

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

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

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

$$\exists j (1 \leq j \leq n); a_j = 1 \Rightarrow S(a_1, a_2, \dots, a_n) = \left[\sum_{j=1}^n a_j, \infty \right).$$

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

1. We put

$$\begin{array}{lll} d_1 = (a_2, a_3, \dots, a_n) & a_j = d_1 a'_j & 2 \leq j \leq n \\ d_2 = (a'_3, a'_4, \dots, a'_n) & a'_j = d_2 a''_j & 3 \leq j \leq n \\ \vdots & \vdots & \vdots \\ d_r = (a_{r+1}^{(r-1)}, a_{r+2}^{(r-1)}, \dots, a_n^{(r-1)}) & a_j^{(r-1)} = d_r a_j^{(r)} & r+1 \leq j \leq n \\ \vdots & \vdots & \vdots \\ d_{n-2} = (a_{n-1}^{(n-3)}, a_n^{(n-3)}) & a_j^{(n-3)} = d_{n-2} a_j^{(n-2)} & n-1 \leq j \leq n \\ d_{n-1} = (a_n^{(n-2)}) & a_n^{(n-2)} = d_{n-1} a_n^{(n-1)} & \end{array}$$

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

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

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 $X_1 = x_1^{(0)}$, $X_2 = x_2^{(0)}$. For all $t \in Z$, $X_1 = x_1^{(0)} - a_2 t$, $X_2 = x_2^{(0)} + a_1 t$ are also rational integral solution of $a_1 X_1 + a_2 X_2 = b$. So the fact to be proved is

$$\{t \in Z; x_1^{(0)} - a_2 t > 0, x_2^{(0)} + a_1 t > 0\} \neq \emptyset \quad \text{i. e.} \quad \left(-\frac{x_2^{(0)}}{a_1}, \frac{x_1^{(0)}}{a_2} \right) \neq \emptyset.$$

But this is obvious by the relation

$$\frac{x_1^{(0)}}{a_2} - \left(-\frac{x_2^{(0)}}{a_1} \right) = \frac{b}{a_1 a_2} > 1.$$

* Lecturer (*Kōshi*) in Mathematics.

Next let us assume

$$b \in (\sum_{j=2}^{n-1} a_j d_j, \infty),$$

and let us adopt as the assumption of induction

$$(\sum_{j=2}^{n-1} a'_j d_j, \infty) \subseteq S(a'_2, a'_3, \dots, a'_n)$$

where a'_j ($2 \leq j \leq n$) have been defined $a_j = d_1 a'_j$ ($2 \leq j \leq n$). Thus the equation $\sum_{j=2}^n a'_j X_j = b_0$ has at least one solution in N for all $b_0 \in (\sum_{j=2}^{n-1} a'_j d_j, \infty)$.

If we can prove the fact that the equation $a_1 X + d_1 Y = b$ has at least one solution $X = x^{(0)}$, $Y = y^{(0)}$ such that $x^{(0)} \in N, y^{(0)} \in (\sum_{j=2}^{n-1} a'_j d_j, \infty)$, 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 $X_1 = x_1^{(0)} \in N, Y_1 = y_1^{(0)} \in N$. 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

$$\begin{aligned} d_1(\sigma) &= (a_{\sigma(2)}, a_{\sigma(3)}, \dots, a_{\sigma(n)}) & a_{\sigma(j)} &= d_1(\sigma) a'_{\sigma(j)} & 2 \leq j \leq n \\ d_2(\sigma) &= (a'_{\sigma(3)}, a'_{\sigma(4)}, \dots, a'_{\sigma(n)}) & a'_{\sigma(j)} &= d_2(\sigma) a'_{\sigma(j)} & 3 \leq j \leq n \\ & \vdots & & \vdots & \vdots \\ d_r(\sigma) &= (a_{\sigma(r+1)}^{(r-1)}, a_{\sigma(r+2)}^{(r-1)}, \dots, a_{\sigma(n)}^{(r-1)}) & a_{\sigma(j)}^{(r-1)} &= d_r(\sigma) a_{\sigma(j)}^{(r-1)} & r+1 \leq j \leq n \\ & \vdots & & \vdots & \vdots \\ d_{n-2}(\sigma) &= (a_{\sigma(n-1)}^{(n-3)}, a_{\sigma(n)}^{(n-3)}) & a_{\sigma(j)}^{(n-3)} &= d_{n-2}(\sigma) a_{\sigma(j)}^{(n-2)} & r-1 \leq j \leq n \\ d_{n-1}(\sigma) &= (a_{\sigma(n)}^{(n-2)}) & a_{\sigma(n)}^{(n-2)} &= d_{n-1}(\sigma) a_{\sigma(n)}^{(n-1)}. \end{aligned}$$

It is obvious $d_{n-1}(\sigma) = a_{\sigma(n)}^{(n-2)}, a_{\sigma(n)}^{(n-1)} = 1$. We put

$$M = \{ \sigma_0 \in \mathfrak{S}_{n-1}; \sum_{j=1}^{n-1} a_{\sigma_0(j)} d_j(\sigma_0) = \text{Min}_{\sigma \in \mathfrak{S}_n} \sum_{j=1}^{n-1} a_{\sigma(j)} d_j(\sigma) \}$$

Following the above proof, we have a result,

$$(\sum_{j=1}^{n-1} a_{\sigma_0(j)} d_j(\sigma_0), \infty) \subseteq S(a_{\sigma_0(1)}, a_{\sigma_0(2)}, \dots, a_{\sigma_0(n)})$$

for any $\sigma_0 \in M$, and this is better than the above result.

With respect to $\sigma \in \mathfrak{S}_n$, the fact

$$a_{\sigma(1)} \leq a_{\sigma(2)} \leq \dots \leq a_{\sigma(n)} \Rightarrow \sigma \in \bar{M}$$

is not always correct and there are two cases where

$$\sum_{j=1}^{n-1} a_{\sigma_0(j)} d_j(\sigma_0) \in S(a_{\sigma_0(1)}, a_{\sigma_0(2)}, \dots, a_{\sigma_0(n)})$$

holds and does not hold.

Example 1. $a_1 = 2, a_2 = 3, a_3 = 4$.

$$\sum_{j=1}^2 a_{\sigma(j)} d_j(\sigma) = \begin{cases} 14 & \text{for } \sigma \in \{\iota = \text{identity of } \mathfrak{S}_3, (23)\} \\ 10 & \text{for } \sigma \in \{(12), (13), (123), (132)\} \end{cases}$$

So $M = \{(12), (13), (123), (132)\}$. But $10 \notin S(a_1, a_2, a_3)$, 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 $X_j = x_j^{(0)} \in N$ ($1 \leq j \leq 3$) and $x_2^{(0)} \equiv 0 \pmod{2}$. Accordingly $3x_2^{(0)} \geq 6$, then $a_1 x_1^{(0)} + a_2 x_2^{(0)} + a_3 x_3^{(0)} \geq 12$. This is a contradiction.

Example 2. $a_1 = 3, a_2 = 4, a_3 = 5$.

$$\sum_{j=1}^2 a_{\sigma(j)} d_j(\sigma) = \begin{cases} 23 & \text{for } \sigma \in \{\iota = \text{identity of } \mathfrak{S}_3, (23)\} \\ 19 & \text{for } \sigma \in \{(12), (132)\} \\ 17 & \text{for } \sigma \in \{(123), (13)\} \end{cases}$$

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

$$[1, \sum_{j=1}^n a_j] \cap S(a_1, a_2, \dots, a_n) = \phi$$

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

So we are interested in the following finite set

$$[\sum_{j=1}^n a_j, \sum_{j=1}^{n-1} a_j d_j] \cap S(a_1, a_2, \dots, a_n).$$

Let us assume

$$S(a'_2, a'_3, \dots, a'_n) = \{c_1, c_2, \dots, c_l\} \cup (b'_0, \infty)$$

where $c_1 < c_2 < \dots < c_l, c_1 = \sum_{j=2}^n a'_j$, and

$$b'_0 = \text{Max}\{x \in N; x \notin S(a'_2, a'_3, \dots, a'_n)\} \leq \sum_{j=2}^{n-1} a'_j d_j,$$

and $a_j (2 \leq j \leq n)$ have been defined as $a_j = d_1 a'_j (2 \leq j \leq n)$. 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

$$S(a_1, a_2, \dots, a_n) = a_1 N + d_1 S(a'_2, a'_3, \dots, a'_n)$$

$$= (a_1 N + \{d_1 c_1, d_1 c_2, \dots, d_1 c_l\}) \cup (a_1 N + d_1 (b'_0 + N))$$

$$= (a_1 N + \{d_1 c_1, d_1 c_2, \dots, d_1 c_l\}) \cup (d_1 b'_0 + S(a_1, d_1)).$$

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 $a_1 a_2 \notin S(a_1, a_2)$, because by $(a_1, a_2) = 1$

$$\left\{ (x_1, x_2) \in N^2; x_2 = \frac{a_1}{a_2} x_1, (0 <) x_1 < a_2 \right\} = \phi,$$

then $\left\{ (x_1, x_2) \in N^2; \frac{x_1}{a_2} + \frac{x_2}{a_1} = 1 \right\} = \phi$.

Next $\varphi : (x_1^{(0)}, x_2^{(0)}) \rightarrow a_1 x_1^{(0)} + a_2 x_2^{(0)}$ 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

$$b \in [a_1 + a_2, a_1 a_2) \cap S(a_1, a_2)$$

$$\Rightarrow \exists (x_1^{(0)}, x_2^{(0)}) \in N^2, b = a_1 x_1^{(0)} + a_2 x_2^{(0)} < a_1 a_2$$

$$\Rightarrow \varphi(x_1^{(0)}, x_2^{(0)}) = b,$$

$$\varphi(x_1^{(0)}, x_2^{(0)}) = \varphi(x_1^{(1)}, x_2^{(1)})$$

$$\Rightarrow a_1 x_1^{(0)} + a_2 x_2^{(0)} = a_1 x_1^{(1)} + a_2 x_2^{(1)}$$

$$\Rightarrow a_1 (x_1^{(0)} - x_2^{(1)}) = a_2 (x_2^{(1)} - x_2^{(0)})$$

$$\Rightarrow x_1^{(0)} \equiv x_2^{(1)} \pmod{a_2} \quad (\text{by } (a_1, a_2) = 1)$$

but $1 \leq x_1^{(0)} \leq a_2 - 1, 1 \leq x_2^{(1)} \leq a_2 - 1$, then $x_1^{(0)} = x_2^{(1)}, x_2^{(0)} = x_1^{(1)}$.

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

$$\begin{aligned} & \text{number of the elements in } [a_1+a_2, a_1a_2) \cap S(a_1a_2) \\ &= \frac{1}{2}(a_1-1)(a_2-1) \\ &= \frac{1}{2}(\text{number of the elements in } [a_1+a_2, a_1a_2)). \end{aligned}$$

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

$$\begin{aligned} & (\text{number of the elements in } [a_1+a_2, a_1a_2) \cap S(a_1, a_2))=1, \\ & S(a_1, a_2)=\{5\} \cup (6, \infty). \end{aligned}$$

i)-2 When $c \geq 2$ i.e. $a_2 \geq 5$, it is obvious that

$$\begin{aligned} & \text{number of the elements in } [a_1+a_2, a_1a_2) \cap S(a_1, a_2) = \frac{a_2-1}{2}, \\ & S(a_1, a_2) = \left\{ 2s+a_2; s=1, 2, \dots, \frac{a_2-1}{2} \right\} \cup (a_1a_2, \infty). \end{aligned}$$

ii) When $a_1 \geq 3$, we put

$$a_2 = a_1q + r, \quad 0 \leq r < a_1.$$

Then $q \geq 1$ and $1 \leq r < a_1$, and

$$a_1a_2 - (a_1+a_2) = a_2(a_1-2) + (a_2-a_1) \geq 5$$

So number of the elements in $[a_1+a_2, a_1a_2) \geq 5$.

Now we put for any k such that $1 \leq k \leq a_1-1$

$$V_k = \left\{ a_1x_1 + a_2x_2 \in N; (k-1)\left(q + \frac{r}{a_1}\right) < x_1 < k\left(q + \frac{r}{a_1}\right), 1 \leq x_2 \leq a_1-k \right\}.$$

Then $[a_1+a_2, a_1a_2) \cap S(a_1, a_2) = \bigcup_{k=1}^{a_1-1} V_k$.

This is obvious by the bijection $\varphi : (x_1^{(0)}, x_2^{(0)}) \rightarrow a_1x_1^{(0)} + a_2x_2^{(0)}$ from $\{(x_1, x_2) \in N^2; a_1x_1 + a_2x_2 < a_1a_2\}$ onto $[a_1+a_2, a_1a_2) \cap S(a_1, a_2)$.

Example 3. $a_1=5, a_2=6, a_3=8$.

As a preparation

$$\begin{aligned} S(2, 5) &= \{2s+5; s=1, 2\} \cup (10, \infty) \\ &= \{7, 9\} \cup (10, \infty), \\ S(3, 4) &= \{7, 10, 11\} \cup (12, \infty), \end{aligned}$$

because by $4=3 \cdot 1+1$,

$$\begin{aligned} V_1 &= \left\{ 3x_1+4x_2; 0 < x_1 \leq 1 + \frac{1}{3}, 1 \leq x_2 \leq 3-1 \right\} \\ V_2 &= \left\{ 3x_1+4x_2; 1 + \frac{1}{3} < x_1 \leq 2\left(1 + \frac{1}{3}\right), 1 \leq x_2 \leq 1 \right\}. \end{aligned}$$

Now $d_1=2, d_2=4$, then

$$\sum_{j=1}^2 a_j d_j = 34, \quad \sum_{j=1}^2 a_j = 19.$$

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 $[19, 34] \cap S(a_1, a_2, a_3) = [19, 34] \cap (5N + 2S(3, 4))$

$$\begin{aligned}
 &= [19, 34] \cap ((5N + \{14, 20, 22\}) \cup (24 + S(2, 5))) \\
 &= \{19, 24, 25, 27, 29, 30, 32, 34\} \cup \{31, 33\} \\
 &= \{19, 24, 25, 27, 29, 30, 31, 32, 33, 34\}.
 \end{aligned}$$

Then $S(a_1, a_2, a_3) = \{19, 24, 25, 27\} \cup \{28, \infty\}$
 and $\text{Max}\{x \in N; x \notin S(a_1, a_2, a_3)\} = 28.$

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

$$\begin{aligned}
 r_{j-2} &= r_{j-1}q_j + r_j \quad (1 \leq j \leq m) \\
 r_{m-1} &= r_m q_{m+1}
 \end{aligned}$$

where $a_1 = r_0, a_2 = r_{-1}$. Then we have

$$r_0 > r_1 > r_2 > \dots > r_{m-1} > r_m > 0$$

and

$$r_m = (a_1, a_2) = 1.$$

For arbitrary rational integer b , let us put

$$S_j = \left\{ \begin{pmatrix} x_1^{(j)} \\ x_2^{(j)} \end{pmatrix} \in Z^2; r_j x_1^{(j)} + r_{j-1} x_2^{(j)} = b \right\} \quad (0 \leq j \leq m),$$

then we have

$$S_0 = \left\{ \begin{pmatrix} x_1^{(0)} \\ x_2^{(0)} \end{pmatrix} \in Z^2; a_1 x_1^{(0)} + a_2 x_2^{(0)} = b \right\},$$

$$S_m = \left\{ \begin{pmatrix} b & -r_{m-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ t \end{pmatrix} \in Z^2; t \in Z \right\},$$

and

$$\begin{pmatrix} x_1^{(j)} \\ x_2^{(j)} \end{pmatrix} \rightarrow Q_j \begin{pmatrix} x_1^{(j-1)} \\ x_2^{(j-1)} \end{pmatrix}, \quad Q_j = \begin{pmatrix} -q_j & 1 \\ 1 & 0 \end{pmatrix}, \quad (1 \leq j \leq m)$$

are the bijection from S_j onto S_{j-1} ($1 \leq j \leq m$). Accordingly the general solution $X_1 = x_1^{(0)}, X_2 = x_2^{(0)}$ of the equation $a_1 X_1 + a_2 X_2 = b$ are given by the following formula.

$$\begin{pmatrix} x_1^{(0)} \\ x_2^{(0)} \end{pmatrix} = Q_1, Q_2, \dots, Q_m \begin{pmatrix} b & -r_{m-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ t \end{pmatrix}, \quad t \in Z.$$

ii) Now let us consider n dimensional case. For n ($n \geq 2$) rational integers a_j ($1 \leq j \leq n$) such that $(a_1, a_2, \dots, a_n) = 1$ and all of them are not negative, we put

$$\alpha = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \quad a_{m(\alpha)} = \text{Min}\{a_j \in Z; 1 \leq j \leq n, a_j > 0\}$$

and

$$\alpha' = \begin{pmatrix} a'_1 \\ a'_2 \\ \vdots \\ a'_n \end{pmatrix}, \quad \text{where } a'_j = a_j - (1 - \delta_{j, m(\alpha)}) a_{m(\alpha)} \left[\frac{a_j}{a_{m(\alpha)}} \right]$$

$$\alpha^{(k+1)} = \alpha^{(k)'} \quad k = 1, 2, 3, \dots$$

Then we have the following result which is easily proved by induction on n ,

$$\exists k_0 \in N; \alpha^{(k_0)} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} m(\alpha^{(k_0)})$$

Now we put for any fixed $b \in Z$

$$S_k = \left\{ \begin{pmatrix} x_{1,k} \\ x_{2,k} \\ \vdots \\ x_{n,k} \end{pmatrix} \in Z^n; \sum_{j=1}^n a_j^{(k)} x_{j,k} = b \right\} \quad (0 \leq k \leq k_0)$$

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

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

and

$$\begin{pmatrix} x_{1,k} \\ x_{2,k} \\ \vdots \\ x_{n,k} \end{pmatrix} \rightarrow Q_k \begin{pmatrix} x_{1,k} \\ x_{2,k} \\ \vdots \\ x_{n,k} \end{pmatrix}, Q_k = \left(\begin{array}{cccccccc} 1 & & & & & & & \\ & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ & & & & -q_{\nu-1}^{(k-1)} & 1 & -q_{\nu+1}^{(k-1)} & \dots -q_n^{(k-1)} \\ & & & & & & 1 & \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{array} \right)$$

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

$$\begin{pmatrix} x_{1,0} \\ x_{2,0} \\ \vdots \\ x_{n,0} \end{pmatrix} = Q_1 \cdot Q_2 \cdot \dots \cdot Q_{k_0} \begin{pmatrix} t_1 \\ \vdots \\ t_{\nu-1} \\ b \\ t_{\nu+1} \\ \vdots \\ t_n \end{pmatrix} \quad \left(\begin{array}{l} \nu = m(a^{(k_0)}) \\ t_l \in Z, 1 \leq l \leq n, l \neq m(a^{(k_0)}) \end{array} \right)$$