

A LINEAR DIOPHANTINE PROBLEM

S. M. JOHNSON

1. Introduction. Let a_1, a_2, \dots, a_t be a set of groupwise relatively prime positive integers. Several authors, **(2; 3; 5; 6)**, have determined bounds for the function $F(a_1, \dots, a_t)$ defined by the property that the equation

$$(1) \quad n = a_1x_1 + a_2x_2 + \dots + a_t x_t$$

has a solution in positive integers x_1, \dots, x_t for $n > F(a_1, \dots, a_t)$. If $F(a_1, \dots, a_t)$ is a function of this type, it is easy to see that

$$(2) \quad G(a_1, \dots, a_t) = F(a_1, \dots, a_t) - a_1 - a_2 - \dots - a_t$$

is the corresponding function for the solvability of (1) in non-negative x 's.

It is well known that a_1a_2 is the best bound for $F(a_1, a_2)$ and $a_1a_2 - a_1 - a_2$ for $G(a_1, a_2)$. Otherwise only in very special cases have the best bounds been found, even for $t = 3$.

In the present paper a symmetric expression is developed for the best bound for $F(a_1, a_2, a_3)$ which solves that problem and gives insight on the general problem for larger values of t . In addition, some relations are developed which may be of interest in themselves.

2. A General Property. For $t \geq 2$, let $B(a_1, a_2, \dots, a_t)$ be the best bound for $F(a_1, a_2, \dots, a_t)$, that is, B is the maximum number N where

$$(3) \quad N \neq \sum_{i=1}^t x_i a_i \quad \text{for any } x_i > 0.$$

Then note that B is the maximum N from a restricted set of numbers N satisfying both (3) and

$$(4) \quad N + a_i = \sum_{j=1}^t y_{ij} a_j, \quad y_{ij} > 0 \text{ for each } i.$$

since the definition of B implies B satisfies (4). Thus, in particular,

$$N = (y_{11} - 1)a_1 + y_{12}a_2 + \dots + y_{1t}a_t, \quad y_{1j} > 0.$$

But by (3), $y_{11} - 1 \leq 0$ so that $y_{11} = 1$ since $y_{11} > 0$. By symmetry we have

THEOREM 1. *For every N satisfying (3) and (4) there are representations of N for each $i = 1, 2, \dots, t$ of the form*

$$(5) \quad N = \sum_{\substack{j=1 \\ j \neq i}}^t y_{ij} a_j, \quad y_{ij} > 0,$$

and B is the maximum such N .

Received October 21, 1957; in revised form March 9, 1959.

3. The Case $t = 3$. A reduction formula. We seek an expression for $B = B(a_1, a_2, a_3)$ having the property that (1) is satisfied for $n > B$ but is not satisfied for $n = B$. Let us first reduce the problem to the case of pairwise relatively prime a 's.

Let $d_{ij} = (a_i, a_j)$, $a_i = b_i d_{ij} d_{ik}$, so that $(b_1, b_2) = (b_2, b_3) = (b_3, b_1) = 1$. Then we have

THEOREM 2.

$$(6) \quad B(a_1, a_2, a_3) = d_{12}d_{23}d_{31}B(b_1, b_2, b_3).$$

Proof. First we show that if we write $d = d_{12}$, $\bar{b}_1 = d_{13}b_1$, $\bar{b}_2 = d_{23}b_2$ so that $(d, a_3) = (\bar{b}_1, \bar{b}_2) = 1$, then

$$(7) \quad B(d\bar{b}_1, d\bar{b}_2, a_3) = dB(\bar{b}_1, \bar{b}_2, a_3).$$

Suppose that $dB(\bar{b}_1, \bar{b}_2, a_3) = d\bar{b}_1x + d\bar{b}_2y + a_3z$, $x, y, z > 0$. Then since $(d, a_3) = 1$, we must have $z = wd$, $w > 0$, so that $B(\bar{b}_1, \bar{b}_2, a_3) = \bar{b}_1x + \bar{b}_2y + a_3w$, $x, y, w > 0$, a contradiction to the definition of $B(\bar{b}_1, \bar{b}_2, a_3)$. In addition, for any positive integer $m > 0$, we show that

$$(8) \quad dB(\bar{b}_1, \bar{b}_2, a_3) + m = d\bar{b}_1x + d\bar{b}_2y + a_3z, \quad x, y, z > 0.$$

We apply a result from (2).

LEMMA 1 (Brauer). *Let a and b be relatively prime positive integers. Then every positive integer m divisible neither by a nor by b is representable either in the form*

$$(9) \quad m = au + bv, \quad u > 0, v > 0,$$

or

$$(10) \quad m = ab - au - bv, \quad b > u > 0, a > v > 0.$$

Letting $d = a$ and $a_3 = b$ in Lemma 1, if (9) holds, we have

$$(11) \quad dB(\bar{b}_1, \bar{b}_2, a_3) + m = d(B(\bar{b}_1, \bar{b}_2, a_3) + u) + va_3 \\ = d\bar{b}_1x + d\bar{b}_2y + a_3(dz + v)$$

by the definition of $B(\bar{b}_1, \bar{b}_2, a_3)$, giving (8).

If (10) holds, we have $0 < u < a_3$, and $0 < v < d$, so that

$$(12) \quad d(B(\bar{b}_1, \bar{b}_2, a_3) + a_3 - u) - va_3 = d\bar{b}_1x + d\bar{b}_2y + (dz - v)a_3,$$

for x, y , and $(dz - v) > 0$, giving (8).

Finally, if $m = ud$, then (8) follows directly. If $m = va_3$, write $m = da_3 + (v - d)a_3$ giving (8). Thus (7) holds. Applying the method of obtaining (7) twice more gives (6) and Theorem 2.

We have thus reduced the problem to where the a 's are pairwise relatively prime. For the moment let $a_1 > a_2 > a_3$. If

$$(13) \quad a_1 = ua_2 + va_3, \quad u, v > 0,$$

then $B(a_1, a_2, a_3) = a_2a_3 + a_1$ as Brauer showed in (2). Otherwise

$$(14) \quad B(a_1, a_2, a_3) < a_ia_j + a_k.$$

4. An expression for $B(a_1, a_2, a_3)$. We develop a symmetric expression for $B(a_1, a_2, a_3)$ for the case of pairwise relatively prime a 's where each $a_i \neq xa_j + ya_k$, $x > 0$, $y > 0$. Later we show that this same form of expression gives the general solution for $t = 3$.

DEFINITION. Let $L_i =$ the minimum positive K_i satisfying

$$(15) \quad K_i a_i = v_{ij} a_j + v_{ik} a_k, \quad v_{ij} \geq 0, v_{ik} \geq 0, \quad i = 1, 2, 3.$$

Such a number exists since $B(a_j, a_k) = a_j a_k < K a_i$ for large K .

THEOREM 3. *Given*

$$(16) \quad (a_1, a_2) = (a_2, a_3) = (a_3, a_1) = 1$$

and

$$(17) \quad L_i > 1, \quad i = 1, 2, 3$$

and

$$(15') \quad L_i a_i = x_{ij} a_j + x_{ik} a_k,$$

then the x_{ij} are uniquely defined and

$$(18) \quad x_{ij} > 0.$$

Since $L_i > 1$, it follows from (10) and (16) that

$$(19) \quad a_i = a_j a_k - v_{ij} a_j - v_{ik} a_k$$

where $0 < v_{ij} < a_k$, $0 < v_{ik} < a_j$. Thus $v_{ik} a_k + a_i = (a_k - v_{ij}) a_j \geq L_j a_j$ and so by symmetry

$$(20) \quad L_j < a_k, \quad \text{for each } j \neq k.$$

If $x_{ji} = 0$, then $L_i a_i = x_{jk} a_k$ and by (16) $L_j = m a_k$, a contradiction to (20). This gives (18). Also the x_{ij} are uniquely determined since if $L_i a_i = x_{ij} a_j + x_{ik} a_k = z_{ij} a_j + z_{ik} a_k$, then by (16) we have $x_{ij} = z_{ij} + m a_k$ and $x_{ik} = z_{ik} - m a_j$. If $m > 0$, $x_{ij} > a_k$. But then for some $d > 0$, $L_i a_i = (a_k + d) a_j + x_{ik} a_k$ and by (19) we get $(L_i - 1) a_i = (d + v_{ij}) a_j + (x_{ik} + v_{ik}) a_k$, contradicting the definition of L_i . Similarly, for $m < 0$.

For $t = 3$ and (16) and (17) we show that there are just two numbers N with properties (3) and (4) so that B is the larger of these numbers. From (5) such a number N has representations of the form

$$(5') \quad N = y_{ij} a_j + y_{ik} a_k \quad i = 1, 2, 3.$$

Next observe that from (18) we have

$$(21) \quad y_{ij} \leq L_j$$

since otherwise for some $d_j > 0$ we would have $N = (L_j + d_j) a_j + y_{ik} a_k = x_{ji} a_i + d_j a_j + (x_{jk} + y_{ik}) a_k$, contradicting (3). From (20) and (21) we have

$$(22) \quad y_{kj} < a_k, \quad y_{kj} < a_i.$$

Next we show that the representations (5') for N are unique for each i . For otherwise $y_{ki}a_i + y_{kj}a_j = z_{ki}a_i + z_{kj}a_j$ and from (16) and (22), $y_{kj} - z_{kj} = ma_i$, $m \leq 0$, and $y_{ki} - z_{ki} = ma$, $m \geq 0$, so that $m = 0$ and $y_{kj} = z_{kj}$, etc.

From (5') and Theorem 1 we now have unique representations of N of the form

$$N = y_{ki}a_i + y_{kj}a_j = y_{ij}a_j + y_{ik}a_k = y_{jk}a_k + y_{ji}a_i.$$

If $y_{kj} = y_{ij}$, then $y_{ki} = ma_k$, contradicting (22). Thus either $y_{kj} < y_{ij}$ or $y_{kj} > y_{ij}$.

Case 1. If

$$(23) \quad y_{kj} < y_{ij}$$

then $y_{ki}a_i = (y_{ij} - y_{kj})a_j + y_{ik}a_k$ so that $y_{ki} \geq L_i$. Thus by (21) we have

$$(24) \quad y_{ki} = L_i.$$

Then by (24) and (5')

$$N = L_i a_i + y_{kj} a_j = y_{ji} a_i + y_{jk} a_k$$

or $(L_i - y_{ji})a_i + y_{kj}a_j = y_{jk}a_k$, where $L_i \geq y_{ji}$ by (21). If $L_i = y_{ji}$ then $y_{kj} = ma_k$, contradicting (22), so that $L_i - y_{ji} > 0$ and $y_{jk} \geq L_k$ by the definition of L_k . But then $y_{jk} = L_k$ by (21). Thus (23) implies that $y_{ki} = L_i$, $y_{jk} = L_k$, and cyclically, $y_{ij} = L_j$. But then by (15')

$$N = (x_{ij} + y_{kj})a_j + x_{ik}a_k = L_j a_j + y_{ik} a_k$$

and by the uniqueness of these representations and by cyclic permutation of subscripts, we have

$$(25) \quad y_{ik} = x_{ik}$$

and

$$(26) \quad L_j = x_{ij} + x_{kj}.$$

Thus if $y_{kj} < y_{ij}$, we get a unique number N where

$$(27) \quad N = L_i a_i + x_{kj} a_j$$

with cyclic permutations of subscripts.

Case 2. If

$$(28) \quad y_{kj} > y_{ij},$$

we get another number where by symmetry

$$(29) \quad N' = L_i a_i + x_{jk} a_k$$

with cyclic permutations of subscripts. $N \neq N'$ since otherwise $x_{jk}a_k = x_{kj}a_j$ which implies $x_{jk} \geq a_j$, which by (25) contradicts (22). Note that these two

numbers are the only numbers with properties (3) and (4) for (16), (17), and $t = 3$. Since B is the largest number with property (3), it satisfies (4) so that B is the maximum of N and N' and we have

THEOREM 4. *Given (16) and (17), then for cyclic permutations of subscripts*

$$(30) \quad B(a_1, a_2, a_3) = L_i a_i + \max(x_{kj} a_j, x_{jk} a_k)$$

and (26) holds.

Also it is easy to verify that C , the corresponding best bound for $G(a_1, a_2, a_3)$, satisfies

$$(31) \quad C(a_1, a_2, a_3) + a_1 + a_2 + a_3 = B(a_1, a_2, a_3).$$

5. A computing algorithm for L_i and x_{ij} . Thus we have shown that finding B is equivalent to finding the set of positive integers L_i and x_{ij} exhibited in the form of a matrix of detached coefficients of the three equations (15') as follows:

a_1	a_2	a_3
$-L_1$	x_{12}	x_{13}
x_{21}	$-L_2$	x_{23}
x_{31}	x_{32}	$-L_3$

In order to develop a simple computing algorithm for these numbers, we need the following result.

LEMMA 2. *Given $(a_1, a_2) = (a_2, a_3) = (a_3, a_1) = 1$, then any system of integers $K_i > 1$ and $v_{ij} > 0$ (not necessarily L_i and x_{ij}) satisfying (15) and (26) $K_i = v_{ji} + v_{ki}$, implies that*

$$(32) \quad K_i K_j - v_{ij} v_{ji} = v_j v_{kj} + v_{ki} K_j = \lambda a_k \geq a_k$$

for some positive integer λ .

If we write

$$v_{jk}(K_i a_i - v_{ij} a_j) = v_{ik} v_{jk} a_k = v_{ik}(K_j a_j - v_{ji} a_i),$$

then

$$(v_{jk} K_i + v_{ik} v_{ji}) a_i = (v_{ik} K_j + v_{jk} v_{ij}) a_j$$

and (32) follows by (16) and (26).

Furthermore, we have

THEOREM 5. *If (16) and (17) hold, then the L_i and x_{ij} in Theorem 4 are characterized by the equations (15') and (26), and*

$$(33) \quad L_i L_j + x_{ij} x_{ji} = a_k,$$

for cyclic permutations of subscripts. That is, $\lambda = 1$ in (32).

Proof. Suppose a system of K_i and v_{ij} satisfy (15), (26), and (33) where at least one $K_i > L_i$, the minimum positive integer satisfying (15).

Case 1. If $K_1 = L_1, K_2 = L_2$, then $K_3 = L_3$ by (26) and Theorem 3.

Case 2. Suppose $K_1 = L_1$, but $K_2 > L_2, K_3 > L_3$.

Then $x_{12} = v_{12}$ and $x_{13} = v_{13}$ by Theorem 3 and by (15), (26), and (33) $a_1 = K_2K_3 - v_{32}v_{23} = K_2K_3 - (K_2 - x_{12})(K_3 - x_{13}) = x_{12}K_3 + x_{13}K_2 - x_{12}x_{13} > x_{12}L_3 + x_{13}L_2 - x_{12}x_{13} = L_2L_3 - x_{32}x_{23} \geq a_1$ by (32), a contradiction to the assumption that $K_2 > L_2, K_3 > L_3$.

Case 3. If $K_1 > L_1, L_2 > K_2, K_3 > L_3$, then first observe that either $v_{ij} > x_{ij}$ or $v_{ik} > x_{ik}$, but not both. For suppose $v_{ij} > x_{ij}$ and $v_{ik} > x_{ik}$. By (33) $v_{ij}v_{jk} + K_jv_{ik} = a_i \leq x_{ij}x_{jk} + L_jx_{ik}$ by (32). Thus $v_{jk} < x_{jk}$. Similarly $v_{ij}K_k + v_{ik}v_{kj} = a_i \leq x_{ij}L_k + x_{ik}x_{kj}$ so that $v_{kj} < x_{kj}$. But then $a_i \leq L_jL_k - x_{jk}x_{kj} < K_jK_k - v_{jk}v_{kj} = a_i$, a contradiction.

In addition either $v_{ji} > x_{ji}$ or $v_{ki} > x_{ki}$ but not both. For suppose $v_{ji} > x_{ji}$ and $v_{ki} > x_{ki}$. By the previous remark $v_{jk} < x_{jk}, v_{kj} < x_{kj}$, leading to the same contradiction obtained above. Thus either v_{12}, v_{23}, v_{31} , or v_{21}, v_{32}, v_{13} are larger than the corresponding x 's. That is $v_{ij} > x_{ij}$ for cyclic permutations of subscripts.

Suppose v_{21}, v_{32}, v_{13} are larger than x_{21}, x_{32}, x_{13} respectively. Then by (26)

$$(K_2 - L_2)a_2 + (x_{23} - v_{23})a_3 = (v_{21} - x_{21})a_1 \geq L_1a_1$$

by the definition of L_1 . Thus $v_{21} > L_1$ and by cyclic permutation of subscripts $v_{32} > L_2, v_{13} > L_3$.

Finally $a_3 \leq L_1L_2 - x_{13}x_{21} < L_1L_2 < v_{21}v_{32} < v_{21}v_{32} + K_2v_{31} = a_3$, a contradiction.

Thus $\lambda = 1$ in (32) implies that $K_i = L_i, v_{ij} = x_{ij}$.

Conversely, $\lambda = 1$ in (32), for $K_i = L_i, v_{ij} = x_{ij}$ etc. By the following computing algorithm we can always find sets of K_i and v_{ij} with $\lambda = 1$ in (32). Thus they are the desired L_i and x_{ij} . Moreover since the x_{ij} are unique by Theorem 3, λ is unique and must equal 1.

The usefulness of Theorem 5 is apparent since it will be easier to find K 's and v 's satisfying (15), (26), and (33) rather than find minimal solutions to (15).

The algorithm follows. First we solve for any a_k in terms of a_i and a_j ; for instance, for $k = 3$, giving

$$(34) \quad v_{21}a_1 - K_2a_2 + a_3 = 0$$

with $0 < v_{21} < a_2, 0 < K_2 < a_1$ by (10), easily done for example as in (4).

Next construct

$$(35) \quad -K_1a_1 + v_{12}a_2 + v_{13}a_3 = 0$$

where

$$v_{13} = \left[\frac{a_1}{K_2} \right], \quad K_1 = a_2 - v_{21}v_{13}, a_1 = K_2v_{13} + v_{12}$$

so that $\lambda = 1$ in (32). If $K_1 > v_{21}$, then $K_1 = L_1$, $K_2 = L_2$, and L_3 can be found by (26). Then apply Theorem 4 for $B(a_1, a_2, a_3)$. If $K_1 \leq v_{21}$, note that $K_1 \nmid v_{21}$. For if $K_1 | v_{21}$, then since $K_1 = a_2 - v_{21}v_{13}$, $K_1 | a_2$. But then in (34) $K_1 | a_3$. Thus $(a_2, a_3) \geq K_1 > 1$, by (17) a contradiction.

Therefore if $K_1 < v_{21}$ we can construct another equation

$$(36) \quad (v_{21} - pK_1)a_1 - (K_2 - pv_{12})a_2 + (1 + pv_{13})a_3 = 0$$

with

$$p = \left\lfloor \frac{v_{21}}{K_1} \right\rfloor.$$

Since $v_{21} - pK_1 > 0$, $K_2' = K_2 - pv_{12}$ forms a smaller value of K_2 in (34).

Note that the pair of equations giving the smallest values of K_1 and K_2 will still give $\lambda = 1$ in (32). At each stage we repeat the above generating of a smaller K_1 or K_2 until eventually $K_1 = L_1$, $K_2 = L_2$. By Theorem 5 this will come about when we obtain equations of the type (34) and (35) with $K_1 > v_{21}$ and $K_2 > v_{12}$.

To illustrate we find $B(137, 251, 256)$. First calculate that

$$a_1 - 75a_2 + 73a_3 = 0.$$

Then by the algorithm we obtain

$$\begin{aligned} 3a_1 + 31a_2 - 32a_3 &= 0, \\ 7a_1 - 13a_2 + 9a_3 &= 0, \\ 17a_1 + 5a_2 - 14a_3 &= 0. \end{aligned}$$

Thus the matrix of detached coefficients is

a_1	a_2	a_3
-24	8	5
7	-13	9
17	5	-14

and $B = 24a_1 + 9a_3 = 5,592$.

It should be pointed out that solving for (34) is not always necessary. Many computational short cuts become apparent after some practice. Note that the suggested algorithm is not merely numerical but gives algebraic relations as well, enabling one to solve all previously solved special cases for $t = 3$ by a unified approach. For example, see the end of the next section.

6. Extensions and restatement of basic theorem. Even if $L_3 = 1$, the statement of Theorems 4 and 5 still holds, dropping the minimality condition on the L_i . In this case, $B = a_1a_2 + a_3$, see (2). But the matrix of coefficients is

a_1	a_2	a_3
$-a_2$	a_1	0
$a_2 - x_{31}$	$-a_1 - x_{32}$	1
x_{31}	x_{32}	-1

with $x_{31} < a_2$. Then $\lambda = 1$, so that Theorem 5 gives the same result $a_1a_2 + a_3$.

Next we show that Theorems 4 and 5 hold even though the a_i 's are not reduced to a pairwise relatively prime set b_1, b_2, b_3 .

We compare the L 's and x_{ij} 's associated with a_1, a_2, a_3 with those L 's and x_{ij} 's associated with b_1, b_2, b_3 . From (15'), $L_i a_i = x_{ij} a_j + x_{ik} a_k$, we see that $d_{jk} | L_i, d_{ij} | x_{ik}, d_{ik} | x_{ij}$. Thus, setting $L_i = d_{jk} L'_i, x_{ik} = d_{ij} x'_{ik}$, we have

$$(35) \quad L_j L_k - x_{jk} x_{kj} = a_i \quad \text{if and only if} \quad L'_j L'_k - x'_{jk} x'_{kj} = b_i,$$

since $d_{ij} d_{ik} (L'_j L'_k - x'_{jk} x'_{kj}) = d_{ij} d_{ik} b_i = a_i$.

Finally, all these results can be collected in the following form:

THEOREM 6. For $(a_1, a_2, a_3) = 1$, define B to be the largest number not of the form $xa_1 + ya_2 + za_3, x, y, z > 0$. Then for cyclic permutation of subscripts

$$B = L_i a_i + \max(x_{jk} a_k, x_{kj} a_j),$$

where

$$L_i a_i = x_{ij} a_j + x_{ik} a_k, \quad L_i > 0, x_{ij} \geq 0, x_{ik} \geq 0, \quad L_i = x_{ji} + x_{ki}$$

and

$$L_i L_j - x_{ij} x_{ji} = a_k.$$

The L 's and x 's can be found either by the computing algorithm discussed in §5, modified to solve first for $d_{ij} a_k$ in terms of a_i and a_j , or by first applying Theorem 2.

In conclusion, observe that the special cases previously obtained for $t = 3$ can be derived directly from the results of this paper.

Example. We can extend the results stated in (5) for $B(a, a + 1, a + z)$. Write $a = kz - u, 0 \leq u < z, k \geq 1, z \geq 2$. Then for $u \leq k + 1$ the coefficient matrix is

$a = a_1 = kz - u$	$a_2 = kz - u + 1$	$a_3 = kz - u + z$
$-(z + k - u)$	$z - u$	$k - 1$
$z - 1$	$-z$	1
$k + 1 - u$	u	$-k$

If $u \leq 1$, then

$$B = L_3 a_3 + x_{12} a_2 = \left(\frac{a + u}{z} \right) (a + z) + (z - u)(a + 1).$$

To correspond to the notation of (5), we solve for $C + 1 = B + 1 - \sum a_i$. Then

$$C + 1 = \left(\frac{a + u}{z}\right)a + (z - 2 - u)a.$$

If $u > 1$, then $B = L_3 a_3 + x_{21} a_1 = k(a + z) + (z - 1)a$, and

$$C + 1 = \left[\frac{a + 1}{z}\right](a + z) + (z - 3)a$$

since

$$\left(\frac{a + u}{z}\right) = \left[\frac{a + 1}{z}\right] + 1.$$

For $t > 3$, Theorem 1 holds and the author has verified that relations analogous to Theorem 4 hold in many cases. However, this will be the subject of a later paper.

REFERENCES

1. P. T. Bateman, *Remark on a recent note on linear forms*, Amer. Math. Monthly, 65 (1958), 517-518.
2. A. T. Brauer, *On a problem of partitions—I*, Amer. J. Math., 64 (1942), 299-312.
3. A. T. Brauer and B. M. Seelbinder, *On a problem of partitions—II*, Amer. J. Math., 76 (1954), 343-346.
4. R. J. Levit, *A minimum solution for a diophantine equation*, Amer. Math. Monthly, 63 (1956), 646-651.
5. J. B. Roberts, *Note on linear forms*, Proc. Amer. Math. Soc. (1956), 465-469.
6. ———, *On a diophantine problem*, Can. J. Math., 9 (1957), 219-223.

The Rand Corporation
Santa Monica, California