Pacific Journal of Mathematics

ON THE SOLUTION OF LINEAR G.C.D. EQUATIONS

DAVID JACOBSON AND KENNETH S. WILLIAMS

Vol. 39, No. 1 May 1971

PACIFIC JOURNAL OF MATHEMATICS
Vol. 39, No. 1, 1971

ON THE SOLUTION OF LINEAR G.C.D. EQUATIONS

DAVID JACOBSON AND KENNETH S. WILLIAMS

Let Z denote the domain of ordinary integers and let $m(\geqq 1)$, $n(\geqq 1)$, $l_i(i=1, \cdots, m)$, $l_{ij}(i=1, \cdots, m; j=1, \cdots, n) \in Z$. We consider the solutions $\boldsymbol{x} \in Z^n$ of

$$\text{G.C.D.}\,(l_{11}x_1 + \cdots + l_{1n}x_n + l_1, \cdots, l_{m1}x_1 + \cdots + l_{mn}x_n + l_m, c) = d\,, \tag{1}$$

where $c(\neq 0)$, $d(\geqq 1) \in Z$ and G.C.D. denotes "greatest common divisor". Necessary and sufficient conditions for solvability are proved. An integer t is called a *solution modulus* if whenever $\boldsymbol{x}$ is a solution of (1), $\boldsymbol{x} + t\boldsymbol{y}$ is also a solution of (1) for all $\boldsymbol{y} \in Z^n$. The positive generator of the ideal in Z of all such solution moduli is called the minimum modulus of (1). This minimum modulus is calculated and the number of solutions modulo it is derived.

1. Introduction. Let Z denote the domain of ordinary integers and let $m(\geqq 1)$, $n(\geqq 1)$, $l_i(i = 1, \cdots, m)$, $l_{ij}(i = 1, \cdots, m; j = 1, \cdots, n) \in Z$. We write $\boldsymbol{l} = (l_1, \cdots, l_m)$ and for each $i = 1, \cdots, m$ we write $\boldsymbol{l}_i = (l_{i1}, \cdots, l_{in})$ and $\boldsymbol{l}'_i = (l_{i1}, \cdots, l_{in}, l_i)$ so that $\boldsymbol{l} \in Z^m$, each $\boldsymbol{l}_i \in Z^n$, and each $\boldsymbol{l}'_i \in Z^{n+1}$. If $\boldsymbol{x} = (x_1, \cdots, x_n) \in Z^n$ we write in the usual way $\boldsymbol{l}_i \cdot \boldsymbol{x}$ for the linear expression $l_{i1}x_1 + \cdots + l_{in}x_n$. We let L denote the $m \times n$ matrix whose ith row is $\boldsymbol{l}_i$ and L' denote the $m \times (n + 1)$ matrix whose ith row is $\boldsymbol{l}'_i$.

Henceforth in this paper we will write the abbreviation G.C.D. for "greatest common divisor" of a finite sequence of integers, not all zero, and consider the solutions $\boldsymbol{x} \in Z^n$ of

$$\text{G.C.D.}\,(\boldsymbol{l}_1 \cdot \boldsymbol{x} + l_1, \cdots, \boldsymbol{l}_m \cdot \boldsymbol{x} + l_m, c) = d\,, \tag{1.1}$$

where $c(\neq 0)$, $d(\geqq 1) \in Z$. A number of authors have either used or proved results concerning special cases of this equation (see for example [1], [5]) so that it is of interest to give a general treatment. This equation is clearly connected with the system

$$\boldsymbol{l}_i \cdot \boldsymbol{x} + l_i \equiv 0 \pmod{d} \ (i = 1, \cdots, m)\,. \tag{1.2}$$

If we denote the number of incongruent solutions modulo d of (1.2) by $N(d, L')$, then $N(d, L') > 0$ is a necessary condition for the solvability of (1.1). A complete treatment of the system (1.2) has been given by Smith [4]. Let D_i = greatest common divisor of the determinants of all the $i \times i$ submatrices in L ($i = 1, \cdots, \min(m, n)$), D'_i = greatest common divisor of the determinants of all the $i \times i$ submatrices in L' ($i = 1, \cdots, \min(m, n+1)$), γ_i = greatest common divisor of d and $\frac{D_i}{D_{i-1}}$, $i = 1, \cdots, \min(m, n)$, where $D_0 = 1$, and γ_i' = greatest common divisor of d and $\frac{D_i'}{D_{i-1}'}$, $i = 1, \cdots, \min(m, n)$, where $D_0' = 1$. Smith has shown that (1.2) is solvable if and only if

$$\prod_{i=1}^{\min(m,n)} \gamma_i = \prod_{i=1}^{\min(m,n)} \gamma_i'$$

and

$$\frac{D_{n+1}'}{D_n'} \equiv 0 \pmod{d}, \text{ if } m > n .$$

When solvable he shows that

$$N(d, L') = \gamma d^{\max(n-m, 0)} ,$$

where

$$\gamma = \prod_{i=1}^{\min(m,n)} \gamma_i .$$

We show in Theorem 1 that the conditions

$$d \mid c,\ N(d, L') > 0,\ \text{G.C.D. } (\boldsymbol{l}_1, \cdots, \boldsymbol{l}_m, d) = \text{G.C.D. } (\boldsymbol{l}_1', \cdots, \boldsymbol{l}_m', c) \tag{1.3}$$

are both necessary and sufficient for solvability of (1.1). When (1.1) is solvable, (1.3) shows that the quantity $g = \text{G.C.D. } (\boldsymbol{l}_1, \cdots, \boldsymbol{l}_m, d)$ is a factor of $\boldsymbol{l}_i$, l_i ($i = 1, \cdots, m$), c and d. Cancelling this factor throughout we obtain the equation

$$\text{G.C.D. } (\boldsymbol{l}_1/g \cdot \boldsymbol{x} + l_1/g, \cdots, \boldsymbol{l}_m/g \cdot \boldsymbol{x} + l_m/g, c/g) = d/g .$$

This equation is equivalent to (1.1) in the sense that every solution of this equation is a solution of (1.1) and vice-versa. Thus we can suppose without loss of generality that

$$\text{G.C.D. } (\boldsymbol{l}_1, \cdots, \boldsymbol{l}_m, d) = 1 .$$

The solution set of (1.1) is denoted by $\mathscr{S}_d^c \equiv \mathscr{S}_d^c(L')$ that is,

$$\mathscr{S}_d^c \equiv \mathscr{S}_d^c(L') = \{\boldsymbol{x} \in Z^n \mid \text{G.C.D. } (\boldsymbol{l}_1 \cdot \boldsymbol{x} + l_1, \cdots, \boldsymbol{l}_m \cdot \boldsymbol{x} + l_m, c) = d\}. \tag{1.4}$$

Moreover when $\mathscr{S}_d^c \neq \emptyset$, we have

$$d \mid c,\ N(d, L') > 0,\ \text{G.C.D. } (\boldsymbol{l}_1', \cdots, \boldsymbol{l}_m', c) = 1 ,$$

and we write e for the integer c/d.

If $t \in Z$, $\boldsymbol{a} = (a_1, \cdots, a_n) \in Z^n$ and $\boldsymbol{b} = (b_1, \cdots, b_n) \in Z^n$, we say that

$\boldsymbol{a}$ and $\boldsymbol{b}$ are congruent modulo t (writing $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{t}$) if and only if $a_i \equiv b_i \pmod{t}$ for each $i = 1, \cdots, n$. This congruence $\equiv$ is an equivalence relationship on Z^n. If $\mathscr{S}_d^c \neq \varnothing$, any integer t for which this equivalence relationship is preserved on $\mathscr{S}_d^c (\subseteq Z^n)$ is called a *solution modulus* of (1.1). Thus a solution modulus t has the property that if $\boldsymbol{x} \in \mathscr{S}_d^c$ then $\boldsymbol{x} + t\boldsymbol{y} \in \mathscr{S}_d^c$ for all $\boldsymbol{y} \in Z^n$. Clearly 0 and $\pm c$ are solution moduli. In Theorem 2 it is shown that the set of all solution moduli with respect to $\mathscr{S}_d^c$ viz.,

$$\mathfrak{M}_d^c \equiv \mathfrak{M}_d^c(L') = \{t \in Z \mid \boldsymbol{x} + t\boldsymbol{y} \in \mathscr{S}_d^c \text{ for all } \boldsymbol{x} \in \mathscr{S}_d^c \text{ and all } \boldsymbol{y} \in Z^n\} ,$$

is a principal ideal of Z. The positive generator of this ideal is denoted by $M_d^c(L')$ and called the *minimum modulus* of the equation (1.1). We show

$$M_d^c \equiv M_d^c(L') = d \prod_{p \mid e, N(pd, L') > 0} p \; . \tag{1.5}$$

(Here and throughout this paper the empty product is to be taken as 1). The product in (1.5) is taken over precisely those primes $p \mid e$ for which the system of congruences $\boldsymbol{l}_i \cdot \boldsymbol{x} + l_i \equiv 0 \pmod{pd}$ $(i = 1, \cdots, m)$ is solvable.

In § 5 we consider the problem of evaluating $\mathfrak{N}_d^c \equiv \mathfrak{N}_d^c(L')$, the number of incongruent solutions $\boldsymbol{x}$ of (1.1) modulo the minimum modulus M_d^c, from which the number of solutions modulo a given modulus can be determined. In Theorem 4 we derive a technical formula which allows the evaluation of $\mathfrak{N}_d^c$ in some important cases (see § 6). In particular we prove that if G.C.D. $(d, e) = 1$ then

$$\mathfrak{N}_d^c = N(d, L') \prod_{p \mid e, N(pd, L') > 0} p^n \left(1 - \frac{1}{p^{r(p, L)}}\right) , \tag{1.6}$$

where $r(p, L)$ is the rank of the matrix $L^{(p)}$ obtained from L by replacing each entry l_{ij} by its residue class modulo p in the finite field Z_p.

Finally in § 7 an alternative approach is given which enables us to generalize a recent result of Stevens [6].

2. A necessary and sufficient condition for $\mathscr{S}_d^c \neq \varnothing$.

We begin by dealing with the case $d = 1$. We prove

LEMMA 1. *$\mathscr{S}_1^c \neq \varnothing$ if and only if*

$$\text{G.C.D.}\,(\boldsymbol{l}_1', \cdots, \boldsymbol{l}_m', c) = 1 . \tag{2.1}$$

Proof. The necessity of (2.1) is obvious. Thus to complete the proof it suffices to show that if (2.1) holds then $\mathscr{S}_1^c \neq \varnothing$. In view of (2.1) for each prime $p \mid c$ there must be some l_i or $l_{ij} \not\equiv 0 \pmod{p}$.

If some $l_i \not\equiv 0 \pmod p$ we let $\boldsymbol{x}^\dagger(p) = \boldsymbol{0}$, otherwise we have some $l_{ij} \not\equiv 0 \pmod p$ and we let $\boldsymbol{x}^\dagger(p) = (0, \cdots, 0, x_j, 0, \cdots, 0)$, where the j^{th} entry x_j is any solution of $l_{ij}x_j \equiv 1 \pmod p$, so that in both cases we have

$$\text{G.C.D. } (\boldsymbol{l}_1 \cdot \boldsymbol{x}^\dagger(p) + l_1, \cdots, \boldsymbol{l}_m \cdot \boldsymbol{x}^\dagger(p) + l_m, p) = 1 .$$

We now determine $\boldsymbol{x}$ by the Chinese remainder theorem so that $\boldsymbol{x} \equiv \boldsymbol{x}^\dagger(p) \pmod p$, for all $p \mid c$. Hence we have

$$\begin{aligned} &\text{G.C.D. } (\boldsymbol{l}_1 \cdot \boldsymbol{x} + l_1, \cdots, \boldsymbol{l}_m \cdot \boldsymbol{x} + l_m, \prod_{p \mid c} p) \\ &= \prod_{p \mid c} \text{G.C.D. } (\boldsymbol{l}_1 \cdot \boldsymbol{x} + l_1, \cdots, \boldsymbol{l}_m \cdot \boldsymbol{x} + l_m, p) \\ &= \prod_{p \mid c} \text{G.C.D. } (\boldsymbol{l}_1 \cdot \boldsymbol{x}^\dagger(p) + l_1, \cdots, \boldsymbol{l}_m \cdot \boldsymbol{x}^\dagger(p) + l_m, p) \\ &= 1 , \end{aligned}$$

proving that $\boldsymbol{x} \in \mathscr{S}_1^c$.

Now we use Lemma 1 to handle the general case $d \geqq 1$. We prove

THEOREM 1. *$\mathscr{S}_d^c \neq \varnothing$ if and only if*

$$d \mid c,\ N(d, L') > 0,\ \text{G.C.D. } (\boldsymbol{l}_1, \cdots, \boldsymbol{l}_m, d) = \text{G.C.D. } (\boldsymbol{l}'_1, \cdots, \boldsymbol{l}'_m, c). \tag{2.2}$$

Proof. The necessity is obvious. Thus to complete the proof we must show that if (2.2) holds then $\mathscr{S}_d^c \neq \varnothing$. As $N(d, L') > 0$ there exists $\boldsymbol{k} \in Z^n$ and $\boldsymbol{h} = (h_1, \cdots, h_m) \in Z^m$ such that

$$\boldsymbol{l}_i \cdot \boldsymbol{k} + l_i = dh_i,\ i = 1, \cdots, m . \tag{2.3}$$

We write $d_1 = d/g$, $\boldsymbol{g}_i = \boldsymbol{l}_i/g \in Z^n$, $\boldsymbol{g}'_i = \boldsymbol{l}'_i/g \in Z^{n+1}$, $g_i = l_i/g \in Z$ $(i = 1, \cdots, m)$ where $g = \text{G.C.D. } (\boldsymbol{l}_1, \cdots, \boldsymbol{l}_m, d)$ and suppose that

$$\text{G.C.D. } (\boldsymbol{g}_1, \cdots, \boldsymbol{g}_m, \boldsymbol{h}, e) > 1 , \tag{2.4}$$

where $e = c/d$. Then there exists a prime p such that

$$\boldsymbol{g}_i \equiv \boldsymbol{0}\ (i = 1, \cdots, m),\ \boldsymbol{h} \equiv \boldsymbol{0},\ e \equiv 0 \pmod p) . \tag{2.5}$$

Now from (2.3) we have

$$\boldsymbol{g}_i \cdot \boldsymbol{k} + g_i = d_1 h_i,\ i = 1, \cdots, m ,$$

and so appealing to (2.5) we deduce $g_i \equiv 0 \pmod p$ $(i = 1, \cdots, m)$, giving $\boldsymbol{g}'_i \equiv \boldsymbol{0} \pmod p$ $(i = 1, \cdots, m)$. Thus we have G.C.D. $(\boldsymbol{g}'_1, \cdots, \boldsymbol{g}'_m, d_1 e) \equiv 0 \pmod p$, which contradicts G.C.D. $(\boldsymbol{g}'_1, \cdots, \boldsymbol{g}'_m, d_1 e) = 1$. Hence our assumption (2.4) is incorrect and we have G.C.D. $(\boldsymbol{g}_1, \cdots, \boldsymbol{g}_m, \boldsymbol{h}, e) = 1$. Thus by Lemma 1 there exists $\boldsymbol{\lambda} \in Z_n$ such that

$$\text{G.C.D. } (\boldsymbol{g}_1 \cdot \boldsymbol{\lambda} + h_1, \cdots, \boldsymbol{g}_m \cdot \boldsymbol{\lambda} + h_m, e) = 1$$

and so $\boldsymbol{x} = d_1 \boldsymbol{\lambda} + \boldsymbol{k} \in \mathscr{S}_d^c$.

3. Throughout the rest of this paper we suppose that $\mathscr{S}_d^c \neq \varnothing$ and G.C.D. $(\boldsymbol{l}_1, \cdots, \boldsymbol{l}_m, d) = 1$. Thus by Theorem 1 we have $d|c$, $N(d, L') > 0$ and G.C.D. $(\boldsymbol{l}'_1, \cdots, \boldsymbol{l}'_m, c) = 1$. Also throughout this paper corresponding to any $\boldsymbol{x} \in \mathscr{S}_d^c$ we define $\boldsymbol{u} \in Z^m$ by $\boldsymbol{u} = (u_1, \cdots, u_m)$, where $\boldsymbol{l}_i \cdot \boldsymbol{x} + l_i = du_i (i = 1, \cdots, m)$, so that G.C.D. $(\boldsymbol{u}, e) = 1$. The following lemmas will be needed later.

LEMMA 2. (i) *If* $\boldsymbol{x} \in \mathscr{S}_d^c$ *and* p *is a prime dividing* e *for which the system of simultaneous congruences*

$$\boldsymbol{l}_i \cdot \boldsymbol{z} + u_i \equiv 0 \pmod{p},\ i = 1, \cdots, m\,, \tag{3.1}$$

is solvable then $N(pd, L') > 0$.

(ii) *Conversely if* p *is a prime dividing* e *for which* $N(pd, L') > 0$ *then there exists* $\boldsymbol{x} \in \mathscr{S}_d^c$ *such that* (3.1) *is solvable.*

Proof. (i) For $\boldsymbol{x} \in \mathscr{S}_d^c$ and z a solution of (3.1) we let $\boldsymbol{w} = \boldsymbol{x} + dz$. Then for $i = 1, \cdots, m$ we have

$$\begin{aligned} \boldsymbol{l}_i \cdot \boldsymbol{w} + l_i &= (\boldsymbol{l}_i \cdot \boldsymbol{x} + l_i) + d\boldsymbol{l}_i \cdot \boldsymbol{z} \\ &= d(u_i + \boldsymbol{l}_i \cdot \boldsymbol{z}) \\ &\equiv 0 \pmod{pd}\,, \end{aligned}$$

showing that $N(pd, L') > 0$.

(ii) We define v_i by $\boldsymbol{l}_i \cdot \boldsymbol{w} + l_i = pdv_i$ $(i = 1, \cdots, m)$ and claim that

$$\text{G.C.D.}\ (\boldsymbol{l}_1, \cdots, \boldsymbol{l}_m, pv_1, \cdots, pv_m, e) = 1\,. \tag{3.2}$$

For if not there is a prime $p'|e$ such that

$$\boldsymbol{l}_i \equiv \boldsymbol{0},\ pv_i \equiv 0 \pmod{p'}\ (i = 1, \cdots, m)\,.$$

Thus from $\boldsymbol{l}_i \cdot \boldsymbol{w} + l_i = d\,pv_i$ we have $l_i \equiv 0 \pmod{p'}$ $(i = 1, \cdots, m)$, giving $\boldsymbol{l}'_i \equiv \boldsymbol{0} \pmod{p'}$ $(i = 1, \cdots, m)$, which contradicts G.C.D. $(\boldsymbol{l}'_1, \cdots, \boldsymbol{l}'_m, \text{de}) = 1$. Hence (3.2) is valid and so by Lemma 1 we can find $\boldsymbol{t} \in Z^n$ such that

$$\text{G.C.D.}\ (\boldsymbol{l}_1 \cdot \boldsymbol{t} + pv_1, \cdots, \boldsymbol{l}_m \cdot \boldsymbol{t} + pv_m, e) = 1\,.$$

We set $\boldsymbol{x} = \boldsymbol{w} + d\,\boldsymbol{t}$ so that for $i = 1, \cdots, m$ we have

$$\boldsymbol{l}_i \cdot \boldsymbol{x} + l_i = d(\boldsymbol{l}_i \cdot \boldsymbol{t} + pv_i)\,,$$

giving

$$\begin{aligned} &\text{G.C.D.}\ (\boldsymbol{l}_1 \cdot \boldsymbol{x} + l_1, \cdots, \boldsymbol{l}_m \cdot \boldsymbol{x} + l_m, c) \\ &\quad = d\ \text{G.C.D.}\ (\boldsymbol{l}_1 \cdot \boldsymbol{t} + pv_1, \cdots, \boldsymbol{l}_m \cdot \boldsymbol{t} + pv_m, e) \\ &\quad = d\,, \end{aligned}$$

so that $\boldsymbol{x} \in \mathscr{S}_d^c$. Finally taking $z = -\boldsymbol{t}$ we see that the system

$$\boldsymbol{l}_i \cdot z + u_i \equiv 0 \pmod{p} \quad (i = 1, \cdots, m)$$

is solvable, as $u_i = \boldsymbol{l}_i \cdot \boldsymbol{t} + pv_i$.

LEMMA 3. *Let t be a positive integer, A a subset of Z^n which consists of $A(t)$ distinct congruence classes modulo t. Now if t' is a positive integer such that $t \mid t'$ then A consists of $(t'/t)^n A(t)$ congruence classes modulo t'.*

Proof. It suffices to prove that a congruence class C modulo t of A consists of $(t'/t)^n$ classes modulo t'. This is clear for if $\boldsymbol{x} \in C$ then so does $\boldsymbol{x} + t\boldsymbol{y}_i$, $(i = 1, \cdots, (t'/t)^n)$, where the $\boldsymbol{y}_i$ are incongruent modulo t'/t, moreover the $\boldsymbol{x} + t\boldsymbol{y}_i$ are incongruent modulo t' and every member of C is congruent modulo t' to one of them.

4. The minumum modulus.

In this section we determine the minimum modulus M_d^c. We prove

THEOREM 2. *If $\mathscr{S}_d^c \neq \varnothing$ and G.C.D. $(\boldsymbol{l}_1, \cdots, \boldsymbol{l}_m, d) = 1$ the minimum modulus M_d^c with respect to $\mathscr{S}_d^c$ is given by*

$$M_d^c = d \prod_{p \mid e, N(pd, L') > 0} p \,. \tag{4.1}$$

Proof. As $\mathscr{S}_d^c \neq \varnothing$, $\mathfrak{M}_d^c$—the set of all solution moduli with respect to $\mathscr{S}_d^c$—is well-defined and moreover $\mathfrak{M}_d^c$ is non-empty as 0 and $\pm c$ belong to $\mathfrak{M}_d^c$. The proof will be accomplished by showing that $\mathfrak{M}_d^c$ is a principal ideal of Z generated by $d \prod_{p \mid e, N(pd, L') > 0} p$.

(i) We begin by showing that $\mathfrak{M}_d^c$ is an ideal of Z. It suffices to prove that if $t_1 \in \mathfrak{M}_d^c$ and $t_2 \in \mathfrak{M}_d^c$ then $t_1 - t_2 \in \mathfrak{M}_d^c$. For any $\boldsymbol{x} \in \mathscr{S}_d^c$ and any $\boldsymbol{y} \in Z^n$ we have $\boldsymbol{x} + t_1\boldsymbol{y} \in \mathscr{S}_d^c$, as $t_1 \in \mathfrak{M}_d^c$. Hence as $t_2 \in \mathfrak{M}_d^c$ we have

$$(\boldsymbol{x} + t_1\boldsymbol{y}) + t_2(-\boldsymbol{y}) \in \mathscr{S}_d^c \,,$$

that is

$$\boldsymbol{x} + (t_1 - t_2)\, \boldsymbol{y} \in \mathscr{S}_d^c \,,$$

so that

$$t_1 - t_1 \in \mathfrak{M}_d^c \,.$$

(ii) Next we show that $k = d \prod_{p \mid e, N(pd, L') > 0} p \in \mathfrak{M}_d^c$.
For $\boldsymbol{x} \in \mathscr{S}_d^c$ and any $\boldsymbol{y} \in Z^n$ we have

$$\begin{aligned}\text{G.C.D.}\ (\boldsymbol{l}_1\cdot(\boldsymbol{x}+k\boldsymbol{y})+l_1, \cdots, \boldsymbol{l}_m\cdot(\boldsymbol{x}+k\boldsymbol{y})+l_m, c) &= \text{G.C.D.}\ (\boldsymbol{l}_1\cdot\boldsymbol{x}+l_1+k(\boldsymbol{l}_1\cdot\boldsymbol{y}), \cdots, \boldsymbol{l}_m\cdot\boldsymbol{x}+l_m+k(\boldsymbol{l}_m\cdot\boldsymbol{y}), de)\\ &= d\ \text{G.C.D.}\ (u_1+k_1(\boldsymbol{l}_1\cdot\boldsymbol{y}), \cdots, u_m+k_1(\boldsymbol{l}_m\cdot\boldsymbol{y}), e)\ ,\end{aligned}$$

where $k_1 = k/d$. To complete the proof we must show that for all $\boldsymbol{y} \in Z^n$ we have

$$\text{G.C.D.}\ (u_1 + k_1(\boldsymbol{l}_1\cdot\boldsymbol{y}), \cdots, u_m + k_1(\boldsymbol{l}_m\cdot\boldsymbol{y}), e) = 1\ .$$

Suppose that this is not the case. Then there exists $\boldsymbol{y}_0 \in Z^n$ and a prime $p|e$ such that $u_i + k_1(\boldsymbol{l}_i\cdot\boldsymbol{y}_0) \equiv 0 \pmod p$ for $i = 1, \cdots, m$. Let $\boldsymbol{z} = \boldsymbol{x} + k\boldsymbol{y}_0$ so that for $i = 1, \cdots, m$ we have

$$\begin{aligned}\boldsymbol{l}_i\cdot\boldsymbol{z} + l_i &= \boldsymbol{l}_i\cdot\boldsymbol{x} + l_i + k(\boldsymbol{l}_i\cdot\boldsymbol{y}_0)\\ &= d(u_i + k_1(\boldsymbol{l}_i\cdot\boldsymbol{y}_0))\ ,\end{aligned}$$

that is,

$$\boldsymbol{l}_i\cdot\boldsymbol{z} + l_i \equiv 0 \pmod{pd}\ ,$$

so that $N(pd, L') > 0$. Hence as $p|e$ we have $p|k_1$ and so $p|u_i$ for $i = 1, \cdots, m$. This is the required contradiction as G.C.D. $(u_1, \cdots, u_m, e) = 1$, since $\boldsymbol{x} \in \mathscr{S}_d^c$.

(iii) In (i) we showed that $\mathfrak{M}_d^c$ is an ideal of Z and since Z is a principal ideal domain, $\mathfrak{M}_d^c$ is principal. Thus by the definition of the minimum modulus M_d^c we have $\mathfrak{M}_d^c = (M_d^c)$. In (ii) we showed that $k \in \mathfrak{M}_d^c$ so that $M_d^c|k$. Hence to show that $M_d^c = k$ we have only to show that $k|M_d^c$.

Now for all $\boldsymbol{x} \in \mathscr{S}_d^c$ and all $\boldsymbol{y} \in Z^n$ we have

$$\text{G.C.D.}\ (\boldsymbol{l}_1\cdot(\boldsymbol{x} + M_d^c\,\boldsymbol{y}) + l_1, \cdots, \boldsymbol{l}_m\cdot(\boldsymbol{x} + M_d^c\,\boldsymbol{y}) + l_m, c) = d\ .$$

Hence

$$\text{G.C.D.}\ (du_1 + M_d^c\,\boldsymbol{l}_1\cdot\boldsymbol{y}, \cdots, du_m + M_d^c\,\boldsymbol{l}_m\cdot\boldsymbol{y}, d\,e) = d\ ,$$

and so we must have

$$M_d^c\,\boldsymbol{l}_i\cdot\boldsymbol{y} \equiv 0 \pmod d\ ,$$

for all $\boldsymbol{y} \in Z^n$ and all i $(1 \leqq i \leqq m)$. Taking in particular $\boldsymbol{y} = (0, \cdots, 0, 1, 0, \cdots, 0)$, where the 1 appears in the j^{th} place we must have for $i = 1, \cdots, m$ and $j = 1, \cdots, n$

$$M_d^c\,l_{ij} \equiv 0 \pmod d\ ,$$

that is

$$\text{G.C.D.}\ (M_d^c\,l_{11}, \cdots, M_d^c\,l_{mn}) \equiv 0 \pmod d$$

or

$$M_d^c \text{ G.C.D. } (\boldsymbol{l}_1, \cdots, \boldsymbol{l}_m) \equiv 0 \pmod{d} .$$

But G.C.D. $(\boldsymbol{l}_1 \cdots, \boldsymbol{l}_m, d) = 1$ so we must have $M_d^c \equiv 0 \pmod{d}$. Thus it suffices to prove that

$$k_1 | \pi_d^c, \textit{ where } k_1 = k/d = \prod_{p|e, N(pd, L')>0} p \textit{ and } \pi_d^c = M_d^c/d .$$

We suppose that $k_1 \nmid \pi_d^c$ so that there exists a prime $p|e$ for which the system $\boldsymbol{l}_i \cdot \boldsymbol{w} + l_i \equiv 0 \pmod{pd}$ $(i = 1, \cdots, m)$ is solvable yet $p \nmid \pi_d^c$. By Lemma 2 (ii) there exists $z \in Z^n$ such that for some $\boldsymbol{x} \in \mathscr{S}_d^c$ we have

$$\boldsymbol{l}_i \cdot \boldsymbol{z} + u_i \equiv 0 \pmod{p}, \ i = 1, \cdots, m .$$

As $p \nmid \pi_d^c$ we can define λ by $\pi_d^c \lambda \equiv 1 \pmod{p}$ and let $\boldsymbol{y} = \lambda z$ so that for $i = 1, \cdots, m$ we have

$$u_i + \pi_d^c \boldsymbol{l}_i \cdot \boldsymbol{y} \equiv 0 \pmod{p} . \tag{4.2}$$

But as M_d^c is the minimum modulus and $\boldsymbol{x} \in \mathscr{S}_d^c$ we must have

$$\text{G.C.D. } (\boldsymbol{l}_1 \cdot (\boldsymbol{x} + M_d^c \boldsymbol{y}) + l_1, \cdots, \boldsymbol{l}_m \cdot (\boldsymbol{x} + M_d^c \boldsymbol{y}) + l_m, c) = d ,$$

that is

$$\text{G.C.D. } (u_1 + \pi_d^c \boldsymbol{l}_1 \cdot \boldsymbol{y}, \cdots, u_m + \pi_d^c \boldsymbol{l}_m \cdot \boldsymbol{y}, e) = 1 ,$$

which is contradicted by (4.2). Hence $\pi_d^c = \prod_{p|e, N(pd, L')>0} p$ and this completes the proof.

We note the following important corollary of Theorem 2.

COROLLARY 1. *$\boldsymbol{x} \in Z^n$ is a solution of*

$$\text{G.C.D. } (\boldsymbol{l}_1 \cdot \boldsymbol{x} + l_1, \cdots, \boldsymbol{l}_m \cdot \boldsymbol{x} + l_m, c) = d \tag{4.3}$$

if and only if

$$\text{G.C.D. } (\boldsymbol{l}_1 \cdot \boldsymbol{x} + l_1, \cdots, \boldsymbol{l}_m \cdot \boldsymbol{x} + l_m, M_d^c) = d . \tag{4.4}$$

Proof. (i) Suppose $\boldsymbol{x}$ is a solution of (4.3). Then we can define u_i $(i = 1, \cdots, m)$ by $\boldsymbol{l}_i \cdot \boldsymbol{x} + l_i = du_i$ and we have

$$\text{G.C.D. } (u_1, \cdots, u_m, e) = 1 .$$

Hence we deduce

$$\text{G.C.D. } (u_1, \cdots, u_m, \prod_{p|e, N(pd, L')>0} p) = 1$$

and so

$$\text{G.C.D.}\ (\boldsymbol{l}_1\cdot\boldsymbol{x} + l_1, \cdots, \boldsymbol{l}_m\cdot\boldsymbol{x} + l_m, d \prod_{p\mid e, N(pd,L')>0} p) = d\ ,$$

which by Theorem 2 is

$$\text{G.C.D.}\ (\boldsymbol{l}_1\cdot\boldsymbol{x} + l_1, \cdots, \boldsymbol{l}_m\cdot\boldsymbol{x} + l_m, M_d^c) = d\ .$$

(ii) Conversely suppose $\boldsymbol{x}$ is a solution of (4.4). Then there exist u_i $(i = 1, \cdots, m)$ such that $l_i\cdot x + l_i = du_i$ and

$$\text{G.C.D.}\ (u_1, \cdots, u_m, \prod_{p\mid e, N(pd,L')>0} \mathrm{p}) = 1\ .$$

Suppose however that

$$\text{G.C.D.}\ (u_1, \cdots, u_m, e) \neq 1\ .$$

Then there exists a prime p such that

$$u_i \equiv 0\ (i = 1, \cdots, m), e \equiv 0\ (\mathrm{mod}\ p), N(pd, L') = 0.$$

But for $i = 1, \cdots, m$ we have

$$\boldsymbol{l}_i\cdot\boldsymbol{x} + l_i = du_i \equiv 0\ (\mathrm{mod}\ pd)\ ,$$

that is $N(pd, L') > 0$, which is the required contradiction. Hence we have

$$\text{G.C.D.}\ (u_1, \cdots, u_m, e) = 1$$

and so

$$\text{G.C.D.}\ (\boldsymbol{l}_1\cdot\boldsymbol{x} + l_1, \cdots, \boldsymbol{l}_m\cdot\boldsymbol{x} + l_m, c) = d\ .$$

5. Number of solutions with respect to the minimum modulus. We begin by evaluating $\mathfrak{N}_1^c$, that is, the number of solutions of (1.1), when $d = 1$, which are incongruent modulo M_1^c. We prove

THEOREM 3. $\mathfrak{N}_1^c = \prod_{p\mid c, N(p,L')>0} p^n\left(1 - \frac{1}{p^{r(p,L)}}\right)$, *where* $r(p, L)$ *is the rank of the matrix* $L^{(p)}$ *obtained from* L *by replacing each entry* l_{ij} *by its residue class modulo* p *in the finite field* Z_p.

Proof. By Corollary 1 the required number of solutions $\mathfrak{N}_1^c$ is just the number of solutions taken modulo M_1^c of

$$\text{G.C.D.}\ (\boldsymbol{l}_1\cdot\boldsymbol{x} + l_1, \cdots, \boldsymbol{l}_m\cdot\boldsymbol{x} + l_m, M_1^c) = 1\ .$$

Thus as $M_1^c = \prod_{p\mid c, N(p,L')>0} p$ is a product of distinct primes, a standard argument involving use of the Chinese remainder theorem shows that this number $\mathfrak{N}_1^c$ is just $\prod_{p \mid M_1^c} \mathfrak{N}(p)$, where $\mathfrak{N}(p)$ is the number of solutions $\boldsymbol{x}$ taken modulo p of

$$\text{G.C.D.}\ (\boldsymbol{l}_1 \cdot \boldsymbol{x} + l_1, \cdots, \boldsymbol{l}_m \cdot \boldsymbol{x} + l_m, p) = 1 . \tag{5.1}$$

Now $\boldsymbol{x}$ is a solution of (5.1) if and only if $\boldsymbol{x}^{(p)}$ is not a solution of the system (T denotes transpose)

$$L^{(p)} \boldsymbol{x}^{(p)T} + \boldsymbol{l}^{(p)T} = \boldsymbol{0}^T .$$

Since $N(p, L') > 0$, this system is consistent over the field Z_p and has $p^{n-r(p,L)}$ solutions. Thus the number of solutions (modulo p) of (5.1) is $p^n - p^{n-r(p,L)} = p^n \left(1 - \frac{1}{p^{r(p,L)}}\right)$, giving

$$\mathfrak{N}_1^c = \prod_{p \mid c, N(p,L') > 0} p^n \left(1 - \frac{1}{p^{r(p,L)}}\right)$$

as required.

In the proof of Theorem 2 we have seen that any solution modulus M of (1.1) is a multiple of M_d^c. As $\mathscr{S}_d^c$ consists of $\mathfrak{N}_d^c$ congruence classes modulo M_d^c, Lemma 3 shows that $\mathscr{S}_d^c$ consists of $(M/M_d^c)^n \mathfrak{N}_d^c$ congruence classes modulo M. Hence by Theorem 3 we have

COROLLARY 2. *The number of solutions $\boldsymbol{x}$ of* (1.1), *with $d = 1$, determined modulo M—a multiple of M_d^c—is*

$$M^n \prod_{p \mid c, N(p,L') > 0} \left(1 - \frac{1}{p^{r(p,L)}}\right) .$$

As a consequence of Corollary 2 we have the linear case of a result recently established by Stevens [6]. A generalization of this result is proved in § 7.

COROLLARY 3. (Stevens) *The number of solutions of*

$$\text{G.C.D.}\ (a_1 x_1 + b_1, \cdots, a_n x_n + b_n, c) = 1 ,$$

taken modulo c, is

$$c^n \prod_{p \mid c} \left(1 - \frac{\nu_1(p) \cdots \nu_n(p)}{p^n}\right) ,$$

where $\nu_i(p)(i = 1, \cdots, n)$ is the number of incongruent solutions modulo p of $a_i x_i + b_i \equiv 0 \pmod{p}$.

Proof. The system

$$a_i x_i + b_i \equiv 0 \pmod{p} \ (i = 1, \cdots, n) ,$$

is solvable if and only if

$$\text{G.C.D. } (a_i, p) \mid b_i \ (i = 1, \cdots, n) ,$$

that is, if and only if

$$p \nmid a_i \text{ or } p \mid \text{G.C.D. } (a_i, b_i) \ (i = 1, \cdots, n) .$$

Hence by Corollary 2 the required number of solutions is

$$c^n \prod_{p \mid c}{}' \left(1 - \frac{1}{p^{r(p)}}\right) , \tag{5.2}$$

where the dash (′) denotes that the product is taken over all p such that $p \nmid a_i$ or $p \mid \text{G.C.D. } (a_i, b_i)$ $(1 \leqq i \leqq n)$ and $r(p)$ is the number of a_i $(i = 1, \cdots, n)$ not divisible by p. As

$$\nu_i(p) = \begin{cases} 1, \ p \nmid a_i \ , \\ 0, \ p \mid a_i, \ p \nmid b_i \ , \\ p, \ p \mid a_i, \ p \mid b_i \ , \end{cases}$$

for $i = 1, \cdots, n$, (5.2) is just

$$c^n \prod_{p \mid c} \left(1 - \frac{\nu_1(p) \cdots \nu_n(p)}{p^n}\right) ,$$

which is the required result.

We now turn to the general case $d \geqq 1$. Let p be a prime and let E denote an equivalence class of $\mathscr{S}_d^c$ consisting of elements of $\mathscr{S}_d^c$ which are congruent modulo d. We assert that if $\boldsymbol{x}^{(1)}, \boldsymbol{x}^{(2)} \in E$ then the system $\boldsymbol{l}_i \cdot \boldsymbol{z}^{(1)} + u_i^{(1)} \equiv 0 \pmod{p}$ $(i = 1, \cdots, n)$ is solvable if and only if the system $\boldsymbol{l}_i \cdot \boldsymbol{z}^{(2)} + u_i^{(2)} \equiv 0 \pmod{p}$ $(i = 1, \cdots, n)$ is solvable. As $\boldsymbol{x}^{(1)} \equiv \boldsymbol{x}^{(2)} \pmod{p}$ there exists $\boldsymbol{t} \in Z^n$ such that $\boldsymbol{x}^{(2)} = \boldsymbol{x}^{(1)} + d\boldsymbol{t}$. Hence for $i = 1, \cdots, n$ we have

$$\begin{aligned} du_i^{(2)} &= \boldsymbol{l}_i \cdot \boldsymbol{x}^{(2)} + l_i \\ &= \boldsymbol{l}_i \cdot \boldsymbol{x}^{(1)} + l_i + d\boldsymbol{l}_i \cdot \boldsymbol{t} \\ &= du_i^{(1)} + d\boldsymbol{l}_i \cdot \boldsymbol{t} \end{aligned}$$

giving

$$u_i^{(2)} = u_i^{(1)} + \boldsymbol{l}_i \cdot \boldsymbol{t} .$$

If there exists $\boldsymbol{z}^{(1)} \in Z^n$ such that $\boldsymbol{l}_i \cdot \boldsymbol{z}^{(1)} + u_i^{(1)} \equiv 0 \pmod{p}$ $(i = 1, \cdots, n)$ letting $\boldsymbol{z}^{(2)} = \boldsymbol{z}^{(1)} - \boldsymbol{t}$ we have $\boldsymbol{l}_i \cdot \boldsymbol{z}^{(2)} + u_i^{(2)} = \boldsymbol{l}_i \cdot \boldsymbol{z}^{(1)} - \boldsymbol{l}_i \cdot \boldsymbol{t} + u_i^{(1)} + \boldsymbol{l}_i \cdot \boldsymbol{t} \equiv 0 \pmod{p}$, which completes the proof of the assertion. Hence the solvability of the system

$$\boldsymbol{l}_i\cdot\boldsymbol{z} + u_i \equiv 0 \pmod p \quad (i = 1, \cdots, n)$$

depends only on the equivalence class E to which $\boldsymbol{x}$ (recall $\boldsymbol{l}_i\cdot\boldsymbol{x} + l_i = du_i$) belongs. Thus we can define a symbol $\delta_p(E)$ as follows:

$$\delta_p(E) = \begin{cases} 1, & \text{if for some } \boldsymbol{x}\in E \text{ (and thus for all } \boldsymbol{x}\in E) \text{ the system} \\ & \boldsymbol{l}_i\cdot\boldsymbol{z} + u_i \equiv 0 \pmod p \ (i = 1, \cdots, m) \text{ is solvable,} \\ 0, & \text{otherwise.} \end{cases}$$

We now prove the following result.

THEOREM 4. $\mathfrak{N}_d^c = \sum_{j=1}^{N(d,L')} \left\{ \prod_{p\mid e, N(pd,L')>0} p^n \left(1 - \frac{1}{p^{r(p,L)}}\right)^{\delta_p(E^{(j)})} \right\}$, *where the* $E^{(j)}$ *denote the* $N(d, L')$ *congruence classes modulo* d *in* $\mathscr{S}_d^c$.

Proof. We let

$$\mathscr{S} = \{\boldsymbol{x}\in Z^n \mid \boldsymbol{l}_i\cdot\boldsymbol{x} + l_i \equiv 0 \pmod d, i = 1, \cdots, m\}$$

so that we have $\mathscr{S}_d^c \subseteqq \mathscr{S}$. Now $\mathscr{S}$ consists of $N(d, L')$ congruence classes modulo d and if we restrict this equivalence relation modulo d to $\mathscr{S}_d^c$, we show that $\mathscr{S}_d^c$ also contains the same number of classes. We write $E(\boldsymbol{x})$ (resp. $E'(\boldsymbol{x})$) for the equivalence class to which $\boldsymbol{x}\in\mathscr{S}_d^c$ (resp. $\boldsymbol{x}\in\mathscr{S}$) belongs. From the proof of Theorem 1 we see that for each $\boldsymbol{x}\in\mathscr{S}$ there exists $\boldsymbol{\lambda}\in Z^n$ such that $\boldsymbol{x} + d\boldsymbol{\lambda}\in\mathscr{S}_d^c$. We define a mapping f from the set of equivalence classes of $\mathscr{S}$ into the set of equivalence classes of $\mathscr{S}_d^c$ as follows: For $\boldsymbol{x}\in\mathscr{S}$

$$f(E'(\boldsymbol{x})) = E(\boldsymbol{x} + d\boldsymbol{\lambda}) .$$

This mapping is well-defined for if $\boldsymbol{x}'\in\mathscr{S}$ is such that $E'(\boldsymbol{x}') = E'(\boldsymbol{x})$ then $E(\boldsymbol{x}' + d\boldsymbol{\lambda}') = E(\boldsymbol{x} + d\boldsymbol{\lambda})$. f is onto for if $\boldsymbol{x}\in\mathscr{S}_d^c$ then $f(E'(\boldsymbol{x})) = E(\boldsymbol{x})$ and is also one-to-one, for if $f(E'(\boldsymbol{x})) = f(E'(\boldsymbol{y}))$, then $E(\boldsymbol{x} + d\boldsymbol{\lambda}) = E(\boldsymbol{y} + d\boldsymbol{\lambda}')$, that is $\boldsymbol{x}\equiv\boldsymbol{y} \pmod d$, giving $E'(\boldsymbol{x}) = E'(\boldsymbol{y})$. Thus the number of equivalence classes of $\mathscr{S}_d^c$ is the same as the number of equivalence classes of $\mathscr{S}$, that is $N(d, L')$.

Since $d \mid M_d^c$, each equivalence class E of $\mathscr{S}_d^c$, consists of a certain number of distinct classes in $\mathscr{S}_d^c$ modulo M_d^c. We now determine this number. If $\boldsymbol{x}\in E$, $\boldsymbol{x} + d\boldsymbol{t}$ also belongs in E if and only if it belongs in $\mathscr{S}_d^c$, that is, if and only if,

$$\text{G.C.D.}\ (\boldsymbol{l}_1\cdot(\boldsymbol{x} + d\boldsymbol{t}) + l_1, \cdots, \boldsymbol{l}_m\cdot(\boldsymbol{x} + d\boldsymbol{t}) + l_m, c) = d ,$$

that is, if and only if,

(5.3) $$\text{G.C.D.}\ (u_1 + \boldsymbol{l}_1 \cdot \boldsymbol{t}, \cdots, u_m + \boldsymbol{l}_m \cdot \boldsymbol{t}, e) = 1 .$$

Thus the number of distinct classes modulo M_d^c contained in E is just the number of distinct classes modulo $\pi_d^c = M_d^c/d$ which satisfy (5.3). But the minimum modulus of (5.3) is $\prod_{p|e} p^{\delta_p(E)}$. By lemma 2 (i) $\delta_p(E) = 1$ implies $N(pd, L') > 0$, so that $\prod_{p|e} p^{\delta_p(E)}$ divides $\prod_{p|e, N(pd,L')>0} p = \pi_d^c$. Writing $\prod_{p|e}^{+}$ for $\prod_{p|e, N(pd,L')>0}$ and $\prod_{p|e}^{0}$ for $\prod_{p|e, N(pd,L')=0}$, the required number of classes is by Corollary 2

$$\begin{aligned} &= \prod_{p|e}^{+} p^n \cdot \prod_{p|e} \left(1 - \frac{1}{p^{r(p,L)}}\right)^{\delta_p(E)} \\ &= \prod_{p|e}^{+} p^n \left(1 - \frac{1}{p^{r(p,L)}}\right)^{\delta_p(E)} \cdot \quad \prod_{p|e}^{0} \left(1 - \frac{1}{p^{r(p,L)}}\right)^{\delta_p(E)} \\ &= \prod_{p|e}^{+} p^n \left(1 - \frac{1}{p^{r(p,L)}}\right)^{\delta_p(E)} , \end{aligned}$$

as $N(pd, L') = 0$ implies $\delta_p(E) = 0$.

Finally letting $E^{(1)}, \cdots, E^{(h)}$ denote the $h = N(d, L')$ distinct equivalence classes in $\mathscr{S}_d^c$ we deduce that the total number of incongruent solutions modulo M_d^c of (1.1) is

$$\sum_{j=1}^{N(d,L')} \left\{ \prod_{p|e, N(pd,L')>0} p^n \left(1 - \frac{1}{p^{r(p,L)}}\right)^{\delta_p(E^{(j)})} \right\} .$$

We remark that $r(p, L) \neq 0$, for $p|e$ and $\delta_p(E) = 1$. Otherwise, if $r(p, L) = 0$, $\boldsymbol{l}_i \equiv \boldsymbol{0} \pmod p$ $(i = 1, \cdots, m)$. But as $\delta_p(E) = 1$ then for $\boldsymbol{x} \in E$ the system $l_i \cdot z + u_i \equiv 0 \pmod p$ $(i = 1, \cdots, m)$ is solvable contradicting G.C.D. $(u_1, \cdots, u_m, e) = 1$.

6. Some special cases.

We note a number of interesting cases of our results.

Corollary 4. *If* G.C.D. $(d, e) = 1$ *then the number* $\mathfrak{N}_d^c$ *of solutions of* (1.1) *modulo* M_d^c *is*

$$\mathfrak{N}_d^c = N(d, L') \prod_{p|e, N(pd,L')>0} p^n \left(1 - \frac{1}{p^{r(p,L)}}\right) .$$

Proof. By Theorem 4 it suffices to show that if G.C.D. $(d, e) = 1$, $p|e$, $N(pd, L') > 0$ then for all $\boldsymbol{x} \in \mathscr{S}_d^c$ we have $\delta_p(E) = 1$, that is the system $\boldsymbol{l}_i \cdot \boldsymbol{z} + u_i \equiv 0 \pmod p$ is solvable. Let $\boldsymbol{w}$ be a solution of $\boldsymbol{l}_i \cdot \boldsymbol{w} + l_i \equiv 0 \pmod{pd}$, say $\boldsymbol{l}_i \cdot \boldsymbol{w} + l_i = pdv_i$ $(i = 1, \cdots, m)$. As $p \nmid d$ we can define $\boldsymbol{z} = d^{-1}(\boldsymbol{w} - \boldsymbol{x})$, where $dd^{-1} \equiv 1 \pmod p$ so that for $i = 1, \cdots, m$ we have

$$\begin{aligned} \boldsymbol{l}_i\cdot\boldsymbol{z} + u_i &= d^{-1}(\boldsymbol{l}_i\cdot\boldsymbol{w} - \boldsymbol{l}_i\cdot\boldsymbol{x}) + u_i \\ &= d^{-1}(pdv_i - l_i - du_i + l_i) + u_i \\ &= dd^{-1}(pv_i - u_i) + u_i \\ &\equiv 0 \pmod{p}\ , \end{aligned}$$

as required.

COROLLARY 5. *If* $N(d, L') = 1$ *then the number* $\mathfrak{N}_d^c$ *of solutions of* (1.1) *modulo* M_d^c *is*

$$\mathfrak{N}_d^c = \prod_{p\mid e, N(pd,L')>0} p^n \left(1 - \frac{1}{p^{r(p,L)}}\right) . \tag{6.1}$$

In particular $N(d, L') = 1$ when L is invertible (mod d), and so $\mathfrak{N}_d^c$ is given by (6.1). Moreover if L is invertible modulo $d \prod_{p\mid e} p$ or c, then (1.1) is solvable and $\mathfrak{N}_d^c = \prod_{p\mid e}(p^n - 1)$.

Proof. This is immediate from Theorem 4 since by Lemma 2(ii), $\delta_p(E) = 1$ for all $p\mid e$, $N(pd, L') > 0$. Also (1.1) is solvable when L is invertible modulo $d \prod_{p\mid e} p$ as

$$\text{G.C.D. } (\boldsymbol{l}_1, \cdots, \boldsymbol{l}_m, d) = \text{G.C.D. } (\boldsymbol{l}'_1, \cdots, \boldsymbol{l}'_m, c) = 1 .$$

COROLLARY 6. *If* L *is invertible modulo* $\prod_{p\mid e, N(pd,L')>0} p$ *then the number of solutious of* (1.1) *modulo* M_d^c *is*

$$\mathfrak{N}_d^c = N(d, L') \prod_{p\mid e, N(pd,L')>0} (p^n - 1) .$$

Proof. Let p be any prime such that $p\mid e$ and $N(pd, \mathrm{L}') > 0$. Then L is invertible modulo p and so for any $\boldsymbol{x} \in \mathscr{S}_d^c$ the system

$$\boldsymbol{l}_i\cdot\boldsymbol{z} + u_i \equiv 0 \pmod{p}\ (1 = 1, \cdots, n)$$

is solvable and so $\delta_p(E^{(j)}) = 1$, $\mathrm{j} = 1, \cdots, N(d, L')$. Moreover as L is invertible modulo p we have $r(p, L) = n$ and the result follows from Theorem 4.

COROLLARY 7. *If*

$$\text{G.C.D. } (a_1, \cdots, a_n, d) = 1 \tag{6.2}$$

the equation

$$\text{G.C.D. } (a_1x_1 + \cdots + a_nx_n + b, c) = d \tag{6.3}$$

is solvable if and only if

$$d \mid c,\ \text{G.C.D. } (a_1, \cdots, a_n, b, c) = 1 . \tag{6.4}$$

The minimum modulus of (6.3) *is*

$$d \prod_{p \mid c/d}' p$$

and the number of solutions $\boldsymbol{x}$ *modulo this minimum modulus is*

$$d^{n-1} \prod_{p \mid c/d}' (p^n - p^{n-1}) ,$$

where the dash (′) *means that the product is taken over those primes* $p \mid c/d$ *such that* G.C.D. $(a_1, \cdots, a_n, p) = 1$.

Proof. According to Smith [4] or Lehmer [3] the number of solutions $\boldsymbol{x}$ taken modulo d of

$$a_1x_1 + \cdots + a_nx_n + b \equiv 0 \pmod{d}$$

is d^{n-1} G.C.D. $(a_1, \cdots, a_n, d)$ if G.C.D. $(a_1, \cdots, a_n, d)$ divides b and 0 otherwise. Thus as G.C.D. $(a_1, \cdots, a_n, d) = 1$, we have $N(d, L') = d^{n-1}$ and so by Theorem 1 (6.3) is solvable if and only if

$$d \mid c, \text{ G.C.D. } (a_1, \cdots, a_n, b, c) = 1 .$$

Now if (6.3) is solvable and $p \mid c/d$ then

$$\text{G.C.D. } (a_1, \cdots, a_n, pd) \mid b$$

if and only if

$$\text{G.C.D. } (a_1, \cdots, a_n, p) = 1 ,$$

in view of (6.2) and (6.4). Thus by Theorem 2 the minimum modulus is

$$d \prod_{p \mid c/d}' p .$$

Finally for $p \mid c/d$, G.C.D. $(a_1, \cdots, a_n, p) = 1$ we have $r(p, L) = 1$ and moreover the congruence $a_1x_1 + \cdots + a_nx_n + u \equiv 0 \pmod{p}$ is always solvable so that $\delta_p(E^{(j)}) = 1, j = 1, \cdots, d^{n-1}$. Hence by Theorem 4 the number of solutions is

$$d^{n-1} \prod_{p \mid c/d}' p^n \left(1 - \frac{1}{p}\right) .$$

We remark that in particular ([5])

$$\text{G.C.D. } (ax + b, c) = 1$$

is solvable if and only if G.C.D. $(a, b, c) = 1$, has minimum modulus $\prod_{p \mid c, p \nmid a} p$, and has $\prod_{p \mid c, p \nmid a} (p - 1)$ solutions x modulo the minimum modulus.

COROLLARY 8. *There is a unique solution of* (1.1) *modulo* M_d^c *if and only if*

(i) $N(d, L') = 1$ *and there is no prime* p *such that*

$$p \mid e, N(pd, L') > 0 \ ,$$

or

(*ii*) $N(d, L') = 1$ *and the only prime* p *such that* $p \mid e, N(pd, L') > 0$, *is* $p = 2$, *and* $r(2, L) = 1$, $n = 1$.

Proof. If (1.1) possesses a unique solution modulo M_d^c, Theorem 4 shows that S can consist only of a single congruence class modulo d. Hence $N(d, L') = 1$. Also by Theorem 4 if there is no prime p such that $p \mid e$ and $N(pd, L') > 0$ then $\mathfrak{N}_d^c = 1$. Suppose however that there is such a prime p. Then by Corollary 5 we have

$$1 = \prod_{p \mid e, N(pd, L') > 0} (p^n - p^{n-r(p,L)}) \ .$$

This occurs if and only if

$$p^n - p^{n-r(p,L)} = 1 \ , \tag{6.5}$$

for all $p \mid e$ with $N(pd, L') > 0$. But the left-hand side of (6.5) is divisible by p unless $r(p, L) = n$. Then $p^n = 2$ and we have $p = 2$, $n = 1$, $r(p, L) = r(2, L) = 1$, which proves the theorem.

7. Another method. Although the formula of Theorem 4 applies to some important cases in § 6, this formula seems difficult to evaluate even for example in the diagonal case

$$\text{G.C.D.}\ (a_1x_1 + b_1, \cdots, a_nx_n + b_n, c) = d \ .$$

The inherent difficulty is in determining for a given prime p which solutions of this equation have the property that the system $a_iz_i + u_i \equiv 0 \pmod p$ $(i = 1, \cdots, n)$ is solvable. We now present another method which in conjunction with previous results yields the diagonal case.

We consider the set $\mathfrak{U}$ of $\boldsymbol{u} \in Z^m$ with G.C.D. $(\boldsymbol{u}, e) = 1$ for which the system

$$\boldsymbol{l}_i \cdot \boldsymbol{x} + l_i \equiv du_i \pmod c \ (i = 1, \cdots, n) \text{ is solvable} \ . \tag{7.1}$$

It is clear that if $\boldsymbol{u} \in \mathfrak{U}$ and $\boldsymbol{u} \equiv \boldsymbol{u}' \pmod e$ then $\boldsymbol{u}' \in \mathfrak{U}$. We denote by K_d^c the number of distinct classes modulo e contained in $\mathfrak{U}$. Let $\mathfrak{N}$ denote the number of solutions $\boldsymbol{x}$ of (1.1) modulo c. We prove

THEOREM 5. $\mathfrak{N} = K_d^c N_c(L^*)$ *where* L^* *is the* $m \times (n+1)$ *matrix*

$[L: 0]$.

Proof. If $\boldsymbol{x} \in \mathcal{S}_d^c$ then there exists $\boldsymbol{u} \in Z^n$ such that $\boldsymbol{l}_i \cdot \boldsymbol{x} + l_i = du_i$ $(i = 1, \cdots, m)$ and G.C.D. $(\boldsymbol{u}, e) = 1$. If $\boldsymbol{x}, \boldsymbol{x}' \in \mathcal{S}_d^c$ are such that $\boldsymbol{x} \equiv \boldsymbol{x}' \pmod e$ then $du_i \equiv du_i' \pmod c$, that is $u_i \equiv u_i' \pmod e$.

Conversely if G.C.D. $(\boldsymbol{u}, e) = 1$ and $\boldsymbol{x}$ satisfies $\boldsymbol{l}_i \cdot \boldsymbol{x} + l_i \equiv du_i \pmod c$ $(i = 1, \cdots, m)$ then $\boldsymbol{l}_i \cdot \boldsymbol{x} + l_i = d(u_i + \lambda_i e)$ and $\boldsymbol{x} \in \mathcal{S}_d^c$ as G.C.D. $(\boldsymbol{u} + \boldsymbol{\lambda} e, e) =$ G.C.D. $(\boldsymbol{u}, e) = 1$.

Thus $\boldsymbol{x} \in \mathcal{S}_d^c$ if and only if $\boldsymbol{x}$ is a solution of $\boldsymbol{l}_i \cdot \boldsymbol{x} + l_i \equiv du_i \pmod c$, where G.C.D. $(\boldsymbol{u}, e) = 1$. Now there are K_d^c incongruent classes of $\boldsymbol{u}$ modulo e, with G.C.D. $(\boldsymbol{u}, e) = 1$, for which (7.1) is solvable. For each one of these, (7.1) has $N_c(L: 0)$ incongruent solutions modulo c. Hence we have

$$\mathfrak{N} = K_d^c N_c(L^*)$$

as required.

We now obtain the following interesting result.

COROLLARY 9. *If* $\boldsymbol{h} \in Z^n$ *and* $e_1, \cdots, e_n$ *are divisors of* e *then the system*

$$u_i \equiv h_i \pmod{e_i} \quad (i = 1, \cdots, n) \tag{7.2}$$

has a solution $\boldsymbol{u} = (u_1, \cdots, u_n)$ *such that* G.C.D. $(\boldsymbol{u}, e) = 1$ *if and only if* G.C.D. $(e_1, \cdots, e_n, h_1, \cdots, h_n, e) = 1$. *When this holds* (7.2) *has*

$$\prod_{i=1}^{n} (e/e_i) \prod_{p|e}{}' \left(1 - \frac{1}{p^{r(p)}}\right)$$

distinct solutions $\boldsymbol{u}$ *modulo* e, *for which* G.C.D. $(\boldsymbol{u}, e) = 1$, *where* $r(p) =$ *number of* e_i $(i = 1, \cdots, n)$ *not divisible by* p, *and the dash* (′) *means that the product is taken over those primes* $p | e$ *such that* $p \nmid e_i$ *or* $p |$ G.C.D. (e_i, h_i) $(i = 1, \cdots, n)$.

Proof. The system (7.2) has a solution $\boldsymbol{u}$ such that G.C.D. $(\boldsymbol{u}, e) = 1$ if and only if

$$\text{G.C.D. } (e_1 x_1 + h_1, \cdots, e_n x_n + h_n, e) = 1 \tag{7.3}$$

is solvable, which by Lemma 1 is the case if and only if G.C.D. $(e_1, \cdots, e_n, h_1, \cdots, h_n, e) = 1$. Applying Theorem 5 to (7.3) we have $\mathfrak{N} = K_1^e N_e(L^*)$ and we note that K_1^e is the number of distinct solutions $\boldsymbol{u}$ modulo e of (7.2) for which G.C.D. $(\boldsymbol{u}, e) = 1$. However $N_e(L*)$ is the number of solutions $\boldsymbol{x}$ modulo e such that $e_i x_i \equiv 0 \pmod e$ $(i = 1, \cdots, n)$. Clearly $N_e(L^*) = \prod_{i=1}^{n} e_i$. By Corollary 2

$$\mathfrak{N} = e^n \prod_{p \mid e, N(p,L')>0} \left(1 - \frac{1}{p^{r(p,L)}}\right),$$

where

$$L' = \begin{pmatrix} e_1 & & & h_1 \\ & \ddots & & \vdots \\ & & e_n & h_n \end{pmatrix}.$$

Now $N(p, L') > 0$ if and only if the system $e_i w_i + h_i \equiv 0 \pmod p$ $(i = 1, \cdots, n)$ is solvable, that is, if and only if G.C.D. $(p, e_i) \mid h_i$ or if and only if $p \nmid e_i$ or $p \mid$ G.C.D (e_i, h_i) $(i = 1, \cdots, n)$. Also $r(p, L)$ is just the number of the e_i $(i = 1, \cdots, n)$ not divisible by p. This completes the proof.

We now obtain a generalization of Steven's result [6] (see Corollary 3).

COROLLARY 10. *The equation*

$$\text{G.C.D. } (a_1x_1 + b_1, \cdots, a_nx_n + b_n, c) = d,$$

where

$$\text{G.C.D. } (a_1, \cdots, a_n, d) = 1,$$

is solvable if and only if

$$d \mid c, \text{ G.C.D. } (a_i, d) \mid b_i \ (i = 1, \cdots, n),$$

$$\text{G.C.D. } (a_1, \cdots, a_n, b_1, \cdots, b_n, c) = 1.$$

The number of solution modulo c is given by

$$\prod_{i=1}^{n} \text{G.C.D. } (a_i, d) \cdot (c/d)^n \cdot \prod_{p \mid c/d} \left(1 - \frac{\nu_1(p) \cdots \nu_n(p)}{p^n}\right),$$

where $\nu_i(p)$ $(i = 1, \cdots, n)$ is the number of incongruent solutions modulo p of $\dfrac{a_i}{\text{G.C.D. } (a_i, d)} x + \dfrac{b_i}{\text{G.C.D. } (a_i, d)} \equiv 0 \pmod p$.

Proof. The necessary and sufficient conditions for solvability are immediate from Theorem 1. When solvable we calculate the number $\mathfrak{N}$ of solutions modulo c using Theorem 5. Thus we require the number of distinct $\boldsymbol{u}$ modulo e with G.C.D. $(\boldsymbol{u}, e) = 1$ such that

$$a_ix_i + b_i \equiv du_i \pmod{de} \ (i = 1, \cdots, n)$$

is solvable, that is,

$$(a_i/d_i)x_i + (b_i/d_i) \equiv (d/d_i)u_i \pmod{d/d_i \cdot e}$$

where $d_i = \text{G.C.D}\ (a_i, d)\ (i = 1, \cdots, n)$.
This is solvable if and only if

$$\text{G.C.D.}\ ((a_i/d_i), (d/d_i)e) \mid (d/d_i)u_i - (b_i/d_i) (i = 1, \cdots, n) ,$$

that is, if and only if,

$$(d/d_i)u_i \equiv (b_i/d_i) \ (\text{mod G.C.D.}\ ((a_i/d_i), e)\ (i = 1, \cdots, n) .$$

This system is equivalent to

$$u_i \equiv h_i \ (\text{mod G.C.D.}\ (a_i/d_i, e))\ (i = 1, \cdots, n) ,$$

where $h_i = (d/d_i)^{-1}b_i/d_i$ and $(d/d_i)^{-1}$ is an inverse of d/d_i modulo G.C.D. $(a_i/d_i, e)$ since G.C.D. $(d/d_i, a_i/d_i, e) = 1$. Thus by Corollary 9 the number of such $\boldsymbol{u}$ is

$$\prod_{i=1}^{n} \frac{e}{\text{G.C.D.}\ ((a_i/d_i), e)} \prod_{p|e}{}' \left(1 - \frac{1}{p^{r(p)}}\right) ,$$

where the dash (′) means that the product is taken over those $p|e$ such that $p|a_i/d_i$ or $p|\text{G.C.D.}\ (a_i/d_i, b_i/d_i)$, $i = 1, \cdots, n$, as $p|\text{G.C.D.}$ $(a_i/d_i, e, h_i)$ if and only if $p|\text{G.C.D.}\ (a_i/d_i, e, b_i/d_i)$ because $(d/d_i)h_i \equiv b_i/d_i$ (mod G.C.D. $(a_i/d_i, e)$ and G.C.D. $(d/d_i, a_i/d_i) = 1$ $(i = 1, \cdots, n)$. Also $r(p)$ is the number of a_i/d_i $(i = 1, \cdots, n)$ not divisible by p.

Next we need the number of incongruent $\boldsymbol{x}$ modulo de such that

$$a_ix_i \equiv 0 \pmod{de}\ (i = 1, \cdots, n) .$$

This is just

$$\begin{aligned} &\prod_{i=1}^{n} \text{G.C.D.}\ (a_i, de) \\ &= \prod_{i=1}^{n} d_i\ \text{G.C.D.}\ (a_i/d_i, (d/d_i)e) \\ &= \prod_{i=1}^{n} d_i\ \text{G.C.D.}\ (a_i/d_i, e) . \end{aligned}$$

Hence by Theorem 5 the required number of solutions is

$$\prod_{i=1}^{n} (d_i\ e) \cdot \prod_{p|e}{}' \left(1 - \frac{1}{p^{r(p)}}\right) ,$$

where the dash (′) means that the product is taken over those $p|e$ such that $p|a_i/d_i$ or $p|\text{G.C.D.}\ (a_i/d_i, b_i/d_i)$, $i = 1, \cdots, n$. This number is

$$\prod_{i=1}^{n} d_i \cdot e^n \cdot \prod_{p|e} \left(1 - \frac{\nu_1(p) \cdots \nu_n(p)}{p^n}\right),$$

as

$$\nu_i(p) = \begin{cases} 1, & p \nmid a_i/d_i, \\ 0, & p \mid a_i/d_i,\ p \nmid b_i/d_i\ , \\ p, & p \mid a_i/d_i,\ p \mid b_i/d_i\ . \end{cases}$$

Finally we state that all formulas are easily modified if we do not assume $g = \text{G.C.D.}\ (l_1, \cdots, l_m, d) = 1$ (See introduction, Theorem 1). For example we list

THEOREM 2′. *If* $\mathscr{S}_d^c \neq \varnothing$ *the minimum modulus* M_d^c *with respect to* (1.1) *is given by*

$$M_d^c = d_1 \prod_{p \mid e, N(pd_1, L'/g) > 0} p\ .$$

COROLLARY 4′. *If* G.C.D. $(d, e) = 1$ *then the number* $\mathfrak{N}_d^c$ *of solutions of* (1.1) *modulo* M_d^c *is*

$$\mathfrak{N}_d^c = N(d, L'/g) \prod_{p \mid e, N(pd_1, L'/g) > 0} p^n \left(1 - \frac{1}{p^{r(p, L/g)}}\right)\ .$$

REFERENCES

1. T. M. Apostol, *Euler's $\varnothing$ − function and separable Gauss sums*, Proc. Amer. Math. Soc., **24** (1970), 482-485.

2. L. E. Dickson, *History of the Theory of Numbers*, Chelsea N.Y., (1952), 88-93.

3. D. N. Lehmer, *Certain theorems in the theory of quadratic residues*, Amer Math. Monthly, **20** (1913), 155-156.

4. H. J. S. Smith, *On systems of linear indeterminate equations and congruences*, Phil. Trans. Lond., **151** (1861), 293-326. (Collected Mathematical Papers Vol. 1, Chelsea N. Y. (1965), 367-409.)

5. R. Spira, *Elementary problem no. E1730*, Amer. Math. Monthly, **72** (1965), 907.

6. H. Stevens, *Generalizations of the Euler $\varnothing$ − function*, Duke Math. J., **38** (1971), 181-186.

Received November 30, 1970, and in revised form April, 1971. This research was supported by a National Research Council of Canada Grant (No. A-7233).

CARLETON UNIVERSITY

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics
Vol. 39, No. 1 May, 1971