MATHEMATISCH CENTRUM
2e Boerhaavestraat 49
AMSTERDAM (O.)

Telefoon 51660
(Administratie, Bibliotheek, Afd. Statistiek, Afd. Zuivere Wiskunde)

Telefoon 56643
(Afd. Toegepaste Wiskunde, Rekenafdeling)

Z.W.-Rapport 1953 - 003

Prime factors of the elements of certain sequences of integers

by

C.G.Lekkerkerker.

1. Introduction.

Very recently we were told by VAN DER POL that the following proposition has been proved by BANG:

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

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

then for each positive integer n, with a finite number of exceptions, there exists a prime q with

$$q \mid u_n, \quad q \nmid u_\nu \quad \text{for } \nu = 1, 2, \ldots, n-1.$$

Moreover BANG raised the question whether this result remains valid, if for ω we take a real quadratic algebraic integer and for $\bar{\omega}$ its conjugate. This has led us to the following theorem, a proof of which is the main object of this report.

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

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

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

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

Then the sequence of rational integers

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

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

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

In this theorem rationality of $\omega, \bar{\omega}$ is not required; it forms a generalization of the proposition of BANG.

Preliminary remarks. In view of $a \neq 0$ and $a^2 + 4b > 0$, the numbers ω and $\bar{\omega}$ evidently are real and different in absolute value. Since interchanging ω and $\bar{\omega}$ does not affect the assertion of the theorem, we may suppose without loss of genereality

(1.5) $$|\omega| > |\bar{\omega}|.$$

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

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

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

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

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) $$\omega^n = u_n\omega + bu_{n-1}, \; \bar{\omega}^n = u_n\bar{\omega} + bu_{n-1} \; (n = 1, 2, \ldots).$$

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

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

hence by (1.6) and (1.7)

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

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

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

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

2. Some lemma's.

In another report[1] periodicity properties, modulo an arbitrary positive integer m, for the sequence defined by (1.7) are studied extensively. Some of the results contained in the lemma's below already were obtained in that report; 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) $$q^t \mid u_n \quad \text{if and only if} \quad c(q^t) \mid n.$$

----

1) H.J.A.Duparc - W.Peremans, Reduced sequences of integers and pseudo-random numbers II, Rapport Z.W. 1952-013, Mathematisch Centrum, Amsterdam (dutch).

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

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

$$A(q,f) \tag{2.2}$$

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

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

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

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

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

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

except when we have simultaneously

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

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

<u>Lemma 3</u>. Let q be a prime with $q \mid b$, $q \mid a$. Let α, β be the positive integers

$$\alpha = A(q,a), \qquad \beta = A(q,b). \tag{2.6}$$

If $2\alpha < \beta$, then

$$A(q,u_n) = (n-1)\alpha \qquad (n = 1, 2, \ldots). \tag{2.7}$$

If $2\alpha \geqslant \beta$, then there exist a positive integer $d=d(q)$ and a monotoneously 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

$$\left.\begin{aligned} &A(q,u_n) = \frac{n-1}{2}\beta \quad \text{if} \quad d \nmid n && (2.8)\\ &A(q,u_n) = \frac{n}{2}\beta + \varphi_q\left(A\left(q,\frac{n}{d}\right)\right) \quad \text{if} \quad d \mid n && (2.9)\end{aligned}\right\} (n = 1,2,\ldots).$$

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:

$$\varphi_q(x) = x-1 + \varphi_q(1) \qquad (x = 1,2,\ldots). \tag{2.10}$$

<u>Lemma 4</u>. Suppose $g = (a,b) > 1$ and put

$$g = q_1^{l_1} q_2^{l_2} \ldots q_\sigma^{l_\sigma}, \tag{2.11}$$

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

$$n = p_1^{r_1} p_2^{r_2} \ldots p_s^{r_s}, \tag{2.12}$$

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

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

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

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

$$(2.15) \qquad \gamma_j = \min\left(A(q_j, a), \tfrac{1}{2}A(q_j, b)\right).$$

Let ε_k be defined by

$$(2.16) \qquad \begin{cases} \varepsilon_k = 1 & \text{if } k \text{ is even} \\ \varepsilon_k = -1 & \text{if } k \text{ is odd} \end{cases} \qquad (k = 1,2,\dots,s).$$

Then we have

$$(2.17) \quad \begin{cases} v_n \left[\prod_{i_1=1}^{s} v(i_1) \right]^{\varepsilon_1} \left[\prod_{\substack{i_1, i_2 = 1 \\ i_1 < i_2}}^{s} v(i_1, i_2) \right]^{\varepsilon_2} \cdots \\ \cdots \left[\prod_{\substack{i_1, i_2, \dots, i_k = 1 \\ i_1 < i_2 < \dots < i_k}}^{s} v(i_1, i_2, \dots, i_k) \right]^{\varepsilon_k} \cdots \left[v(1,2,\dots,s) \right]^{\varepsilon_s} \leqslant \\ \leqslant K.(q_1^{\gamma_1} q_2^{\gamma_2} \cdots q_\sigma^{\gamma_\sigma})^n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) \end{cases}$$

where $K = K(a,b)$ is a constant not depending on n.

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

$$(2.18) \quad \begin{cases} \{x_1, x_2, \dots, x_w\} = \left[\prod_{i_1=1}^{w} x_{i_1} \right]^{-\varepsilon_1} \left[\prod_{\substack{i_1, i_2 = 1 \\ i_1 < i_2}}^{w} (x_{i_1}, x_{i_2}) \right]^{-\varepsilon_2} \cdots \\ \cdots \left[\prod_{\substack{i_1, i_2, \dots, i_k = 1 \\ i_1 < i_2 < \dots < i_k}}^{w} (x_{i_1}, x_{i_2}, \dots, x_{i_k}) \right]^{-\varepsilon_k} \cdots \\ \cdots \left[(x_1, x_2, \dots, x_w) \right]^{-\varepsilon_w}, \end{cases}$$

where ε_k is given by (2.16) and where $\{a_1, a_2, \dots, a_n\}$ 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. For given q and t, let c be the smallest positive integer with $q^t \mid u_c$. First we prove by induction on h, that we have

(3.1) $$q^t \mid u_{hc} \quad \text{for } h = 1,2,\ldots$$

By definition of c the relation (3.1) is true for h = 1. If (3.1) holds for a certain value of h, then by (1.9) we have $u_{(h+1)c} = u_{hc+c} = u_{hc}u_{c+1} + bu_{hc-1}u_c \equiv 0 \pmod{q^t}$. Hence (3.1) is proved.

Secondly we prove that, if $q \nmid b$ and if n is a positive integer with $q^t \mid u_n$, we have $c \mid n$. Put $n = hc + r$, where $0 \leqslant r < c$ 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 $q \mid u_{hc-3}, \ldots, q \mid u_1$; 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.

The second part of the lemma follows from these two facts. First we have $q \nmid u_1$. Secondly, if $q \nmid u_n$, then $q \nmid u_{n+1}$ $(n = 1,2,\ldots)$, 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 $q \nmid a$.

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 $k = A(q,u_n)$. Then $u_n = eq^h$ with $q \nmid e$, $h \geqslant 1$. Applying (1.8) we find

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

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

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

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 ω by $\bar{\omega}$. Hence we have

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

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

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

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

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

If $q=2$, then again (3.2) is valid; it has the form

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

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

$$(3.4a) \qquad u_{2n} = ebu_{n-1}\,2^{h+1} + e^2a2^{2h} \quad (h = A(2,u_{c(2)})).$$

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

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

Hence, by induction on n, we see that (2.7) is true for $n = 1,2,\ldots$

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

$$(3.7) \qquad A(q,u_n) \geq (n-1)\alpha = \frac{n-1}{2}\beta \quad (n = 1,2,\ldots);$$

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

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

$$A(q,u_n^*) = k^* + A(q, \frac{n}{c^*}) \text{ if } c \mid n,$$

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 $c^* | n$, $2c^* \nmid n$. From these facts follow (2.8), (2.9), (2.10) if we take

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

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

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

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

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

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

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

in view of

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

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} $(m = 0,1,2,\dots)$, analoguous to the relations (1.7) for the numbers u_n. We have

$$\begin{aligned} u_{2m+4} &= au_{2m+3} + bu_{2m+2} \\ u_{2m+3} &= au_{2m+2} + bu_{2m+1} \\ u_{2m+2} &= au_{2m+1} + bu_{2m}, \end{aligned}$$

so elimination of u_{2m+1} and u_{2m+3} yields

$$\begin{aligned} au_{2m+1} &= u_{2m+2} - bu_{2m} \\ u_{2m+4} &= bu_{2m+2} + a(au_{2m+2} + bu_{2m+1}) \\ &= (a^2+2b)\, u_{2m+2} - b^2 u_{2m}. \end{aligned}$$

In view of $a|u_0$, $a|u_2$ we have $a|u_{2m}$ for all m.
We put

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

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

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

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

$$\begin{aligned} A(q,u_m^*) &= 0 \quad \text{if } c^* \nmid m, \\ A(q,u_m^*) &= k^* + A(q, \tfrac{m}{c^*}) \quad \text{if } c^*|m; \end{aligned}$$

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

A further property of the sequence $\{u_n^*\}$ 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 $q > 2$

$$u_{2q}\omega + u_{2q-1} = \omega^{2q} = (a\omega + b)^q$$

$$= \sum_{n=0}^{q} \binom{q}{n} a^n \omega^n b^{q-n} = \sum_{n=1}^{q} \binom{q}{n} a^n (u_n\omega + bu_{n-1}) b^{q-n} + b^q,$$

$$u_{2q} = \sum_{n=1}^{q} \binom{q}{n} a^n b^{q-n} u_n = \sum_{n=1}^{q} X_n, \text{ say.}$$

By (3.8) and (3.9) we have

$$A(q,X_1) = A(q,qab^{q-1}) = 1 + \alpha + (q-1)\beta, \quad A(q,X_q) = q\alpha + \frac{q-1}{2}\beta$$

$A(q,X_n) = 1+n\alpha+(q-n)\beta + \frac{n-1}{2}\beta = 1+n\alpha+(q-1-\frac{n-1}{2})\beta$ if n is odd and $2 \leq n \leq q-1$

$$A(q,X_n) \geq 1+n\alpha+(q-n)\beta+\alpha+\frac{n-2}{2}\beta$$
$$= 1+(n+1)\alpha+(q-1-\frac{n}{2})\beta \quad \text{if } n \text{ is even and } 2 \leq n \leq q-1.$$

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

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

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

$$(3.12) \qquad A(q,u^*_m) = A(q,m).$$

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

$$(3.12a) \qquad A(2,u^*_m) = A(2,\tfrac{m}{2}) + k^*(2).$$

Taking $d(q) = 2$, $\varphi_q(0) = \alpha-\beta$, $\varphi_q(x) = x+\varphi_q(0)$ if $q > 2$,
$d(2) = 2$, $\varphi_2(0) = \alpha-\beta$, $\varphi_2(1) = \alpha-\beta+k^*(2)$,
$\varphi_2(x) = x-1+\varphi_2(1)$ $(x = 1,2,\ldots)$,

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 $q_1, q_2, \ldots, q_\sigma$ of g. Let α and β 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 α, β, n

I $\quad 2\alpha < \beta$

II $\quad 2\alpha \geq \beta$ and $d \nmid n$

III $\quad 2\alpha \geq \beta$; $d \mid \frac{n}{p_i}$ if and only if $i = 1,2,\ldots,s_1$ where s_1 is an integer with $1 \leq s_1 \leq s$; $q \neq p_1, p_2, \ldots, p_{s_1}$

IV $\quad 2\alpha \geq \beta$; $q = p_1$; $d \mid \frac{n}{p_i}$ if and only if $i = 1,2,\ldots,s_1$ where s_1 is an integer with $2 \leq s_1 \leq s$

V $\quad 2\alpha \geq \beta$; $q = p_1$; $d \mid n$;
$\frac{n}{d} = q^t$ where t is a non negative integer.

It is obvious that in each case, after having arranged the prime facto[illegible] of n in (2.12) in a suitable way, (exactly) one of the cases I-V occurs.

In the sequel $i_1, i_2, \ldots, i_k$ are always supposed to form a set of unequal positive integers with increasing order.

<u>Case I</u>. 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 admissable set $(i_1, i_2, \ldots, i_k)$

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

In view of the form of M_1 this yields

$$A(q,M_1) = A(q,u_n) - \sum_{i_1} A(q,u(i_1)) + \sum_{i_1,i_2} A(q,u(i_1,i_2)) - \ldots$$

$$\ldots + (-1)^k \sum_{i_1,i_2,\ldots,i_k} A(q,u(i_1,i_2,\ldots,i_k)) + \ldots + (-1)^s A(q,u(1,2,\ldots,s))$$

$$= n\alpha . \left[1 - \sum_{i_1=1}^{s} \frac{1}{p_{i_1}} + \sum_{i_1,i_2} \frac{1}{p_{i_1}p_{i_2}} - \ldots + (-1)^s \frac{1}{p_1p_2\ldots p_s}\right]$$

$$-\alpha . \left[1 - \binom{s}{1} + \binom{s}{2} - \ldots + (-1)^s\right],$$

hence in view of $s \geq 1$

$$A(q,M_1) = n\alpha \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right).$$

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

$A(q,v(i_1,i_2,\ldots,i_k)) = \frac{1}{2}\beta . \frac{n}{p_{i_1}p_{i_2}\ldots p_{i_k}} - \frac{1}{2}\beta$. This yields

$$A(q,M_1) = \tfrac{1}{2}n\beta \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right).$$

<u>Case III</u>. We have $d|n$. Applying (2.8) and (2.9) we obtain

$$A(q,v_n) = \tfrac{1}{2}\beta n + \varphi_q(A(q,\tfrac{n}{d}))$$

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

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

$A(q,\frac{n}{dp_{i_1}p_{i_2}\ldots p_{i_k}}) = A(q,\frac{n}{d})$ if $i_k \leq s_1$ and $d \nmid \frac{n}{p_{i_1}p_{i_2}\ldots p_{i_k}}$ 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

$$A(q,M_1) = \tfrac{1}{2}\beta n + b_0 + b_1 - \sum_{i_1=1}^{s} \left(\tfrac{1}{2}\beta\frac{n}{p_{i_1}} + b_0\right) - \sum_{i_1=1}^{s_1} b_1 +$$

$$+ \sum_{i_1,i_2} (\tfrac{1}{2}\beta \frac{n}{p_{i_1}p_{i_2}} + b_0) + \sum_{i_1,i_2 \leq s_1} b_1 - \ldots$$

$$\ldots + (-1)^{s_1} \sum_{i_1,i_2,\ldots,i_{s_1}} (\tfrac{1}{2}\beta \frac{n}{p_{i_1}p_{i_2} \ldots p_{i_{s_1}}} + b_0)$$

$$+ (-1)^{s_1} b_1 + \ldots + (-1)^s . (\tfrac{1}{2}\beta \frac{n}{p_1p_2 \ldots p_s} + b_0) \quad {}^{2)}$$

$$= \tfrac{1}{2}\beta n . \left[1 - \sum_{i_1} \frac{1}{p_{i_1}} + \sum_{i_1,i_2} \frac{1}{p_{i_1}p_{i_2}} - \ldots + (-1)^s \frac{1}{p_1p_2 \ldots p_s} \right]$$

$$+ b_0 . \left[1 - \binom{s}{1} + \binom{s}{2} - \ldots + (-1)^s \right] + b_1 . \left[1 - \binom{s_1}{1} + \binom{s_1}{2} - \ldots + (-1)^{s_1} \right] .$$

Since the coefficients of b_0 and b_1 vanish in view of $s \geqslant 1$, $s_1 \geqslant 1$, we find

$$A(q,M_1) = \tfrac{1}{2}n\beta \prod_{i=1}^{s} (1 - \frac{1}{p_i}) .$$

<u>Case IV.</u> In view of (2.8), (2.9) and the assumptions of this case we get

$$A(q,v_n) = \tfrac{1}{2}\beta n + \varphi_q(A(q,\tfrac{n}{d}))$$

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

Hence, putting $-\tfrac{1}{2}\beta = b_0$, $\varphi_q(A(q,\frac{n}{dp_1})) + \tfrac{1}{2}\beta = b_1$, $\varphi_q(A(q,\tfrac{n}{d})) - \varphi_q(A(q,\frac{n}{dp_1})) = b_2$, we find (in the finite sums writing down only the first terms)

$$A(q,M_1) = \tfrac{1}{2}\beta n + b_0 + b_1 + b_2 - \sum_{i_1=1}^{s} (\tfrac{1}{2}\beta \frac{n}{p_{i_1}} + b_0) - \sum_{i_1=1}^{s_1} b_1 - \sum_{i_1=2}^{s_1} b_2$$

$$+ \sum_{i_1,i_2} (\tfrac{1}{2}\beta \frac{n}{p_{i_1}p_{i_2}} + b_0) + \sum_{i_1,i_2 \leq s_1} b_1 + \sum_{2 \leq i_1,i_2 \leq s_1} b_2 - \ldots$$

$$= \tfrac{1}{2}\beta n . \left[1 - \sum_{i_1} \frac{1}{p_{i_1}} + \sum_{i_1,i_2} \frac{1}{p_{i_1}p_{i_2}} - \ldots \right] + b_0 . \left[1 - \binom{s}{1} + \binom{s}{2} - \ldots \right]$$

$$+ b_1 . \left[1 - \binom{s_1}{1} + \binom{s_1}{2} - \ldots \right] + b_2 . \left[1 - \binom{s_1 - 1}{1} + \binom{s_1 - 1}{2} - \ldots \right] .$$

Thus again we find

$$A(q,M_1) = \tfrac{1}{2}\beta n \prod_{i=1}^{s} (1 - \frac{1}{p_i}) ,$$

---

2) If s_1 is equal to s, then the terms with s_1 are the last terms of this sum.

since in the case considered we even have $s_1 - 1 \geq 1$.

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

$$A(q,v_n) = \tfrac{1}{2}\beta n + \varphi_q(A(q,\tfrac{n}{d})) = \tfrac{1}{2}\beta n + \varphi_q(t)$$

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

hence, putting $-\frac{1}{2}\beta = b_0$, $\varphi_q(t-1) + \frac{1}{2}\beta = b_1$, we obtain

$$A(q,M_1) = \tfrac{1}{2}\beta n + b_0 + b_1 + \varphi_q(t) - \varphi_q(t-1) - \sum_{i_1=1}^{s}(\tfrac{1}{2}\beta \frac{n}{p_{i_1}} + b_0) - b_1 +$$

$$+ \sum_{i_1,i_2} (\tfrac{1}{2}\beta \frac{n}{p_{i_1}p_{i_2}} + b_0) - \dots + (-1)^k \sum_{i_1,i_2,\dots,i_k} (\tfrac{1}{2}\beta \frac{n}{p_{i_1}p_{i_2}\dots p_{i_k}} + b_0) + \dots$$

$$\dots + (-1)^s (\tfrac{1}{2}\beta \frac{n}{p_1p_2 \dots p_s} + b_0)$$

$$= \tfrac{1}{2}\beta n . \left[1 - \sum_{i_1} \frac{1}{p_{i_1}} + \sum_{i_1,i_2} \frac{1}{p_{i_1}p_{i_2}} - \dots + (-1)^s \frac{1}{p_1p_2 \dots p_s} \right]$$

$$+ b_0 . \left[1 - \binom{s}{1} + \binom{s}{2} - \dots + (-1)^s \right] + b_1 - b_1 + \varphi_q(t) - \varphi_q(t-1).$$

Therefore

$$A(q,M_1) = \tfrac{1}{2}\beta n \prod_{i=1}^{s} (1 - \frac{1}{p_i}) + \varphi_q(t) - \varphi_q(t-1), \text{ if } t \geq 1.$$

If $t = 0$, the deduction remains valid, if only we replace $\varphi_q(t-1)$ by $-\frac{1}{2}\beta$. Hence

$$A(q,M_1) = \tfrac{1}{2}\beta n \prod_{i=1}^{s} (1 - \frac{1}{p_i}) + \varphi_q(0) + \tfrac{1}{2}\beta \text{ if } t = 0.$$

Combining the results we see

$$A(q,M_1) = n.\min(\alpha, \tfrac{1}{2}\beta) . \prod_{i=1}^{s} (1 - \frac{1}{p_i}) + \delta,$$

where δ is unequal to zero if and only if q is one of the primes $p_1, p_2, \dots, p_s$ and moreover $2\alpha \geq \beta$, $\frac{n}{d} = q^t$ with a non negative integer t. In this exceptional case, as we see from the proof of lemma 3, δ is equal to $\varphi_q(t) - \varphi_q(t-1) = 1$ if $t \geq 2$ in virtue of (2.10); if $t = 1$, then $\delta = \varphi_q(1) - \varphi_q(0) = 1$ or $k^*(q)$; if $t = 0$, then $\delta = \varphi_q(0) + \frac{1}{2}\beta = k^*(q)$ or 1 in the case $2\alpha = \beta$ and $\delta = \varphi_q(0) + \frac{1}{2}\beta = \alpha - \frac{1}{2}\beta$ in the case $2\alpha > \beta$ (in this case we have $d = 2$, hence $q = 2$). At any rate, since for given a and b the numbers α, β, d, $k^*(q)$ only depend on q, we conclude that only for a finite number of values of n the number δ has a value $\neq 0,1$. Hence δ is bounded, say by Δ. Thus, noting (2.15), for each $j = 1,2,\dots,\sigma$ follows

$$A(q_j,M_1) \leq n\gamma_j \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) + \Delta .$$

This proves (2.17) with $K = (q_1 q_2 \ldots q_\sigma)^{\Delta}$.

Proof of lemma 5.[3] Without loss of generality we may suppose $x_1, x_2, \ldots, x_w$ to be positive. Let q be a prime. Put $A(q,x_i) = \tau_i$ and arrange the numbers x_i such that we have $\tau_1 \leq \tau_2 \leq \ldots \leq \tau_w$. Then the number of factors q contained in the different products, which occur in the right hand member of (2.18) successively are equal to

$$\tau_1 + \tau_2 + \ldots + \tau_w,$$

$$\binom{w-1}{1}\tau_1 + \binom{w-2}{1}\tau_2 + \ldots + \binom{2}{1}\tau_{w-2} + \tau_{w-1},$$

$$\binom{w-1}{2}\tau_1 + \binom{w-2}{2}\tau_2 + \ldots + \binom{3}{2}\tau_{w-3} + \tau_{w-2},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\binom{w-1}{w-2}\tau_1 + \tau_2,$$

$$\tau_1 ,$$

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

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

$$\left\{1 - \binom{w-1}{1} + \binom{w-1}{2} - \ldots + (-1)^{w-2}\binom{w-1}{w-2} + (-1)^{w-1}\right\}\tau_1 +$$

$$+ \left\{1 - \binom{w-2}{1} + \binom{w-2}{2} - \ldots + (-1)^{w-3}\binom{w-2}{w-3} + (-1)^{w-2}\right\}\tau_2 + \ldots$$

$$\ldots + (1 - 2 + 1)\tau_{w-2} + (1-1)\tau_{w-1} + \tau_w$$

$$= \tau_w = A(q, \{x_1, x_2, \ldots, x_w\}).$$

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

4. Proof of the theorem.

Let $\{u_n\}$ be the sequence defined by (1.1). We consider a fixed inte $n > 1$. 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 $q_1, q_2, \ldots, q_\sigma$ are also contained in u_n. We put

(4.1) $$|u_n| = q_1^{t_1} q_2^{t_2} \ldots q_\sigma^{t_\sigma} q_{\sigma+1}^{t_{\sigma+1}} \ldots q_{\sigma+\tau}^{t_{\sigma+\tau}},$$ [4]

---

3) This lemma already was proved by J.G.VAN DER CORPUT, Nieuw Archief voor Wiskunde (2), 12 (1912).

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

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),

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

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

$$(4.3)\qquad u(i_1,i_2,\dots,i_k) = v(i_1,i_2,\dots,i_k).\bar{u}(i_1,i_2,\dots,i_k).$$

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

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

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

$$(4.5)\qquad M = q_1^{t_1}q_2^{t_2}\cdots q_\sigma^{t_\sigma}q_{\sigma+1}^{t_{\sigma+1}}\cdots q_{\sigma+\tau_1}^{t_{\sigma+\tau_1}} = v_n.q_{\sigma+1}^{t_{\sigma+1}}\cdots q_{\sigma+\tau_1}^{t_{\sigma+\tau_1}}$$

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

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 $q_j|u_n$ and lemma 1 we have $q_j \nmid b$. Again by lemma 1, this implies that the values of m with $q_j|u_m$ 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 $c(q_j)\left|\dfrac{n}{p_i}\right.$, i.e. $q_j|u(i)$ 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

$$(4.6)\qquad A(q_j,u_n) - A(q_j,\{\bar{u}(1),\bar{u}(2),\dots,\bar{u}(s)\}) = \begin{cases} 0 \text{ or } 1 \text{ always } (j=\sigma+1,\dots,\sigma+\tau_1) \\ 0 \text{ if } q_j \neq p_1,p_2,\dots,p_s \end{cases}$$

Consider a prime q_j with $\sigma+1 \leq j \leq \sigma+\tau_1$. Let i_0 be an integer with $1\leq i_0 \leq s$, $c(q_j)\left|\dfrac{n}{p_{i_0}}\right.$. 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

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

is equal to $A(q_j,u_n)$ if q_j differs from $p_1,p_2,\ldots,p_s$ and is equal to $A(q_j,u_n)$ or $A(q_j,u_n) - 1$ if q_j is one of the primes $p_1,p_2,\ldots,p_s$. This proves (4.6).

From (4.6) we immediately conclude, M being given by (4.5),

$$M \leqslant q_1^{t_1} q_2^{t_2} \ldots q_\sigma^{t_\sigma} \cdot p_1p_2 \ldots p_s \cdot \{\bar{u}(1),\bar{u}(2),\ldots,\bar{u}(s)\}\ ^{5)}.$$

$$\leqslant n\, v_n \{\bar{u}(1),\bar{u}(2),\ldots,\bar{u}(s)\}. \tag{4.7}$$

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

$$(\bar{u}(i_1),\bar{u}(i_2),\ldots,\bar{u}(i_k)) = |\bar{u}(i_1,i_2,\ldots,i_k)|.\ ^{5)}$$

Applying lemma 5, (4.2) and (4.3) we obtain

$$\{\bar{u}(1),\bar{u}(2),\ldots,\bar{u}(s)\} =$$

$$= \left|\Big[\prod_{i_1} \bar{u}(i_1)\Big]^{-\varepsilon_1} \cdot \Big[\prod_{i_1<i_2} \bar{u}(i_1,i_2)\Big]^{-\varepsilon_2} \ldots \Big[\bar{u}(1,2,\ldots,s)\Big]^{-\varepsilon_s}\right|$$

$$= \Big[\prod_{i_1} v(i_1)\Big]^{\varepsilon_1} \cdot \Big[\prod_{i_1<i_2} v(i_1,i_2)\Big]^{\varepsilon_2} \ldots \Big[v(1,2,\ldots,s)\Big]^{\varepsilon_s}.$$

$$\left|\Big[\prod_{i_1} u(i_1)\Big]^{-\varepsilon_1} \cdot \Big[\prod_{i_1<i_2} u(i_1,i_2)\Big]^{-\varepsilon_2} \ldots \Big[u(1,2,\ldots,s)\Big]^{-\varepsilon_s}\right|.$$

In virtue of lemma 4 from (4.7) we now get

$$M \leqslant \frac{K_n(q_1^{\gamma_1} q_2^{\gamma_2} \ldots q_\sigma^{\gamma_\sigma})\, n \prod_{i=1}^{s} (1-\frac{1}{p_i})}{\left|\Big[\prod_{i_1} u(i_1)\Big]^{\varepsilon_1} \cdot \Big[\prod_{i_1<i_2} u(i_1,i_2)\Big]^{\varepsilon_2} \ldots \Big[u(1,2,\ldots,s)\Big]^{\varepsilon_s}\right|}. \tag{4.8}$$

---

5) The least common multiple and the greatest common divisor are always understood to be positive.

Put $z = \left|\frac{\bar{\omega}}{\omega}\right|$. Then by (1.5) we have

(4.9) $$0 < z < 1.$$

For each positive integer m and $\varepsilon = \pm 1$ from (1.1) and (4.9) we obtain

$$|(\omega-\bar{\omega})u_m|^{\varepsilon} = |\omega^m-\bar{\omega}^m|^{\varepsilon} = |\omega|^{\varepsilon m}(1-(\tfrac{\bar{\omega}}{\omega})^m)^{\varepsilon} \geqslant |\omega|^{\varepsilon m}(1 - z^m).$$

Hence we get

$$|u(i_1,i_2,\dots,i_k)|^{\varepsilon_k} \geqslant |\omega|^{\varepsilon_k \cdot \frac{n}{p_{i_1}p_{i_2}\cdots p_{i_k}}}(1 - z^{\frac{n}{p_{i_1}p_{i_2}\cdots p_{i_k}}})|\omega-\bar{\omega}|^{-\varepsilon_k},$$

$$\left|u_n\left[\prod_{i_1} u(i_1)\right]^{\varepsilon_1}\cdot\left[\prod_{i_1<i_2} u(i_1,i_2)\right]^{\varepsilon_2}\cdots\left[u(1,2,\dots,s)\right]^{\varepsilon_s}\right|$$

$$\geqslant |\omega|^{n(1-\sum_{i_1}\frac{1}{p_{i_1}}+\sum_{i_1<i_2}\frac{1}{p_{i_1}p_{i_2}}-\dots+(-1)^s\frac{1}{p_1p_2\cdots p_s})}.$$

$$(1-z^n).\prod_{i_1}(1-z^{\frac{n}{p_{i_1}}})\prod_{i_1<i_2}(1-z^{\frac{n}{p_{i_1}p_{i_2}}})\dots(1-z^{\frac{n}{p_1p_2\cdots p_s}})|\omega-\bar{\omega}|^{-1+\binom{s}{1}-\binom{s}{2}+\dots-(-1)^s}.$$

Each number $\frac{n}{p_{i_1}p_{i_2}\cdots p_{i_k}}$ 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 $\frac{n}{p_{i_1}p_{i_2}\cdots p_{i_k}}$.

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) $$\frac{M}{|u_n|} < \frac{K_n}{B}\left(\frac{q_1^{\gamma_1}q_2^{\gamma_2}\cdots q_{\sigma}^{\gamma_{\sigma}}}{|\omega|}\right)^{n\prod_{i=1}^{s}(1-\frac{1}{p_i})}.$$

By (1.3) we have $|\omega\bar{\omega}| = |b|$, so by (1.5) we get $|\omega| > \sqrt{|b|}$. Furthermore it follows from (2.15)

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

So the number $\Theta = \frac{1}{|\omega|}q_1^{\gamma_1}q_2^{\gamma_2}\cdots q_{\sigma}^{\gamma_{\sigma}}$ is positive and smaller than 1, whereas it does no depend on n.

The exponent of Θ in (4.10) can be estimated by means of a result of E. Landau concerning Euler's φ-function. For if $\varphi(n)$ is Euler's φ-function, i.e. if $\varphi(n)$ denotes the number of integers m with $1 \leq m < n$, $(m,n) = 1$, then, by a well known result in the elementary theory of numbers, we have $\prod_{i=1}^{s}(1-\frac{1}{p_i}) = \frac{\varphi(n)}{n}$, and E.Landau proved [6])

(4.11) $$\lim_{n\to\infty} \inf \frac{\varphi(n)}{n} \log\log n = e^{-C},$$

where C is Euler's constant.

Hence $n\,\theta^{n\prod_{i=1}^{s}(1-\frac{1}{p_i})} = \theta^{\frac{n}{\log\log n}\left(\frac{\varphi(n)}{n}\log\log n - \frac{\log n \log\log n}{\log \theta^{-1}}\right)}$

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

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 $q_1,\ldots,q_\sigma$ occur; writing $n^* = p_1p_2\ldots p_s$ and inspecting the relation (4.7) and the proof of (4.10) we find

$$\frac{1}{u_n} M < \frac{n^*}{B}\left(\frac{1}{\omega}\right)^{n\prod_{i=1}^{s}(1-\frac{1}{p_i})} = \frac{n^*}{B}\left(\frac{1}{\omega}\right)^{\varphi(n)},$$

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

The formula

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

gives very rapidly the value B = 0.473 ...

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, θ not depending on n; $\theta < 1$) for almost all values of n and this can be done by elementary methods.

---

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