ON $h$-BASES FOR $n$

Öystein J. Rødseth

1. Introduction.

The sum $A + B$ of two non-empty integer sequences $A, B$ is defined to be the sequence of all distinct integers of the form

$$a + b; \quad a \in A, \ b \in B.$$ 

The sum of more than two sequences is defined similarly. In particular, for a positive integer $h$, we write $hA$ for the $h$-fold sum $A + A + \ldots + A$.

We shall be concerned with finite integer sequences

$$B_k : 0 = b_0 < b_1 < \ldots < b_k,$$

and their duals

$$B_k^* : 0 = b_0^* < b_1^* < \ldots < b_k^*,$$

where

$$b_i^* = b_k - b_{k-i}, \quad i = 0, 1, \ldots, k.$$ 

Note that $\gcd B_k = \gcd B_k^*$ ($k \geq 1$).

If an integer $M$ has an integral representation

$$M = b_1x_1 + b_2x_2 + \ldots + b_kx_k, \quad x_i \geq 0,$$

we shall say that $M$ is dependent on $B_k$. If $\gcd B_k = 1$, it is well known that every sufficiently large integer is dependent on $B_k$. In this case we denote the largest integer not dependent on $B_k$, the Frobenius number of $B_k$, by $g(B_k)$ or by $g(b_1, b_2, \ldots, b_k)$.

For integers $a, b$ we use $[a, b]$ to denote the set of integers in the interval $a \leq x \leq b$. We also use $[x]$ to denote the integral part of a real number $x$.

An integer sequence

$$(1.1) \quad A_k : 0 = a_0 < a_1 < a_2 < \ldots < a_k$$

is called an $h$-basis for a non-negative integer $n$ if $[0, n] \subseteq hA_k$ (Rohrbach [15]).

In this paper we consider the $h$-range $n(h, A_k)$ of $A_k$ ("die Reichweite von $A_k$

Received March 19, 1980.
bezüglich h''), which is the largest n for which \( A_k \) is an h-basis. Thus \( A_k \) is an h-basis for n if and only if \( 0 \leq n \leq n(h, A_k) \).

In the literature, the h-range has been considered from two different points of view, named the local and the global case by Selmer [18]. In the local case, h and \( A_k \) are considered as given, and the problem consists in determining \( n(h, A_k) \). In the global case, h and k are considered as given, and the problem consists in determining the extremal h-range

\[
n(h, k) = \max_{A_k} n(h, A_k),
\]

and also the corresponding extremal bases, i.e. the bases \( A_k \) for which \( n(h, k) = n(h, A_k) \). In this paper we shall mainly be concerned with the local problem.

Given the sequence (1.1), \( k \geq 1 \), we write \( A_{k-1} \) for the sequence

\[
A_{k-1} : 0 = a_0 < a_1 < \ldots < a_{k-1}.
\]

We define \( h_0 = h_0(A_k) \) to be the smallest positive h for which

\[
a_k \leq n(h, A_k),
\]

or, equivalently, as the smallest positive h for which

\[
a_k \leq n(h, A_{k-1}) + 1.
\]

Putting \( n(0, A_k) = 0 \), we then have \( n(h, A_k) = n(h, A_{k-1}) \) if \( 0 \leq h < h_0 \).

We trivially have \( n(h, A_1) = h \). Thus \( h_0(A_2) = a_2 - 1 \). Stöhr [20] showed that

\[
n(h, A_2) = a_2(h + 3 - a_2) - 2, \quad h \geq h_0 - 1,
\]

from which it also follows that

\[
h_0(A_3) = a_2 + \left[ \frac{a_3}{a_2} \right] - 2.
\]

Meures [11] was the first to discover that there is a connection between the h-range and the Frobenius number: Given \( A_k \), if h is sufficiently large, then

\[
n(h, A_k) = a_k h - g(A_k^*) - 1.
\]

Let \( h_1 = h_1(A_k) \) be the smallest \( h \geq h_0 - 1 \) for which (1.4) is valid. Then (1.4) is true for all \( h \geq h_1 \). (For details, see Section 2.) In particular we have \( h_1(A_1) = h_0(A_1) - 1 = 0 \), and since

\[
g(A_k^*) = a_2^2 - 3a_2 + 1,
\]

we also have, by (1.2), that \( h_1(A_2) = h_0(A_2) - 1 \).

Hofmeister [5] introduced a special type of h-range called regular. An integral representation
(1.5) \[ M = a_1 r_1 + a_2 r_2 + \ldots + a_k r_k, \quad r_i \geq 0, \]
is regular if
\[ \sum_{i=1}^{j} a_i r_i < a_{j+1}, \quad j = 1, 2, \ldots, k - 1. \]

Thus, to represent $M$ regularly, $a_k$ is used a maximal number of times, then $a_{k-1}$ is used a maximal number of times, and so on.

Now, the regular $h$-range of $A_k$ is defined as the largest $n$ for which all integers $M, 0 \leq M \leq n$, have a regular representation (1.5) with $r_1 + r_2 + \ldots + r_k \leq h$. The regular $h$-range of $A_k$ was completely determined by Hofmeister [5, Satz 1].

For each positive integer $M$, let $\Lambda(M)$ denote the least number of elements of $A_k$ with sum $M$. Also, put $\Lambda(0) = 0$. Then $M \in hA_k$ if and only if $\Lambda(M) \leq h$.

If, for each $M \geq 0$, we have
\[ \Lambda(M) = \sum_{i=1}^{k} r_i, \]
where the $r_i$ are those appearing in the regular representation (1.5) of $M$, then the basis $A_k$ is called pleasant ("angenehm").

For certain sequences $A_k$, the $h$-range equals the regular $h$-range. In particular, this is so if $A_k$ is pleasant. In this case we have $h_1(A_k) = h_0(A_k) - 1$ (Meures [11]). Some sufficient, but very restrictive, conditions for $A_k$ to be pleasant have been given by Zöllner [23], Hofmeister [7], [8], and Djawadi [3].

In particular, put $a_3 = qa_2 - s$, $0 \leq s < a_2$. Then $A_3$ is pleasant if and only if $s < q$ (Djawadi [3]), and Hofmeister’s result on the regular $h$-range gives us
\[ (1.6) \quad n(h, A_3) = a_3(h + 1 - h_0) + a_2 \left[ \frac{a_3}{a_2} \right] - 2, \quad h \geq h_0 - 1. \]

This result also contains some of the special results on $n(h_0, A_3)$ given by Salié [16].

In the case where Djawadi’s condition $s < q$ is not satisfied, and algorithm for the computation of $n(h, A_3)$ has been given by Windecker [22]. From these results it follows that
\[ n(h + 1, A_3) = a_3 + n(h, A_3) \quad \text{for all } h \geq h_0, \]
which is equivalent to $h_1(A_3) \leq h_0(A_3)$. Using (1.4) and the result on the Frobenius number given in [13] (and also by Siering [19]), we get other algorithms for $n(h, A_3)$, which are simpler to apply than that of Windecker.

Unfortunately, in spite of several missing details, Windecker’s proof of his
algorithm is very long; it is also rather difficult to follow. In this paper we give a shorter and simpler deduction of the main facts about \( n(h, A_3) \).

Most of the previous authors on this subject have been concerned with the global problem. Apart from some tabulated values of \( n(h, k) \) for small \( h \) and \( k \) (see Mossige [12] for some results and further references), the exact value of \( n(h, k) \), however, is known only for \( k=1 \) (trivial), \( k=2 \), \( k=3 \), and for \( h=1 \) (trivial).

Stöhr [20] showed that

\[
n(h, 2) = \left\lfloor \frac{h^2 + 6h + 1}{4} \right\rfloor,
\]

and that the corresponding extremal bases are given by 0, 1, \((h+3)/2\) if \( h \) is odd, and by 0, 1, \((h+3 \pm 1)/2\) if \( h \) is even. (This is an easy consequence of (1.2).)

Hofmeister [6] solved the global problem for \( k=3 \) and \( h \) greater than some effectively computable constant. Hertsch [4] showed that Hofmeister’s results are valid for all \( h \geq 500 \). Recently, Hofmeister [9] showed that his results are valid for all \( h \geq 200 \), and using the Univac 1110 at the University of Bergen, Mossige [12] showed that Hofmeister’s results are also valid if \( 23 \leq h < 200 \).

Using Theorem 1’ of this paper, we can show that Hofmeister’s results are true for all \( h \geq 96 \). In our proof, the \( v \) defined in Section 3 plays the role of Hofmeister’s “s-Stelle”. But apart from this difference and some simplifications, our proof and that of Hofmeister [6], [9] (giving \( h \geq 200 \)) are rather similar. In this paper, therefore we are content with giving a lower bound for \( n(h, 3) \), which is an easy consequence of Theorem 1’.

2. The connection with the Frobenius number.

Let \( N_l = N_l(h, A_k) \) be the smallest non-negative integer which is \( \equiv l \pmod{a_k} \) and does not belong to \( hA_k \). Then

\[
n(h, A_k) = \min_{l \in L} N_l - 1,
\]

where \( L \) is some complete residue system modulo \( a_k \).

Recalling the definition of \( A \) given in Section 1, we have \( A(N_l) \geq h + 1 \). On the other hand, if \( N_l \geq a_k \), then \(-a_k + N_l \not\in hA_k\), so that \( A(N_l) \leq h + 1 \). If \( N_l < a_k \), then \( h < h_0 \), and \( A(N_l) \leq h_0 \). Thus

\[
A(N_l) = h + 1 \quad \text{if} \quad h \geq h_0 - 1.
\]

Let \( t^*_l = t_l(A_k^*) \) be the smallest integer which is \( \equiv l \pmod{a_k} \) and dependent on \( A_k^* \). Then \( t^*_l \) has an integral representation
(2.3) \[ t^*_i = \sum_{i=1}^{k-1} a^*_i x_i^{(l)}, \quad x_i^{(l)} \geq 0. \]

By a lemma of Brauer and Shockley [2], we also have

(2.4) \[ g(A^*_k) = -a + \max_{l \in L} t^*_l. \]

Now, let \( x_i \) be non-negative integers such that

\[ N_l = \sum_{i=1}^{k} a_i x_i, \quad A(N_l) = \sum_{i=1}^{k} x_i. \]

Then, using (2.2), we get

(2.5) \[ N_l = a_k (h+1) - \sum_{i=1}^{k-1} a^*_i x_i, \quad h \geq h_0 - 1. \]

Since

\[ \sum_{i=1}^{k-1} a^*_i x_i \equiv -N_l \equiv -l \pmod{a_k}, \]

we have, by the definition of \( t^*_l \),

\[ \sum_{i=1}^{k-1} a^*_i x_i = a_k w + t^*_l, \quad w \geq 0. \]

Hence, by (2.5),

\[ N_l = a_k (h+1-w) - t^*_l, \quad w \geq 0, \]

and, by (2.1) and (2.4),

(2.6) \[ n(h, A_k) \leq a_k h - g(A^*_k) - 1, \quad h \geq h_0 - 1. \]

On the other hand, for some integer \( u \) we have

\[ N_l = a_k u - t^*_l, \]

so that, by (2.3),

\[ N_l = a_k \left( u - \sum_{i=1}^{k-1} x_i^{(-l)} \right) + \sum_{i=1}^{k-1} a_i x_i^{(-l)}. \]

Hence, if

\[ N_l = \sum_{i=1}^{k-1} a_i x_i^{(-l)}, \]

then
\[ h + 1 = \Lambda(N_i) \leq u , \]

and

\[ N_i \geq a_k(h + 1) - t^*_{-1} . \]

By (2.1), (2.4), and (2.6), we now get

**Lemma 1.** Given \( A_k \) and \( h \geq h_0 - 1 \). For each non-negative integer \( M \), satisfying

\[ M \leq -a_k + \sum_{i=1}^{k-1} a_i x_i^{(-M)} , \]

suppose that \( M \in hA_k \). Then

\[ (2.7) \quad n(h, A_k) = a_k h - g(A_k^*) - 1 . \]

The \( x_i^{(-M)} \) depend only on the residue of \( M \) modulo \( a_k \). Hence, if \( h \) is sufficiently large, then Meure's formula (2.7) is valid. Thus there is a smallest \( h \geq h_0 - 1 \) for which (2.7) is true. We denote this smallest \( h \) by \( h_1 = h_1(A_k) \).

By (2.2), we have

\[ N_i(h + i, A_k) \geq a_k i + N_i(h, A_k), \quad i \geq 0, \ h \geq h_0 - 1 . \]

Hence, by (2.1),

\[ (2.8) \quad n(h + i, A_k) \geq a_k i + n(h, A_k), \quad i \geq 0, \ h \geq h_0 - 1 . \]

Now, if \( h = h_1 + i, \ i \geq 0 \), then

\[ n(h, A_k) \geq a_k i + n(h_1, A_k) = a_k h - g(A_k^*) - 1 . \]

In combination with (2.6) this gives us

**Proposition 1** (Meures [11]). Given \( A_k \), then (2.7) is valid for all \( h \geq h_1 \).

As mentioned in the Introduction, if \( k \geq 3 \), then \( h_1 \leq h_0 \). However, by an example we now show that if \( k > 3 \), then the situation is rather different.

We may alternatively describe \( h_1 \) as the smallest \( h \geq h_0 - 1 \) for which

\[ [0, a_k h - g(A_k^*) - 1] \subseteq hA_k . \]

Since \( M \in hA_k \) if and only if \( a_k h - M \in hA_k^* \) (Meures [11]), we may dually characterize \( h_1 \) as the smallest \( h \geq h_0 - 1 \) for which

\[ [g(A_k^*) + 1, a_k h] \subseteq hA_k^* . \]

In particular, if \( a_k^* = 1 \), then \( g(A_k^*) = -1 \), so that

\[ (2.9) \quad h_1 \geq a_k^* - 1 = a_k - a_k - 2 - 1 \quad \text{if} \quad h_0 \geq 2 . \]
Now, given \( h_0 \geq 2, \ k \geq 3 \), take \( A_k \) to be the sequence
\[
0, 1, 2, \ldots, k-2, (k-2)h_0 + 1, (k-2)h_0 + 2 .
\]
Then \( h_0 = h_0(A_k) \), and by (2.9),
\[
h_1 - h_0 \geq (k-3)(h_0 - 1) .
\]
(This relation is, in fact, valid with equality.)
Hence, for each \( k \geq 4 \) there exist sequences \( A_k \) for which the difference \( h_1 - h_0 \)
is greater than any given integer.
We shall, however, give some upper bounds for \( h_1 \) in terms of \( h_0 \) and \( A_k \). For this purpose, we require the lemma below.

**Lemma 2.** Given \( A_k \) and \( h' \geq h_0 - 1 \). Then the following three statements are equivalent:

(i) \( n(h+1, A_k) = a_k + n(h, A_k) \) for all \( h \geq h' \);

(ii) \( \Lambda(a_k + n(h, A_k) + 1) = h + 2 \) for all \( h \geq h' \);

(iii) \( h' \geq h_1 \).

**Proof.** Since
\[
\Lambda(n(h + 1, A_k) + 1) = h + 2 ,
\]
(i) implies (ii).
Assuming (ii), we get
\[
a_k + n(h', A_k) \geq n(h' + i, A_k) \quad \text{for all } i \geq 0 .
\]
Hence, if \( i \) is sufficiently large, then, by Lemma 1,
\[
a_k + n(h', A_k) \geq a_k(h' + i) - g(A_k^*) - 1 ,
\]
and, by (2.6), (2.7) is satisfied for \( h = h' \). Thus (iii) is true.
Finally, (i) is an obvious consequence of (iii).

In particular, if \( A_k \) is pleasant, then
\[
\Lambda(a_k + M) = 1 + \Lambda(M) \quad \text{for all } M \geq 0 .
\]
Hence the statement (ii) of Lemma 2 is satisfied for \( h' = h_0 - 1 \). Thus \( h_1 = h_0 - 1 \), as mentioned in the Introduction.
Since \( A_2 \) is always pleasant, this gives us
\[
n(h, A_2) = a_2(h + 1 - h_0) + n(h_0 - 1, A_1), \quad h \geq h_0 - 1 ;
\]
that is (1.2). (It is, of course, possible to give a much simpler direct proof of (1.2).)
Next, suppose that \( h_0 - 1 \leq h < h_1 \). By (2.6) and the definition of \( h_1 \), we have
\[
(2.10) \quad a_k + n(h_1 - 1, A_k) + 1 \in h_1 A_k.
\]
Since \( n(h_1 - 1, A_k) + 1 \notin (h_1 - 1)A_k \), the left hand side of (2.10) does, in fact, belong to \( h_1 A_{k-1} \), so that
\[
a_k + n(h_1 - 1, A_k) + 1 \leq a_{k-1} h_1.
\]
Now, using (2.8), we get
\[
a_k (h_1 - h) + n(h, A_k) + 1 \leq a_{k-1} h_1,
\]
so that
\[
n(h, A_k) \leq a_{k-1} (h + 1) - a_k - 1.
\]
Thus we have, as discovered independently by Selmer [18],

**PROPOSITION 2.** Given \( A_k \); if \( h \geq h_0 - 1 \), and
\[
n(h, A_k) \geq a_{k-1} (h + 1) - a_k,
\]
then \( h \geq h_1 \).

Putting \( n_0 = n(h_0 - 1, A_{k-1}) \), we have the

**COROLLARY 1 (Meurers [11]).** Given \( A_k \), then \( h_1 = h_0 - 1 \), or
\[
h_1 \leq \left[ \frac{a_k (h_0 - 1) - n_0 - 1}{a_k - a_{k-1}} \right].
\]

**PROOF.** If \( h \geq h_0 - 1 \), then, by (2.8),
\[
n(h, A_k) \geq a_k (h - h_0 + 1) + n_0.
\]
Hence, if
\[
(2.11) \quad a_k (h - h_0 + 1) + n_0 \geq a_{k-1} (h + 1) - a_k,
\]
then, by Proposition 2, we have \( h \geq h_1 \).

Since, (2.11) is equivalent to
\[
h \geq \left[ \frac{a_k (h_0 - 1) - n_0 - 1}{a_k - a_{k-1}} \right],
\]
the result follows.

Using the trivial bound \( n_0 \geq h_0 - 1 \), Corollary 1 gives us
\[ h_1 \leq \max \left\{ h_0 - 1, \left\lfloor \frac{(a_k - 1)(h_0 - 1) - 1}{a_k - a_{k-1}} \right\rfloor \right\}. \]

It is easily seen that the second argument dominates for \( h_0 \geq 2, \ k \geq 3. \) Hence

\[ h_1 \leq \left\lfloor \frac{(a_k - 1)(h_0 - 1) - 1}{a_k - a_{k-1}} \right\rfloor, \quad h_0 \geq 2, \ k \geq 3. \quad (2.12) \]

From the trivial bound

\[ h_0 \leq \max_{1 \leq i < k} \{ a_{i+1} - a_i \}, \quad k \geq 2, \quad (2.13) \]

it follows that \( h_0 \leq a_k - k + 1. \) Thus, by (2.12), we also have

\[ h_1 \leq \left\lfloor \frac{(a_k - 1)(a_k - k) - 1}{a_k - a_{k-1}} \right\rfloor, \quad a_k > k > 2. \]

This bound is usually far too large. However, it does not depend on any \( h \)-range, neither directly (the \( n_0 \) above) nor indirectly (through \( h_0 \)).

Next, put

\[ d_i = \gcd(a_i, \ldots, a_k), \quad i = 1, 2, \ldots, k - 1; \]
\[ d_k = a_k, \quad d_{k+1} = 0; \]

and let

\[ \beta_k = \sum_{i=1}^{k} a_i \left( \frac{d_{i+1}}{d_i} - 1 \right). \]

Then, if \( M > \beta_k \), we have by the theorem of Weidner [21],

\[ A(a_k + M) = 1 + A(M). \]

Hence, by Lemma 2, we have the

**Proposition 3.** Given \( A_k \); if \( h \geq h_0 - 1 \) and \( n(h, A_k) \geq \beta_k \), then \( h \geq h_1 \).

Since \( g(A_k) \leq \beta_k \) (Brauer [1]), we have \(-1 \leq \beta_k \), so that

\[ h_0 - 1 \leq h_0 + \left\lfloor \frac{\beta_k - h_0}{a_k} \right\rfloor, \quad k \geq 2. \]

In combination with (2.8), Proposition 3 thus gives us

**Corollary 2.** Given \( A_k, k \geq 2, \) then

\[ h_1 \leq h_0 + \left\lfloor \frac{\beta_k - h_0}{a_k} \right\rfloor. \]
Moreover, we have
\[
\beta_k \leq \sum_{i=1}^{k-1} a_{k-1}(d_{i+1} - d_i) - a_k = a_{k-1}a_k - a_{k-1} - a_k
\]
(with equality if \(d_{k-1} = 1\)), so that Corollary 2 gives us

**Corollary 3.** Given \(A_k, k \geq 2\), then \(h_1 \leq h_0 + a_k - 2\).

Finally, in addition to the trivial bound (2.13), we now prove the

**Proposition 4.** Given \(A_k, k \geq 2\), we have

\[
(2.14) \quad h_0 \leq 1 + \max_{1 \leq i < k} \left[ \frac{a_{i+1} - 2}{i} \right].
\]

**Proof.** Let \(\alpha_k(M)\) denote the number of positive integers in \(hA_k\) not exceeding \(M\). Then

\[
\alpha_1(M) = i \quad \text{if} \ a_i \leq M < a_{i+1}, \quad i = 1, 2, \ldots, k-1.
\]

Denote the right hand side of (2.14) by \(h'\). Then

\[
h' \cdot \alpha_1(M) \geq M \quad \text{for} \ M = 1, 2, \ldots, a_k - 1,
\]

and as an easy consequence of "the counting number form" of the \((\alpha + \beta)\)-theorem of H. B. Mann (or, directly from Dyson's theorem; see Mann [10, Chap. 3]), it follows that \(\alpha_k(a_k - 1) = a_k - 1\); that is \([0, a_k - 1] \subseteq h'A_k\). Hence \(h_0 \leq h'\).

**Remark.** Some of the results given in this section may also be extended to sequences \(A_k : 0 = a_0 < a_1 < \ldots < a_k\), where \(a_1\) is an arbitrary positive integer, and \(\gcd A_k = 1\).

In this case we assume \(h\) to be so large that \(g(A_k) + 1 \in hA_k\). We then define \(n(h, A_k)\) as the largest \(n\) for which

\[
[g(A_k) + 1, n] \subseteq hA_k.
\]

If \(h\) is sufficiently large, then (2.7) is valid also in this case. It is also possible to prove that

\[
|hA_k| = n(A_k) + n(A_k^*), \quad h \text{ large,}
\]

where \(|hA_k|\) denotes the number of integers in the relative complement of \(hA_k\) in \([0, a_kh]\), and \(n(A_k)\) (not to be confused with the \(h\)-range of \(A_k\)) is the
number of non-negative integers not dependent on $A_k$. (For some results on $n(A_k)$ and further references, see Selmer [17] and Rødseth [13], [14].)

In particular, it is a simple matter to show that

$$|hA_2| = n(A_2) + n(A_2^*) = \frac{1}{2}(a_2 - 1)(a_2 - 2), \quad h \geq a_2 - 2,$$

where the absence of $a_1$ is easily explained by considering the mapping $a_1x + a_2y \rightarrow x + a_2y$, $0 \leq x < a_2$.

Let us again assume that $a_1 = 1$, and let $h_2 = h_2(A_k)$ be the smallest $h \geq h_0 - 1$ satisfying

$$|hA_k| = n(A_k^*).$$

Then (2.15) is true for all $h \geq h_2$. We have $h_2 \geq h_1$. However, Propositions 2 and 3 with their consequences remain valid when $h_1$ is replaced by $h_2$. It is also possible to prove, using the results of the following two sections, that $h_2(A_3) \leq h_0(A_3)$. (For the value of $n(A_3^*)$, see Rødseth [13, Th. 2].)

3. Preliminaries on $k = 3$.

We now consider the sequence $A_3$: $0 = a_0 < 1 = a_1 < a_2 < a_3$. Putting $a_3 = s_0$, $a_2 = s_0$, we shall use the Euclidean algorithm in the form (cf. [13])

$$s_{-1} = q_1s_0 - s_1, \quad 0 \leq s_1 < s_0$$
$$s_0 = q_2s_1 - s_2, \quad 0 \leq s_2 < s_1$$
$$s_1 = q_3s_2 - s_3, \quad 0 \leq s_3 < s_2$$

$$\ldots$$

$$s_{m-2} = q_ms_{m-1} - s_m, \quad 0 \leq s_m < s_{m-1}$$
$$s_{m-1} = q_{m+1}s_m, \quad 0 = s_{m+1} < s_m.$$

We also recursively define integers $P_i$, $Q_i$, $R_i$ for $i = -1, \ldots, m+1$, by

$$P_{i+1} = q_{i+1}P_i - P_{i-1}, \quad P_0 = 1, P_{-1} = 0$$
$$Q_{i+1} = q_{i+1}Q_i - Q_{i-1}, \quad Q_0 = 0, Q_{-1} = -1$$
$$R_{i+1} = q_{i+1}R_i - R_{i-1}, \quad R_0 = a_2 - 1, R_{-1} = a_3 - 1.$$

Now,
\[
\frac{a_3}{a_2} = q_1 + \frac{-1}{q_2 + \frac{-1}{q_3 + \frac{-1}{\ddots + \frac{-1}{q_{m+1}}}}} = q_1 + \frac{-1}{q_2 + \ldots + q_{m+1}},
\]
where the \(i\)th convergent is given by
\[
q_1 + \frac{-1}{q_2 + \ldots + q_i} = \frac{P_i}{Q_i}, \quad i = 1, \ldots, m+1,
\]
and where \(\gcd(P_i, Q_i) = 1\), because of the relation
\[
P_iQ_{i+1} - P_{i+1}Q_i = 1, \quad i = -1, \ldots, m.
\]
In particular, we thus have \(P_{m+1} = a_3/s_m\), \(Q_{m+1} = a_2/s_m\).
For later references, we also list the following easily proved formulae:
\begin{align*}
(3.3) \quad & a_3Q_i = a_2P_i - s_i \\
(3.4) \quad & a_3R_i = (a_3 - 1)s_i - (a_3 - a_2)P_i \\
(3.5) \quad & s_iQ_{i+1} - s_{i+1}Q_i = a_2.
\end{align*}
Since \(q_i \geq 2\), we have \(P_i < P_{i+1}, Q_i < Q_{i+1}\), and \(R_{i+1} < R_i\). We also have
\[
(3.6) \quad R_i = Q_i - P_i + s_i,
\]
and
\[
(3.7) \quad -\frac{1}{s_m}(a_3 - a_2) = R_{m+1} \ldots < R_0 = a_2 - 1.
\]
Hence there is a unique integer \(v = v(A_3), 0 \leq v \leq m\), satisfying
\[
(3.8) \quad R_{v+1} \leq 0 < R_v.
\]
For \(-1 \leq i \leq m\), we define subsets \(X_i, Y_i\) of the fundamental point lattice by
\[
X_i = \{(x, y) \mid 0 \leq x < s_i - s_{i+1}, \quad 0 \leq y < P_{i+1}\}
\]
\[
Y_i = \{(x, y) \mid 0 \leq x < s_i, \quad 0 \leq y < P_{i+1} - P_i\}.
\]
We shall say that two lattice points \((x, y)\) and \((x', y')\) are congruent if
\[
x + a_2y \equiv x' + a_2y' \pmod{a_3}.
\]
It is easily seen that \( X_i \cup Y_i \) contains just \( a_3 \) elements. We continue to show that these \( a_3 \) elements are incongruent.

**Lemma 3.** If \((x,y) \in X_{i-1} \cup Y_{i-1}, 0 \leq i \leq m\), then the lattice point

\[
(x', y') = \left( x - s_i \left\lfloor \frac{x}{s_i} \right\rfloor, y + p_i \left\lfloor \frac{x}{s_i} \right\rfloor \right)
\]

belongs to \( X_i \cup Y_i \) and is congruent to \((x,y)\).

**Proof.** By (3.3), we have

\[
x' + a_2 y' = x + a_2 y' + a_3 q_i \left\lfloor \frac{x}{s_i} \right\rfloor.
\]

Hence \((x',y')\) is congruent to \((x,y)\).

We now show that \((x',y') \in X_i \cup Y_i\). Clearly, \(0 \leq x' < s_i\). If \((x,y) \in X_{i-1}\), then

\[
y' < p_i + p_i \left\lfloor \frac{s_{i-1} - s_i - 1}{s_i} \right\rfloor = p_{i+1} - (p_i - p_{i-1}) < p_{i+1},
\]

since \(\left\lfloor \frac{(s_{i-1} - 1)}{s_i} \right\rfloor = q_{i+1} - 1\).

If \((x,y) \in Y_{i-1}\), then

\[
y' < p_i - p_{i-1} + p_i \left\lfloor \frac{s_{i-1} - 1}{s_i} \right\rfloor = p_{i+1}.
\]

Thus we have

\[
0 \leq x' < s_i \quad \text{and} \quad 0 \leq y' < p_{i+1}.
\]

Let us now assume that \(x' \geq s_i - s_{i+1}\) and \(y' \geq p_{i+1} - p_i\). If \((x,y) \in X_{i-1}\), then

\[
p_{i+1} - p_i \leq y + p_i \left\lfloor \frac{x}{s_i} \right\rfloor < p_i + p_i \left\lfloor \frac{x}{s_i} \right\rfloor,
\]

so that \(q_{i+1} - 2 \leq \left\lfloor x/s_i \right\rfloor\), which gives us

\[
x = x' + s_i \left\lfloor \frac{x}{s_i} \right\rfloor \geq s_i - s_{i+1} + s_i(q_{i+1} - 2) = s_{i-1} - s_i;
\]

a contradiction.

If \((x,y) \in Y_{i-1}\), then

\[
p_{i+1} - p_i \leq y + p_i \left\lfloor \frac{x}{s_i} \right\rfloor < p_i - p_{i-1} + p_i \left\lfloor \frac{x}{s_i} \right\rfloor,
\]

\[\text{Math. Scand. 48 — 12}\]
so that \( q_{i+1} - 1 \leq [x/s_i] \), which gives us

\[
x' = x' + s_i \left\lceil \frac{x}{s_i} \right\rceil \geq s_i - s_{i+1} + s_i(q_{i+1} - 1) = s_{i-1},
\]

and again we have reached a contradiction.

Hence we have \( x' < s_i - s_{i+1} \) or \( y' < P_{i+1} - P_i \), which, in combination with (3.10), shows that \((x', y') \in X_i \cup Y_i\).

Because of Lemma 3, for each \( i = 0, \ldots, m \), we may define a function

\[
\varphi: X_{i-1} \cup Y_{i-1} \to X_i \cup Y_i
\]

by putting \( \varphi(x, y) = (x', y') \), for \((x', y') \) given by (3.9).

If \((x, y) \in X_{i-1} \cup Y_{i-1}\), then \([x/s_i] = [y'/P_i]\). Hence \( \varphi \) has an inverse

\[
\varphi^{-1}: X_i \cup Y_i \to X_{i-1} \cup Y_{i-1}
\]

given by

\[
\varphi^{-1}(x', y') = \left( x' + s_i \left\lceil \frac{y'}{P_i} \right\rceil, y' - P_i \left\lceil \frac{y'}{P_i} \right\rceil \right).
\]

Thus \( \varphi \) is a bijection, and, by Lemma 3, \( \varphi \) also has the property that if \((x, y) \in X_{i-1} \cup Y_{i-1}\), then \((x, y)\) and \(\varphi(x, y)\) are congruent lattice points.

Since

\[
X_{-1} \cup Y_{-1} = \{(x, 0) \mid 0 \leq x < a_3\},
\]

it follows that \( X_i \cup Y_i \) consists of \( a_3 \) incongruent lattice points. Thus the set

\[
\{x + a_2y \mid (x, y) \in X_i \cup Y_i\}
\]

forms a complete residue system modulo \( a_3 \) for each \( i = -1, \ldots, m \).

Now fix \( r, 0 \leq r < a_3 \). Let \((x_i, y_i)\) be the unique lattice point in \( X_i \cup Y_i \) which is congruent to \((r, 0)\), \( i = -1, \ldots, m \). Then

\[
(3.11) \quad x_i + a_2y_i = x_{i-1} + a_2y_{i-1} + a_3Q_i \left\lceil \frac{x_{i-1}}{s_i} \right\rceil, \quad i \geq 0.
\]

Recalling the definition of \( t_i^* = t_i(A_3^*) \) given in Section 2, we now prove

**Lemma 4.** We have \( t_{i,r}^* = (a_3 - 1)x_v + (a_3 - a_2)y_v \).

**Proof.** A more general result is proved in [13]. However, for the convenience of the reader, we include a proof of this lemma.
By the definition of $t^*_r$, there are non-negative integers $x, y$ such that

$$t^*_r = (a_3 - 1)x + (a_3 - a_2)y.$$  

We choose such a pair $(x, y)$ for which $y$ is minimal. By (3.4), we have

$$t^*_r - a_3 R_v = (a_3 - 1)(x - s_v) + (a_3 - a_2)(y + P_v).$$

Since $R_v$ is a positive integer, and $t^*_r$ is the smallest integer $\equiv -r \pmod{a_3}$ with a representation (3.12), we have $x < s_v$.

Similarly,

$$t^*_r + a_3 R_{v+1} = (a_3 - 1)(x + s_{v+1}) + (a_3 - a_2)(y - P_{v+1}),$$

and if $R_{v+1} < 0$, then $y < P_{v+1}$. Also in the case $R_{v+1} = 0$, we have $y < P_{v+1}$, because of the minimality of $y$.

Finally,

$$t^*_r - a_3 (R_v - R_{v+1}) = (a_3 - 1)(x - s_v + s_{v+1}) + (a_3 - a_2)(y + P_v - P_{v+1}),$$

so that $x < s_v - s_{v+1}$ or $y < P_{v+1} - P_v$.

Hence $(x, y) \in X_v \cup Y_v$. Since $x + a_2 y \equiv -t^*_r \equiv r \pmod{a_3}$, we thus have $(x, y) = (x_v, y_v)$.

For $h_0 = h_0(A_3)$ given by (1.3), we now prove the

**Lemma 5.** For $1 \leq i \leq v$, we have

$$x_{i-1} + y_{i-1} + Q_i - 1 \leq h_0 \quad \text{if } P_i \leq s_i$$

(3.13)

$$x_i + y_i + R_i - 1 \leq h_0 \quad \text{if } P_i > s_i.$$  

(3.14)

**Proof.** For $m \geq 1$, we have $s_1 > 0$. Hence, by (1.3), $h_0 = a_2 + q_1 - 3$.

Put

$$\gamma_i = \max_{(x, y) \in X_i} \{x + y\} = s_i - s_{i+1} + P_{i+1} - 2,$$

and

$$\delta_i = \max_{(x, y) \in Y_i} \{x + y\} = s_i + P_{i+1} - P_i - 2.$$  

We first prove (3.13) and therefore assume that $P_i \leq s_i$. Then $\gamma_{i-1} < \delta_{i-1}$, and it is sufficient to show that

$$\delta_{i-1} + Q_i - 1 \leq h_0.$$  

(3.15)

By (3.5), we have

$$h_0 - \delta_{i-1} - Q_i + 1 = (Q_i - 1)s_{i-1} - Q_i s_i - P_i + P_{i-1} - Q_i + q_1.$$
and, since \( s_{i-1} \geq s_i + 1 \),
\[
h_0 - \delta_{i-1} - Q_i + 1 \geq (Q_i - Q_{i-1} - 1)s_i - P_i + P_{i-1} + q_1 - 1 .
\]
Using the assumption \( P_i \leq s_i \), we further get
\[
(3.16) \quad h_0 - \delta_{i-1} - Q_i + 1 \geq (Q_i - Q_{i-1} - 2)P_i + P_{i-1} + q_1 - 1 .
\]
If \( Q_i - Q_{i-1} - 2 \geq 0 \), we thus have
\[
\delta_{i-1} + Q_i - 1 \leq h_0 - q_1 .
\]
If \( Q_i - Q_{i-1} - 2 \leq -1 \), then \( i = 1 \) or \( q_2 = \ldots = q_i = 2 \). Hence
\[
(3.17) \quad Q_j = j, \quad P_j = (q_1 - 1)j + 1 \quad \text{for } 0 \leq j \leq i ,
\]
and the right hand side of (3.16) equals 0. This completes the proof of (3.15).

In the proof of (3.15) we did not explicitly use the assumption \( i \leq v \). However, it follows from (3.6) that the conditions \( i \geq 1 \) and \( P_i \leq s_i \) imply \( i \leq v \).

Next we prove (3.14) and therefore assume that \( P_i > s_i \). Then \( \gamma_i > \delta_i \), and it is sufficient to show that
\[
(3.18) \quad \gamma_i + R_i - 1 \leq h_0 .
\]

By (3.5) and (3.6), we have
\[
h_0 - \gamma_i - R_i + 1 = (Q_{i+1} - 2)s_i - (Q_i - 1)s_i + 1 - P_i + Q_i + P_i + q_1 ,
\]
and, since \( s_{i+1} \leq s_i - 1 \), we get
\[
h_0 - \gamma_i - R_i + 1 \geq (Q_{i+1} - Q_i - 1)s_i - P_i + P_i + q_1 - 1 .
\]
Since \( i \leq v \), we have \( R_i \geq 1 \) by (3.7) and (3.8), so that, by (3.6), \( s_i \geq 1 + P_i - Q_i \).

Hence, using (3.1) and (3.2), we get
\[
(3.19) \quad h_0 - \gamma_i - R_i + 1 \geq (q_{i+1}(Q_i - 1) - Q_i - Q_{i-1})(P_i - Q_i) +
+ P_{i-1} - Q_{i-1} + q_1 - 2 .
\]
Thus, if \( q_{i+1}(Q_i - 1) - Q_i - Q_{i-1} \geq 0 \), then (3.18) is true.

Since \( P_i > s_i \) and \( v \geq 1 \), we have \( i \geq 2 \). Hence, if \( q_{i+1}(Q_i - 1) - Q_i - Q_{i-1} \leq -1 \), then \( q_2 = \ldots = q_{i+1} = 2 \). Thus, by (3.17), the right hand side of (3.19) equals 0, and (3.18) is true also in this case.

4. Determination of \( n(h, A_3) \).

We now prove that if \( k = 3 \) and \( h \geq h_0 \), then the hypotheses of Lemma 1 are satisfied. In the notation of the preceding section, by Lemma 4, we then have to show that for each \( r, 0 \leq r \leq a_3 \), the sequence
(4.1) \[ r < r + a_3 < r + 2a_3 < \ldots < x_v + a_2y_v - a_3 \]
is a subsequence of \( h_0A_3 \).

If \( v = 0 \), then the sequence (4.1) is empty, and \( h_1 = h_0 - 1 \). We therefore assume that \( v \geq 1 \).

By (3.11), we have
\[ r = x_0 + a_2y_0 \leq x_1 + a_2y_1 \leq \ldots \leq x_v + a_2y_v. \]

Given \( i, 1 \leq i \leq v \), suppose that \( x_{i-1} \geq s_i \). We then show that the integer
\[ M = x_{i-1} + a_2y_{i-1} + a_3z, \quad 0 \leq z < Q_i \frac{x_{i-1}}{s_i}, \]
belongs to \( h_0A_3 \).

Put
\[ z = Q_i \left[ \frac{z}{Q_i} \right] + z'. \]

By (3.3), we then have \( M = x' + a_2y' + a_3z' \), where
\[ x' = x_{i-1} - s_i \left[ \frac{z}{Q_i} \right] \geq 0, \quad y' = y_{i-1} + P_i \left[ \frac{z}{Q_i} \right], \quad 0 \leq z' < Q_i. \]

and
\[ x' + y' + z' \leq x_{i-1} + y_{i-1} + (P_i - s_i) \left[ \frac{z}{Q_i} \right] + Q_i - 1. \]

If \( P_i \leq s_i \), then
\[ x' + y' + z' \leq x_{i-1} + y_{i-1} + Q_i - 1. \]

Since \( z < Q_i \frac{x_{i-1}}{s_i} \) and \( (x_i, y_i) = \phi(x_{i-1}, y_{i-1}) \), we get, using (3.6),
\[ x' + y' + z' \leq x_i + y_i + R_i - 1 \quad \text{if} \quad P_i > s_i. \]

In both cases we have, by Lemma 5, that \( x' + y' + z' \leq h_0 \), as required.

**Theorem 1.** We have
\[ n(h, A_3) = a_3h - g(A_3^*) - 1 \quad \text{for all} \quad h \geq h_0, \]
where \( h_0 \) is given by (1.3).

By (2.4) and Lemma 4, this theorem may be given the more explicit form:
Theorem 1'. In the notation of Section 3, we have
\[ n(h, A_3) = a_3(h+1) - (a_3-1)(s_v-1) - (a_3-a_2)(P_{v+1} - 1) + \min \{ (a_3-1)s_{v+1}, (a_3-a_2)P_v \} - 1 \]
for \( h \geq h_0 \), where \( v \) is determined by (3.8).

More briefly, Theorem 1 states that \( h_1(A_3) \leq h_0(A_3) \). If \( v = 0 \), that is if Djawadi’s condition \( s_1 < q_1 \) is satisfied, then we know that \( h_1(A_3) = h_0(A_3) - 1 \), and Theorem 1’ coincides with (1.6). If \( v \geq 1 \), it is not difficult to see that \( h_1(A_3) = h_0(A_3) - 1 \). Thus \( h_1(A_3) = h_0(A_3) \) if \( v \geq 1 \).

For relatively prime positive integers \( a, b, c \), an algorithmic formula for the Frobenius number \( g(a, b, c) \) was given in [13]. Using Th. 1 in [13], we then get Theorem 1’ from Theorem 1, by putting \( a=a_3, b=a_3-1, c=a_3-a_2 \). Similar algorithmic formulae for \( n(h, A_3) \) arise by pairing \( a_3, a_3-1, a_3-a_2 \) with \( a, b, c \), in other ways. (See Selmer [18].)

Suppose that \( h \geq 2 \), and let \( \beta, \gamma \) be integers satisfying \( 2 \leq \gamma \leq \beta, 2\beta \leq h+2 \). Put
\[ a_2 = 2\beta - \gamma + 1, \quad a_3 = a_2\gamma - \beta. \]

Then \( q_1 = \gamma, s_1 = \beta, q_2 = 2, s_2 = \gamma - 1, R_1 = 1 - \gamma + \beta \geq 1, R_2 = 2 - \gamma \leq 0 \), so that \( v = 1 \), and Theorem 1’ gives us
\[ n(h, A_3) = a_3(h+5 - \beta - \gamma) - 2(\beta - \gamma + 2), \]
which shows that Hilfssatz 1 of Hofmeister [6] is valid with equality.

Hofmeister (Satz 2) made the following choice:
\[ \beta = \left\lceil \frac{4(h+1)}{9} \right\rceil + 2, \quad \gamma = \left\lceil \frac{2h}{9} \right\rceil + 2. \]

Now, for \( h \geq 18 \), (4.2) gives us
\[ n(h, A_3) = \frac{4}{81}h^3 + \frac{2}{3}h^2 + \varepsilon_1h + \varepsilon_0, \]
where the coefficients \( \varepsilon_1, \varepsilon_0 \) depend on the residue of \( h \) modulo 9.

It is now known (cf. Section 1) that this choice of \( A_3 \) gives us the unique extremal basis for each \( h \geq 23 \).

Acknowledgment. The author gratefully acknowledges his indebtedness to Professor E. S. Selmer and Professor G. R. Hofmeister. In particular, Professor Selmer read through an earlier version of the manuscript making a number of helpful comments, and Professor Hofmeister supplied us with copies of the most difficult accessible references.
REFERENCES


ROGALAND DISTRIKTSHØGSKOLE
BOX 2540, ULLANDHAUG
N-4001 STAVANGER
NORWAY