PACIFIC JOURNAL OF MATHEMATICS
Vol. 55, No. 1, 1974

LINEAR *GCD* EQUATIONS

DAVID JACOBSON

Let R be a GCD domain. Let A be an $m \times n$ matrix and B an $m \times 1$ matrix with entries in R. Let $c \neq 0$, $d \in R$. We consider the linear GCD equation $GCD(AX + B, c) = d$. Let S denote its set of solutions. We prove necessary and sufficient conditions that S be nonempty. An element t in R is called a solution modulus if $X + tR^n \subseteq S$ whenever $X \in S$. We show that if c/d is a product of prime elements of R, then the ideal of solution moduli is a principal ideal of R and its generator t_0 is determined. When R/t_0R is a finite ring, we derive an explicit formula for the number of distinct solutions (mod t_0) of $GCD\ (AX + B, c) = d$.

1. Introduction. Let R be a GCD domain. As usual GCD $(a_1, \cdots, a_m)$ will denote a greatest common divisor of the finite sequence of elements $a_1, \cdots, a_m$ of R.

Let A be an $m \times n$ matrix with entries a_{ij} in R and let B be an $m \times 1$ matrix with entries b_i in R for $i = 1, \cdots, m$; $j = 1, \cdots, n$. Let $c \neq 0$, d be elements of R. In this paper we consider the "linear GCD equation"

$$(1.1)\qquad \begin{aligned} GCD(a_{11}x_1 + \cdots + a_{1n}x_n + b_1, \cdots, \\ a_{m1}x_1 + \cdots + a_{mn}x_n + b_m, c) = d\ . \end{aligned}$$

Letting X denote the column of unknows $x_1, \cdots, x_n$ in (1.1), we shall find it convenient to abbreviate the equation (1.1) in matrix notation by

$$(1.2)\qquad GCD(AX + B, c) = d\ .$$

Of course we allow a slight ambiguity in viewing (1.1) as an equation, since the GCD is unique only up to a unit.

Let R^n denote the set of $n \times 1$ matrices with entries in R. We let $S \equiv S(A, B, c, d)$ denote the set of all solutions of (1.1), that is

$$S = \{X \in R^n \mid GCD(AX + B, c) = d\}\ .$$

If S is nonempty, we say that (1.1) or (1.2) is solvable. Note that X satisfies $GCD(AX + B, d) = d$ if and only if X is a solution of the linear congruence system $AX + B \equiv 0(\text{mod}\ d)$.

We show in Proposition 1 that if (1.1) is solvable, then $d \mid c$, $AX + B \equiv 0(\text{mod}\ d)$ has a solution and $GCD(A, d) = GCD(A, B, c)$. Here $GCD(A, d) = GCD(a_{11}, \cdots, a_{1n}, \cdots, a_{m1}, \cdots, a_{mn}, d)$ and $GCD(A, B, c) = GCD(A, b_1, \cdots, b_m, c)$. Conversely we show in Proposition 3 that if the above conditions hold and $e = c/d$ is atomic, that is e is a product of prime elements of R, then (1.1) is solvable. (Also see Proposition 4).

Let the solution set S of (1.1) be nonempty. We say that t in R is a solution modulus of (1.1) if given X in S and $X \equiv X'(\text{mod } t)$, then X' is in S. We let $M \equiv M(A, B, c, d)$ denote the set of all solution moduli of (1.1). We show in Theorem 2 that M is an ideal of R and if $e = c/d$ is atomic, then M is actually a principal ideal generated by $d/g(p_1 \cdots p_k)$, where $g = GCD(A, d)$ and $\{p_1, \cdots, p_k\}$ is a maximal set of nonassociated prime divisors of e such that for each p_i, the system $AX + B \equiv 0(\text{mod } dp_i)$ is solvable. This generator $d/g(p_1 \cdots p_k)$ denoted by t_0 is called the minimum modulus of (1.1).

In § 4 we assume that R/t_0R is a finite ring and we derive an explicit formula for the number of distinct equivalence classes of $R^n(\text{mod } t_0)$ comprising S. We denote this number by $N_{t_0} \equiv N_{t_0}(A, B, c, d)$. Let $A' = A/g$ and $d' = d/g$. Let $L = \{X + d'R^n \mid A'X \equiv 0(\text{mod } d')\}$ and $L_i = \{X + d'R^n \mid A'X \equiv 0(\text{mod } d'p_i)\}$ for $i = 1, \cdots, k$. In Theorem 3 we show that

$$N_{t_0} = |L| \prod_{i=1}^{k} (|R/p_iR|^n - |R/p_iR|^{n-(r_i+s_i)}) \tag{1.3}$$

where r_i is rank $A'(\text{mod } p_i)$ and s_i is the dimension of the R/p_iR vector space L/L_i.

The formula (1.3) is applied in some important cases. For example in Corollary 6 we determine N_{t_0} when R is a principal ideal domain.

This paper is an extension and generalization to GCD domains, of the results obtained over the ring of integers Z in [2].

2. Solvability of $GCD\ (AX + B, c) = d$.

PROPOSITION 1. *If $GCD\ (AX + B, c) = d$ is solvable, then the following conditions hold.*

(2.1) (i) $d \mid c$,

(ii) $AX + B \equiv 0(\text{mod } d)$ *is solvable,*

(iii) $GCD(A, d) = GCD(A, B, c)$.

Proof. Let X satisfy $GCD(AX + B, c) = d$. Then clearly (i) $d \mid c$ and (ii) $AX + B \equiv 0(\text{mod } d)$. Let $AX + B = dU$ where U is an $m \times 1$ matrix with entries u_i for $i = 1, \cdots, m$. Then $GCD(dU, c) = GCD(du_1, \cdots, du_m, c) = d$. Let $g = GCD(A, d)$ and $h = GCD(A, B, c)$. Then $B \equiv 0(\text{mod } g)$ as $AX - dU = B$ and $g \mid c$ as $d \mid c$, which shows that $g \mid h$. Also $dU \equiv 0(\text{mod } h)$, so that $h \mid GCD(dU, c)$, that is $h \mid d$. Thus $h \mid g$, which proves (iii).

PROPOSITION 2. *Let e in R have the following property*

(I) *$GCD(AX+B, e)=1$ is solvable whenever $GCD(A, B, e)=1$. Suppose that $c=de$, $AX+B\equiv 0(\mathrm{mod}\ d)$ is solvable and $GCD(A, d)=GCD(A, B, c)$. Then $GCD(AX+B, c)=d$ is solvable.*

Proof. There exist X' in R^n and V in R^m such that $AX'+B=dV$. Let $g=GCD(A, d)$ and let A' denote the matrix with entries a_{ij}/g and B' the matrix with entries b_i/g for $i=1, \cdots, m$; $j=1, \cdots, n$. Then $A'X'+B'=d'V$ where $d'=d/g$. We claim that $GCD(A', V, e)=1$. For let h be any divisor of $GCD(A', V, e)$. Then $B'\equiv 0(\mathrm{mod}\ h)$ and $h \mid GCD(A', B', c')$ where $c'=d'e$. However, $GCD(A', B', c')=1$ as $g=GCD(A, B, c)$. Hence h is a unit, that is $GCD(A', V, e)=1$. So by property (I), there is a Y in R^n such that $GCD(A'Y+V, e)=1$. Thus $GCD(A(d'Y)+dV, de)=d$ and if we set $X=X'+d'Y$, then $GCD(AX+B, c)=d$, establishing the proposition.

We show in Proposition 3 that if e is atomic, then e satisfies property (I).

We require the following useful lemmas.

LEMMA 1. *Let $e=p_1\cdots p_k$ be a product of nonassociated prime elements $p_1, \cdots, p_k$ in R. If $GCD(A, B, e)=1$, then $GCD(AX+B, e)=1$ is solvable.*

Proof. Let $GCD(A, B, e)=1$. We use induction on k. Let $k=1$. If $GCD(B, p_1)=1$, then $X=0$ satisfies $GCD(AX+B, p_1)=1$. Suppose that $B\equiv 0(\mathrm{mod}\ p_1)$. Then $GCD(A, p_1)=1$. Hence there is a j such that $GCD(a_{1j}, \cdots, a_{mj}, p_1)=1$. Let X^j in R^n have a 1 in the jth position and o's elsewhere. Then $GCD(AX^j+B, p_1)=GCD(AX^j, p_1)=1$. Thus $GCD(AX+B, p_1)=1$ is solvable. Now let $k>1$ and let $e'=p_1\cdots p_{k-1}$. By the induction assumption there is X' in R^n such that $GCD(AX'+B, e')=1$. Let $B'=AX'+B$. We claim that $GCD(Ae', B', p_k)=1$. If $GCD(A, p_k)=1$, then $GCD(Ae', B', p_k)=1$. Suppose that $A\equiv 0(\mathrm{mod}\ p_k)$. If $B'\equiv 0(\mathrm{mod}\ p_k)$, then $B\equiv 0(\mathrm{mod}\ p_k)$, contradicting the hypothesis that $GCD(A, B, e)=1$. Hence $GCD(B', p_k)=1$, establishing the claim. So there exists a Y in R^n such that $GCD((Ae')Y+B', p_k)=1$. Let $X=X'+e'Y$. Then $X\equiv X'(\mathrm{mod}\ e')$ yields that $AX+B\equiv B'(\mathrm{mod}\ e')$. Thus $GCD(AX+B, e')=1$ since $GCD(B', e')=1$. Also

$$GCD(AX+B, p_k)=GCD((Ae')Y+B', p_k)=1\ ,$$

so that $GCD(AX+B, e'p_k)=1$, completing the proof.

LEMMA 2. *Suppose that e is an atomic element of R.*

(*) *Let* $\{p_1, \cdots, p_k\}$ *be a maximal set of nonassociated prime divisors of* e *such that for each* p_i, *the system* $AX + B \equiv 0(\text{mod } dp_i)$ *is solvable .*

Then X *is a solution of* $GCD(AX + B, c) = d$ *if and only if* $GCD(AX + B, de_0) = d$, *where* $c = de$ *and* $e_0 = p_1 \cdots p_k$.

Proof. Since e is atomic, it is clear that we may select a set $\{p_1, \cdots, p_k\}$ as defined in (*). If this set is empty, we let $e_0 = 1$. Suppose that X satisfies $GCD(AX + B, c) = d$. Then there is U in R^m such that $AX + B = dU$ and $GCD(U, e) = 1$. Since $e_0 \mid e$, $GCD(U, e_0) = 1$ and thus $GCD(dU, de_0) = d$, that is, $GCD(AX + B, de_0) = d$.

Conversely let X satisfy $GCD(AX + B, de_0) = d$. Then $AX + B = dU$ and $GCD(U, e_0) = 1$. Suppose there is a prime $p \mid e$ and $U \equiv 0(\text{mod } p)$. Then $AX + B \equiv 0(\text{mod } dp)$ and the maximal property of the set $\{p_1, \cdots, p_k\}$ shows that p is an associate of some p_i. So $U \equiv 0(\text{mod } p_i)$, contradicting that $GCD(U, e_0) = 1$. Hence $GCD(U, p) = 1$ for all primes $p \mid e$ and thus $GCD(U, e) = 1$, that is $GCD(AX + B, c) = d$.

PROPOSITION 3. *Suppose that* $c = de$, $AX + B \equiv 0(\text{mod } d)$ *is solvable and* $GCD(A, d) = GCD(A, B, c)$. *If* e *is atomic, then* $GCD(AX + B, c) = d$ *is solvable.*

Proof. Let e be atomic. By Proposition 2 it suffices to show that e satisfies property (I). Thus let $GCD(A_0, B_0, e) = 1$ where A_0 is an $m \times n$ matrix and B_0 is an $m \times 1$ matrix. By Lemma 2, $GCD(A_0X + B_0, e) = 1$ is solvable if and only if $GCD(A_0X + B_0, e_0) = 1$ is solvable where $e_0 = p_1 \cdots p_k$ is a product of nonassociated prime divisors of e. However by Lemma 1, $GCD(A_0X + B_0, e_0) = 1$ is solvable since $GCD(A_0, B_0, e_0) = 1$. Thus (I) holds and $GCD(AX + B, c) = d$ is solvable.

THEOREM 1. *Let* R *be a GCD domain. Consider the following condition*

(II) $GCD(a_1x + b_1, \cdots, a_mx + b_m, c) = 1$ *is solvable if*

$$GCD(a_1, \cdots, a_m, b_1, \cdots, b_m, c) = 1 ;$$

(i) *If* R *satisfies* (II), *then* $GCD(AX + B, c) = 1$ *is solvable whenever* $GCD(A, B, c) = 1$.

(ii) *If* R *is a Bezout domain such that* $GCD(ax + b, c) = 1$ *is solvable whenever* $GCD(a, b, c) = 1$, *then* R *satisfies* (II).

Proof. (i) Let R satisfy (II). Let $GCD(A, B, c) = 1$ where A

is an $m \times n$ matrix. We prove that $GCD(AX + B, c) = 1$ is solvable by induction of n. For $n = 1$, solvability is granted by the supposition (II). Let $n > 1$ and let A' denote the $m \times (n-1)$ matrix with entries $a_{i,j+1}$ for $i = 1, \cdots, m$; $j = 1, \cdots, n-1$. If $c' = GCD(a_{11}, \cdots, a_{1m}, c)$, then $GCD(A', B, c') = 1$. Hence by the induction assumption, there exist $x_2, \cdots, x_n$ in R such that $GCD(a_{12}x_2 + \cdots + a_{1n}x_n + b_1, \cdots, a_{m1}x_2 + \cdots + a_{mn}x_n + b_m, c') = 1$. If $b'_i = a_{i2}x_2 + \cdots + a_{in}x_n + b_i$ for $i = 1, \cdots, m$, then $GCD(a_{11}, \cdots, a_{m1}, b'_1, \cdots, b'_m, c) = 1$. Thus by (II), there exists x_1 in R such that $GCD(a_{11}x_1 + b'_1, \cdots, a_{m1}x_1 + b'_m, c) = 1$. So if X in R^n has entries $x_1, x_2, \cdots, x_n$, then $GCD(AX + B, c) = 1$, completing the proof of (i).

(ii) Let R be a Bezout domain, that is a domain in which every finitely generated ideal is principal. Suppose that R has the property that $GCD(ax + b, c) = 1$ is solvable if $GCD(a, b, c) = 1$. Let

$$GCD(a_1, \cdots, a_m, b_1, \cdots, b_m, c) = 1 .$$

Let A and B denote the $m \times 1$ matrices with entries $a_1, \cdots, a_m$ and $b_1, \cdots, b_m$ respectively. Then by [3, Theorem 3.5], there exists an invertible $m \times m$ matrix P such that PA has entries $a, 0, \cdots, 0$. Also it is clear that $GCD(PA, PB, c) = 1$. Let PB have entries $b, b'_2, \cdots, b'_m$. Thus by hypothesis, $GCD(ax + b, c') = 1$ is solvable where $c' = GCD(b'_2, \cdots, b'_m, c)$. Hence $GCD(Ax + B, c) = 1$ is solvable, that is R satisfies (II).

As an immediate consequence of the preceding propositions and Theorem 1, we state

PROPOSITION 4. *Let R be a UFD or a Bezout domain such that $GCD(ax + b, c) = 1$ is solvable if $GCD(a, b, c) = 1$. Then $GCD(AX + B, c) = d$ is solvable if and only if $d \mid c$, $AX + B \equiv 0 (\mathrm{mod}\ d)$ is solvable and $GCD(A, d) = GCD(A, B, c)$.*

We remark that we do not know whether there exists a GCD domain in which (II) is not valid. Any Bezout domain satisfying (II) is an elementary divisor domain [3, Theorem 5.2].

We conclude this section with the following result.

PROPOSITION 5. *Let R be a Bezout domain. Suppose that* (0) *$GCD(ax + b, c) = 1$ is solvable whenever $GCD(a, b) = 1$ and $a \mid c$. Then $GCD(ax + b, c) = 1$ is solvable whenever $GCD(a, b, c) = 1$.*

Proof. Let $GCD(a, b, c) = 1$. If $a' = GCD(a, c)$, then $GCD(a', b) = 1$ and $a' \mid c$. By the assumption (0), there is x' in R such that $GCD(a'x' + b, c) = 1$. If $u = a'x' + b$, then $a' \mid (u - b)$ and since R is a Bezout domain, there is an x in R such that $ax + b \equiv u (\mathrm{mod}\ c)$.

Thus $GCD(ax + b, c) = 1$ since $GCD(u, c) = 1$.

Let $a \mid c$ and let $\nu: R/cR \to R/aR$ be the epimorphism given by $\nu(r + cR) = r + aR$ for all r in R. Let G(resp. G') denote the group of units of R/cR(resp. R/aR). If $\nu': G \to G'$ is the induced homomorphism, then note that (0) is equivalent to the condition that $\nu'(G) = G'$. (See [5].)

3. The minimum modulus. Let the solution set S of $GCD(AX + B, c) = d$ be nonempty. Then

$$M = \{t \in R \mid X + tR^n \subseteq S \text{ for all } X \in S\}$$

is the set of solution moduli of $GCD(AX + B, c) = d$.

Note that $c \in M$ for if $X \in S$ and $X \equiv X'(\mathrm{mod}\, c)$, then $AX + B \equiv AX' + B(\mathrm{mod}\, c)$, so that $d = GCD(AX' + B, c)$.

It is obvious that $M = R$, that is $S = R^n$ if and only if $d = GCD(A, d) = GCD(A, B, c)$ and $GCD(A/d(X) + B/d, c/d) = 1$ for all X in R^n.

THEOREM 2. *Let R be a GCD domain. Let $GCD(AX + B, c) = d$ be solvable. Let $e = c/d = \prod_{i=1}^k e_i$. Let $\hat{e}_i = e_1 \cdots e_{i-1}e_{i+1} \cdots e_k$ for $i = 1, \cdots, k$.*

(1) *M is an ideal of R,*

(2) *$M \supseteq \bigcap_{i=1}^k M_i$ where M_i is the ideal of solution moduli for $GCD(AX + B, de_i) = d$.*

(3) *If each $\hat{e}_i$ satisfies property* (I) *of Proposition* 2, *then $M = \bigcap_{i=1}^k M_i$ and M is a principal ideal if each M_i is principal.*

(4) *If e is atomic, then M is a principal ideal generated by $d/g(p_1 \cdots p_k)$ where $g = GCD(A, d)$ and $\{p_i, \cdots, p_k\}$ is defined in* (*) *of Lemma* 2.

Proof.

(1) As S is nonempty, the set M is well-defined and o, c belong to M. Let t_1, t_2 be in M and let $r \in R$. Let $X \in S$ and let $Y \in R^n$. Then $X + t_1Y \in S$ and hence $(X + t_1Y) + t_2(-Y) \in S$, that is $X + (t_1 - t_2)Y \in S$ which shows that $t_1 - t_2 \in M$. Also $X + t_1(rY) \in S$, that is $X + (t_1r)Y \in S$. So $t_1r \in M$ and thus M is an ideal of R.

(2) As $d \mid c$ we let $c = de$. Let S_i denote the solution set of $GCD(AX + B, de_i) = d$ where $e = \prod_{i=1}^k e_i$. Then clearly $S = \bigcap_{i=1}^k S_i$. Let $t \in \bigcap_{i=1}^k M_i$. Let $X \in S$ and let $Y \in R^n$. Then $X + tY \in \bigcap_{i=1}^k S_i$ since $X \in \bigcap_{i=1}^k S_i$. So $X + tY \in S$, that is $t \in M$, which proves that $M \supseteq \bigcap_{i=1}^k M_i$.

(3) Assume that each $\hat{e}_i$ satisfies property (I). We prove that $M \subseteq M_i$ for $i = 1, \cdots, k$. As $g = GCD(A, d) = GCD(A, B, c)$, let $A' = A/g$, $B' = B/g$, and $d' = d/g$. Let i be fixed and let $X_i \in S_i$.

Then $A'X_i + B' = d'U$ where $GCD(U, e_i) = 1$. We claim that $GCD(e_iA', U, \hat{e}_i) = 1$. For let h be a divisor of $GCD(e_iA', U, \hat{e}_i)$. Then $A' \equiv 0(\text{mod}\, h)$ since $GCD(h, e_i) = 1$. Thus $h \mid GCD(A', B', d'e)$, that is $h \mid 1$. So by assumption there exists X' in R^n such that

$$GCD((e_iA')X' + U, \hat{e}_i) = 1 .$$

Let $X = X_i + d'e_iX'$. Then for $j = 1, \cdots, k$,

$$\begin{aligned} &GCD(A'X + B', d'e_j) \\ &\quad = d'\, GCD((e_iA')X' + U, e_j) = d' . \end{aligned}$$

Hence $X \in \bigcap_{j=1}^k S_j$, that is $X \in S$. Now let $t \in M$ and let $Y \in R^n$. Then $X + tY \in S$ and so $X + tY \in S_i$. However, $X + tY \equiv X_i + tY(\text{mod}\, d'e_i)$ and thus $X_i + tY \in S_i$, that is $t \in M_i$, which proves that $M \subseteqq M_i$. So by (2), $M = \bigcap_{i=1}^k M_i$. Moreover, if each M_i is a principal ideal, say $M_i = t_iR$, then $\bigcap_{i=1}^k M_i$ is a principal ideal generated by the $LCM(t_1, \cdots, t_k)$.

(4) Let t be any element of M. We show that $d/g \mid t$ where $g = GCD(A, d)$. First note that S is the solution set of $GCD(A'X + B', d'e) = d'$ where $A' = A/g$, $B' = B/g$, and $d' = d/g$. Let $X \in S$ and let $A'X + B' = d'U$. Then $GCD(A'(X + tY) + B', d'e) = d'$ for all Y in R^n. So $GCD((A't)Y + d'U, d'e) = d'$ and thus $(A't)Y \equiv 0(\text{mod}\, d')$ for all Y in R^n. Hence $A't \equiv 0(\text{mod}\, d')$ and since $GCD(A', d') = 1$, it follows that $d' \mid t$.

Now suppose that e is atomic. By Lemma 2, S is also the solution set of $GCD(A'X + B', d'e_0) = d'$ where $e_0 = p_1 \cdots p_k$ and $\{p_1, \cdots, p_k\}$ is defined in (*). Thus M is also the ideal of solution moduli of $GCD(A'X + B', d'e_0) = d'$. Let M_i' denote the ideal of solution moduli of $GCD(A'X + B', d'p_i) = d'$ for $i = 1, \cdots, k$. Then Lemma 1 shows that (3) can be applied to yield that $M = \bigcap_{i=1}^k M_i'$. We prove that each M_i' is a principal ideal generated by $d'p_i$. Clearly $d'p_i \in M_i'$ for $i = 1, \cdots, k$. Let i be fixed and let t be any element in M_i'. Then as shown earlier, $d' \mid t$ say $t = d't'$. By (*) there exists X in R^n such that $A'X + B' \equiv 0(\text{mod}\, d'p_i)$. Thus $GCD(A', p_i) = 1$ since $GCD(A', B', d'e) = 1$. So there is a j for which $GCD(A'E_j, p_i) = 1$ where E_j is the $n \times 1$ matrix with 1 in the jth position and o's elsewhere.

Now assume that $GCD(t', p_i) = 1$. Let $X' = X + tE_j$. Then $GCD(A'(X' - X), d'p_i) = d'\, GCD(t'A'E_j, p_i) = d'$ since $GCD(t'A'E_j, p_i) = 1$. So $GCD(A'X' - A'X, d'p_i) = d'$ and thus $GCD(A'X' + B', d'p_i) = d'$ as $B \equiv -A'X(\text{mod}\, d'p_i)$. Hence $GCD(A'(X' + t(-E_j)) + B', d'p_i) = d'$ since $t \in M_i'$. That is $GCD(A'X + B', d'p_i) = d'$ and thus $d'p_i \mid d'$, which contradicts that p_i is a nonunit. So the assumption that $GCD(t', p_i) = 1$ is untenable, that is $p_i \mid t'$. Thus $d'p_i \mid t$ proving that

$M_i' = d'p_iR$. However $M = \bigcap_{i=1}^k M_i'$, so that M is a principal ideal generated by the $LCM(d'p_1, \cdots, d'p_k)$, that is M is generated by $d'p_1 \cdots p_k$.

The generator $d'p_1 \cdots p_k$ of M is called the minimum modulus of $GCD(AX + B, de) = d$.

4. The number of solutions with respect to a modulus. Let $GCD(AX + B, c) = d$ be solvable where $e = c/d$ is atomic. If t in R is a solution modulus of $GCD(AX + B, c) = d$, then S consists of equivalence classes of $R^n(\text{mod}\, t)$. If R/tR is also a finite ring, we let $N_t \equiv N_t(A, B, c, d)$ denote the number of distinct equivalence classes of $R^n(\text{mod}\, t)$ comprising S.

For R/tR finite, let $|t| = |R/tR|$ denote the number of elements in R/tR. Note that if $t_0 \mid t$, then each equivalence class of $R^n(\text{mod}\, t_0)$ consists of $|t/t_0|^n = (|t|/|t_0|)^n$ classes of $R^n(\text{mod}\, t)$. Thus if t is a solution modulus and t_0 denotes the mininum modulus of $GCD(AX + B, c) = d$, then $N_t = |t/t_0|^n N_{t_0}$. In Theorem 3, we explicitly determine N_{t_0}.

The following lemma is also of independent interest.

LEMMA 3. *Let R be a GCD domain and suppose that R/dR is a finite ring. Let $p_1, \cdots, p_k$ be nonassociated elements such that R/p_iR is a finite field for $i = 1, \cdots, k$. Let A be an $m \times n$ matrix and let r_i denote the rank of $A(\text{mod}\, p_i)$ for $i = 1, \cdots, k$. Let $\mathscr{L} = \{X \in R^n \mid AX \equiv 0(\text{mod}\, d)\}$ and $L = \{X + dR^n \mid X \in \mathscr{L}\}$. Let $e_0 = \prod_{i=1}^k p_i$ and let $\mathscr{L}' = \{X \in R^n \mid AX \equiv 0(\text{mod}\, de_0)\}$ and $L' = \{X + de_0R^n \mid X \in \mathscr{L}'\}$. Let $\mathscr{L}_i = \{X \in R^n \mid AX \equiv 0(\text{mod}\, dp_i)\}$ and $L_i = \{X + dR^n \mid X \in \mathscr{L}_i\}$ for $i = 1, \cdots, k$. Let $H = \{X + e_0R^n \mid X \in \mathscr{L}'\}$ and $H_i = \{X + p_iR^n \mid X \in \mathscr{L}_i\}$ for $i = 1, \cdots, k$. Then*

(1) $$|L'| = |L|\,|H|$$

and

$$|H| = \prod_{i=1}^{k} |H_i|\,.$$

(2) *L/L_i is an R/p_iR vector space of dimension s_i and $|H_i| = |R/p_iR|^{n-(r_i+s_i)}$ for $i = 1, \cdots, k$.*

(3) *$s_i = 0$ if and only if for each X in $\mathscr{L}$ there exists X' in $\mathscr{L}_i$ such that $X' \equiv X(\text{mod}\, d)$.*

(4) *If $GCD(d, p_i) = 1$, then $s_i = 0$.*

(5) *$|L| = 1$ if and only if $n = \text{rank}\, A(\text{mod}\, p)$ for each prime $p \mid d$.*

Proof.

(1) In the obvious way, L, L', and H are R-modules. Let $\sigma: L' \to H$ denote the R-homomorphism defined by $\sigma(X + de_0R^n) = X + e_0R^n$ for all X in $\mathscr{L}'$. Then clearly $\operatorname{Ker}\sigma = \{e_0Y + de_0R^n \mid Y \in \mathscr{L}\}$ so that $L \cong \operatorname{Ker}\sigma$ under the R-isomorphism $\tau: L \to \operatorname{Ker}\sigma$ defined by $\tau(Y + dR^n) = e_0Y + de_0R^n$ for all Y in $\mathscr{L}$. Thus $|L'| = |L||H|$ since $\operatorname{Im}\sigma = H$. We now show that H is isomorphic to $\bigoplus_{i=1}^k H_i$, the direct sum of the R-modules H_i. Let $\gamma: H \to \bigoplus_{i=1}^k H_i$ denote the R-homomorphism defined by $\gamma(X + e_0R^n) = (X + p_1R^n, \cdots, X + p_kR^n)$ for all X in $\mathscr{L}'$. If $X + e_0R^n \in \operatorname{Ker}\gamma$, then $X \equiv 0(\operatorname{mod} p_i)$ for $i = 1, \cdots, k$, that is $X \equiv 0(\operatorname{mod} e_0)$, which shows that γ is $1-1$. To show that $\operatorname{Im}\gamma = \bigoplus_{i=1}^k H_i$, let $X_i \in \mathscr{L}_i$ for $i = 1, \cdots, k$. Since R/dR is finite, it is easy to verify that d is atomic. Thus let $d = d_0\prod_{i=1}^k p_i^{m_i}$ where $m_i \geqq 0$ and $GCD(d_0, p_i) = 1$. By the Chinese remainder theorem there exists X in R^n such that $X \equiv 0(\operatorname{mod} d_0)$ and $X \equiv X_i(\operatorname{mod} p_i^{m_i+1})$ for $i = 1, \cdots, k$. However, $AX_i \equiv 0(\operatorname{mod} p_i^{m_i+1})$ for $i = 1, \cdots, k$, so that $AX \equiv 0 \operatorname{mod} (d_0\prod_{i=1}^k p_i^{m_i+1})$, that is $AX \equiv 0(\operatorname{mod} de_0)$. Thus $X + e_0R^n \in H$ and $\gamma(X + e_0R^n) = (X_1 + p_1R^n, \cdots, X_k + p_kR^n)$. Hence γ is an isomorphism and $|H| = \prod_{i=1}^k |H_i|$.

(2) Let $L_i' = \{X + dp_iR^n \mid X \in \mathscr{L}_i\}$ for $i = 1, \cdots, k$. Let i be fixed. Let $\nu: L_i' \to L_i$ denote the R-homomorphism defined by $\nu(X + dp_iR^n) = X + dR^n$ for all X in $\mathscr{L}_i$. Then clearly $\operatorname{Ker}\nu = \{dY + dp_iR^n \mid AY \equiv 0(\operatorname{mod} p_i)\}$ and it follows that

$$|\operatorname{Ker}\nu| = |R/p_iR|^{n-r_i} \equiv |p_i|^{n-r_i}$$

where $r_i = \operatorname{rank} A(\operatorname{mod} p_i)$. Thus $|L_i'| = |p_i|^{n-r_i}|L_i|$ since $\operatorname{Im}\nu = L_i$. However by (1), $|L_i'| = |L||H_i|$. Also since L_i is an R-submodule of L, the quotient module L/L_i is defined and $|L| = |L_i||L/L_i|$. Thus we obtain that $|H_i||L/L_i| = |p_i|^{n-r_i}$. We now show that L/L_i is an R/p_iR vector space. Let $\langle X\rangle = X + dR^n$ for X in R^n. Then $L/L_i = \{\langle X\rangle + L_i \mid X \in \mathscr{L}\}$. For r in R, let $\bar{r} = r + p_iR$ in R/p_iR. We define $\bar{r}(\langle X\rangle + L_i) = \langle rX\rangle + L_i$ for all r in R and X in $\mathscr{L}$. We claim that this is a well-defined R/p_iR multiplication on L/L_i. For let $\bar{r} = \bar{r}'$ and $\langle X\rangle + L_i = \langle X'\rangle + L_i$, where $r, r' \in R$ and $X, X' \in \mathscr{L}$. Then $r - r' \equiv o(\operatorname{mod} p_i)$ and $\langle X\rangle - \langle X'\rangle \in L_i$, that is $\langle X - X'\rangle \in L_i$. Thus there exists Y in $\mathscr{L}_i$ such that $\langle X - X'\rangle = \langle Y\rangle$. We must show that $\langle rX\rangle + L_i = \langle r'X'\rangle + L_i$, that is $\langle rX - r'X'\rangle \in L_i$. We write $rX - r'X' = (r - r')X + r'(X - X')$. However, $X - X' \equiv Y(\operatorname{mod} d)$ and thus $r(X - X') \equiv rY(\operatorname{mod} d)$. So $rX - r'X' \equiv (r - r')X + rY(\operatorname{mod} d)$ and $(r - r')X + rY \in \mathscr{L}_i$. Hence $\langle rX - r'X'\rangle \in L_i$, which establishes the claim. It follows immediately that L/L_i is an R/p_iR vector space since L/L_i is an R-module.

Let s_i denote the dimension of the R/p_iR vector space L/L_i.

Then $|L/L_i| = |p_i|^{s_i}$ and as $|H_i||L/L_i| = |p_i|^{n-r_i}$, we obtain that $|H_i||p_i|^{s_i} = |p_i|^{n-r_i}$. Thus $0 \leqq s_i \leqq n - r_i$ and $|H_i| = |p_i|^{n-(r_i+s_i)}$, which completes the proof of (2).

(3) As $|L| = |L_i||p_i|^{s_i}$, it is immediate that $s_i = 0$ if and only if $L = L_i$, that is if and only if for each X in $\mathscr{L}$ there exists X' in $\mathscr{L}_i$ such that $X' \equiv X (\text{mod } d)$.

(4) Suppose that $GCD(d, p_i) = 1$. Let $X \in \mathscr{L}$. By the Chinese remainder theorem there exists X' in R^n such that $X' \equiv X(\text{mod } d)$ and $X' \equiv 0(\text{mod } p_i)$. Thus $AX' \equiv 0(\text{mod } dp_i)$, so that $s_i = 0$ by (3).

(5) Let p be a prime dividing d and let $d = d_1 p$. Then $L = \{X + d_1 p R^n \mid X \in \mathscr{L}\}$. However as shown in the proof of (2), $|L| = |p|^{n-r_0}|L_0|$ where $r_0 = \text{rank } A(\text{mod } p)$ and $L_0 = \{X + d_1 R^n \mid X \in \mathscr{L}\}$. Thus if $|L| = 1$, then $n = \text{rank } A(\text{mod } p)$ for any prime $p \mid d$. The converse is trivial.

THEOREM 3. *Let R be a GCD domain. Let $GCD(AX + B, c) = d$ be solvable and suppose that $e = c/d$ is atomic. Let $A' = A/g$ and $d' = d/g$ where $g = GCD(A, d)$. Let $t_0 = d' \prod_{i=1}^{k} p_i$ denote the minimum modulus of $GCD(AX + B, c) = d$ where $\{p_1, \cdots, p_k\}$ is defined in (*) of Lemma 2. Suppose that R/t_0R is a finite ring. Let $L = \{X + d'R^n \mid A'X \equiv 0(\text{mod } d')\}$ and $L_i = \{X + d'R^n \mid A'X \equiv 0(\text{mod } d'p_i)\}$ for $i = 1, \cdots, k$. Then*

$$N_{t_0} = |L| \prod_{i=1}^{k} (|p_i|^n - |p_i|^{n-(r_i+s_i)}) \tag{4.1}$$

where r_i denotes rank $A'(\text{mod } p_i)$ *and s_i denotes the dimension of the R/p_iR vector space L/L_i.*

Proof. Let S denote the solution set of $GCD(AX + B, c) = d$. As $g = GCD(A, B, c)$, let $B' = B/g$. Then by Lemma 2, S is also the solution set of $GCD(A'X + B, d'e_0) = d'$ where $e_0 = \prod_{i=1}^{k} p_i$. Let $\mathscr{S}$ denote the set of X in R^n such that $A'X + B' \equiv 0(\text{mod } d')$. Let $\mathscr{S}_i$ denote the set of X in R^n such that $A'X + B' \equiv 0(\text{mod } d'p_i)$ for $i = 1, \cdots, k$. It is clear that $S = \mathscr{S} \backslash \bigcup_{i=1}^{k} \mathscr{S}_i$. Let $T_0 = \{X + t_0R^n \mid X \in S\}$. Then $|T_0|$ is what we have denoted by N_{t_0}. Also let $T = \{X + t_0R^n \mid X \in \mathscr{S}\}$ and $T_i = \{X + t_0R^n \mid X \in \mathscr{S}_i\}$ for $i = 1, \cdots, k$. Hence $T_0 = T \backslash \bigcup_{i=1}^{k} T_i$ and by the method of inclusion and exclusion

$$N_{t_0} = |T_0| = \sum_{I} (-1)^{|I|} |T_I| \tag{4.2}$$

where the summation is over all subsets I of

$$I_k = \{1, \cdots, k\} \text{ and } T_I = \bigcap_{i=1} T_i .$$

Now let $\mathscr{S}_I = \bigcap_{i \in I} \mathscr{S}_i$ and $d'_I = d' \prod_{i \in I} p_i$ for each subset I of

I_k. Then it is easy to see that $\mathscr{S}_I$ is the set of X in R^n such that $A'X + B' \equiv 0(\text{mod } d'_I)$ and $T_I = \{X + t_0R^n \mid X \in \mathscr{S}_I\}$. Let $T'_I = \{X + d'_IR^n \mid X \in \mathscr{S}_I\}$ and let $I' = I_k \backslash I$. Then $|T_I| = |T'_I| \prod_{i \in I'} |p_i|^n$, since $X + d'_IR^n$ consists of $|t_0/d'_I|^n = \prod_{i \in I'} |p_i|^n$ distinct classes of $R^n(\text{mod } t_0)$.

Let $\mathscr{L}_I$ denote the set of X in R^n such that $A'X \equiv 0(\text{mod } d'_I)$. Let $L'_I = \{X + d'_IR^n \mid X \in \mathscr{L}_I\}$. As $\mathscr{S}_i$ is nonempty for $i = 1, \cdots, k$, an argument involving the Chinese remainder theorem shows that each $\mathscr{S}_I$ is nonempty. Hence it follows that $|T'_I| = |L'_I|$. Let $L = \{X + d'R^n \mid X \in \mathscr{L}_\phi\}$ and $L_i = \{X + d'R^n \mid X \in \mathscr{L}_{\{i\}}\}$ for $i = 1, \cdots, k$. Then (1) and (2) of Lemma 3 yield that $|L'_I| = |L| \prod_{i \in I} |p_i|^{n-(r_i+s_i)}$ where $r_i = \text{rank } A'(\text{mod } p_i)$ and $s_i =$ dimension of the R/p_iR vector space L/L_i.

Hence by (4.2),

$$N_{t_0} = |L| \sum_I (-1)^{|I|} \prod_{i \in I} |p_i|^{n-(r_i+s_i)} \prod_{i \in I'} |p_i|^n$$

where the summation is over all subsets I of I_k and $I' = I_k \backslash I$. Thus we may write

$$N_{t_0} = |L| \prod_{i=1}^{k} |p_i|^n \sum_I (-1)^{|I|} \prod_{i \in I} |p_i|^{-(r_i+s_i)}$$

where the summation is over all subsets I of I_k. However,

$$\prod_{i=1}^{k} (1 - |p_i|^{-(r_i+s_i)}) = \sum_I (-1)^{|I|} \prod_{i \in I} |p_i|^{-(r_i+s_i)} ,$$

which yields the formula (4.1) for N_{t_0}. This completes the proof of the theorem.

We remark that if $p_i^{m_i}$ is the highest power of p_i dividing d', then s_i is also the dimension of the R/p_iR vector space K_i^0/K_i where $K_i^0 = \{X + p_i^{m_i}R^n \mid A'X \equiv 0(\text{mod } p_i^{m_i})\}$ and

$$K_i = \{X + p_i^{m_i}R^n \mid A'X \equiv 0(\text{mod } p_i^{m_i+1})\} .$$

Also note that $r_i \geqq 1$ for $i = 1, \cdots, k$.

In Corollaries 1 and 2, the notation is the same as in Theorem 3.

COROLLARY 1. *Let $GCD(AX + B, c) = d$ be solvable and suppose that $e = c/d$ is atomic. Let R/t_0R be finite where $t_0 = d' \prod_{i=1}^{k} p_i$ is the minimum modulus of $GCD(AX + B, c) = d$.*

(i) *If $GCD(d', e) = 1$, then*

$$N_{t_0} = |L| \prod_{i=1}^{k} (|p_i|^n - |p_i|^{n-r_i}) . \tag{4.3}$$

(ii) *If $|L| = 1$, then*

$$N_{t_0} = \prod_{i=1}^{k} (|p_i|^n - |p_i|^{n-r_i}) , \tag{4.4}$$

where $r_i = n$ *if* $p_i \mid d'$.

(iii) *If* $n' = \text{rank } A' (\text{mod } p_i)$ *for* $i = 1, \cdots, k$, *where* n' *denotes the smaller of* m *and* n, *then*

$$N_{t_0} = |L| \prod_{i=1}^{k} (|p_i|^n - |p_i|^{n-n'}) . \tag{4.5}$$

(iv) $N_{t_0} = 1$ *if and only if* (a) $|L| = 1$ *and there exists no prime* $p \mid e$ *such that* $AX + B \equiv 0 (\text{mod } dp)$ *is solvable, or* (b) $n = 1$ *and* $|p| = 2$ *for any prime* $p \mid e$ *such that* $AX + B \equiv 0 (\text{mod } dp)$ *is solvable.*

Proof.

(i) If $GCD(d', p_i) = 1$, then (4) of Lemma 3 shows that $s_i = 0$ in (4.1). Hence if $GCD(d', e) = 1$, then $s_i = 0$ for $i = 1, \cdots, k$, which yields (4.3).

(ii) Suppose that $|L| = 1$. If $p_i \mid d'$, then $n = r_i$ by (5) of Lemma 3 and thus $s_i = 0$ since $s_i \leqq n - r_i$. However if $GCD(d', p_i) = 1$, then $s_i = 0$, so that (4.4) is immediate from (4.1).

In particular if $d = 1$, then N_{t_0} is given by (4.4). If A' is invertible (mod d'), then (4.4) also applies.

(iii) If $n = r_i$, then $s_i = 0$. If $m = r_i$, then the criterion in (3) shows that $s_i = 0$. Thus (4.5) follows from (4.1).

(iv) Suppose that $N_{t_0} = 1$. Then by (4.1), $|L| = 1$ and thus $s_i = 0$ for $i = 1, \cdots, k$. If p_i is a prime dividing e such that $AX + B \equiv 0 (\text{mod } dp_i)$ is solvable, then $|p_i|^n - |p_i|^{n-r_i} = 1$, so that $n = r_i = 1$ and $|p_i| = 2$. Thus either (a) or (b) holds. Conversely if (a) holds, then $N_{t_0} = 1$. If $n = 1$, then clearly $|L| = 1$ and hence (b) implies that $N_{t_0} = 1$.

COROLLARY 2. *Let* $GCD(AX + B, c) = d$ *be solvable and let* $e = c/d$. *Suppose that* R/cR *is a finite ring. Then*

$$N_c = |L| \, |ge|^n \prod_{i=1}^{k} (1 - |p_i|^{-(r_i + s_i)}) . \tag{4.6}$$

Proof. Since R/cR is finite, e is atomic. Thus $t_0 = d' \prod_{i=1}^{k} p_i$ is the minimum modulus of $GCD(AX + B, c) = d$. Also R/t_0R is finite since $t_0 \mid c$, so that N_{t_0} is given by (4.1). However $N_c = |c/t_0|^n N_{t_0}$, which yields the result (4.6).

COROLLARY 3. *Suppose that* R/cR *is a finite ring. Then* $GCD(a_1x_1 + \cdots + a_nx_n + b, c) = d$ *is solvable if and only if* $d \mid c$ *and* $GCD(a_1, \cdots, a_n, d) = GCD(a_1, \cdots, a_n, b, c)$. *Let* $a'_j = a_j/g$ *for* $j = 1, \cdots, n$

where $g = GCD(a_1, \cdots, a_n, d)$. *Let* $\{p_1, \cdots, p_k\}$ *be a maximal set of nonassociated prime divisors of* $e = c/d$ *such that* $GCD(a'_1, \cdots, a'_n, p_i) = 1$ *for* $i = 1, \cdots, k$. *Then*

$$N_c = |c|^{n-1}|ge|\prod_{i=1}^{k}(1 - |p_i|^{-1}) . \tag{4.7}$$

Proof. Suppose that $c = de$ and $g = GCD(a_1, \cdots, a_n, b, c)$. Since R/cR is finite, d is atomic and R/pR is a finite field for any prime $p \mid d$. Hence as $g \mid b$, a standard argument shows that $a_1x_1 + \cdots + a_nx_n + b \equiv o(\mathrm{mod}\ d)$ is solvable and has $|g||d|^{n-1}$ distinct solutions $(\mathrm{mod}\ d)$. Thus $GCD(a_1x_1 + \cdots + a_nx_n + b, c) = d$ is solvable since e is atomic. Let $d' = d/g$ and $b' = b/g$. Since $GCD(a'_1, \cdots, a'_n, d'p_i) = 1$ and $R/d'p_iR$ is finite, $a'_1x_1 + \cdots + a'_nx_n + b' \equiv 0(\mathrm{mod}\ d'p_i)$ is solvable for $i = 1, \cdots, k$. It follows that $t_0 = d'\prod_{i=1}^{k} p_i$ is the minimum modulus of $GCD(a_1x_1 + \cdots + a_nx_n + b, c) = d$. Let A' denote the $1 \times n$ matrix $(a'_1, \cdots, a'_n)$. Then rank $A'(\mathrm{mod}\ p_i) = 1$ for $i = 1, \cdots, k$. Also $a'_1x_1 + \cdots + a'_nx_n \equiv o(\mathrm{mod}\ d')$ has $|d'|^{n-1}$ distinct solutions $(\mathrm{mod}\ d')$. Thus by (iii) of Corollary 1,

$$N_{t_0} = |d'|^{n-1}\prod_{i=1}^{k}(|p_i|^n - |p_i|^{n-1}) ,$$

which yields (4.7).

COROLLARY 4. *Suppose that* R/cR *is a finite ring where* $c = de$. *Let* $g = GCD(a_1, \cdots, a_m, d)$ *and* $a'_i = a_i/g$ *for* $i = 1, \cdots, m$. *Then* $GCD(a_1x + b_1, \cdots, a_mx + b_m, c) = d$ *is solvable if and only if*

(1) $GCD(a_i, d) \mid b_i$ *for* $i = 1, \cdots, m$,

(2) $a'_ib_j \equiv a'_jb_i(\mathrm{mod}\ d)$ *for* $1 \leqq i < j \leqq m$,

(3) $g = GCD(a_1, \cdots, a_m, b_1, \cdots, b_m, c)$.

Let $\{p_1, \cdots, p_k\}$ *be a maximal set of nonassociated prime divisors of* e *such that for each* p_h, $GCD(a_i, dp_h) \mid b_i$ *for* $i = 1, \cdots, m$ *and* $a'_i \equiv a'_jb_i(\mathrm{mod}\ dp_h)$ *for* $1 \leqq i < j \leqq m$. *Then*

$$N_c = |ge|\prod_{h=1}^{k}(1 - |p_h|^{-1}) .$$

Proof. Let A and B denote the $m \times 1$ matrices with entries $a_1, \cdots, a_m$ and $b_1, \cdots, b_m$ respectively. Since R/dR is finite, the reader may easily verify that the system $Ax + B \equiv 0(\mathrm{mod}\ d)$ is solvable if and only if (1) and (2) hold. Thus as e is atomic, $GCD(Ax + B, c) = d$ is solvable if and only if (1), (2), and (3) hold. Let $GCD(Ax + B, c) = d$ be solvable and let $d' = d/g$. Then it follows that $t_0 = d'\prod_{h=1}^{k} p_h$ is the minimum modulus of $GCD(Ax + B, c) = d$. Let A' denote the $m \times 1$ matrix with entries $a'_1, \cdots, a'_m$. Then rank $A'(\mathrm{mod}\ p_i) = 1$ for

$i = 1, \cdots, k$. Also the system $A'x \equiv 0 (\text{mod } d')$ has only the solution $x \equiv o(\text{mod } d')$. Thus by (iii) of Corollary 1, $N_{t_0} = \prod_{h=1}^{k} (|p_h| - 1)$. Hence $N_c = |ge| \prod_{h=1}^{k} (1 - |p_h|^{-1})$.

COROLLARY 5. *Let $c = de$ where e is atomic. Let $g = GCD(a_1, \cdots, a_n, d)$ and $d' = d/g$. Suppose that $R/d'R$ is a finite ring. Then $GCD(a_1x_1 + b_1, \cdots, a_nx_n + b_n, c) = d$ is solvable if and only if $GCD(a_j, d) \mid b_j$ for $j = 1, \cdots, n$ and $g = GCD(a_1, \cdots, a_n, b_1, \cdots, b_n, c)$. Suppose that $R/(\prod_{i=1}^{k} p_i)R$ is finite where $\{p_1, \cdots, p_k\}$ is a maximal set of nonassociated prime divisors of e such that for each p_i, $GCD(a_j, dp_i) \mid b_j$ for $j = 1, \cdots, n$. Then $t_0 = d' \prod_{i=1}^{k} p_i$ is the minimum modulus of $GCD(a_1x_1 + b_1, \cdots, a_nx_n + b_n, c) = d$. Let $d_j = GCD(a_j, d)$ and $d'_j = d_j/g$ for $j = 1, \cdots, n$. Then*

$$N_{t_0} = \prod_{j=1}^{n} |d'_j| \prod_{i=1}^{k} (|p_i|^n - |p_i|^{n-t_i}) \tag{4.8}$$

where t_i denotes the number of j in $\{1, \cdots, n\}$ for which

$$GCD\left(\frac{a_j}{d_j}, p_i\right) = 1 .$$

Proof. Suppose that $d_j \mid b_j$ for $j = 1, \cdots, n$. Let $a'_j = a_j/g$ and $b'_j = b_j/g$ for $j = 1, \cdots, n$. Let A and A' denote the $n \times n$ diagonal matrices with entries $a_1, \cdots, a_n$ and $a'_1, \cdots, a'_n$ respectively. Let B and B' denote the $n \times 1$ matrices with entries $b_1, \cdots, b_n$ and $b'_1, \cdots, b'_n$ respectively. Then the system $A'X + B' \equiv 0(\text{mod } d')$ is solvable since $GCD(a'_j, d') \mid b'_j$ for $j = 1, \cdots, n$ and $R/d'R$ is finite. Thus the system $AX + B \equiv 0(\text{mod } d)$ is solvable. Hence if $g = GCD(a_1, \cdots, a_n, b_1, \cdots, b_n, c)$, then $GCD(AX + B, c) = d$ is solvable.

Assume that $GCD(AX + B, c) = d$ is solvable. It follows that $t_0 = d' \prod_{i=1}^{k} p_i$ is the minimum modulus of $GCD(AX + B, c) = d$. Let $L = \{X + d'R^n \mid A'X \equiv 0(\text{mod } d')\}$. Let

$$\mathscr{L}_i = \{X \in R^n \mid A'X \equiv 0(\text{mod } d'p_i)\}$$

and $L_i = \{X + d'R^n \mid X \in \mathscr{L}_i\}$ for $i = 1, \cdots, k$. Then by (4.1),

$$N_{t_0} = |L| \prod_{i=1}^{k} (|p_i|^n - |p_i|^{n-(r_i+s_i)})$$

where $r_i = \text{rank } A'(\text{mod } p_i)$ and s_i is the dimension of the R/p_iR vector space L/L_i. Clearly $|L| = \prod_{j=1}^{n} |d'_j|$ since $d'_j = GCD(a'_j, d')$ for $j = 1, \cdots, n$. Let $L'_i = \{X + d'p_iR^n \mid X \in \mathscr{L}_i\}$ and $H_i = \{X + p_iR^n \mid X \in \mathscr{L}_i\}$ for $i = 1, \cdots, k$. Then (1) and (2) of Lemma 3 show that $|L'_i| = |L| |H_i|$ where $|H_i| = |p_i|^{n-(r_i+s_i)}$ for $i = 1, \cdots, k$. However, $GCD(a'_j, d'p_i) = d'_j GCD(a_j/d_j, p_i)$ and thus

$$|L'_i| = |L| \prod_{j=1}^{n} \left| GCD\left(\frac{a_j}{d_j}, p_i\right)\right|$$

for $i = 1, \cdots, k$. Hence $|p_i|^{n-(r_i+s_i)} = \prod_{j=1}^{n} |GCD(a_j/d_j, p_i)|$ and thus $|p_i|^{n-(r_i+s_i)} = |p_i|^{n-t_i}$, since t_i is the number of j in $\{1, \cdots, n\}$ for which $GCD(a_j/d_j, p_i) = 1$. So $t_i = r_i + s_i$ for $i = 1, \cdots, k$, which yields (4.8).

Note that if R/cR is finite, then

$$N_c = \prod_{j=1}^{n} |d_j e| \prod_{i=1}^{k} (1 - |p_i|^{-t_i}) .$$

COROLLARY 6. *Let R be a principal ideal domain. Let A be an $m \times n$ matrix of* rank *r and let $\alpha_1, \cdots, \alpha_r$ be the invariant factors of A. Let B be an $m \times 1$ matrix and let $(A\colon B)$ have* rank *r' and invariant factors $\beta_1, \cdots, \beta_{r'}$. Then $GCD(AX + B, c) = d$ is solvable if and only if* (1) $d \mid c$, (2) $GCD(\alpha_1, d) = GCD(\beta_1, c)$, (3) $GCD(\alpha_j, d) = GCD(\beta_j, d)$ *for* $j = 1, \cdots, r$ *and* $\beta_{r'} \equiv$ o(mod d) *if* $r' = r + 1$.

Let $\{p_1, \cdots, p_k\}$ be a maximal set of nonassociated prime divisors of $e = c/d$ such that each p_i satisfies (3′) $GCD(\alpha_j, dp_i) = GCD(\beta_j, dp_i)$ *for $j = 1, \cdots, r$ and $\beta_{r'} \equiv$ o(mod dp_i) if $r' = r + 1$. Let $d_j = GCD(\alpha_j, d)$ for $j = 1, \cdots, r$ and $d' = d/d_1$. Then $t_0 = d' \prod_{i=1}^{k} p_i$ is the minimum modulus of $GCD(AX + B, c) = d$. Suppose that R/t_0R is finite. Then*

$$N_{t_0} = |d'|^{n-r} \prod_{j=1}^{r} |d'_j| \prod_{i=1}^{k} (|p_i|^n - |p_i|^{n-t_i}) \tag{4.9}$$

where $d'_j = d_j/d_1$ and t_i denotes the largest j in $\{1, \cdots, r\}$ for which $GCD(\alpha_j/d_j, p_i) = 1$.

Proof. Since R is a principal ideal domain, it is well-known that there exist invertible matrices P and Q such that $PAQ = A_0$ where A_0 is an $m \times n$ matrix in "diagonal form", with nonzero entries $\alpha_1, \cdots, \alpha_r$ and $\alpha_j \mid \alpha_{j'}$ if $j < j'$. The elements $\alpha_1, \cdots, \alpha_r$ are called the invariant factors of A and $\alpha_j = D_j/D_{j-1}$ where D_j denotes the *GCD* of the determinants of all the $j \times j$ submatrices of A. Clearly $GCD(A, d) = GCD(\alpha_1, \cdots, \alpha_r, d)$, that is $GCD(A, d) = GCD(\alpha_1, d)$ since $\alpha_1 \mid \alpha_j$ for $j = 1, \cdots, r$. Similarly $GCD(A, B, c) = GCD(\beta_1, c)$. However, it is also well-known that the system $AX + B \equiv 0 \pmod{d}$ is solvable if and only if condition (3) holds (see [4]). Thus $GCD(AX + B, c) = d$ is solvable if and only if (1), (2), and (3) hold.

Let $GCD(AX + B, c) = d$ be solvable and let $c = de$. Then $t_0 = d' \prod_{i=1}^{k} p_i$ is the minimum modulus of $GCD(AX + B, c) = d$. Suppose that R/t_0R is finite. Let S denote the set of X in R^n such that $GCD(AX + B, c) = d$. Let $PB = B_0$ and let S' denote the set of Y in R^n such that $GCD(A_0Y + B_0, c) = d$. Then clearly $X \in S$ if and only if $Y = Q^{-1}X \in S'$. Thus $GCD(AX + B, c) = d$ and $GCD(A_0Y + B_0, c) = d$ have the same ideal of solution moduli. Let $T_0 = \{X + t_0R^n \mid X \in S\}$ and $T'_0 = \{Y + t_0R^n \mid Y \in S'\}$. Then the mapping $f\colon T_0 \to T'_0$ is a bijection, where $f(X + t_0R^n) = Q^{-1}X + t_0R^n$ for all X in S. Hence $|T_0| = |T'_0|$, that is $N_{t_0} = |T'_0|$. Let B_0 have entries $b_1^0, \cdots, b_m^0$ and let $c_0 = GCD(b_{r+1}^0, \cdots, b_m^0, c)$. Then S' is the set of solutions of the linear GCD equation

$$(4.10)\qquad \begin{aligned} GCD(\alpha_1 y_1 + b_1^0, \cdots, \alpha_r y_r + b_r^0, 0\cdot y_{r+1} + 0\,, \\ \cdots, 0\cdot y_n + 0, c_0) = d\,. \end{aligned}$$

Thus $t_0 = d' \prod_{i=1}^{k} p_i$ is also the minimum modulus of (4.10) and hence by (4.8) of Corollary 5,

$$N_{t_0} = |d'|^{n-r} \prod_{j=1}^{r} |d'_j| \prod_{i=1}^{k} (|p_i|^n - |p_i|^{n-t_i})$$

where $d'_j = d_j/d_1$ and t_i is the largest j in $\{1, \cdots, r\}$ for which $GCD(\alpha_j/d_j, p_i) = 1$ since $\alpha_j/d_j \mid \alpha_{j'}/d_{j'}$ if $j < j'$.

If R/cR is finite, then

$$N_c = |c|^{n-r} \prod_{j=1}^{r} |d_j e| \prod_{i=1}^{k} (1 - |p_i|^{-t_i})\,.$$

Finally we remark that the formula for N_{t_0} in (4.1) applies to the class $\mathscr{D}$ of GCD domains R which contain at least one element p such that R/pR is a finite field. Some immediate examples are the integers $\boldsymbol{Z}$, the localizations $\boldsymbol{Z}_{(p)}$ at primes p in $\boldsymbol{Z}$ and $F[X]$ where F is a finite field.

However, an example of such a ring R in $\mathscr{D}$ which is not a *PID* is the subring R of $\boldsymbol{Q}[X]$ consisting of all polynomials whose constant term is in $\boldsymbol{Z}$. Indeed R is a Bezout domain which cannot be expressed as an ascending union of *PID*'s [1]. Clearly if p is a prime in $\boldsymbol{Z}$, then R/pR is isomorphic to the finite field $\boldsymbol{Z}/p\boldsymbol{Z}$.

We are also indebted to Professor W. Heinzer for the following construction of a ring R in $\mathscr{D}$ which is a *UFD* but not a *PID*. Let F be a finite field. Let Y be an element of the formal power series ring $F[[X]]$ such that X and Y are algebraically independent over F. Let V denote the rank one discrete valuation ring $F[[X]] \cap F(X, Y)$ and let $R = F[X, Y][1/X] \cap V$. Then R/XR is isomorphic to F and R is a *UFD*.

References

1. P. M. Cohn, *Bezout rings and their subrings*, Proc. Camb. Phil. Soc., **64** (1968), 251–264.

2. D. Jacobson and K. S. Williams, *On the solution of linear GCD equations*, Pacific J. Math., **39** (1971), 187-206.
3. I. Kaplansky, *Elementary divisors and modules*, Trans. Amer. Math. Soc., **66** (1949), 464-491.
4. H. J. S. Smith, *On systems of linear indeterminate equations and congruences*, Phil. Trans. London, **151** (1861), 293-326. (Collected Mathematical Papers Vol. **1**, Chelsea, N.Y.), (1965), 367-409.
5. R. Spira, *Elementary problem no. E*1730, Amer. Math. Monthly, **72** (1965), 907.

Received February 22, 1974 and in revised form September 3, 1974. This research was supported in part by NRC Grant-A8749.

UNIVERSITY OF NEW BRUNSWICK