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 $(a_1, a_2, ... , a_n) = 1$ we consider the set

$$ S(a_1, a_2, ... , a_n) = \{ \sum_{j=1}^{n} a_j x_j \in N ; x_j \in N, (1 \leq j \leq n) \}. $$

Obviously $b \in S(a_1, a_2, ... , a_n)$ 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

$$ \sum_{j=1}^{n} a_j = (\sum_{j=1}^{n} a_j, \infty). $$

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

1. We put

$$ d_1 = (a_2, a_3, ... , a_n) $$

$$ d_2 = (a_1', a_3', ... , a_n') $$

$$ \vdots $$

$$ d_r = (a_{r+1}', a_{r+2}', ... , a_n', a_{r+1}^{(r-1)}', a_{r+2}^{(r-1)}', \ldots , a_n^{(r-1)}') $$

$$ \vdots $$

$$ d_{n-2} = (a_{n-2}', a_{n-3}', \ldots , a_1^{(n-2)}', a_2^{(n-2)}', \ldots , a_{n-3}'', a_{n-2}'', \ldots , a_1''', a_2''', \ldots , a_{n-3}'''', a_{n-2'''}, \ldots , a_1''''), $$

$$ d_{n-1} = (a_1''''') $$

It is obvious that $d_{n-1} = a_1^{(n-2)}$, $a_n^{(n-1)} = 1$. Now we can prove

$$ (\sum_{j=1}^{n-1} a_j d_j, \infty) \subseteq S(a_1, a_2, ... , a_n) $$

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 $X_1 = x_1^{(4)}$, $X_2 = x_2^{(4)}$. For all $t \in Z$, $X_1 = x_1^{(4)} - a_2 t$, $X_2 = x_1^{(4)} + a_1 t$ are also rational integral solution of $a_1 X_1 + a_2 X_2 = b$. So the fact to be proved is

$$ \{ t \in Z ; x_1^{(4)} - a_2 t > 0, x_1^{(4)} + a_1 t > 0 \} \neq \emptyset $$

i.e. $-\left( \frac{x_1^{(4)}}{a_1}, \frac{x_1^{(4)}}{a_2} \right) \neq \emptyset$.

But this is obvious by the relation

$$ \frac{x_1^{(4)}}{a_2} \left( \frac{-x_1^{(4)}}{a_1} \right) = \frac{b}{a_1 a_2} > 1. $$

* Lecturer (Kōshi) in Mathematics.
Next let us assume
\[ b \in (\sum_{j=1}^{n-1} a_j d_j, \infty), \]
and let us adopt as the assumption of induction
\[ \left( \sum_{j=1}^{n-1} a_j d_j, \infty \right) \subseteq S(a'_1, a'_2, \ldots, a'_n) \]
where \( a'_j \) (\( 2 \leq j \leq n \)) have been defined \( a_j = d_j a'_j \) (\( 2 \leq j \leq n \)). Thus the equation \( \sum_{j=1}^{n-1} a_j X_j = b \) has at least one solution in \( \mathbb{N} \) for all \( b \in (\sum_{j=1}^{n-1} a_j d_j, \infty) \).

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

We can improve on this result by changing the order of \( a_j \) (\( 1 \leq j \leq n \)) suitably. Namely let us \( \mathfrak{S}_n \) be symmetric group of degree \( n \). For any \( \sigma \in \mathfrak{S}_n \) we put
\[ d_\sigma(i) = (a_{\sigma(i)}(2), a_{\sigma(i)}(3), \ldots, a_{\sigma(i)}(n)) \]
where \( a_{\sigma(i)}(j) \) have been defined \( a_{\sigma(i)}(j) = d_\sigma(i) a_{\sigma(i)}(j) \) (\( 2 \leq j \leq n \)).

It is obvious \( d_{n-1}(\sigma) = a_{n-1}^{(n-2)}, a_{n-1}^{(n-2)} = 1 \). We put
\[ M = \left\{ \sigma \in \mathfrak{S}_n \mid \sum_{j=1}^{n-1} a_{\sigma(i)}(j) d_\sigma(i) = \min \sum_{\sigma \in S(\mathfrak{S}_n)} a_{\sigma(i)}(j) d_\sigma(i) \right\} \]
Following the above proof, we have a result,
\[ \left( \sum_{j=1}^{n-1} a_{\sigma(i)}(j) d_\sigma(i), \infty \right) \subseteq S(a_{\sigma(i)}(1), a_{\sigma(i)}(2), \ldots, a_{\sigma(i)}(n)) \]
for any \( \sigma \in M \), and this is better than the above result.

With respect to \( \sigma \in \mathfrak{S}_n \), the fact
\[ a_{\sigma(1)} \leq a_{\sigma(2)} \leq \ldots \leq a_{\sigma(n)} \Rightarrow \sigma \in M \]
is not always correct and there are two cases where
\[ \sum_{j=1}^{n-1} a_{\sigma(i)}(j) d_\sigma(i) \in S(a_{\sigma(i)}(1), a_{\sigma(i)}(2), \ldots, a_{\sigma(i)}(n)) \]
holds and does not hold.

Example 1. \( a_1 = 2, a_2 = 3, a_3 = 4 \).
\[ \sum_{j=1}^{n-1} a_{\sigma(j)}(j) d_\sigma(i) = \begin{cases} 14 & \text{for } \sigma \in \{e=\text{identity of } \mathfrak{S}_3, (23)\} \\ 10 & \text{for } \sigma \in \{(12), (13), (123), (132)\} \end{cases} \]
So \( M = \{ (12), (13), (123), (132) \} \). 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 \( X_1 = x^{(j)} \in N (1 \leq j \leq 3) \) and \( x_i^{(j)} \equiv 0 \mod 2 \). Accordingly \( 3x^{(j)} \geq 6, \) then \( a_1 x^{(j)} + a_2 x^{(j)} + a_3 x^{(j)} \geq 12 \). This is a contradiction.

Example 2. \( a_1 = 3, a_2 = 4, a_3 = 5 \).
\[ \sum_{j=1}^{n-1} a_{\sigma(j)}(j) d_\sigma(i) = \begin{cases} 23 & \text{for } \sigma \in \{e=\text{identity of } \mathfrak{S}_3, (23)\} \\ 19 & \text{for } \sigma \in \{(12), (132)\} \\ 17 & \text{for } \sigma \in \{(13), (123)\} \end{cases} \]
So \( M = \{ (13), (123) \} \). 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
\[
[1, \sum_{j=1}^{n} a_j] \cap S(a_1, a_2, \ldots, a_n) = \emptyset
\]
\[
\sum_{j=1}^{n} a_j \in S(a_1, a_2, \ldots, a_n).
\]
So we are interested in the following finite set
\[
[\sum_{j=1}^{n} a_j, \sum_{j=1}^{n-1} a_j d_j] \cap S(a_1, a_2, \ldots, a_n).
\]
Let us assume
\[
S(a'_1, a'_2, \ldots, a'_n) = \{c_1, c_2, \ldots, c_{n}\} \cup \{b'_n, \infty\}
\]
where \( c_1 < c_2 \cdots < c_{n} = \sum_{j=1}^{n} a'_j, \) and
\[
b'_n = \max\{x \in N; x \in S(a'_1, a'_2, \ldots, a'_n) \leq \sum_{j=1}^{n-1} a'_j d_j, \}
\]
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
\[
\sum_{j=1}^{n} a_j x_j = a_1 x_1 + d_1 \sum_{j=2}^{n} a'_j x_j
\]
we have
\[
S(a_1, a_2, \ldots, a_n) = a_1 N + d_1 S(a'_1, a'_2, \ldots, a'_n)
\]
\[
= (a_1 N + \{d_1 c_1, d_1 c_2, \ldots, d_1 c_{n}\}) \cup (a_1 N + d_1 \{b'_n + N\})
\]
\[
= (a_1 N + \{d_1 c_1, d_1 c_2, \ldots, d_1 c_{n}\}) \cup (d_1 b'_n + S(a_1, d_1))
\]
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 \( a_1 a_2 \in S(a_1, a_2), \) because by \( (a_1, a_2) = 1 \)
\[
\{(x_1, x_2) \in N^2; \ x_2 = \frac{a_1}{a_2} x_1, (0 < x_1 < a_2) \} = \emptyset,
\]
then
\[
\{(x_1, x_2) \in N^2; \ \frac{x_1}{a_2} + \frac{x_2}{a_1} = 1 \} = \emptyset
\]
Next \( \varphi: (x^{(0)}, x^{(1)}) \to a_1 x^{(1)} + a_2 x^{(0)} \) is a bijection from \( \{(x_1, x_2) \in N^2; \ a_1 x_1 + a_2 x_2 < a_1 a_2\} \) onto \( a_1 + a_2, a_1 a_2) \cap S(a_1, a_2). \) This result was suggested by Mr. T. Nagashima, who is a lecturer at Hitotsubashi University. The reason is
\[
b \in [a_1 + a_2, a_1 a_2] \cap S(a_1, a_2)
\]
\[
\Rightarrow \exists (x^{(0)}, x^{(1)}) \in N^2 \ b = a_1 x^{(1)} + a_2 x^{(0)} < a_1 a_2
\]
\[
\Rightarrow \varphi(x^{(0)}, x^{(1)}) = b
\]
\[
\varphi(x^{(0)}, x^{(1)}) = \varphi(x^{(1)}, x^{(1)})
\]
\[
\Rightarrow a_1 x^{(1)} + a_2 x^{(0)} = a_1 x^{(1)} + a_2 x^{(1)}
\]
\[
\Rightarrow a_1 (x^{(1)} - x^{(0)}) = a_2 (x^{(2)} - x^{(0)})
\]
\[
\Rightarrow x^{(0)} \equiv x^{(1)} \ (\text{mod} a_2) \quad \text{(by} \ (a_1, a_2) = 1)\]
but \( 1 \leq x^{(0)} \leq a_2 - 1, \) \( 1 \leq x^{(1)} \leq a_2 - 1, \) then \( x^{(0)} = x^{(1)} \), \( x^{(2)} = x^{(1)}. \)

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_1\}).
So we have
\[
\frac{1}{2}(a_1-1)(a_2-1)
\]
and
\[
\frac{1}{2}(\text{number of the elements in } [a_1+a_2, a_1a_2])
\]
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 \( (a_1, a_2)=1 \),

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

\[
i)-2 \quad \text{When } c\geq2 \text{ i.e. } a_2\geq5, \text{ it is obvious that } \text{number of the elements in } [a_1+a_2, a_1a_2] \cap S(a_1, a_2)\frac{a_2-1}{2},
\]
\[
S(a_1, a_2)=\left\{2s+a_2; s=1, 2, \ldots, \frac{a_2-1}{2}\right\} \cup (a_1a_2, \infty).
\]

ii) When \( a_1\geq3 \), we put \( a_2=a_1q+r, 0\leq r<a_1 \).

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

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 \( 4=3\cdot1+1, \)
\[
V_1=\left\{3x_1+4x_2; 0<x_1 \leq 1+\frac{1}{3}, 1 \leq x_2 \leq 3-1\right\}
\]
\[
V_2=\left\{3x_1+4x_2; 1+\frac{1}{3} \leq x_1 \leq 2\left(1+\frac{1}{3}\right), 1 \leq x_2 \leq 1\right\}.
\]

Now \( d_1=2, d_2=4, \) then
\[
\sum_{j=1}^{2} a_jd_j=34, \quad \sum_{j=1}^{2} a_j=19.
\]
By
\[
(34, \infty) \subseteq S(a_1, a_2, a_3), \quad (0, 19) \cap S(a_1, a_2, a_3)=\phi.
\]
we have
\[
[19, 34]\cap S(a_1, a_2, a_3)=\phi.
\]
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
\[
[19, 34]\cap S(a_1, a_2, a_3)=\phi.
\]
Then
\[ S(a_1, a_2, a_3) = \{19, 24, 25, 27\} \cup (28, \infty) \]
and
\[ \text{Max}\{x \in N; x \in S(a_1, a_2, a_3)\} = 28. \]

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
\[
\begin{align*}
  r_{j-1} &= r_{j-1}q_j + r_j \\
  r_{m-1} &= r_mq_{m+1}
\end{align*}
\]
where \(a_1 = r_0, a_2 = r_{-1}\). Then we have
\[
\begin{align*}
  r_0 > r_1 > r_2 > \cdots > r_{m-1} > r_m > 0
\end{align*}
\]
and
\[ r_m = (a_1, a_2) = 1. \]

For arbitrary rational integer \(b\), let us put
\[
S_j = \left\{ \left( \frac{x^{(j)}}{x_2^{(j)}} \right) \in \mathbb{Z}^2; r_j, x_1^{(j)} + r_{j-1}x_2^{(j)} = b \right\} \quad (0 \leq j \leq m),
\]
then we have
\[
S_m = \left\{ \left( \frac{x_1^{(m)}}{x_2^{(m)}} \right) \in \mathbb{Z}; a_1x_1^{(m)} + a_2x_2^{(m)} = b \right\},
\]
and
\[
\left( \begin{array}{c}
  x_1^{(j)} \\
  x_2^{(j)}
\end{array} \right) \rightarrow Q_j \left( \begin{array}{c}
  x_1^{(j)} \\
  x_2^{(j)}
\end{array} \right), \quad Q_j = \left( \begin{array}{cc}
  -q_j & 1 \\
  1 & 0
\end{array} \right),
\]
\[ (1 \leq j \leq m) \]
are the bijection from \(S_j\) onto \(S_{j-1}\) \((1 \leq j \leq m)\). Accordingly the general solution \(X_1 = x_1^{(m)}, X_2 = x_2^{(m)}\) of the equation \(a_1X_1 + a_2X_2 = b\) are given by the following formula.
\[
\left( \begin{array}{c}
  x_1^{(m)} \\
  x_2^{(m)}
\end{array} \right) = Q_1Q_2\cdots Q_m \left( \begin{array}{c}
  b \\
  0 \\
  1
\end{array} \right), \quad t \in \mathbb{Z}.
\]

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
\[
a = \begin{pmatrix}
a_1 \\
a_2 \\
\vdots \\
a_n
\end{pmatrix},
a_{m(n)} = \text{Min}\{a_j \in \mathbb{Z}; 1 \leq j \leq n, a_j > 0\}
\]
and
\[
a' = \begin{pmatrix}
a'_1 \\
a'_2 \\
\vdots \\
a'_n
\end{pmatrix}, \quad \text{where} \quad a'_j = a_j - (1 - \delta_{j, m(n)})a_{m(n)} \left[ \frac{a_j}{a_{m(n)}} \right]
\]
\[ a_{k+1} = a^{(k)}, \quad k = 1, 2, 3, \ldots \]

Then we have the following result which is easily proved by induction on \(n\),
\[
\exists k_0 \in N; \quad a^{(k_0)} = \begin{pmatrix}
0 \\
\vdots \\
1 \\
0 \\
0
\end{pmatrix} m(a^{(k_0)})
\]

Now we put for any fixed \( b \in \mathbb{Z} \)

\[
S_k = \left\{ \begin{pmatrix} x_{1,k} \\ x_{2,k} \\ \vdots \\ x_{n,k} \\ b \\ t_{\nu-1} \\ t_{\nu+1} \\ \vdots \\ t_n \end{pmatrix} \in \mathbb{Z}^n; \sum_{j=1}^n a_j^{(i)} x_{j,k} = b \right\} \quad (0 \leq k \leq k_0)
\]

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

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

and

\[
Q_k = \begin{pmatrix}
1 & 1 & \cdots & 1 \\
-q_1^{(k-1)} & -q_2^{(k-1)} & \cdots & -q_n^{(k-1)} \\
1 & -q_1^{(k-1)} & \cdots & -q_n^{(k-1)} \\
\vdots & \ddots & \ddots & \ddots \\
1 & \cdots & 1 & 1
\end{pmatrix}
\]

where \( \nu = m(a^{(k-1)}), \quad q_j^{(k-1)} = \left[ \frac{a_j^{(k-1)}}{m(a^{(k-1)})} \right], \quad 1 \leq j \leq n, \ j \neq m(a^{(k-1)}) \), 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,

\[
Q_1 \cdot Q_2 \cdots Q_{k_0} Q_k \begin{pmatrix} t_1 \\ \vdots \\ t_{\nu-1} \\ b \\ t_{\nu+1} \\ \vdots \\ t_n \end{pmatrix} = \begin{pmatrix} x_{1,0} \\ x_{2,0} \\ \vdots \\ x_{n,0} \end{pmatrix} \quad \nu = m(a^{(k_0)}), \quad t_1 \in \mathbb{Z}, \ 1 \leq \nu \leq n, \ \nu \neq m(a^{(k_0)}).