<table>
<thead>
<tr>
<th>Title</th>
<th>On Diophantine Equation of 1st Degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Onari, Setsuo</td>
</tr>
<tr>
<td>Citation</td>
<td>Hitotsubashi journal of arts and sciences, 9(1): 44-49</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1968-09</td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Text Version</td>
<td>publisher</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://doi.org/10.15057/4272">http://doi.org/10.15057/4272</a></td>
</tr>
</tbody>
</table>
ON DIOPHANTINE EQUATION OF 1st DEGREE

By SETSUO ONARI*

Throughout this paper \( N \) and \( Z \) are the set of all natural numbers and rational integers respectively. We use the symbols of interval \([ , ]\), \([ , )\) etc. as the symbols of intervals defined on linearly ordered set \( Z \).

For \( n \) \((n \geq 2)\) elements \( a_j \in N \) \((1 \leq j \leq n)\) such that \((a_1, a_2, \ldots, a_n) = 1\) we consider the set

\[
S(a_1, a_2, \ldots, a_n) = \left\{ \sum_{j=1}^{n} a_j x_j \in N; \ x_j \in N, \ (1 \leq j \leq n) \right\}.
\]

Obviously \( b \in S(a_1, a_2, \ldots, a_n) \) is equivalent to the fact that Diophantine equation of 1st degree \( \sum_{j=1}^{n} a_j x_j = b \) has at least one solution in \( N \), and it is obvious

\[
\sum_{j=1}^{n} a_j \in S(a_1, a_2, \ldots, a_n) = \left[ \sum_{j=1}^{n} a_j, \infty \right).
\]

So throughout this paper we assume \( a_j \geq 2 \) for all \( j \) \((1 \leq j \leq n)\).

1. We put

\[
d_1 = (a_2, a_3, \ldots, a_n) \quad \quad a_j = d_1 a_j' \quad \quad 2 \leq j \leq n
\]

\[
d_2 = (a_3, a_4, \ldots, a_n) \quad \quad a_j = d_2 a_j' \quad \quad 3 \leq j \leq n
\]

\[
\vdots
\]

\[
d_{r-1} = (a_{r+1}, a_{r+2}, \ldots, a_n) \quad \quad a_j' = d_{r-1} a_j'' \quad \quad r \leq j \leq n
\]

\[
d_{n-1} = (a_{n-2}, a_{n-3}) \quad \quad a_j'' = d_{n-2} a_j''' \quad \quad n-1 \leq j \leq n
\]

It is obvious that \( d_{n-1} = a_n^{(n-2)} \), \( a_n^{(n-1)} = 1 \). Now we can prove

\[
\left\{ \sum_{j=1}^{n-1} a_j d_j, \infty \right\} \subseteq S(a_1, a_2, \ldots, a_n)
\]

by induction on \( n \).

If \( n = 2 \), then \( d_1 = a_2 \). Let us prove that the equation

\[
a_1 X_1 + a_2 X_2 = b
\]

has at least one solution in \( N \) for all \( b \in N \) such that \( a_1 a_2 < b \). By the assumption \((a_1, a_2) = 1\) the equation has at least one rational integral solution, which we denote \( X_1 = x_1^{(a)}, X_2 = x_2^{(a)} \). For all \( t \in Z \), \( X_1 = x_1^{(a)} - a_2 t \), \( X_2 = x_2^{(a)} + a_1 t \) are also rational integral solution of \( a_1 X_1 + a_2 X_2 = b \).

So the fact to be proved is

\[
\{ t \in Z; x_1^{(a)} - a_2 t > 0, x_1^{(a)} + a_1 t > 0 \} \neq \emptyset \quad \quad \text{i.e.} \quad \quad \left( -\frac{x_1^{(a)}}{a_1}, \frac{x_1^{(a)}}{a_2} \right) \neq \emptyset.
\]

But this is obvious by the relation

\[
\frac{x_1^{(a)}}{a_2} - \frac{x_1^{(a)}}{a_1} = \frac{b}{a_1 a_2} > 1.
\]

* Lecturer (Kōshi) in Mathematics.
Next let us assume
\[ b \in \left( \sum_{j=2}^{n-1} a_j d_j, \infty \right), \]
and let us adopt as the assumption of induction
\[ \left( \sum_{j=2}^{n-1} a_j d_j, \infty \right) \subseteq S\left( a_1', a_2', \ldots, a_n' \right) \]
where \( a_j' \) \((2 \leq j \leq n)\) have been defined \( a_j = d_a a_j' \) \((2 \leq j \leq n)\). Thus the equation \( \sum_{j=2}^{n-1} a_j X_j = b \) has at least one solution in \( N \) for all \( b \in \left( \sum_{j=2}^{n-1} a_j d_j, \infty \right) \).

If we can prove the fact that the equation \( a_1 X + d_1 Y = b \) has at least one solution \( X = x^{(\ell)} \), \( Y = y^{(\ell)} \) such that \( x^{(\ell)} \in N \), \( y^{(\ell)} \in \left( \sum_{j=2}^{n-1} a_j d_j, \infty \right) \), then we finish the proof. But it is equivalent to the fact that \( a_1 X_1 + d_1 (Y_1 + \sum_{j=2}^{n-1} a_j d_j) = b \), i.e. \( a_1 X_1 + d_1 Y_1 = b - \sum_{j=2}^{n-1} a_j d_j \) has at least one solution \( X_1 = x^{(\ell)} \in N \), \( Y_1 = y^{(\ell)} \in N \). But this is guaranteed by the assumption \( b \in \left( \sum_{j=2}^{n-1} a_j d_j, \infty \right) \).

We can improve on this result by changing the order of \( a_j \) \((1 \leq j \leq n)\) suitably. Namely let us \( S_n \) be symmetric group of degree \( n \). For any \( \sigma \in S_n \) we put
\[
\begin{align*}
    d_1(\sigma) &= (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_n)) \\
    d_2(\sigma) &= (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_n)) \\
    & \vdots \\
    d_r(\sigma) &= (\sigma(a_{r-1}), \sigma(a_{r-2}), \ldots, \sigma(a_{n-1})) \\
    & \vdots \\
    d_{n-1}(\sigma) &= (\sigma(a_{n-2}), \sigma(a_{n-3})) \\
    d_n(\sigma) &= (\sigma(a_{n-1}), \sigma(a_n))
\end{align*}
\]
It is obvious \( d_{n-1}(\sigma) = a_n^{(n-1)} \), \( a_n^{(n-1)} = 1 \). We put
\[
M = \{ \sigma \in S_n ; \sum_{j=1}^{n-1} a_{\sigma(a_j)} d_j(\sigma) = \min \left\{ \sum_{j=1}^{n-1} a_{\sigma(a_j)} d_j(\sigma) \right\} \}
\]
Following the above proof, we have a result,
\[
\left( \sum_{j=1}^{n-1} a_{\sigma(a_j)} d_j(\sigma), \infty \right) \subseteq S\left( a_{\sigma(a_1)}, a_{\sigma(a_2)}, \ldots, a_{\sigma(a_n)} \right)
\]
for any \( \sigma \in M \), and this is better than the above result.

With respect to \( \sigma \in S_n \), the fact
\[
\sigma(a_1) \leq \sigma(a_2) \leq \ldots \leq \sigma(a_n) \Rightarrow \sigma \in M
\]
is not always correct and there are two cases where
\[
\sum_{j=1}^{n-1} a_{\sigma(a_j)} d_j(\sigma) \in S\left( a_{\sigma(a_1)}, a_{\sigma(a_2)}, \ldots, a_{\sigma(a_n)} \right)
\]
holds and does not hold.

Example 1. \( a_1 = 2, a_2 = 3, a_3 = 4 \).
\[
\sum_{j=1}^{n-1} a_{\sigma(a_j)} d_j(\sigma) = \begin{cases} 14 & \text{for } \sigma \in \{ \varepsilon \text{= identity of } S_3 \}, (23) \\ 10 & \text{for } \sigma \in \{ (12), (13), (23), (123) \} \end{cases}
\]
So \( M = \{ (12), (13), (23), (123) \} \). But \( 10 \in S(a_1, a_2, a_3) \), because if \( 10 \in S(a_1, a_2, a_3) \), the equation \( a_1 X_1 + a_2 X_2 + a_3 X_3 = 10 \) has at least one solution \( X_1 = x^{(\ell)} \in N \) \((1 \leq j \leq 3)\) and \( x^{(\ell)} \equiv 0 \) \( \pmod{2} \). Accordingly \( 3 x_1^{(\ell)} \geq 6 \), then \( a_1 x_1^{(\ell)} + a_2 x_2^{(\ell)} + a_3 x_3^{(\ell)} \geq 12 \). This is a contradiction.

Example 2. \( a_1 = 3, a_2 = 4, a_3 = 5 \).
\[
\sum_{j=1}^{n-1} a_{\sigma(a_j)} d_j(\sigma) = \begin{cases} 23 & \text{for } \sigma \in \{ \varepsilon \text{= identity of } S_3 \}, (23) \\ 19 & \text{for } \sigma \in \{ (12), (132) \} \\ 17 & \text{for } \sigma \in \{ (123), (13) \} \end{cases}
\]
So \( M = \{ (123), (13) \} \). But \( 17 \in S(a_1, a_2, a_3) \), because the equation \( a_1 X_1 + a_2 X_2 + a_3 X_3 = 17 \) has a
solution $X_1=2$, $X_2=X_3=1$.

2. It is obvious that 
\[ \{1, \sum_{j=1}^{n} a_j\} \cap S(a_1, a_2, \ldots, a_n) = \emptyset \]
\[ \sum_{j=1}^{n} a_j \notin S(a_1, a_2, \ldots, a_n). \]
So we are interested in the following finite set
\[ \{ \sum_{j=1}^{n} a_j, \sum_{j=1}^{n} a_j, \ldots, a_n \} \cap S(a_1, a_2, \ldots, a_n). \]
Let us assume
\[ S(a'_j, a'_j, \ldots, a'_n) = \{ c_1, c_2, \ldots, c_t \} \cup (b', \infty) \]
where $c_1 < c_2 < \cdots < c_t$, $c_t = \sum_{j=1}^{n} a'_j$, and
\[ b'_t = \max \{ x \in N; x \notin S(a'_j, a'_j, \ldots, a'_n) \} \leq \sum_{j=1}^{n} a'_j d_j, \]
and $a'_j$ ($2 \leq j \leq n$) have been defined as $a'_j = d_j a'_j$ ($2 \leq j \leq n$). By the relation
\[ \sum_{j=1}^{n} a_j x_j = a_1 x_1 + d_1 \sum_{j=1}^{n} a'_j x_j \]
we have
\[ S(a_1, a_2, \ldots, a_n) = a_1 N + d_s S(a'_1, a'_2, \ldots, a'_n) \]
\[ = a_1 N + \{ d_1 c_1, d_2 c_2, \ldots, d_t c_t \} \cup (a_1 N + d_s (b'_t + N)) \]
\[ = a_1 N + \{ d_1 c_1, d_2 c_2, \ldots, d_t c_t \} \cup (d_s b'_t + S(a'_1, a'_2)). \]
Accordingly the problem is generally reduced to consider the set $S(a_1, a_2)$.

3. Let us consider the special case $n=2$. $a_1, a_2$ are two elements of $N$ such that $(a_1, a_2) = 1$ and $a_1 < a_2$. (If $a_1 = a_2$, then $a_1 = a_2 = 1$ by the assumption $(a_1, a_2) = 1$).

At first $a_1 a_2 \notin S(a_1, a_2)$, because by $(a_1, a_2) = 1$
\[ \{ (x_1, x_2) \in N^2; \ x_2 = \frac{x_1}{a_2}, (0 < x_1 < a_2) \} = \emptyset, \]
then
\[ \{ (x_1, x_2) \in N^2; \ \frac{x_1}{a_2} + \frac{x_2}{a_1} = 1 \} = \emptyset. \]
Next $\varphi : (x^{(1)}, x^{(2)}) \rightarrow a_1 x^{(1)} + a_2 x^{(2)}$ is a bijection from $\{(x_1, x_2) \in N^2; \ a_1 x_1 + a_2 x_2 < a_1 a_2 \}$ onto $[a_1 + a_2, a_2 a_2) \setminus S(a_1, a_2)$. This result was suggested by Mr. T. Nagashima, who is a lecturer at Hitotsubashi University. The reason is
\[ b \in [a_1 + a_2, a_2 a_2) \cap S(a_1, a_2) \]
\[ \Rightarrow \exists (x_1^{(1)}, x_2^{(1)}) \in N^2, \ b = a_1 x_1^{(1)} + a_2 x_2^{(1)} < a_1 a_2 \]
\[ \Rightarrow \varphi (x_1^{(1)}, x_2^{(1)}) = b, \]
\[ \varphi (x_1^{(1)}, x_2^{(1)}) = \varphi (x_1^{(1)}, x_2^{(1)}) \]
\[ \Rightarrow a_1 x_1^{(1)} + a_2 x_2^{(1)} = a_1 x_1^{(1)} + a_2 x_2^{(1)} \]
\[ \Rightarrow a_1 (x_1^{(1)} - x_2^{(1)}) = a_2 (x_2^{(1)} - x_2^{(1)}) \]
\[ \Rightarrow x_2^{(1)} \equiv x_2^{(1)} \pmod{a_2} \] (by $(a_1, a_2) = 1$)
but $1 \leq x_1^{(1)} \leq a_2 - 1$, $1 \leq x_2^{(1)} \leq a_2 - 1$, then $x_1^{(1)} = x_1^{(1)}$, $x_2^{(1)} = x_2^{(1)}$.
Next we have
\[ \text{number of the elements in } \{(x_1, x_2) \in N^2; \ a_1 x_1 + a_2 x_2 < a_1 a_2 \} \]
\[ = \frac{1}{2} \text{number of the elements in } \{(x_1, x_2) \in N^2; \ 0 < x_1 < a_2, 0 < x_2 < a_2 \}. \]
So we have
\[
\text{number of the elements in } [a_1+a_2, a_1a_2] \cap S(a_1, a_2) = \frac{1}{2} (a_1-1)(a_2-1)
\]
\[
= \frac{1}{2} \text{(number of the elements in } [a_1+a_2, a_1a_2]).
\]

Let us consider \( S(a_1, a_2) \) more precisely.

i) When \( a_1 = 2 \), there exists \( c \) in \( N \) such that \( a_2 = 2c+1 \) by \((a_1, a_2) = 1\),

i)-1 When \( c = 1 \) i.e. \( a_2 = 3 \), it is obvious that
\[
\text{number of the elements in } [a_1+a_2, a_1a_2] \cap S(a_1, a_2) = 1,
\]
\[
S(a_1, a_2) = \{5\} \cup (6, \infty).
\]

i)-2 When \( c \geq 2 \) i.e. \( a_2 \geq 5 \), it is obvious that
\[
\text{number of the elements in } [a_1+a_2, a_1a_2] \cap S(a_1, a_2) = \frac{a_2-1}{2},
\]
\[
S(a_1, a_2) = \left\{2s+a_2; s=1, 2, ..., \frac{a_2-1}{2}\right\} \cup (a_1a_2, \infty).
\]

ii) When \( a_1 \geq 3 \), we put
\[
a_2 = a_1q+r, \ 0 \leq r < a_1.
\]
Then \( q \geq 1 \) and \( 1 \leq r < a_1 \), and
\[
a_2 - (a_1 + a_2 - (a_1q + 1) + (a_2 - a_1) \geq 5
\]
So number of the elements in \([a_1+a_2, a_1a_2] \cap S(a_1, a_2) = \frac{a_2-1}{2},
\]
\[
S(a_1, a_2) = \left\{2s+a_2; s=1, 2, ..., \frac{a_2-1}{2}\right\} \cup (a_1a_2, \infty).
\]

Example 3. \( a_1 = 5, a_2 = 6, a_3 = 8 \).

As a preparation
\[
S(2, 5) = \{2s+5; s=1, 2\} \cup (10, \infty)
\]
\[
= \{7, 9\} \cup (10, \infty),
\]
\[
S(3, 4) = \{7, 10, 11\} \cup (12, \infty),
\]
because by \( 4 = 3 \cdot 1 + 1 \),
\[
V_1 = \left\{3x_1 + 4x_2; 0 < x_1 \leq 1 + \frac{1}{3}, 1 \leq x_2 \leq 3 - 1\right\}
\]
\[
V_2 = \left\{3x_1 + 4x_2; 1 + \frac{1}{3} < x_1 \leq 2 \left(1 + \frac{1}{3}\right), 1 \leq x_2 \leq 1\right\}.
\]

Now \( d_1 = 2, d_2 = 4 \), then
\[
\sum_{j=1}^{5} a_j d_j = 34, \quad \sum_{j=1}^{5} a_j = 19.
\]
Accordingly
\[
(34, \infty) \subseteq S(a_1, a_2, a_3), \quad (0, 19) \cap S(a_1, a_2, a_3) = \phi.
\]
By
\[
5x_1 + 6x_2 + 8x_3 = 5x_1 + 2(3x_2 + 4x_3)
\]
we have
\[
[19, 34] \cap (5N + 2S(3, 4))
\]
4. Finally I state formulae which give us general solution of Diophantine equation of 1st degree.
i) For two rational integers \(a_1, a_2\) such that \((a_1, a_2)=1\) and \(a_1 < a_2\), let us put
\[
 r_{j-2} = r_{j-1} q_j + r_j \quad (1 \leq j \leq m)
\]
where \(a_1 = r_0, a_2 = r_{-1}\). Then we have
\[
 r_0 > r_1 > r_2 > \cdots > r_{m-1} > r_m > 0
\]
and
\[
 r_m = (a_1, a_2) = 1.
\]
For arbitrary rational integer \(b\), let us put
\[
 S_j = \left\{ \frac{x_j^{(p)}}{x_j^{(q)}} \in \mathbb{Z}^2; \; r_j x_1^{(p)} + r_{j-1} x_2^{(p)} = b \right\} \quad (0 \leq j \leq m),
\]
then we have
\[
 S_0 = \left\{ \frac{x_1^{(p)}}{x_2^{(p)}} \in \mathbb{Z}^2; \; a_1 x_1^{(p)} + a_2 x_2^{(p)} = b \right\},
\]
\[
 S_m = \left\{ \begin{pmatrix} b & -r_{m-1} \\ 0 & 1 \end{pmatrix} \middle| \begin{pmatrix} 1 \\ t \end{pmatrix} \in \mathbb{Z}^2; \; t \in \mathbb{Z} \right\},
\]
and
\[
 \left( \frac{x_1^{(p)}}{x_2^{(p)}} \right) \rightarrow Q_j \left( \frac{x_1^{(q)}}{x_2^{(q)}} \right), \quad Q_j = \begin{pmatrix} -q_j & 1 \\ 1 & 0 \end{pmatrix}, \quad (1 \leq j \leq m)
\]
are the bijection from \(S_j\) onto \(S_{j-1}\) \((1 \leq j \leq m)\). Accordingly the general solution \(X_1 = x_1^{(p)}, X_2 = x_2^{(p)}\) of the equation \(a_1 X_1 + a_2 X_2 = b\) are given by the following formula.
\[
 \left( \begin{array}{c} x_1^{(p)} \\ x_2^{(p)} \end{array} \right) = Q_1 Q_2 \cdots Q_m \begin{pmatrix} b \\ -r_{m-1} \end{pmatrix} \begin{pmatrix} 1 \\ t \end{pmatrix}, \quad t \in \mathbb{Z}.
\]

ii) Now let us consider \(n\) dimensional case. For \(n (n \geq 2)\) rational integers \(a_j (1 \leq j \leq n)\) such that \((a_1, a_2, \ldots, a_n)=1\) and all of them are not negative, we put
\[
 a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \quad a_{m(k)} = \text{Min}\{a_j \in \mathbb{Z}; \; 1 \leq j \leq n, \; a_j > 0\}
\]
and
\[
 a' = \begin{pmatrix} a_1' \\ a_2' \\ \vdots \\ a_n' \end{pmatrix} \quad \text{where} \quad a_j' = a_j - (1 - \delta_{j,m(k)}) a_{m(k)} \frac{a_j}{a_{m(k)}},
\]
\[
 a_{k(k+1)} = a_{k(k)} \quad k = 1, 2, 3, \ldots.
\]
Then we have the following result which is easily proved by induction on \(n\).
\[
 \exists k_0 \in \mathbb{N}; \; a^{(k+1)} = \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix} m(a^{(k)})
\]
Now we put for any fixed \( b \in \mathbb{Z} \)

\[
S_k = \{ \begin{bmatrix} x_1, k \\ x_2, k \\ \vdots \\ x_n, k \end{bmatrix} \in \mathbb{Z}^n; \sum_{j=1}^n a_j \cdot x_j = b \} \quad (0 \leq k \leq k_0)
\]

Then \( S_0 \) is the set of all solutions in \( \mathbb{Z} \) of \( \sum_{j=1}^n a_j X_j = b \)

\[
S_{k_0} = \{ \begin{bmatrix} t_1 \\ \vdots \\ t_{v-1} \\ t_v + 1 \\ \vdots \\ t_{v+1} \\ \vdots \\ b \\ \vdots \\ t_n \end{bmatrix} \in \mathbb{Z}^n; t_{l} = \text{arbitrary element in } \mathbb{Z} \text{ for } 1 \leq l \leq n, l \neq m(a^{(k_0)}) \}
\]

and

\[
\begin{bmatrix} x_1, k \\ x_2, k \\ \vdots \\ x_n, k \end{bmatrix} \rightarrow Q_k \begin{bmatrix} x_1, k \\ x_2, k \\ \vdots \\ x_n, k \end{bmatrix}, \quad Q_k = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ -q_1^{(k-1)} & -q_2^{(k-1)} & \cdots & -q_n^{(k-1)} \end{pmatrix}
\]

where \( \nu = m(a^{(k-1)}) \), \( q_j^{(k-1)} = \left[ \frac{a_j^{(k-1)}}{d_m(a^{(k-1)})} \right], 1 \leq j \leq n, j \neq m(a^{(k-1)}) \), is a bijection from \( S_k \) onto \( S_{k-1} \).

Accordingly the general solution \( X_j = x_{j, 0} \) \((1 \leq j \leq n)\) of equation \( \sum_{j=1}^n a_j X_j = b \) is given by the following formula,

\[
\begin{bmatrix} x_1, 0 \\ x_2, 0 \\ \vdots \\ x_n, 0 \end{bmatrix} = Q_1 \cdot Q_2 \cdots Q_{k_0} \begin{bmatrix} t_1 \\ \vdots \\ t_{v-1} \\ b \\ \vdots \\ t_n \end{bmatrix}, \quad \nu = m(a^{(k_0)})
\]

where \( t_{l} \in \mathbb{Z}, 1 \leq l \leq n, l \neq m(a^{(k_0)}) \).