (2.8), (2.13) we have  $A(q, v_n) = \frac{n-1}{2}\beta$ ,

$$A(q, v(i_1, i_2, \dots, i_k)) = \frac{1}{2} \beta n \cdot (p_{i_1} p_{i_2} \dots p_{i_k})^{-1} - \frac{1}{2} \beta.$$

This yields  $A(q, M_1) = \frac{1}{2} \beta \varphi(n)$ .

*Case III.* We have  $d \mid n$ . Applying (2.8) and (2.9) we obtain

$$\begin{aligned} A(q, v_n) &= \frac{1}{2} \beta n + \varphi_q \left( A \left( q, \frac{n}{d} \right) \right) \\ A(q, v(i_1, i_2, \dots, i_k)) &= \begin{cases} \frac{1}{2} \beta \cdot \frac{n}{p_{i_1} p_{i_2} \dots p_{i_k}} + \varphi_q \left( A \left( q, \frac{n}{d} \right) \right) & \text{if } i_k \leq s_1 \\ \frac{1}{2} \beta \cdot \frac{n}{p_{i_1} p_{i_2} \dots p_{i_k}} - \frac{1}{2} \beta & \text{if } i_k > s_1, \end{cases} \end{aligned}$$

since in view of the assumptions we have  $d \mid \frac{n}{p_{i_1} p_{i_2} \dots p_{i_k}}$ ,

$$A \left( q, \frac{n}{p_{i_1} p_{i_2} \dots p_{i_k}} \right) = A \left( q, \frac{n}{d} \right) \text{ if } i_k \leq s_1 \text{ and } d \nmid \frac{n}{p_{i_1} p_{i_2} \dots p_{i_k}} \text{ if } i_k > s_1.$$

Putting  $-\frac{1}{2}\beta = b_0$ ,  $\varphi_q(A(q, \frac{n}{d})) + \frac{1}{2}\beta = b_1$ , we find

$$\begin{aligned} A(q, M_1) &= \frac{1}{2}\beta n + b_0 + b_1 - \sum_{i_1=1}^s \left( \frac{1}{2}\beta \frac{n}{p_{i_1}} + b_0 \right) - \sum_{i_1=1}^{s_1} b_1 + \\ &+ \sum^{(2)} \left( \frac{1}{2}\beta \frac{n}{p_{i_1} p_{i_2}} + b_0 \right) + \sum_{i_1, i_2 \leq s_1} b_1 - \dots \\ &\dots + (-1)^{s_1} \sum^{(s_1)} \left( \frac{1}{2}\beta \frac{n}{p_{i_1} p_{i_2} \dots p_{i_{s_1}}} + b_0 \right) + (-1)^{s_1} b_1 + \dots \\ &\dots + (-1)^s \left( \frac{1}{2}\beta \frac{n}{p_1 p_2 \dots p_s} + b_0 \right)^3 \\ &= \frac{1}{2}\beta n \cdot \left[ 1 - \sum^{(1)} \frac{1}{p_{i_1}} + \sum^{(2)} \frac{1}{p_{i_1} p_{i_2}} - \dots + (-1)^s \frac{1}{p_1 p_2 \dots p_s} \right] \\ &+ b_0 \cdot \left[ 1 - \binom{s}{1} + \binom{s}{2} - \dots + (-1)^s \right] + b_1 \cdot \left[ 1 - \binom{s_1}{1} + \binom{s_1}{2} - \dots + (-1)^{s_1} \right]. \end{aligned}$$

Since the coefficients of  $b_0$  and  $b_1$  vanish in view of  $s \geq 1$ ,  $s_1 \geq 1$ , we find  $A(q, M_1) = \frac{1}{2}\beta\varphi(n)$ .

*Case IV.* In view of (2. 8), (2. 9) and the assumptions of this case we get

$$\begin{aligned} A(q, v_n) &= \frac{1}{2}\beta n + \varphi_q \left( A \left( q, \frac{n}{d} \right) \right) \\ A(q, v(i_1, i_2, \dots, i_k)) &= \begin{cases} \frac{1}{2}\beta n + \varphi_q \left( A \left( q, \frac{n}{d} \right) \right) & \text{if } i_1 > 1, i_k \leq s_1 \\ \frac{1}{2}\beta n + \varphi_q \left( A \left( q, \frac{n}{dq} \right) \right) & \text{if } i_1 = 1, i_k \leq s_1 \\ \frac{1}{2}\beta n - \frac{1}{2}\beta & \text{if } i_k > s_1. \end{cases} \end{aligned}$$

Hence, putting

$$-\frac{1}{2}\beta = b_0, \varphi_q \left( A \left( q, \frac{n}{dp_1} \right) \right) + \frac{1}{2}\beta = b_1, \varphi_q \left( A \left( q, \frac{n}{d} \right) \right) - \varphi_q \left( A \left( q, \frac{n}{dp_1} \right) \right) = b_2,$$

we find (in the finite sums writing down only the first terms)

$$\begin{aligned} A(q, M_1) &= \frac{1}{2}\beta n + b_0 + b_1 + b_2 - \sum_{i_1=1}^s \left( \frac{1}{2}\beta \frac{n}{p_{i_1}} + b_0 \right) - \sum_{i_1=1}^{s_1} b_1 - \sum_{i_1=2}^{s_1} b_2 \\ &+ \sum_{i_1, i_2} \left( \frac{1}{2}\beta \frac{n}{p_{i_1} p_{i_2}} + b_0 \right) + \sum_{i_1, i_2 \leq s_1} b_1 + \sum_{2 \leq i_1, i_2 \leq s_1} b_2 - \dots \\ &= \frac{1}{2}\beta n \cdot \left[ 1 - \sum^{(1)} \frac{1}{p_{i_1}} + \sum^{(2)} \frac{1}{p_{i_1} p_{i_2}} - \dots \right] + b_0 \cdot \left[ 1 - \binom{s}{1} + \binom{s}{2} - \dots \right] \\ &+ b_1 \cdot \left[ 1 - \binom{s_1}{1} + \binom{s_1}{2} - \dots \right] + b_2 \cdot \left[ 1 - \binom{s_1-1}{1} + \binom{s_1-1}{2} - \dots \right]. \end{aligned}$$

Thus we find the same result as in cases II, III.

*Case V.* Now we have in view of  $\frac{n}{d} = q^t$ , assuming  $t \geq 1$

$$\begin{aligned} A(q, v_n) &= \frac{1}{2}\beta n + \varphi_q \left( A \left( q, \frac{n}{d} \right) \right) = \frac{1}{2}\beta n + \varphi_q(t) \\ A(q, v(i_1, i_2, \dots, i_k)) &= \begin{cases} \frac{1}{2}\beta n + \varphi_q(t-1) & \text{if } k=1, i_1=1 \\ \frac{1}{2}\beta n - \frac{1}{2}\beta & \text{if } i_k > 1, \end{cases} \end{aligned}$$

<sup>3)</sup> If  $s_1$  is equal to  $s$ , then the terms with  $s_1$  are the last terms of this sum.



since there are  $\tau_{i_1}$  factors  $q$  contained in the number  $\{x_{i_1}, x_{i_2}, \dots, x_{i_k}\}$  and since there are  $\binom{w-1}{k-1}$  admissible sets  $(i_1, i_2, \dots, i_k)$  with  $i_1 = 1$ ,  $\binom{w-2}{k-1}$  admissible sets  $(i_1, i_2, \dots, i_k)$  with  $i_1 = 2$ , etc  $(k = 1, 2, \dots, w)$ .

Hence the total number of factors  $q$ , contained in the right hand member of (2.18) is equal to

$$\begin{aligned} & \left\{ 1 - \binom{w-1}{1} + \binom{w-1}{2} - \dots + (-1)^{w-2} \binom{w-1}{w-2} + (-1)^{w-1} \right\} \tau_1 + \\ & + \left\{ 1 - \binom{w-2}{1} + \binom{w-2}{2} - \dots + (-1)^{w-3} \binom{w-2}{w-3} + (-1)^{w-2} \right\} \tau_2 + \dots \\ & \dots + (1 - 2 + 1) \tau_{w-2} + (1 - 1) \tau_{w-1} + \tau_w \\ & = \tau_w = A(q, \{x_1, x_2, \dots, x_w\}). \end{aligned}$$

This being true for each prime  $q$  the lemma is proved.

*(To be continued)*

# MATHEMATICS

## PRIME FACTORS OF THE ELEMENTS OF CERTAIN SEQUENCES OF INTEGERS

### II

BY

C. G. LEKKERKERKER

(Communicated by Prof. J. F. KOKSMA at the meeting of March 28, 1953)

#### 4 Proof of the theorem

Let  $\{u_n\}$  be the sequence defined by (1.1). We consider a fixed integer  $n > 1$ . Let the factorization of  $n$  and  $g = (a, b)$  be given by (2.11) and (2.12). Then, on account of  $n > 1$ , by lemma 1 the primes  $q_1, q_2, \dots, q_\sigma$  are also contained in  $u_n$ . We put

$$(4.1) \quad |u_n| = q_1^{t_1} q_2^{t_2} \dots q_\sigma^{t_\sigma} q_{\sigma+1}^{t_{\sigma+1}} \dots q_{\sigma+\tau}^{t_{\sigma+\tau}}, \quad ^5)$$

where  $q_{\sigma+1}, \dots, q_{\sigma+\tau}$  are primes, different from each other and different from  $q_1, q_2, \dots, q_\sigma$  and where  $t_1, t_2, \dots, t_{\sigma+\tau}$  are positive integers (in our notation we have  $t_j = A(q_j, u_n)$  for  $j = 1, 2, \dots, \sigma + \tau$ ).

Furthermore we put,  $v_m$  being given by (2.13),

$$(4.2) \quad \begin{cases} \tilde{u}_m = \frac{u_m}{v_m} & (m = 1, 2, \dots) \\ u(i_1, i_2, \dots, i_k) = u_m, \quad \tilde{u}(i_1, i_2, \dots, i_k) = \tilde{u}_m \text{ with} \\ m = \frac{n}{p_{i_1} p_{i_2} \dots p_{i_k}} \quad (1 \leq i_1 < i_2 < \dots < i_k \leq s), \end{cases}$$

hence,  $v(i_1, i_2, \dots, i_k)$  being given by (2.14),

$$(4.3) \quad u(i_1, i_2, \dots, i_k) = v(i_1, i_2, \dots, i_k) \cdot \tilde{u}(i_1, i_2, \dots, i_k).$$

Our method of proof consists in considering all those prime factors  $q_j$  of  $u_n$ , which also divide one of the numbers  $u_2, u_3, \dots, u_{n-1}$ ; we suppose the factors of  $u_n$  in (4.1) to be arranged such that the prime factors with that property are given by

$$(4.4) \quad q_1, q_2, \dots, q_\sigma, q_{\sigma+1}, \dots, q_{\sigma+\tau_1} \quad (0 \leq \tau_1 \leq \tau).$$

If we can show that for each  $n$ , with a finite number of exceptions, the corresponding number

$$(4.5) \quad M = q_1^{t_1} q_2^{t_2} \dots q_\sigma^{t_\sigma} q_{\sigma+1}^{t_{\sigma+1}} \dots q_{\sigma+\tau_1}^{t_{\sigma+\tau_1}} \dots = v_n \cdot q_{\sigma+1}^{t_{\sigma+1}} \dots q_{\sigma+\tau_1}^{t_{\sigma+\tau_1}}$$

is smaller than  $|u_n|$ , then the theorem is proved.

<sup>5)</sup> The integers  $u_m$  and also the integers  $\tilde{u}_m$  below can be negative for some indices  $m$ . So in (4.1) it is necessary to take the absolute value.

If  $q_j$  is a prime with  $\sigma + 1 \leq j \leq \sigma + \tau_1$ , then it does not divide both  $a$  and  $b$ , hence on account of  $q_j \mid u_n$  and lemma 1 we have  $q_j \nmid b$ . Again by lemma 1, this implies that the values of  $m$  with  $q_j \mid u_m$  are given by the multiples of a certain positive integer,  $c(q_j)$ . Since  $q_j$  is one of the numbers (4. 4),  $c(q_j)$  is a proper divisor of  $n$ , hence  $c(q_j) \mid np_i^{-1}$  i.e.  $q_j \mid u(i)$  for at least one of the numbers  $i = 1, 2, \dots, s$ . So, by (2. 13) and (4. 2), the primes  $q_{\sigma+1}, \dots, q_{\sigma+\tau_1}$  all are contained in  $\{\bar{u}(1), \bar{u}(2), \dots, \bar{u}(s)\}$ .

We now prove

$$(4. 6) \quad \begin{cases} A(q_j, u_n) - A(q_j, \{\bar{u}(1), \bar{u}(2), \dots, \bar{u}(s)\}) = \\ = \begin{cases} 0 \text{ or } 1 \text{ always } (j = \sigma + 1, \dots, \sigma + \tau_1) \\ 0 \text{ if } q_j \neq p_1, p_2, \dots, p_s \end{cases} \end{cases}$$

Consider a prime  $q_j$  with  $\sigma + 1 \leq j \leq \sigma + \tau_1$ . Let  $i_0$  be an integer with  $1 \leq i_0 \leq s$ ,  $c(q_j) \mid np_{i_0}^{-1}$ . Then, by lemma 2,  $A(q_j, \bar{u}(i_0)) = A(q_j, u(i_0))$  is equal to  $A(q_j, u_n) = A(q_j, \bar{u}_n)$  if  $q_j \neq p_{i_0}$  and equal to  $A(q_j, u_n) - 1$  if  $q_j = p_{i_0}$ . Hence we find that

$$A(q_j, \{\bar{u}(1), \bar{u}(2), \dots, \bar{u}(s)\}) = \max_{i=1,2,\dots,s} A(q_j, \bar{u}(i))$$

is equal to  $A(q_j, u_n)$  if  $q_j$  differs from  $p_1, p_2, \dots, p_s$  and is equal to  $A(q_j, u_n)$  or  $A(q_j, u_n) - 1$  if  $q_j$  is one of the primes  $p_1, p_2, \dots, p_s$ . This proves (4. 6).

From (4. 6) we immediately conclude,  $M$  being given by (4. 5),

$$(4. 7) \quad \begin{cases} M \leq q_1^{t_1} q_2^{t_2} \dots q_{\sigma}^{t_{\sigma}} \cdot p_1 p_2 \dots p_s \cdot \{\bar{u}(1), \bar{u}(2), \dots, \bar{u}(s)\} \\ \leq n v_n \{\bar{u}(1), \bar{u}(2), \dots, \bar{u}(s)\}. \end{cases}$$

Next, in order to apply lemma 5, we determine the greatest common divisor  $(\bar{u}(i_1), \bar{u}(i_2), \dots, \bar{u}(i_k))$ , where  $i_1, i_2, \dots, i_k$  are integers with  $1 \leq i_1 < i_2 < \dots < i_k \leq s$ . If  $q$  is a prime and  $t$  is a positive integer such that  $q^t \mid (\bar{u}(i_1), \bar{u}(i_2), \dots, \bar{u}(i_k))$ , then  $q$  is one of the primes  $q_{\sigma+1}, \dots, q_{\sigma+\tau_1}$ , i.e.  $q \nmid b$ . From  $q \nmid b$ ,  $q^t \mid u(i_1), q^t \mid u(i_2), \dots, q^t \mid u(i_k)$  and lemma 1 it follows that  $c(q^t)$  divides  $np_{i_1}^{-1}, np_{i_2}^{-1}, \dots, np_{i_k}^{-1}$ , hence divides also  $n \cdot (p_{i_1} p_{i_2} \dots p_{i_k})^{-1}$ , i.e.  $q^t \mid u(i_1, i_2, \dots, i_k)$ , which in view of  $q \nmid b$  implies  $q^t \mid \bar{u}(i_1, i_2, \dots, i_k)$ . If on the other hand we have  $q^t \mid \bar{u}(i_1, i_2, \dots, i_k)$ , then we also have  $q \nmid b$ ; furthermore  $q^t \mid u(i_1, i_2, \dots, i_k)$  yields  $q^t \mid u(i_1), q^t \mid u(i_2), \dots, q^t \mid u(i_k)$ , hence  $q^t \mid \bar{u}(i_1), q^t \mid \bar{u}(i_2), \dots, q^t \mid \bar{u}(i_k)$  in view of  $q \nmid b$ . By these considerations we learn

$$(\bar{u}(i_1), \bar{u}(i_2), \dots, \bar{u}(i_k)) = |\bar{u}(i_1, i_2, \dots, i_k)|.$$

Applying lemma 5, (4. 2) and (4. 3) we obtain

$$\begin{aligned} \{\bar{u}(1), \bar{u}(2), \dots, \bar{u}(s)\} &= \\ &= |[\prod^{(1)} \bar{u}(i_1)]^{-\varepsilon_1} \cdot [\prod^{(2)} \bar{u}(i_1, i_2)]^{-\varepsilon_2} \dots [\bar{u}(1, 2, \dots, s)]^{-\varepsilon_s}| \\ &= [\prod^{(1)} v(i_1)]^{\varepsilon_1} \cdot [\prod^{(2)} v(i_1, i_2)]^{\varepsilon_2} \dots [v(1, 2, \dots, s)]^{\varepsilon_s} \cdot \\ &|[\prod^{(1)} u(i_1)]^{-\varepsilon_1} \cdot [\prod^{(2)} u(i_1, i_2)]^{-\varepsilon_2} \dots [u(1, 2, \dots, s)]^{-\varepsilon_s}|. \end{aligned}$$

In virtue of lemma 4 from (4. 7) we now get

$$(4. 8) \quad M \leq \frac{Kn(q_1^{\gamma_1} q_2^{\gamma_2} \dots q_\sigma^{\gamma_\sigma})^{\varphi(n)}}{|\prod^{(1)} u(i_1)]^{\varepsilon_1} \cdot [\prod^{(2)} u(i_1, i_2)]^{\varepsilon_2} \dots [u(1, 2, \dots, s)]^{\varepsilon_s}|}.$$

Put  $z = |\frac{\tilde{\omega}}{\omega}|$ . Then by (1. 5) we have

$$(4. 9) \quad 0 < z < 1.$$

For each positive integer  $m$  and  $\varepsilon = \pm 1$  from (1. 1) and (4. 9) we obtain

$$|(\omega - \tilde{\omega}) u_m|^\varepsilon = |\omega^m - \tilde{\omega}^m|^\varepsilon = |\omega|^\varepsilon \left(1 - \left(\frac{\tilde{\omega}}{\omega}\right)^m\right)^\varepsilon \geq |\omega|^\varepsilon (1 - z^m).$$

Hence we get

$$|u(i_1, i_2, \dots, i_k)|^{\varepsilon_k} \geq |\omega|^{\varepsilon_k n \cdot (p_{i_1} p_{i_2} \dots p_{i_k})^{-1}} (1 - z^{n \cdot (p_{i_1} p_{i_2} \dots p_{i_k})^{-1}}) |\omega - \tilde{\omega}|^{-\varepsilon_k},$$

so in the right hand member of (4. 8) the numerator is minorised by

$$\frac{1}{|u_n|} |\omega|^{\varphi(n)} \cdot (1 - z^n) \cdot \prod^{(1)} (1 - z^{n p_{i_1}^{-1}}) \dots (1 - z^{n(p_1 p_2 \dots p_s)^{-1}}) \cdot |\omega - \tilde{\omega}|^{-1 + \binom{s}{1}} \dots.$$

Each number  $n \cdot (p_{i_1} p_{i_2} \dots p_{i_k})^{-1}$  is a positive integer, whereas in virtue of the uniqueness of factorization in the ring of rational integers to different sets  $(i_1, i_2, \dots, i_k)$  belong different numbers  $n \cdot (p_{i_1} p_{i_2} \dots p_{i_k})^{-1}$ . Hence in the last relation the product of the terms involving  $z$  is minorized by  $\prod_{m=1}^{\infty} (1 - z^m)$ , which in view of (4. 9) is a convergent infinite product with a positive value  $B$ . This number  $B$  obviously does not depend on  $n$ ; it can be computed by means of theta series. Returning to (4. 8) we may conclude

$$(4. 10) \quad \frac{M}{|u_n|} < \frac{Kn}{B} \left( \frac{q_1^{\gamma_1} q_2^{\gamma_2} \dots q_\sigma^{\gamma_\sigma}}{|\omega|} \right)^{\varphi(n)}.$$

By (1. 3) we have  $|\omega \tilde{\omega}| = |b|$ , so by (1. 5) we get  $|\omega| > \sqrt{|b|}$ . Furthermore it follows from (2. 15)

$$q_1^{\gamma_1} q_2^{\gamma_2} \dots q_\sigma^{\gamma_\sigma} \leq (q_1^{A(a_1, b)} q_2^{A(a_2, b)} \dots q_\sigma^{A(a_\sigma, b)})^{\frac{1}{2}} \leq |b|^{\frac{1}{2}}.$$

So the number  $\theta = \frac{1}{|\omega|} q_1^{\gamma_1} q_2^{\gamma_2} \dots q_\sigma^{\gamma_\sigma}$  is positive and smaller than 1, whereas it does not depend on  $n$ .

The exponent of  $\theta$  in (4. 10) can be estimated by means of a result of E. LANDAU concerning EULER's  $\varphi$ -function. LANDAU proved <sup>6)</sup>

$$(4. 11) \quad \liminf_{n \rightarrow \infty} \frac{\varphi(n)}{n} \log \log n = e^{-C},$$

where  $C$  is EULER's constant. Hence

$$n \theta^{\varphi(n)} = \theta^{\frac{n}{\log \log n} \left( \frac{\varphi(n)}{n} \log \log n - \frac{\log n \log \log n}{n \log \theta} \right)}$$

<sup>6)</sup> E. LANDAU, Über den Verlauf der zahlentheoretischen Funktion  $\varphi(x)$ , Archiv der Mathematik und Physik (3), 5, 86-91 (1903).



tends to zero for  $n \rightarrow \infty$ , since  $\theta$  is a fixed number between 0 and 1 and since the form between brackets has the positive limes inferior  $e^{-\theta}$ .

This proves the existence of a positive integer  $n_0$ , such that  $\frac{M}{u_n} < 1$  if  $n > n_0$ , which establishes the truth of the theorem.

#### *Final remarks*

1. In order to find in a concrete example the exceptional integers  $n$ , which do not possess the property mentioned in the theorem, we can not use (4.11) as it stands, since it does not provide the construction of an index  $n_0$  such that  $M < |u_n|$  if  $n > n_0$ . We consider for instance the case  $a = b = 1$ . Then  $\{u_n\}$  is the sequence of FIBONACCI, and  $g = 1$ . Thus no primes  $q_1, \dots, q_s$  occur; writing  $n^* = p_1 p_2 \dots p_s$  and inspecting the relation (4.7) and the proof of (4.10) we find

$$\frac{1}{u_n} M < \frac{n^*}{B} \left( \frac{1}{\omega} \right)^{\varphi(n)},$$

where

$$\omega = \frac{1 + \sqrt{5}}{2} = 1,618 \dots, B = \prod_{m=1}^{\infty} (1 - z^m) \text{ with } z = \frac{\tilde{\omega}}{\omega} = \frac{3 - \sqrt{5}}{2}.$$

The formula

$$\prod_{m=1}^{\infty} (1 - z^m)^3 = 1 - 3z + 5z^3 - 7z^6 + 9z^{10} - 11z^{15} + \dots$$

gives very rapidly the value  $B = 0.473 \dots$

Hence  $\frac{1}{u_n} M$  is certainly smaller than 1, if we have

$$^{10}\log B + \varphi(n) ^{10}\log \omega - ^{10}\log n^* > 0,$$

i.e.

$$0.209 \varphi(n) - ^{10}\log n^* > 0.325.$$

Using the last relation and a table of FIBONACCI's sequence we easily find that the exceptional values of  $n$ , i.e. the values of  $n$  such that  $u_n$  does not contain "new" primes, are given by

$$n = 1, 2, 6, 12.$$

2. Of course it is not necessary for the proof to use the relation (4.11); it is sufficient to show that we have  $\frac{Kn^*}{B} \theta^{\varphi(n)} < 1$  ( $K, B, \theta$  not depending on  $n$ ;  $\theta < 1$ ) for almost all values of  $n$  and this can be done by elementary methods.