Title	On the linear diophantine problem of Frobenius in three variables
Author(s)	Morikawa, Ryozo
Citation	長崎大学教養部紀要. 自然科学篇. 1997, 38(1), p.1-17
Issue Date	1997-09
URL	http://hdl.handle.net/10069/16663
Right	

長崎大学教養部紀要（自然科学篇）終刊号　第38巻　第1号（1997年9月）

On the linear diophantine problem of Frobenius in three variables

Ryozo Morikawa

(Received June 16, 1997)

1. Introduction

Let $a_1, \dots, a_k$ be a set of positive integers with $\gcd(a_1, \dots, a_k) = 1$. We say that an integer n is **N**-dependent on $\{a_1, \dots, a_k\}$ if there exist positive integers x_i $(1 \leqq i \leqq k)$ such that

(1) $n = x_1 a_1 + \cdots\cdots + x_k a_k$.

The problem of Frobenius consists in determining the largest integer which is *not* **N**-dependent on $\{a_1, \dots, a_k\}$. We denote the number by $F(a_1, \dots, a_k)$. We treat in this paper the problem for $k = 3$. It must be noted the result obtained in this paper gives a prototype of a general theory for the problem of Frobenius. But even in case $k = 4$, many new phenomena are observed, and we need further investigations. The case $k = 4$ will be treated elsewhere.

The starting point of our investigation is that of Johnson [4] and of Brauer-Shockley [1]. And we refer to the paper of Davison [2] which has a close relation with our result. The paper gives also a survey of the current investigations. For the general background of the problem, we refer to Erdös-Graham [3] pp. 85-86.

Now we explain the contents of this paper. Let **N** and **Z** mean as usual. And $(a_1, \dots, a_k)$ means the gcd $(a_1, \dots, a_k)$. We take three positive integers a, b and c with $(a, b, c) = 1$. Let $F(a, b, c)$ be the Frobenius number, which will be noted in some places simply by F.

In §2, we reconstruct the discussion of Brauer-Shockley [1] from a somewhat different standpoint. We first ascertain Theorem 1 which is the main result of

[1]. It asserts, in brief, $F = \mathrm{Max}(F_1, F_2)$ where F_i 's are determined by {a, b, c}. (For k = 4, if the situation is normal, we obtain F by comparing six numbers F_i $(1 \leqq i \leqq 6)$. Note that $6 = (4-1)!$ and $2 = (3-1)!$. But as noted above, new phenomena appear even in case k = 4, and the cardinality 6 considerably varies according to the proportions of a_i $(1 \leqq i \leqq 4)$.)

In § 3, Theorem 2 gives formulas which represents a, b, c and F by using six positive integers b_i, c_i $(1 \leqq i \leqq 3)$. (Conversely starting from {a, b, c}, we obtain b_i, c_i $(1 \leqq i \leqq 3)$ by aid of the algorithm given by Davison [2].)

In § 4, we apply above results to study $F/(abc)^{1/2} = \theta(a, b, c)$. We express θ as a function of three parameters (p, q, r) with $0 < p < 1$, $0 < q < 1$ and $0 < r < 1$. We obtain a precise knowledge about the value of θ including the inequality $\theta > \sqrt{3}$. (This inequality is given by Davison [2].)

In § 5, we continue the study by drawing curves $\theta(p, q, r) = \text{const}$. Those Figures show that θ remains rather small as anticipated in [2]. (But we could not give a proof of the conjectures given in § 4 of [2].)

2. F = Max (F_1, F_2)

Let a, b, c $\in$ **N** with (a, b, c) = 1. We start with two usuful Lemmas which are given by Johnson [4].

Lemma 1 (Johnson [4] Theorem 1). *The Frobenius number* F(a, b, c) *is* **N**-*dependent on any of* {b, c}, {c, a} *and* {a, b}.

Proof. Since F + a is **N**-dependent on {a, b, c}, we have $F + a = xa + yb + zc$ with $(x, y, z) \in \mathbf{N}^3$. If $x > 1$, then $F = (x-1)a + yb + zc$. It contradicts the definition of F. Thus x = 1. Namely we have $F = yb + zc$. The same reasoning works for {c, a} and {a, b}.

Lemma 2 (Johnson [4] Theorem 2). *Let* $(b, c) = d > 1$. *Then we have* $F(a, b, c) = d\,F(a, b/d, c/d)$.

Proof. We put b = b'd and c = c'd. By Lemma 1, we put F = yb + zc with (y, z) $\in \mathbf{N}^2$. Thus F = d(yb'+zc'). We put F'= F/d , and show the relation F' = F(a, b', c'). First we ascertain that F' is not **N**-dependent on {a, b', c'} . If F'= ua + vb' + wc' with (u, v, w) $\in \mathbf{N}^3$, then F = dF'= uda + vb + wc. It contradicts the definition of F. Next we take n $\in$ **N** with n > F'. Here nd > F. Thus we have nd = xa + yb + zc with (x, y, z) $\in \mathbf{N}^3$. And the relation d | b and d | c implies d | x. Therefore we obtain the relation n = (x/d) a + yb' + zc'. These two properties assert F'= F (a, b', c').

As is well known, if a is **N**-dependent on {b, c} , we have F (a, b, c) = a + bc. By virtue of this fact and of Lemma 2, we may hereafter impose the following condition on {a, b, c} .

(#) a, b, c are coprime positive integers and none of a, b, c does not **N**-dependent on the other two members.

Note that the second condition of (#) implies
(*) a, b, c $\geqq$ 2.

Our aim of this § is to characterize F among the numbers which satisfy the property stated in Lemma 1. As noted in §1, the discussion of this § owes much to Brauer-Shockley. We introduce the following terminology and notation:

We call a form of the following type (2) is a 0-form.
(2) xa + yb + zc = 0 with (x, y, z) $\in \mathbf{Z}^3$.
We consider the set (x, y, z) of (2) as a vector and denote it as **w** = (x, y, z). We frequently call (2) as a 0-form (x, y, z) or a 0-form **w**. We put
(3) W = { (x, y, z) $\in \mathbf{Z}^3$: ax + by + cz = 0 } .

Lemma 3. *We take* {a, b, c} *with* (#) *and* W as (3). *Then* W *makes a* **Z**-*module of rank* 2. *As a base system of* W, *we can choose* $\mathbf{v}_1$ = (1, −v, w) *and* $\mathbf{v}_2$ = (0, c, −b) *which satisfy the following* (4).
(4) 0 < v < c *and* 0 < w < b.

Conversely the vector system $\{\mathbf{v}_1, \mathbf{v}_2\}$ *is determined uniquely by* (4).

Proof. The first assertion of Lemma is obvious. And $(b, c) = 1$ implies the third assertion. Thus we consider the second assertion. Since $(a, b, c) = 1$, there exist two numbers $v, w \in \mathbf{Z}$ for which $a = bv - cw$. By translating v modulo c, we may assume $0 < v < c$. ($(a, c) = 1$ and $(*)$ implies $v \neq 0$.) Now $w < 0$ means a to be **N**-dependent on $\{b, c\}$, and $(a, b) = 1$ and $(*)$ implies $w \neq 0$. Thus we have $w \in \mathbf{N}$. And $a > 0$ and $0 < v < c$ imply $w < b$.

Now we introduce the following two sets of 0-forms.

(5) $B = \{ (x, -y, z) : xa - yb + zc = 0$ and $x, y, z \in \mathbf{N} \}$

$C = \{ (x, y, -z) : xa + yb - zc = 0$ and $x, y, z \in \mathbf{N} \}$

Lemma 4. (i) *We take* $\mathbf{b} = (b_1, -b_2, b_3) \in B$ *and* $\mathbf{c} = (c_1, c_2, -c_3) \in C$ *for which*

$b_2 = \mathrm{Min}\ y$ *among* $(x, -y, z) \in B$,

$c_3 = \mathrm{Min}\ z$ *among* $(x, y, -z) \in C$.

Then **b** *and* **c** *are determined uniquely by above conditions. And we have*

(6) $2 \leqq b_2 < \mathrm{Min}\ (a, c)$ *and* $2 \leqq c_3 < \mathrm{Min}\ (a, b)$.

(ii) $\{\mathbf{b}, \mathbf{c}\}$ *makes a basis system of* W.

(iii) *We put* $\mathbf{a} = \mathbf{b} + \mathbf{c}$. *Let* $\mathbf{a} = (a_1, -a_2, -a_3)$. Then $a_i \in \mathbf{N}$.

(iv) The 0-form **a** is characterized by the following property.

$a_1 = \mathrm{Min}\ x$ *for which* $xa - yb - zc = 0$ *and* $(x, y, z) \in \mathbf{N}^3$.

Proof. First we treat (i) for **b**. The number b_2 is characterized as the minimum value for which $b_2 b$ becomes **N**-dependent on $\{a, c\}$. By (#), we see $b_2 \geqq 2$. And (4) implies $b_2 \leqq v < c$. Now interchanging c and a, we obtain $b_2 < a$. Now assume that $b_2 b$ allows the following two expressions.

(7) $b_2 b = b_1 a + b_3 c$ with $b_1, b_3 \in \mathbf{N}$,

$= \widehat{b_1} a + \widehat{b_3} c$ with $\widehat{b_1}, \widehat{b_3} \in \mathbf{N}$.

Since (a, c) = 1, $b_1 > c$ or $\hat{b}_1 > c$. Let $b_1 > c$. By the same reasoning used in Lemma 3, we have

(8) $b = ta - uc$ with $0 < t < c$, $0 < u < a$ and t, u in **N**.

By (7) and (8), we obtain the following relation with coefficients in **N** :

$$(b_2 - 1)b = (b_1 - t)a + (b_3 + u)c.$$

It contradicts the minimality of b_2 . Thus we obtain (i) for **b**. The same reasoning works for **c**.

(*Proof of* (ii)) We study properties of 0-form **w** by expressing it as $\mathbf{w} = g\mathbf{v}_1 + h\mathbf{v}_2$ with $(g, h) \in \mathbf{Z}^2$. We define f by f (**w**) = (g, h). Note that

(9) $g\mathbf{v}_1 + h\mathbf{v}_2 = (g, -gv + ch, gw - bh)$.

And we use Figure 1 as an aid to the discussion. In the Figure, Q = (b, w), R = (c, v), $P_1 = f(\mathbf{b}) = (g_1 , h_1)$, $P_2 = f(\mathbf{c}) = (g_2 , h_2)$ and $P_3 = f(\mathbf{a}) = (g_3, h_3)$.

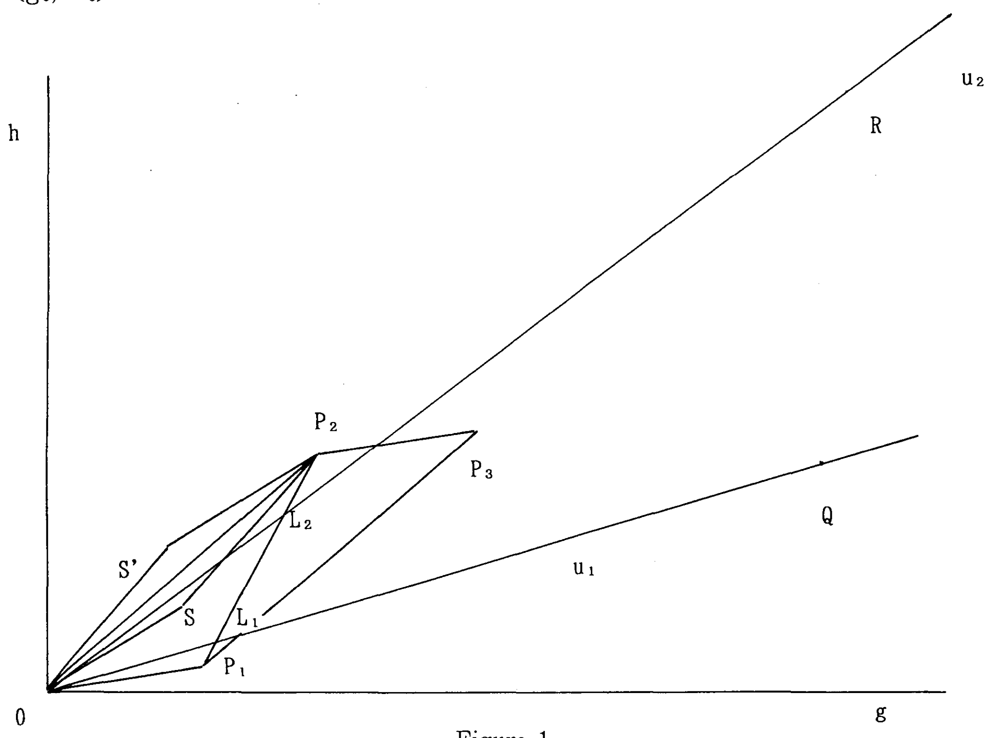

Figure 1.

For the explanation of Figure 1, we note the following two facts.

(a) By the definition of **b** and **c**, we have

$$h_1 / g_1 < w/b < v/c < h_2 / g_2 .$$

(b) **b** is characterized by the property that the area of $\triangle$ ORP$_1$ ($= b_2/2$) attains the minimum value among $\triangle$ ORP with $P \in f(B)$. (We denote by $\triangle$ ABC the area of triangle ABC.)

To ascertain (ii), we show that the parallelotope $OP_1 P_3 P_2$ contains no latice points except the four vertices of it. Assume the existence of another lattice point $S = (g_0, h_0)$. By virtue of symmetry of a parallelotope, we may assume $S \in \triangle OP_1 P_2$. Furthermore by the minimality of **b** and **c**, we may assume $S \in \triangle OL_1 L_2$ where L_1 and L_2 are the intersetions of $\overline{P_1 P_2}$ and two lines u_1 and u_2 respectively.

Now we separate into two cases.

(In case $g_2 \geqq g_1$) We make the parallelotope $OSP_2 S'$ as in Figure 1. Let $S' = (g', h')$. Since $\overline{OS}$ is contained in $\triangle OL_1 L_2$, we have

(10) $\triangle OQS' \leqq \triangle OQP_2$ ($< b/2$).

Note that except the case $g_1 = g_2 = g_0$, $g' = g_2 - g_0 > 0$. Let $g' > 0$. Then S' is in f(C) and the minimality of P_2 and the uniqueness of **c** induce $S' = P_2$ and $S = O$. Next we treat the case $g_1 = g_2 = g_0$. Then $h_1 < h_0 < h_2$. Hence $S' = (0, h_2 - h_0)$. Thus $2 \triangle OS'Q = b(h_2 - h_0)$. It contradicts (10).

(In case $g_1 > g_2$) We make parallelotope $OS'P_1 S$. Here the same reasoning works and we get (ii).

We note here the following relation which is equivalent to (ii).

(11) $g_1 h_2 - g_2 h_1 = 1$.

(*Proof of* (iii)) If $P_3 \in f(B)$, it contradicts the minimality of b_2. And also we see $P_3 \notin f(C)$. Thus we ascertain that P_3 does not lie on u_1. Since $(b, w) = 1$, $P_3 \in u_1$ means $P_3 = (tb, tw)$ with $t \in \mathbf{N}$. Thus $g_1 + g_2 = tb$ and $h_1 + h_2 = tw$. By (11) we have $(tb - g_2) h_2 - g_2 (tw - h_2) = t(h_2 b - g_2 w) = 1$. Thus $c_3 = 1$, which contadicts (6). The same reasoning works for u_2 and we get (iii).

(*Proof of* (iv)) We put

$$A = \{(x, -y, -z) : ax - by - cz = 0,\ (x, y, z) \in \mathbf{N}^3,\ y < b_2,\ z < c_3\}.$$

Note that (iii) shows $\mathbf{a} \in A$. Let two elements $(x_i, -y_i, -z_i)$ $(i = 1, 2)$ be in A. Here we show that

(12) $x_1 \fallingdotseq x_2$ and $x_1 > x_2$ implies $y_1 > y_2$ and $z_1 > z_2$.

Let $x_1 \geqq x_2$ and make the 0-form $(x_1 - x_2, -y_1 + y_2, -z_1 + z_2) = \mathbf{x}$. If $x_1 = x_2$, then $(b, c) = 1$ implies $|y_1 - y_2| \geqq c$, which contradicts the property $1 \leqq y_i < b_2 < c$. Thus we have $x_1 > x_2$. Since $\mathbf{x}$ is a 0-form, at least one of

(13) $-y_1 + y_2$, $-z_1 + z_2$

is negative. But if exactly one of (13) is negative, it contradicts the minimality of $\mathbf{b}$ or $\mathbf{c}$. Thus we obtain (12).

Next we assume the existence of $\hat{\mathbf{a}} = (\hat{a}_1, -\hat{a}_2, -\hat{a}_3)$ in A for which $\hat{a}_1 < a_1$. By (12), we see that $f(\hat{\mathbf{a}})$ lies in the parallelotope $OP_1P_3P_2$. It contradicts (11).

Now we put

$$V = V_1 \cup V_2 \quad \text{with}$$
$$V_1 = \{ (y, z) \in \mathbf{N}^2 : y \leqq b_2, z \leqq a_3 \},$$
$$V_2 = \{ (y, z) \in \mathbf{N}^2 : y \leqq a_2, z \leqq c_3 \}.$$

And for (y, z) in $\mathbf{N}^2$, we define

$$H(y, z) = by + cz.$$

Lemma 5. (i) $\{ H(y, z) : (y, z) \in V \}$ *makes a complete residue system modulo* a.

(ii) *Take* $(y_0, z_0) \in V$. *Then* $H(y_0, z_0)$ *is the minimum among*

$$\{ H(y, z) : H(y, z) \equiv H(y_0, z_0) \pmod a, \ (y, z) \in \mathbf{N}^2 \}.$$

Proof. We say two lattice points (y_i, z_i) $(i = 1, 2)$ to be *congruent* if $H(y_1, z_1) \equiv H(y_2, z_2) \pmod a$. We consider the following three translations of lattice points.

$$S_1(y, z) = (y - b_2, z + b_3), \quad S_2(y, z) = (y + c_2, z - c_3),$$
$$S_3(y, z) = (y - a_2, z - a_3).$$

As easily seen, these three relations satisfy

$S_i(y, z)$ is congruent to (y, z) and $H(y, z) > H(S_i(y, z))$ $(1 \leqq i \leqq 3)$.

Hence for a lattice point of $\mathbf{N}^2 - V$, we obtain a congruent point with a smaller H-value by operating a suitable S_i. Since H-value is a positive integer for $(y, z) \in \mathbf{N}^2$, this process terminates at some point of V.

Next assume that two points (y_1, z_1) and (y_2, z_2) of V are conguruent. We have

(14) $(y_1 - y_2)b + (z_1 - z_2)c = xa$ with $x \in \mathbf{Z}$.

Now (6) implies that none of the coefficients of (14) cannot be 0. Thus we may assume $x > 0$ and there are the following three possibilities.

(A) $y_1 > y_2$, $z_1 > z_2$ (B) $y_1 < y_2$, $z_1 > z_2$ (C) $y_1 > y_2$, $z_1 < z_2$.

Here (B) or (C) contradicts the minimality of **b** or **c**. And the impossibility of (A) follows from (12) and the minimality of **a**.

Now we state Theorem 1 which is the main theorem of [1]

Theorem 1. *Let* a, b *and* c $\in \mathbf{N}$ *and satisy* (#). *Notations being as above, we have* $F(a, b, c) = \text{Max}\ (H(b_2, a_3), H(a_2, c_3))$.

Proof. We put $M = \text{Max}\ H(y, z)$ for $(y, z) \in V$. Then by the convexity of H, we have $M = \text{Max}\ (H(b_2, a_3), H(a_2, c_3))$. We show $F(a, b, c) = M$. First assume $M = xa + yb + zc$ with $(x, y, z) \in \mathbf{N}^3$. Then $M - xa = H(y, z)$, which contradicts (ii) of Lemma 5. On the other hand for $n > M$, we can choose $x \in \mathbf{N}$ so that $n - xa = H(y_0, z_0)$ with $(y_0, z_0) \in V$. Thus $n = xa + y_0 b + z_0 c$.

3. Expression of a, b, c and F with six parameters.

Lemma 6. *Let* $\mathbf{b} = (b_1, -b_2, b_3)$ *and* $\mathbf{c} = (c_1, c_2, -c_3)$ *be the vectors determined from* {a, b, c} *with* (#) *as in* §2. *Then we have*

(15) $a = b_2 c_3 - b_3 c_2$, $b = b_1 c_3 + b_3 c_1$, $c = b_1 c_2 + b_2 c_1$.

Proof. The assertion of Lemma 5 implies that the cardinality of the lattice points of V is a. Thus we have the first relation of (15). We note here the symmetric nature of **a** given in (iv) of Lemma 5. Namely by starting from {b, a, c} , we obtain 0-forms $(a_2, -a_1, a_3)$ and $(c_2, c_1, -c_3)$ which play a role of **b** and **c** stated in §2. Hence we obtain

$$b = a_1 c_3 - a_3 c_1 = (b_1 + c_1)c_3 - c_1(c_3 - b_3) = b_1 c_3 + c_1 b_3 .$$

The relation (15) for c follows with a similar reasoning.

As shown in Lemmas 4 and 6, $\mathbf{b} = (b_1, -b_2, b_3)$ and $\mathbf{c} = (c_1, c_2, -c_3)$ made from $\{a, b, c\}$ with (#) satisfies the following (♮).

(♮) $b_i, c_i \in \mathbf{N}$, $(b_i, c_i) = 1$ $(1 \leqq i \leqq 3)$, $b_2 > c_2$ and $c_3 > b_3$.

We show here the set $\{\mathbf{b}, \mathbf{c}\}$ is characterized by (♮).

Lemma 7. *Take* $\{a, b, c\}$ *with* (#). *Let* $\hat{\mathbf{b}} = (\hat{b}_1, -\hat{b}_2, \hat{b}_3)$ *and* $\hat{\mathbf{c}} = (\hat{c}_1, \hat{c}_2, -\hat{c}_3)$ *satisfy the following* ($\hat{♮}$).

($\hat{♮}$) $\hat{b}_i, \hat{c}_i \in \mathbf{N}$, $(\hat{b}_i, \hat{c}_i) = 1$ $(1 \leqq i \leqq 3)$, $\hat{b}_2 > \hat{c}_2$, $\hat{c}_3 > \hat{b}_3$.

$$a = \hat{b}_2 \hat{c}_3 - \hat{b}_3 \hat{c}_2 , \quad b = \hat{b}_1 \hat{c}_3 + \hat{b}_3 \hat{c}_1 , \quad c = \hat{b}_1 \hat{c}_2 + \hat{b}_2 \hat{c}_1 .$$

Then $\hat{\mathbf{b}} = \mathbf{b}$ and $\hat{\mathbf{c}} = \mathbf{c}$.

Proof. It is an easy calculation to see that $\hat{\mathbf{b}}$ and $\hat{\mathbf{c}}$ are 0-forms for $\{a, b, c\}$. Thus by (ii) of Lemma 4, they are **Z**-combinations of **b** and **c**. We put

$$\begin{pmatrix} s & t \\ u & v \end{pmatrix}\begin{pmatrix} b_1 & -b_2 & b_3 \\ c_1 & c_2 & -c_3 \end{pmatrix} = \begin{pmatrix} \widehat{b_1} & -\widehat{b_2} & \widehat{b_3} \\ \widehat{c_1} & \widehat{c_2} & -\widehat{c_3} \end{pmatrix} \quad \text{with } s, t, u, v \in \mathbf{Z}.$$

Here $\begin{vmatrix} s & t \\ u & v \end{vmatrix}\begin{vmatrix} -b_2 & b_3 \\ c_2 & -c_3 \end{vmatrix} = \begin{vmatrix} -\widehat{b_2} & \widehat{b_3} \\ \widehat{c_2} & -\widehat{c_3} \end{vmatrix} = a$ implies the relation

(16) $sv - tu = 1.$

By ($\hat{♮}$), we obtain the following eight inequalities.

(A) $sb_1 + tc_1 > 0$ (B) $tc_2 < sb_2$ (C) $sb_3 > tc_3$

(D) $ub_1 + vc_1 > 0$ (E) $vc_2 > ub_2$ (F) $ub_3 < vc_3$

(G) $sb_2 - tc_2 > vc_2 - ub_2$

(H) $vc_3 - ub_3 > sb_3 - tc_3$

By (B), $s \leqq 0$ implies $t < 0$, which contradicts (A). Thus we have $s > 0$. By a similar way, we have $v > 0$. Thus (16) implies $tu \geqq 0$. We consider separating according the signatures of t and u.

($t = 0$) Let $t = 0$. Then (16) implies $s = v = 1$. By (G), $(1 + u)b_2 > c_2$. Hence $u \geqq 0$. On the other hand (E) and (♮) induces $u \leqq 0$. Namely $u = 0$.

($u = 0$) By the same reasoning, we obtain $s = v = 1$ and $t = 0$.

($t > 0,\ u > 0$) Now (C) and (♮) imply $s > t$. And (E) and (♮) induce $v > u$.

Thus $sv - tu \geqq (t + 1)(u + 1) - tu \geqq 3$, which contradicts (16).

($t < 0,\ u < 0$) We put $-t = t'$ and $-u = u'$. From (G) and (H), we get

(17) $\quad (s - u') > (v - t')(c_2 / b_2) > (s - u')(b_3 c_2 / b_2 c_3)$.

By (♮), we see $1 > b_3 c_2 / b_2 c_3 > 0$. Thus (17) implies $s > u'$ and $v > t'$. Since $tu = t'u'$, these inequalities contradict (16).

Thus we see the only possible case is $s = v = 1$, and $t = u = 0$.

Remark. From numerically given $\{a, b, c\}$ with (#), we obtain b_i, c_i ($1 \leqq i \leqq 3$) by using the Davison's algorithm given in [2]. Strictly speaking, it gives a method to obtain b_2, b_3, c_2, c_3 and F. As easily seen,

$$b_1 = (b_2 b - b_3 c)/a \quad \text{and} \quad c_1 = (c_3 c - c_2 b)/a.$$

Theorem 2. *We take six numbers* b_i, c_i ($1 \leqq i \leqq 3$) *which satisfy* (♮). *Then* $\{a, b, c\}$ *given by* (15) *satisfy* (#) *except the condition* $(a, b, c) = 1$. *In case* $(a, b, c) = 1$, *we have* $F(a, b, c) = \mathrm{Max}(F_1, F_2)$ *where*

$$F_1 = b_1 b_2 c_3 + b_1 c_2 c_3 + c_1 b_2 c_3 - b_1 c_2 b_3,$$

$$F_2 = b_1 b_2 c_3 + c_1 b_2 b_3 + c_1 b_2 c_3 - c_1 c_2 b_3.$$

Proof. We assume $(a, b, c) = 1$, and show that the set $\{a, b, c\}$ satisfy the other conditions of (#). Assume $(b, c) > 1$, and take a prime p for which $p \mid (b, c)$.

(Case 1) If $p \nmid b_1$, then $p \mid b$ implies $c_3 \equiv -\hat{b}_1 c_1 b_3 \pmod p$ with $\hat{b}_1$ for which $\hat{b}_1 b_1 \equiv 1 \pmod p$. And $p \mid c$ implies $c_2 \equiv -\hat{b}_1 b_2 c_1 \pmod p$. These two relations imply $p \mid a$. It contradits $(a, b, c) = 1$.

(Case 2) If $p \mid b_1$, then $(b_1, c_1) = 1$ and $p \mid b$ imply $p \mid b_3$. Similarly $p \mid b_2$. Thus we have $p \mid a$.

Hence we see $(b, c) = 1$. Similar reasoning works for the other pairs .

Next we show that a cannot be **N**-dependent on $\{b, c\}$. Let $a = tb + uc$ with $(t, u) \in \mathbf{N}^2$. Substituting this relation to $b_1 a - b_2 b + b_3 c = 0$, we have $(b_2 - b_1 t)b = c(b_3 + b_1 u)$. Now $(b, c) = 1$ implies $b_2 \equiv b_1 t \pmod{c}$. And noting $b_2 > b_1 t$, we get a contradiction to (6). We obtain the desired property for the other pairs by a symmetric reasoning.

The other assertions of Theorem follows easily from Lemma 7 and Theorem 1.

4. Properties of $F/(abc)^{1/2}$

In [2], the author proved the inequality $F/(abc)^{1/2} \geqq \sqrt{3}$. We put

(18) $\theta(a, b, c) = F(a, b, c)/(abc)^{1/2}$, $\theta_i = F_i/(abc)^{1/2}$ $(i = 1, 2)$.

We introduce three parameters (p, q, r) so that

(19) $p(b_1 + c_1) = b_1$, $qb_2 = c_2$, $c_3(1 - r) = b_3$.

Now by (♮), we see $(p, q, r) \in E$ where

$$E = \{ (p, q, r) : 0 < p < 1, 0 < q < 1, 0 < r < 1 \}.$$

By Theorem 2, we have

$$\theta_1(a, b, c) = (1 + pqr)/S(p, q, r),$$

(20) $\theta_2(a, b, c) = (1 + (1 - p)(1 - q)(1 - r))/S(p, q, r)$

where $S(p, q, r) = \{(1 - p + pq)(1 - q + qr)(1 - r + rp)\}^{1/2}$

In this § we use three expressions $\theta_i(a, b, c)$, $\theta_i(p, q, r)$ and $\theta_i(P)$ where $(a, b, c) \in \mathbf{N}^3$, $(p, q, r) \in E$ and $P = (p, q, r)$ respectively. (We think there is no fear of ambiguity.)

We fix $p = \alpha$ and let (q, r) run through the following $S(\alpha)$:

$$S(\alpha) = \{ (q, r) : 0 \leqq q \leqq 1, 0 \leqq r \leqq 1, p = \alpha \}.$$

(We let $S(\alpha)$ contain the boundary of it for the convenience of our discussion.) We name the four vertices of $S(\alpha)$ as follows.

$$A = (0, 0), B = (1, 0), C = (1, 1), D = (0, 1).$$

Note that (20) has a symmetry with respect to

$$(p, q, r) \to (1 - p, 1 - q, 1 - r).$$

Thus we may restrict our research to α which satisfies

(21) $0 < \alpha \leqq 1/2$.

Fact 1. We put $L(\alpha)$ so that

(22) $L(\alpha) = \{(q, r) \in S(\alpha) : r = (1-\alpha)(1-q)/(1-\alpha-q+2q\alpha)\}$.

Then for $(q, r) \in S(\alpha)$,

$$\theta_1 = \theta_2 \text{ if and only if } (q, r) \in L(\alpha).$$

Fact 2. $L(\alpha)$ is a convex curve in $S(\alpha)$ which links B and D. And it divides $S(\alpha)$ into two domains $D_i(\alpha)$ $(i = 1, 2)$ for which

$$\theta = \theta_i \text{ if and only if } (q, r) \in D_i(\alpha).$$

We first study the value of θ for $(q, r) \in L(\alpha)$.

Fact 3. We obtain

(23) $\theta = (1 - q + \alpha q)/\{(1-\alpha+q\alpha)(1-q)\alpha\}^{1/2}$ for $(q, r) \in L(\alpha)$.

Under some calculations, we see that the value of (23) takes its minimum value $2(1-\alpha+\alpha^2)^{1/2}$ at the point $T_0(\alpha)$ where

(24) $T_0(\alpha) = ((1-2\alpha+2\alpha^2)/(1-\alpha+2\alpha^2), (1-\alpha)/(2-3\alpha+2\alpha^2))$.

Note that $\theta(D) = 1/(\alpha-\alpha^2)^{1/2}$ and $\theta(B) = \infty$.

Next we investigate the values of θ in $D_1(\alpha)$. We see that (21) implies $\partial\theta_1/\partial q > 0$ for $(q, r) \in D_1$. And $\partial\theta_1/\partial r = 0$ at $r = (2q-1)/q(2-\alpha)$. We put

(25) $T_1(\alpha) = (1/(1+\alpha), (1-\alpha)/(2-\alpha))$.

Fact 4. $T_1(\alpha) \in L(\alpha)$. And $\partial\theta_1/\partial r = 0$ at T_1. For q_0 with $q_0 > 1/(1+\alpha)$, the point $Q_0 = (q_0, (2q_0-1)/q_0(2-\alpha))$ is in $D_1(\alpha)$. At Q_0, we have $\partial\theta_1/\partial r = 0$ and $\theta(Q_0) = 2\{q_0/(1-\alpha+q_0\alpha)\}^{1/2}$.

For the behaviour of θ in $D_2(\alpha)$, we study it by starting from a point of $L(\alpha)$ and moving along a line r = const. By calculating $\partial\theta_2/\partial q$, we obtain the following analogous result to Fact 4.

Fact 5. At $T_1(\alpha)$ of (25), $\partial\theta_2/\partial q = 0$. And for $r_0 < (1-\alpha)/(2-\alpha)$, the point $R_0 = ((\alpha+r_0-\alpha r_0)/(1-r_0)(1+\alpha), r_0)$ is in $D_2(\alpha)$. At R_0

$,\partial\theta_2/\partial q = 0$ and $\theta_2(R_0) = 2\{(1-r_0)/(1-r_0+\alpha r_0)\}^{1/2}$. And we put $S_0 = (q_1, (\alpha + q_1 - q_1\alpha)/(1-\alpha+q_1-q_1\alpha))$ for $q_1 < (1-2\alpha)/(1-\alpha)$. Then we see $\partial\theta_2/\partial r = 0$ at S_0, and $\theta_2(S_0) = 2\{(1-\alpha)/(1-\alpha+q_1\alpha)\}^{1/2}$.

(The role of these three points Q_0, R_0 and S_0 is illustrated in Figure 2.)

Next we consider the values of θ at the boundary of $S(\alpha)$. The values at the four vertices are given by

(26) $\theta(A) = (2-\alpha)/(1-\alpha)^{1/2}$, $\theta(B) = \infty$, $\theta(C) = (1+\alpha)/\sqrt{\alpha}$,
$\theta(D) = 1/(\alpha-\alpha^2)^{1/2}$.

Now it is rather an easy task to obtain the following fact.

Fact 6. $(0 \leqq q \leqq 1,\ r = 1)$ We have $\theta = \theta_1 = (1+q\alpha)/\{\alpha(1-\alpha+q\alpha)\}^{1/2}$. Starting from $\theta(D)$, θ increses as q increases, and reach $\theta(C)$.

$(q = 1,\ 0 \leqq r \leqq 1)$ In this case, $\theta = \theta_1 = (1+\alpha r)/\{r(1-r+\alpha r)\}^{1/2}$. Starting from $\theta(C)$, θ decreases with decreasing r, and takes the minimum value 2 at $r = 1/(2-\alpha)$. After that θ increases and tend to ∞ $(=\theta(B))$.

$(q = 0,\ 0 \leqq r \leqq 1)$ $\theta = \theta_2 = (2-\alpha-r+r\alpha)/\{(1-\alpha)(1-r+r\alpha)\}^{1/2}$. Starting from $\theta(A)$, θ decreses and take the minimum value 2 at $r = \alpha/(1-\alpha)$. After that θ increases to $\theta(D)$.

$(0 \leqq q \leqq 1,\ r = 0)$ $\theta = \theta_2 = (2-\alpha-q+q\alpha)/\{(1-q)(1-\alpha+q\alpha)\}^{1/2}$. Starting from $\theta(A)$, θ decreases and take the minimum value 2 at $q = \alpha/(1+\alpha)$. After that θ increses to ∞.

Collecting above facts we see first that the minimum value of θ in $S(\alpha)$ is $2(1-\alpha+\alpha^2)^{1/2} = \theta(T_0(\alpha))$. Thus the minimum value of θ in E is $\sqrt{3}$ taken at $(1/2, 1/2, 1/2)$. But strictly speaking, $p = q = r = 1/2$ induces $a = b = c = 3$, and it contradicts (#). Thus we obtain the inequality

$$\theta(a, b, c) > \sqrt{3} \quad \text{for } \{a, b, c\} \text{ with (\#)}.$$

5. Curves C (β)

To visualize the nature of θ in S(α), we consider the curve

$C(\beta) = \{(q, r) \in S(\alpha): \theta(\alpha, q, r) = \beta\}$ for $\beta \geqq 2(1-\alpha+\alpha^2)^{1/2}$.

The shape of C(β) in S(α) varies according to the values of β. Here we give Figure 2 which illustrates curves C(β) for $\alpha = 1/3$ and several β's. (We think it may aid in understanding our discussion.)

(i) $C(\beta) = T_0$ for $\beta = 2(1-\alpha+\alpha^2)^{1/2}$. As β increases from that, C(β) makes a curve which encircles T_0. On the curve, some of Q_0, R_0 and S_0 appear as shown in Figure 2.

(ii) As indicated in Fact 6, the first critical phenomenon appears at $\beta = 2$. The curve C(2) makes a closed curve which contains three points $(0, \alpha/(1-\alpha)) = S_0$, $(\alpha/(1+\alpha), 0) = R_0$ and $(1, 1/(2-\alpha)) = Q_0$ on the boundary of S(α). (Figure 3 illustrates the curves C(2) for $\alpha = 1/2$, $1/4$ and $1/10$.)

(iii) As β exceeds 2, the curve C(β) splits to 3 (or less) curves. We name the curves as shown in Figure 4.
The cardinality and shape of $C_i(\beta)$ depends on the order of magnitude of the four numbers θ(A), θ(C), θ(D) and β.

(The behaviour of $C_1(\beta)$)
For β with $2 < \beta < \theta(A)$, $C_1(\beta)$ is a curve which links the following two

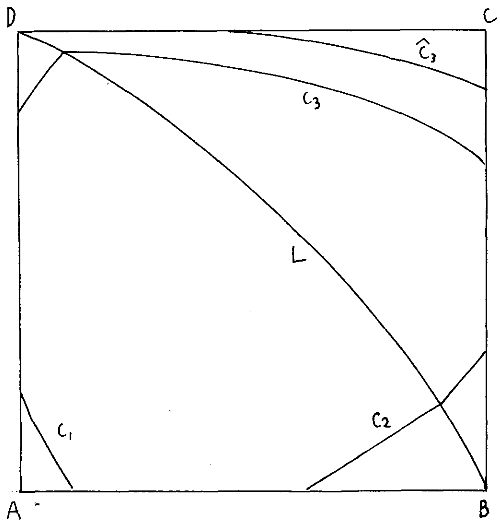

Figure 4.

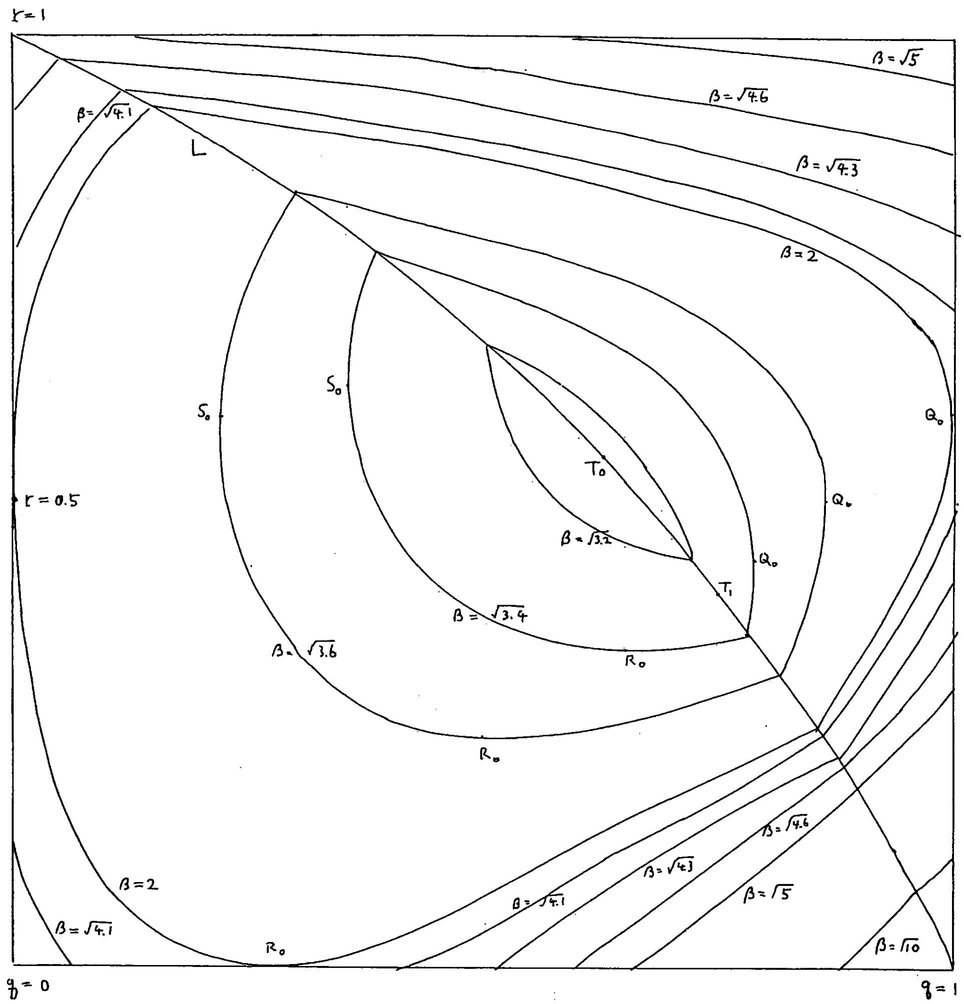

Figure 2.

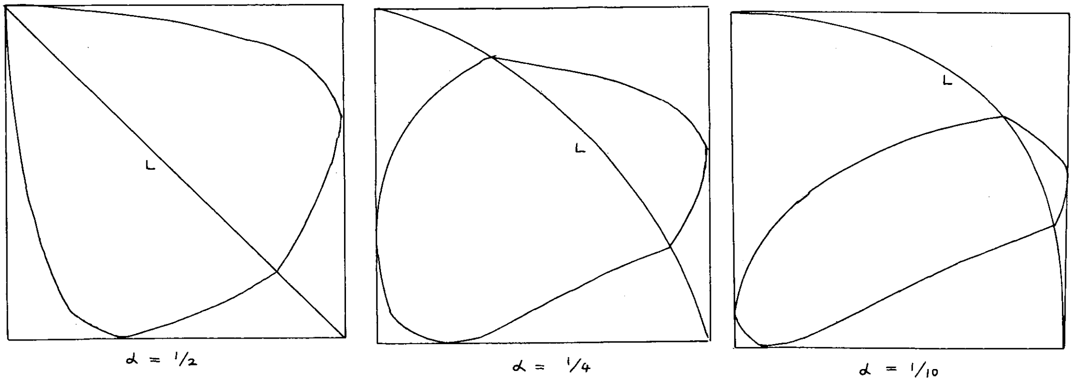

Figure 3.

points :

$$\left(0,\ \frac{2(2-\alpha)-\beta^2(1-\alpha)-(1-\alpha)\beta\sqrt{\beta^2-4}}{2(1-\alpha)}\right),\ \left(\frac{2(2-\alpha)(1-\alpha)+(2\alpha-1)\beta^2-\beta\sqrt{\beta^2-4}}{2((1-\alpha)^2+\alpha\beta^2)},\ 0\right).$$

For $\beta > \theta(A)$, $C_1(\beta) = \phi$.

(The behaviour of $C_2(\beta)$)

For β with $2 < \beta$, $C_2(\beta)$ is a curves which links the following two points :

$$\left(\frac{2(2-\alpha)(1-\alpha)+(2\alpha-1)\beta^2+\beta\sqrt{\beta^2-4}}{2((1-\alpha)^2+\alpha\beta^2)},\ 0\right),\ \left(1,\ \frac{(\beta^2-2\alpha)-\beta\sqrt{\beta^2-4}}{2(\alpha^2+(1-\alpha)\beta^2)}\right).$$

And it tends to B as $\beta \to \infty$.

(The behaviour of $C_3(\beta)$)

For β with $2 < \beta < \theta(D)$, $C_3(\beta)$ is a curve as shown in Figure 4, which links the following two points :

$$\left(0,\ \frac{2(2-\alpha)-\beta^2(1-\alpha)+(1-\alpha)\beta\sqrt{\beta^2-4}}{2(1-\alpha)}\right),\ \left(1,\ \frac{(\beta^2-2\alpha)+\beta\sqrt{\beta^2-4}}{2(\alpha^2+(1-\alpha)\beta^2)}\right).$$

(The behabiour of $\hat{c}_3(\beta)$)

For β with $\theta(D) < \beta < \theta(C)$, the curve of type $\hat{c}_3(\beta)$ appears, which links the following two points :

$$\left(\frac{\alpha\beta^2-2+\alpha\beta\sqrt{\beta^2-4}}{2\alpha},\ 1\right),\ \left(1,\ \frac{(\beta^2-2\alpha)+\beta\sqrt{\beta^2-4}}{2(\alpha^2+(1-\alpha)\beta^2)}\right).$$

And for β with $\beta > \theta(C)$, this curve disappears.

Fact 7. As shown above, for $\beta > (1+\alpha)/\sqrt{\alpha}$, there appears $C_2(\beta)$ only. It means that the value of θ remains, as anticipated by the author of [2], in a reasonable zone for most of {a, b, c} with (#). But we failed answering the conjectures stated in [2]. (We need more precise knowledge of the distribution of (p, q, r) of {a, b, c} with Max (a, b, c) $<$ n and (a, b, c) = 1.)

References

[1] A. Brauer — E. Shockley, On a problem of Frobenius, J. Reine Angew. Math. 211 (1962), 215-220.
[2] J. L. Davison, On the linear diophantine problem of Frobenius, J. Number Theory 48 (1994), 353-363.
[3] P. Erdös - R. L. Graham, Old and new problems and results in combinatorial number theory, Geneve (1980).
[4] S. M. Johnson, A linear diophantine problem, Canad. J. Math. 12 (1960), 390-398.