INTEGER SOLUTIONS OF LINEAR DIOPHANTINE EQUATIONS FORM A GROUP

Ajai Choudhry

Abstract. It is shown that the set of integer solutions of a single Diophantine equation, or of several simultaneous linear Diophantine equations, in an arbitrary number of variables, say n, is a group with respect to a suitably defined binary operation. Further, the aforesaid group is the direct sum of n cyclic groups.

1. Introduction. Various methods of obtaining integer solutions of the linear Diophantine equation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{1}$$

or the simultaneous linear Diophantine equations

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2, \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m, \end{aligned} \tag{2}$$

have been given by several mathematicians [1, 2, 3, 4, 6]. Necessary and sufficient conditions for the solvability of equations (1) and (2) are also known [2, 5]. The object of this note is to show that when integer solutions of (1) or of the simultaneous equations (2) exist, the set of these integer solutions can be given a group structure with respect to a suitably defined binary operation. We also show that this group is the direct sum of n cyclic groups.

We first prove a couple of preliminary lemmas. In the first lemma we show that for a fixed integer k, the set of integers, denoted by Z, is a group with respect to a suitable binary operation defined in terms of k, and we examine the structure of this group. This is generalized in Lemma 2 where we show that the set Z^n is a group with respect to a suitable binary operation defined in terms of a fixed n-tuple $(k_1, k_2, \ldots, k_n)$. We use these results to prove the main theorem about the group structure of the set of integer solutions of linear Diophantine equations.

2. Preliminary Lemmas.

Lemma 1. For any fixed integer k, the set Z of integers is an abelian group under the binary operation $\oplus_k$ defined by $a \oplus_k b = a + b - k$ where

a and b are any two arbitrary integers. The group $(Z, +)$ is isomorphic to the group $(Z, \oplus_k)$. Further, $(Z, \oplus_k)$ is a cyclic group with two generators $1 + k$ and $-1 + k$ and each subgroup S of $(Z, \oplus_k)$ is a cyclic group of the form $S = \{ma + k \mid m \in Z\}$ where a is a fixed integer.

Proof. It is readily seen that $\oplus_k$ is a well-defined commutative binary operation and that Z is closed under the operation $\oplus_k$. We note that for any three arbitrary integers a, b, and c, we have the relations

$$a \oplus_k (b \oplus_k c) = a \oplus_k (b + c - k) = a + b + c - 2k,$$
$$(a \oplus_k b) \oplus_k c = (a + b - k) \oplus_k c = a + b + c - 2k,$$

which show that $a \oplus_k (b \oplus_k c) = (a \oplus_k b) \oplus_k c$ so that the binary operation $\oplus_k$ is associative. Next we observe that for any integer a,

$$a \oplus_k k = a + k - k = k,$$
$$a \oplus_k (2k - a) = a + (2k - a) - k = k.$$

It follows from these relations that k acts as the identity element and $2k - a$ is the inverse of the arbitrary integer a with respect to the operation $\oplus_k$. Thus, $(Z, \oplus_k)$ is an abelian group.

The mapping $\phi: Z \to Z$ defined by $\phi(a) = a + k$ is readily seen to be a one-to-one onto mapping. Further,

$$\begin{aligned} \phi(a + b) &= a + b + k = (a + k) + (b + k) - k \\ &= (a + k) \oplus_k (b + k) = \phi(a) \oplus_k \phi(b). \end{aligned}$$

Thus, the groups $(Z, +)$ and $(Z, \oplus_k)$ are isomorphic.

The group $(Z, +)$ is known to be a cyclic group with two generators 1 and -1. Since $(Z, \oplus_k)$ is isomorphic to the group $(Z, +)$, it follows that the group $(Z, \oplus_k)$ is also cyclic and it has two generators $1 + k$ and $-1 + k$. Each subgroup of $(Z, +)$ is a cyclic group. Correspondingly, each subgroup of $(Z, \oplus_k)$ is also a cyclic group. For any integer $a \in (Z, \oplus_k)$ and any positive integer m, the m^{th} "multiple" of a with respect to $\oplus_k$, denoted by $m *_k a$, may be defined recursively, by

$$\begin{aligned} m *_k a &= \underbrace{a \oplus_k a \oplus_k \cdots \oplus_k a}_{m \text{ summands}} \\ &= ((m - 1) *_k a) \oplus_k a, \end{aligned}$$

while $0 *_k a = k$. It is easily seen that $2 *_k a = 2a - k,\ 3 *_k a = 3a - 2k$, and, in general, $m *_k a = ma - (m-1)k$. Moreover, since the inverse of a with respect to $\oplus_k$ is $(2k - a)$, we get

$$-m *_k a = m *_k (2k - a) = m(2k - a) - (m-1)k = -ma + (m+1)k.$$

We will now determine the subgroup of $(Z^n, \oplus_k)$ generated by the arbitrary element $a + k$. In view of the relations

$$m *_k (a + k) = m(a + k) - (m-1)k = ma + k,$$
$$-m *_k (a + k) = -m(a + k) + (m+1)k = -ma + k,$$

it follows that the cyclic subgroup of $(Z, \oplus_k)$ generated by $(a + k)$ is of the form $\{ma + k \mid m \in Z\}$. This can also be inferred directly from the one-to-one correspondence established by the mapping ϕ between the cyclic subgroups of the isomorphic groups $(Z, +)$ and $(Z, \oplus_k)$. Moreover, since $(a + k)$ is an arbitrary element of $(Z, \oplus_k)$, all the subgroups of $(Z, \oplus_k)$ are cyclic groups of the form $S = \{ma + k \mid m \in Z\}$, the generator of the subgroup S being $(a + k)$. This completes the proof.

Lemma 2. For any fixed n-tuple $k = (k_1, k_2, \ldots, k_n) \in Z^n$, the set Z^n of all integral n-tuples is an abelian group under the binary operation $\oplus_k$ defined by

$$(a_1, a_2, \ldots, a_n) \oplus_k (b_1, b_2, \ldots, b_n) = (a_1 + b_1 - k_1, a_2 + b_2 - k_2, \ldots, a_n + b_n - k_n),$$

where $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ are any two arbitrary integral n-tuples. The group $(Z^n, +)$, with component-wise addition, is isomorphic to the group $(Z^n, \oplus_k)$. Further, each subgroup of $(Z^n, \oplus_k)$ is the direct sum of n cyclic groups, the j^{th} cyclic group of this direct sum is a subgroup of the group $(Z, \oplus_{k_j})$ and is of the form $\{ma + k_j \mid\ m \in Z\}$ for some $a \in Z$.

Proof. Given any fixed integral n-tuple $k = (k_1, k_2, \ldots, k_n)$, we construct for each $j,\ j = 1, 2, \ldots, n$, the group $(Z, \oplus_{k_j})$ as in Lemma 1. The direct sum of these n groups is easily seen to be the group $(Z^n, \oplus_k)$ where $\oplus_k$ is the binary operation as defined in this lemma. Thus,

$$(Z^n, \oplus_k) = (Z, \oplus_{k_1}) \oplus (Z, \oplus_{k_2}) \oplus \cdots \oplus (Z, \oplus_{k_n}),$$

where $\oplus$ is used to denote the direct sum of the groups concerned. This shows that $(Z^n, \oplus_k)$ is an abelian group with identity $(k_1, k_2, \ldots, k_n)$. Moreover, the inverse of the arbitrary integral n-tuple $(a_1, a_2, \ldots, a_n)$ with respect to the operation $\oplus_k$ is easily seen to be the n-tuple $(2k_1 - a_1, 2k_2 - a_2, \ldots, 2k_n - a_n)$.

We now prove that the group $(Z^n, +)$, with component-wise addition, is isomorphic to the group $(Z^n, \oplus_k)$. The mapping $\phi\colon Z^n \to Z^n$ defined by

$$\phi(a_1, a_2, \ldots, a_n) = (a_1 + k_1,\ a_2 + k_2, \ldots, a_n + k_n)$$

is readily seen to be a one-to-one onto mapping. Further, for any two n-tuples $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ belonging to the group $(Z^n, +)$,

$$\begin{aligned}
&\phi((a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n)) \\
&\quad = \phi(a_1 + b_1,\ a_2 + b_2, \ldots, a_n + b_n) \\
&\quad = (a_1 + b_1 + k_1,\ a_2 + b_2 + k_2,\ \ldots, a_n + b_n + k_n) \\
&\quad = ((a_1 + k_1) + (b_1 + k_1) - k_1,\ \ldots,\ (a_n + k_n) + (b_n + k_n) - k_n) \\
&\quad = (a_1 + k_1,\ a_2 + k_2,\ \ldots,\ a_n + k_n) \oplus_k (b_1 + k_1,\ b_2 + k_2,\ \ldots,\ a_n + b_n) \\
&\quad = \phi(a_1, a_2, \ldots, a_n) \oplus_k \phi(b_1, b_2, \ldots, b_n).
\end{aligned}$$

Thus, the groups $(Z^n, +)$ and $(Z^n, \oplus_k)$ are isomorphic.

Finally, we note that for each j, $j = 1, 2, \ldots, n$, the projection mapping π_j from the direct sum $(Z, \oplus_{k_1}) \oplus (Z, \oplus_{k_2}) \oplus \cdots \oplus (Z, \oplus_{k_n})$, that is the group $(Z^n, \oplus_k)$, to the group $(Z, \oplus_{k_j})$ defined by

$$\pi_j(a_1, a_2, \ldots, a_j, \ldots, a_n) = a_j$$

is a homomorphism. The homomorphic image of any subgroup of $(Z^n, \oplus_k)$ with respect to the projection mapping π_j is a subgroup of the group $(Z, \oplus_{k_j})$ and, in view of Lemma 1, it is a cyclic subgroup of $(Z, \oplus_{k_j})$ consisting of integers of the form $\{ma + k_j \mid\ m \in Z\}$ for some $a \in Z$. Moreover, each subgroup of $(Z^n, \oplus_k)$ can be written as the direct sum of its n homomorphic images under the projection mappings $\pi_j,\ j = 1, 2, \ldots, n$. Thus, each subgroup of $(Z^n, \oplus_k)$ is the direct sum of n cyclic groups; the j^{th} cyclic group of this direct sum is a subgroup of the group $(Z, \oplus_{k_j})$ and consists of integers of the form $\{ma + k_j \mid\ m \in Z\}$ for some $a \in Z$. This completes the proof.

3. The Group of Integer Solutions of Linear Diophantine Equations.

Theorem. When the conditions of solvability of the simultaneous linear Diophantine equations

$$\sum_{j=1}^{n} a_{ij} x_j = b_i,\ i = 1, 2 \ldots, m, \tag{3}$$

are satisfied, the nonempty set of integer solutions of these equations forms an abelian group with respect to a binary operation which may be defined such that any arbitrarily chosen integer solution of (3) acts as the identity element of the group. Further, the aforesaid group is the direct sum of n cyclic groups.

Proof. Let S be the nonempty set of integer solutions $(x_1, x_2, \ldots, x_n)$ of (3), and let $(k_1, k_2, \ldots, k_n) \in S$ be an arbitrary integer solution of (3) so that

$$\sum_{j=1}^{n} a_{ij}k_j = b_i,\ i = 1, 2, \ldots, m. \tag{4}$$

Clearly $S \subset Z^n$, and we will now prove that S is in fact a subgroup of the group $(Z^n, \oplus_k)$ constructed in Lemma 2. The identity element of $(Z^n, \oplus_k)$ is $(k_1, k_2, \ldots, k_n)$ which, by definition, is an element of the set S. To prove that the set S is a subgroup of $(Z^n, \oplus_k)$, we will show that S is closed under the operation $\oplus_k$ and that the inverse of each element of S is also an element of S.

Let $X = (X_1, X_2, \ldots, X_n) \in S$ and $Y = (Y_1, Y_2, \ldots, Y_n) \in S$ be any two integer solutions of (3) so that

$$\sum_{j=1}^{n} a_{ij}X_j = b_i,\ i = 1, 2, \ldots, m \tag{5}$$

and

$$\sum_{j=1}^{n} a_{ij}Y_j = b_i,\ i = 1, 2, \ldots, m. \tag{6}$$

We note that

$$X \oplus_k Y = (X_1 + Y_1 - k_1,\ X_2 + Y_2 - k_2,\ \ldots,\ X_n + Y_n - k_n), \tag{7}$$

and for each i we have,

$$\begin{aligned}\sum_{j=1}^{n} a_{ij}(X_j + Y_j - k_j) &= \sum_{j=1}^{n} a_{ij}X_j + \sum_{j=1}^{n} a_{ij}Y_j - \sum_{j=1}^{n} a_{ij}k_j,\\ &= b_i. \end{aligned} \tag{8}$$

It follows that $X \oplus_k Y$ is an integer solution of (3) and hence, $(X \oplus_k Y) \in S$. This shows that the set S is closed under the binary operation $\oplus_k$.

We have already seen while considering the group $(Z^n, \oplus_k)$ that the inverse of any element $X = (X_1, X_2, \ldots, X_n)$ with respect to the binary operation $\oplus_k$ is

$$X^{-1} = (2k_1 - X_1, 2k_2 - X_2, \ldots, 2k_n - X_n) = (X_1', X_2', \ldots, X_n').$$

We note that for each i we have

$$\begin{aligned} \sum_{j=1}^{n} a_{ij} X_j' &= \sum_{j=1}^{n} a_{ij}(2k_j - X_j) \\ &= 2\sum_{j=1}^{n} a_{ij} k_j - \sum_{j=1}^{n} a_{ij} X_j \\ &= b_i. \end{aligned} \tag{9}$$

This shows that $(X_1', X_2', \ldots, X_n')$ is a solution of (3) and hence, $X^{-1} \in S$. Thus, the inverse of each element of S is also an element of S and hence, S is a subgroup of the group $(Z^n, \oplus_k)$.

It is now an immediate consequence of Lemma 2 that the set S of solutions of the simultaneous linear equations (3) is an abelian group which is the direct sum of n cyclic groups; the j^{th} cyclic group of this direct sum is a subgroup of the group $(Z, \oplus_{k_j})$ and is of the form $\{ma + k_j,\ m \in Z\}$ for some $a \in Z$. This completes the proof.

Corollary. If the linear Diophantine equation (1) is solvable, its integer solutions form a group.

This is an immediate consequence of the theorem.

Acknowledgment. I am grateful to the referee for his comments which have led to improvements in the paper.

References

1. J. Bond, "Calculating the General Solution of a Linear Diophantine Equation," *American Math. Monthly,* 74 (1967), 955–957.
2. L. E. Dickson, *History of the Theory of Numbers,* Vol. 2, Chelsea Publishing Company, New York, 1952, reprint.
3. S. Kertzner, "The Linear Diophantine Equation," *American Math. Monthly,* 88 (1981), 200–203.
4. D. H. Lehmer, "A Note on the Linear Diophantine Equation," *American Math. Monthly,* 48 (1941), 240–246.

5. L. J. Mordell, *Diophantine Equations,* Academic Press, London, 1969.

6. B. Rosser, "A Note on the Linear Diophantine Equation," *American Math. Monthly,* 48 (1941), 662–666.

Mathematics Subject Classification (2000): 11D04

Ajai Choudhry
D-6/1 Multi-Storey Flats
Sector 13
R. K. Puram
New Delhi - 110066
INDIA
email: ajaic203@yahoo.com