Wojciech Guzicki — Treść zadania, Opracowanie
Marcin Mucha — Program

Skoczki

Skoczek porusza się po nieskończonej szachownicy. Każdy z ruchów, jakie może wykonać skoczek, można opisać parą liczb całkowitych — para (a,b) odpowiada możliwości wykonania ruchu z pola o współrzędnych (x,y) na pole $(x+a,y+b)$ lub $(x-a,y-b)$. Dla każdego skoczka określony jest zestaw takich par, opisujących ruchy jakie może wykonywać skoczek. Zakładamy, że pola, na które może ruszyć się skoczek z pola $(0,0)$ nie leżą wszystkie na jednej prostej.

Powiemy, że dwa skoczki są równoważne, jeżeli dla obu skoczków zbiory pól, do jakich mogą dotrzeć z pola $(0,0)$ (być może w wielu ruchach) są takie same. (Przy czym równoważne skoczki mogą docierać do tych pól w różnych liczbach kroków). Można pokazać, że dla każdego skoczka istnieje równoważny mu skoczek, którego ruchy są opisane za pomocą tylko dwóch par liczb.

Zadanie

Twoje zadanie polega na napisaniu programu, który:

- *wczyta ze standardowego wejścia pary liczb całkowitych opisujące ruchy skoczka,*
- *wyznaczy dwie pary liczb całkowitych opisujące skoczka równoważnego danemu skoczkowi,*
- *wypisze wyznaczone dwie pary liczb na standardowe wyjście.*

Wejście

W pierwszym wierszu standardowego wejścia zapisana jest jedna liczba całkowita n, liczba par liczb opisujących ruchy danego skoczka, $3 \leqslant n \leqslant 100$. W kolejnych n wierszach zapisane są pary liczb opisujące ruchy danego skoczka, po jednej w wierszu. W każdym z tych wierszy zapisane są po dwie liczby całkowite a_i i b_i oddzielone pojedynczym odstępem, $-100 \leqslant a_i, b_i \leqslant 100$. Zakładamy, że $(a_i, b_i) \neq (0,0)$.

Wyjście

W pierwszym wierszu standardowego wyjścia należy wypisać dwie liczby całkowite a i b oddzielone pojedynczym odstępem, $-10\,000 \leqslant a,b \leqslant 10\,000$. W drugim wierszu należy zapisać dwie liczby całkowite c i d oddzielone pojedynczym odstępem, $-10\,000 \leqslant c,d \leqslant 10\,000$. Powinny to być takie liczby całkowite, że skoczek, którego ruchy są opisane parami (a,b) i (c,d) jest równoważny skoczkowi opisanemu w danych wejściowych.

Przykład

Dla danych wejściowych:

```
3
24 28
15 50
12 21
```

poprawne wyjście może mieć np. postać:

```
468 1561
2805 9356
```

lub:

```
3 0
0 1
```

Rozwiązanie

Wprowadzenie – kraty na płaszczyźnie

Problem przedstawiony w zadaniu sprowadza się do zagadnienia znajdowania bazy kraty na płaszczyźnie. Pojęcie kraty jest omówione dokładnie w [11] (zadanie „Tomki”, str. 217 – 222). Tutaj je tylko krótko przypomnimy.

Definicja 1 Niech $\vec{a}_1,\ldots,\vec{a}_n$ będą dowolnymi niezerowymi wektorami na płaszczyźnie. Zbiór $L(\vec{a}_1,\ldots,\vec{a}_n)$ zdefiniowany w następujący sposób:

$$L(\vec{a}_1,\ldots,\vec{a}_n)=\left\{m_1\cdot\vec{a}_1+\ldots+m_n\cdot\vec{a}_n:\ m_1,\ldots,m_n\in\mathbb{Z}\right\}$$

nazywamy *kratą* rozpiętą przez wektory $\vec{a}_1,\ldots,\vec{a}_n$. Jeśli $\vec{c}=m_1\cdot\vec{a}_1+\ldots+m_n\cdot\vec{a}_n$, to wektor $\vec{c}$ nazywamy *kombinacją liniową* wektorów $\vec{a}_1,\ldots,\vec{a}_n$, a liczby $m_1,\ldots,m_n$ nazywamy *współczynnikami* tej kombinacji. Krata rozpięta przez n wektorów składa się zatem ze wszystkich kombinacji liniowych tych n wektorów, przy czym wszystkie współczynniki tych kombinacji są liczbami całkowitymi.

W dalszym ciągu będziemy korzystać z następującego prostego warunku równości dwóch krat. Przypuśćmy, że mamy dwie kraty $L(\vec{a}_1,\ldots,\vec{a}_m)$ oraz $L(\vec{b}_1,\ldots,\vec{b}_n)$. Wówczas jeśli

$$\vec{a}_1,\ldots,\vec{a}_m\in L(\vec{b}_1,\ldots,\vec{b}_n)\quad\text{oraz}\quad\vec{b}_1,\ldots,\vec{b}_n\in L(\vec{a}_1,\ldots,\vec{a}_m),$$

to

$$L(\vec{a}_1,\ldots,\vec{a}_m)=L(\vec{b}_1,\ldots,\vec{b}_n).$$

Definicja 2 Wektory $\vec{a}_1,\ldots,\vec{a}_n$ nazywamy wektorami *liniowo niezależnymi*, jeśli dla dowolnych liczb rzeczywistych $t_1,\ldots,t_n$ wektor

$$t_1\cdot\vec{a}_1+\ldots+t_n\cdot\vec{a}_n$$

jest wektorem zerowym tylko wówczas, gdy wszystkie liczby $t_1, \ldots, t_n$ są zerami. Wektory nazywamy *liniowo zależnymi*, jeśli nie są liniowo niezależne. Jeśli wektory generujące kratę są liniowo niezależne, to mówimy, że tworzą one *bazę* tej kraty.

Można udowodnić, że na płaszczyźnie każdy zbiór wektorów liniowo niezależnych składa się z co najwyżej dwóch wektorów. Ponadto dwa wektory na płaszczyźnie są liniowo zależne wtedy i tylko wtedy, gdy są równoległe. Z tego wynika, że jeśli wszystkie wektory kraty są równoległe, to baza tej kraty składa się z tylko jednego wektora. Jeśli zaś w kracie istnieją dwa wektory nierównoległe, to baza tej kraty musi składać się z dokładnie dwóch wektorów. Nasze zadanie polega zatem na znalezieniu co najwyżej dwuelementowej bazy kraty rozpiętej przez n wektorów, z których każdy ma obie współrzędne całkowite.

Rozwiązanie pierwsze

Przedstawimy dwa rozwiązania naszego zadania — jako pierwsze opiszemy bardziej ogólne (patrz porównanie rozwiązań w rozdziale **Uwagi końcowe**). Schemat postępowania w obu rozwiązaniach będzie taki sam. Pokażemy jak wejściowy zbiór wektorów $\overrightarrow{a}_1, \overrightarrow{a}_2, \ldots, \overrightarrow{a}_n$ można redukować krok po kroku zmniejszając jego moc, by na końcu otrzymać bazę złożoną z dwóch wektorów (bądź z jednego wektora, gdy zbiór wejściowy składa się z wektorów równoległych). Podstawowym krokiem algorytmu będzie zastąpienie trójelementowego (odpowiednio dwuelementowego) zbioru wektorów generującego kratę przez zbiór dwuelementowy (odpowiednio jednoelementowy) generujący tę samą kratę.

Na początku pokażemy kilka własności kombinacji liniowych wektorów, w których dopuszczamy *współczynniki wymierne* kombinacji. Niech $\overrightarrow{a} = [x_a, y_a]$ i $\overrightarrow{b} = [x_b, y_b]$ będą dwoma niezerowymi wektorami o współrzędnych całkowitych. W zależności od ich wzajemnego położenia zachodzą następujące fakty.

Fakt 1 *Niech $\overrightarrow{a}$ i $\overrightarrow{b}$ będą wektorami równoległymi. Wtedy istnieje liczba wymierna t taka, że $\overrightarrow{b} = t \cdot \overrightarrow{a}$.*

Dowód Przypuśćmy, że $x_a \neq 0$. Przyjmijmy

$$t = \frac{x_b}{x_a}.$$

Ponieważ wektory $\overrightarrow{a}$ i $\overrightarrow{b}$ są równoległe, więc

$$\begin{vmatrix} x_a & x_b \\ y_a & y_b \end{vmatrix} = 0,$$

czyli $x_a \cdot y_b = x_b \cdot y_a$. Stąd wynika, że $y_a = \frac{x_a}{x_b} \cdot y_b$, a więc

$$t \cdot \overrightarrow{a} = \left[x_a \cdot \frac{x_b}{x_a}, y_a \cdot \frac{x_b}{x_a} \right] = [x_b, y_b] = \overrightarrow{b}.$$

Oczywiście liczba t jest wymierna.

■

Fakt 2 *Załóżmy, że wektory $\overrightarrow{\boldsymbol{a}}$ i $\overrightarrow{\boldsymbol{b}}$ nie są równoległe. Wtedy dla dowolnego wektora $\overrightarrow{\boldsymbol{c}}$ o współrzędnych całkowitych istnieją liczby wymierne t i u takie, że*

$$\overrightarrow{\boldsymbol{c}} = t \cdot \overrightarrow{\boldsymbol{a}} + u \cdot \overrightarrow{\boldsymbol{b}}.$$

Dowód Oznaczmy $\overrightarrow{\boldsymbol{c}} = [x_c, y_c]$. Poszukiwane liczby t i u są rozwiązaniem układu równań

$$\begin{cases} x_a \cdot t + x_b \cdot u &= x_c \\ y_a \cdot t + y_b \cdot u &= y_c \end{cases},$$

czyli

$$t = \frac{\begin{vmatrix} x_c & x_b \\ y_c & y_b \end{vmatrix}}{\begin{vmatrix} x_a & x_b \\ y_a & y_b \end{vmatrix}} \quad \text{oraz} \quad u = \frac{\begin{vmatrix} x_a & x_c \\ y_a & y_c \end{vmatrix}}{\begin{vmatrix} x_a & x_b \\ y_a & y_b \end{vmatrix}}.$$

Oczywiście liczby t i u są wymierne, a więc mamy poszukiwane współczynniki wymierne. ■

W przedstawionych faktach pokazaliśmy, jak można zredukować liczbę wektorów „generujących”, gdy dopuszczamy w kombinacjach liniowych współczynniki wymierne. Teraz powróćmy do krat i rozważania kombinacji liniowych o *współczynnikach całkowitych*. Ponownie oddzielnie rozważymy przypadek wektorów równoległych i nierównoległych.

Lemat 3 *Dla wektorów równoległych $\overrightarrow{\boldsymbol{a}}$ i $\overrightarrow{\boldsymbol{b}}$ istnieje wektor $\overrightarrow{\boldsymbol{c}}$ taki, że $L(\overrightarrow{\boldsymbol{a}}, \overrightarrow{\boldsymbol{b}}) = L(\overrightarrow{\boldsymbol{c}})$.*

Dowód W fakcie 1 pokazaliśmy, że istnieje liczba wymierna t taka, że

$$\overrightarrow{\boldsymbol{b}} = t \cdot \overrightarrow{\boldsymbol{a}},$$

zatem przyjmując $t = \frac{p}{q}$ dla $\mathrm{NWD}(p,q) = 1$ mamy

$$q \cdot \overrightarrow{\boldsymbol{b}} \quad = \quad p \cdot \overrightarrow{\boldsymbol{a}}. \tag{1}$$

Szukamy wektora $\overrightarrow{\boldsymbol{c}}$ takiego, że

$$\overrightarrow{\boldsymbol{a}} = m \cdot \overrightarrow{\boldsymbol{c}}, \quad \overrightarrow{\boldsymbol{b}} = n \cdot \overrightarrow{\boldsymbol{c}} \quad \text{oraz}$$

$$\overrightarrow{\boldsymbol{c}} \quad = \quad k \cdot \overrightarrow{\boldsymbol{a}} + l \cdot \overrightarrow{\boldsymbol{b}} \tag{2}$$

dla pewnych liczb całkowitych k, l, m i n. Stąd równość (1) przybiera postać

$$qn \cdot \overrightarrow{\boldsymbol{c}} = pm \cdot \overrightarrow{\boldsymbol{c}},$$

a równość (2) postać

$$\overrightarrow{\boldsymbol{c}} = km \cdot \overrightarrow{\boldsymbol{c}} + ln \cdot \overrightarrow{\boldsymbol{c}}.$$

Przyjmując $m = q$ oraz $n = p$ mamy więc

$$\overrightarrow{\boldsymbol{c}} = (kq + lp) \cdot \overrightarrow{\boldsymbol{c}}.$$

Wystarczy więc wybrać takie liczby k i l, by

$$kq + lp = 1.$$

Jest to możliwe, gdyż liczby p i q są względnie pierwsze, stąd liczby k i l można obliczyć na przykład za pomocą rozszerzonego algorytmu Euklidesa (patrz [17]). ■

Podsumujmy rozwiązanie w przypadku, gdy wektory $\overrightarrow{a}$ i $\overrightarrow{b}$ są równoległe. Wtedy istnieją liczby całkowite p i q, takie że $q \cdot \overrightarrow{b} = p \cdot \overrightarrow{a}$ oraz $\mathrm{NWD}(p,q) = 1$. Wystarczy znaleźć liczby całkowite k i l takie, że

$$kq + lp = 1,$$

a następnie przyjąć $\overrightarrow{c} = k \cdot \overrightarrow{a} + l \cdot \overrightarrow{b}$. Wówczas oczywiście $\overrightarrow{c} \in L(\overrightarrow{a}, \overrightarrow{b})$, a ponadto zachodzą równości:

$$\begin{aligned}
q \cdot \overrightarrow{c} &= q(k \cdot \overrightarrow{a} + l \cdot \overrightarrow{b}) = kq \cdot \overrightarrow{a} + lq \cdot \overrightarrow{b} = (1 - lp) \cdot \overrightarrow{a} + lq \cdot \overrightarrow{b} = \\
&= \overrightarrow{a} - lp \cdot \overrightarrow{a} + lq \cdot \overrightarrow{b} = \overrightarrow{a} + l(q \cdot \overrightarrow{b} - p \cdot \overrightarrow{a}) = \overrightarrow{a}, \\
p \cdot \overrightarrow{c} &= p(k \cdot \overrightarrow{a} + l \cdot \overrightarrow{b}) = kp \cdot \overrightarrow{a} + lp \cdot \overrightarrow{b} = kp \cdot \overrightarrow{a} + (1 - kq) \cdot \overrightarrow{b} = \\
&= kp \cdot \overrightarrow{a} + \overrightarrow{b} - kq \cdot \overrightarrow{b} = \overrightarrow{b} + k(p \cdot \overrightarrow{a} - q \cdot \overrightarrow{b}) = \overrightarrow{b}.
\end{aligned}$$

To dowodzi, że $\overrightarrow{a}, \overrightarrow{b} \in L(\overrightarrow{c})$, czyli $L(\overrightarrow{a}, \overrightarrow{b}) = L(\overrightarrow{c})$. Ostatecznie więc zastąpiliśmy dwa równoległe wektory generujące kratę przez jeden.

Lemat 4 *Załóżmy, że wektory $\overrightarrow{a}$ i $\overrightarrow{b}$ nie są równoległe. Niech $\overrightarrow{c}$ będzie dowolnym wektorem o współrzędnych całkowitych. Pokażemy, że istnieją wektory $\overrightarrow{d}$ i $\overrightarrow{e}$ takie, że*

$$L(\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{c}) = L(\overrightarrow{d}, \overrightarrow{e}).$$

Dowód lematu przeprowadzimy najpierw dla pewnych przypadków szczególnych. Potem rozważymy sytuację ogólną i pokażemy jak można wówczas udowodnić lemat odwołując się do pokazanych wcześniej przypadków.

Na wstępie przypomnijmy, iż z faktu 2 wiemy już, że istnieją liczby wymierne t i u takie, że

$$\overrightarrow{c} = t \cdot \overrightarrow{a} + u \cdot \overrightarrow{b}.$$

Jeśli $u = 0$, to $\overrightarrow{c} = t \cdot \overrightarrow{a}$, więc wektory $\overrightarrow{a}$ i $\overrightarrow{c}$ są równoległe. Z lematu 3 istnieje zatem wektor $\overrightarrow{d}$ taki, że $L(\overrightarrow{a}, \overrightarrow{c}) = L(\overrightarrow{d})$. Wówczas oczywiście

$$L(\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{c}) = L(\overrightarrow{b}, \overrightarrow{d}).$$

Analogiczna sytuacja ma miejsce, gdy $t = 0$.

Przypuśćmy teraz, że obie liczby t i u są różne od zera. Wtedy istnieją liczby całkowite (różne od zera) p, q i r takie, że

$$r \cdot \overrightarrow{c} = p \cdot \overrightarrow{a} + q \cdot \overrightarrow{b}. \tag{3}$$

Możemy oczywiście wybrać liczby p, q i r tak, by nie miały wspólnego dzielnika większego od 1 (choć każde dwie mogą mieć taki wspólny dzielnik).

Dowód (*Przypadek szczególny*) Przypuśćmy najpierw, że liczby p i r są względnie pierwsze:

$$\mathrm{NWD}(p,r) = 1.$$

Pokażemy, że istnieje wtedy wektor $\overrightarrow{d}$ taki, że

$$L(\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{c}) = L(\overrightarrow{b}, \overrightarrow{d}).$$

Poszukiwany wektor $\overrightarrow{d}$ musi być kombinacją liniową wektorów $\overrightarrow{a}$, $\overrightarrow{b}$ i $\overrightarrow{c}$ o współczynnikach całkowitych, spełniającą równości:

$$\begin{aligned} \overrightarrow{a} &= k \cdot \overrightarrow{b} + l \cdot \overrightarrow{d}, && (4) \\ \overrightarrow{c} &= m \cdot \overrightarrow{b} + n \cdot \overrightarrow{d} && (5) \end{aligned}$$

dla pewnych liczb całkowitych k, l, m i n. To oznacza, iż równość (3) musi mieć postać

$$rm \cdot \overrightarrow{b} + rn \cdot \overrightarrow{d} = kp \cdot \overrightarrow{b} + lp \cdot \overrightarrow{d} + q \cdot \overrightarrow{b}. \tag{6}$$

Ponieważ $\overrightarrow{b}$ i $\overrightarrow{d}$ są niezależne (nierównoległe), więc równość (6) zachodzi wtedy i tylko wtedy, gdy

$$rm - kp = q \quad \text{oraz} \quad rn = lp. \tag{7}$$

Liczby k, l, m i n spełniające warunki (7) możemy dobrać w następujący sposób. Najpierw przyjmujemy $n = p$ oraz $l = r$, a następnie (za pomocą rozszerzonego algorytmu Euklidesa) znajdujemy takie liczby m_0 i k_0, że

$$rm_0 - pk_0 = 1.$$

Wreszcie przyjmujemy $m = m_0 q$ oraz $k = k_0 q$. Wówczas oczywiście $rm - pk = q$, a równości (4) i (5) przyjmują postać

$$\begin{aligned} \overrightarrow{a} &= k_0 q \cdot \overrightarrow{b} + r \cdot \overrightarrow{d}, && (8) \\ \overrightarrow{c} &= m_0 q \cdot \overrightarrow{b} + p \cdot \overrightarrow{d}. && (9) \end{aligned}$$

Mnożąc obie strony równości (8) przez m_0, równości (9) przez k_0, a następnie odejmując je stronami, otrzymujemy

$$m_0 \cdot \overrightarrow{a} - k_0 \cdot \overrightarrow{c} = (rm_0 - pk_0) \cdot \overrightarrow{d},$$

czyli

$$\overrightarrow{d} = m_0 \cdot \overrightarrow{a} - k_0 \cdot \overrightarrow{c}. \tag{10}$$

Stąd (oraz z równości (8) i (9)) oczywiście wynika, że

$$L(\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{c}) = L(\overrightarrow{b}, \overrightarrow{d}).$$

■

Podsumujmy rozwiązanie w *przypadku szczególnym*. Mamy wektory $\overrightarrow{a}$, $\overrightarrow{b}$ i $\overrightarrow{c}$ oraz liczby całkowite p, q i r spełniające równość (3). Dodatkowo zakładamy, że liczby r i p są względnie pierwsze. Za pomocą rozszerzonego algorytmu Euklidesa znajdujemy liczby m_0 i k_0 takie, że $rm_0 - pk_0 = 1$ i definiujemy wektor

$$\overrightarrow{d} = m_0 \cdot \overrightarrow{a} - k_0 \cdot \overrightarrow{c}.$$

Możemy sprawdzić, że zachodzą równości:

$$\begin{aligned}
k_0 q \cdot \overrightarrow{b} + r \cdot \overrightarrow{d} &= k_0 q \cdot \overrightarrow{b} + m_0 r \cdot \overrightarrow{a} - k_0 r \cdot \overrightarrow{c} = \\
&= k_0 q \cdot \overrightarrow{b} + m_0 r \cdot \overrightarrow{a} - k_0 p \cdot \overrightarrow{a} - k_0 q \cdot \overrightarrow{b} = \\
&= (m_0 r - k_0 p) \cdot \overrightarrow{a} = \overrightarrow{a}, \\
m_0 q \cdot \overrightarrow{b} + p \cdot \overrightarrow{d} &= m_0 q \cdot \overrightarrow{b} + m_0 p \cdot \overrightarrow{a} - k_0 p \cdot \overrightarrow{c} = \\
&= m_0 q \cdot \overrightarrow{b} + m_0 p \cdot \overrightarrow{a} - (m_0 r - 1) \cdot \overrightarrow{c} = \\
&= m_0 q \cdot \overrightarrow{b} + m_0 p \cdot \overrightarrow{a} - m_0 r \cdot \overrightarrow{c} + \overrightarrow{c} = \\
&= m_0 (p \cdot \overrightarrow{a} + q \cdot \overrightarrow{b} - r \cdot \overrightarrow{c}) + \overrightarrow{c} = \overrightarrow{c}.
\end{aligned}$$

To dowodzi, że $L(\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{c}) = L(\overrightarrow{b}, \overrightarrow{d})$.

Dowód (*Sytuacja ogólna*) Rozważmy teraz sytuację, gdy liczby występujące w równości (3) są dowolne, czyli liczba r być może nie jest względnie pierwsza z p.

Najpierw znajdujemy liczby r_1 i r_2 takie, że $r = r_1 r_2$, $\mathrm{NWD}(r_1, q) = 1$ oraz $\mathrm{NWD}(r_2, p) = 1$. Na przykład możemy przyjąć, że liczba r_1 jest iloczynem tych czynników pierwszych liczby r, które są dzielnikami p, a r_2 jest iloczynem pozostałych czynników pierwszych r. Wówczas równość (3) ma postać

$$r_2 \cdot r_1 \cdot \overrightarrow{c} \quad = \quad p \cdot \overrightarrow{a} + q \cdot \overrightarrow{b}. \tag{11}$$

Zauważmy, że w powyższym wzorze współczynniki przy wektorach $\overrightarrow{a}$ i $r_1 \cdot \overrightarrow{c}$ są względnie pierwsze, stąd dla trójki wektorów $\overrightarrow{a}$, $\overrightarrow{b}$ i $r_1 \cdot \overrightarrow{c}$ możemy zastosować postępowanie opisane w *przypadku szczególnym*. Znajdujemy więc liczby m_0 i k_0 takie, że $r_2 m_0 - pk_0 = 1$ i definiujemy wektor $\overrightarrow{d}$ analogicznie jak we wzorze (10)

$$\overrightarrow{d} = m_0 \cdot \overrightarrow{a} - k_0 (r_1 \cdot \overrightarrow{c}).$$

Wtedy

$$L(\overrightarrow{b}, \overrightarrow{d}) = L(\overrightarrow{a}, \overrightarrow{b}, r_1 \cdot \overrightarrow{c}).$$

Ponieważ rozszerzając zbiory generujące dwóch krat o ten sam wektor nadal otrzymujemy równe kraty, więc mamy (ostatnią równość otrzymujemy dzięki wyeliminowaniu ze zbioru generującego jednego z dwóch wektorów równoległych):

$$L(\overrightarrow{b}, \overrightarrow{d}, \overrightarrow{c}) = L(\overrightarrow{a}, \overrightarrow{b}, r_1 \cdot \overrightarrow{c}, \overrightarrow{c}) = L(\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{c}).$$

Następnie dla wektora $r_1 \cdot \overrightarrow{c}$ mamy równość analogiczną do (9)

$$r_1 \cdot \overrightarrow{c} = m_0 q \cdot \overrightarrow{b} + p \cdot \overrightarrow{d}. \tag{12}$$

Zauważmy, że ponieważ $\mathrm{NWD}(r_1, q) = 1$, także liczby m_0 i r_1 muszą być względnie pierwsze. Gdyby nie były i liczba $s > 1$ byłaby ich wspólnym dzielnikiem, to liczba s byłaby także dzielnikiem p (ze wzoru (12)) i stąd także dzielnikiem $r_2m_0 - pk_0$. Ponieważ ostatnia liczba jest równa 1, więc dochodzimy w ten sposób do sprzeczności. Zatem $\mathrm{NWD}(r_1, m_0) = 1$, czyli także $\mathrm{NWD}(r_1, m_0q) = 1$. To pozwala nam ponownie zastosować rozumowanie analogiczne jak w *przypadku szczególnym* tym razem dla wektorów $\vec{c}$, $\vec{b}$ i $\vec{d}$ powiązanych zależnością (12). W ten sposób znajdujemy wektor $\vec{e}$ taki, że

$$L(\vec{b}, \vec{d}, \vec{c}) = L(\vec{d}, \vec{e}).$$

Ostatecznie więc

$$L(\vec{a}, \vec{b}, \vec{c}) = L(\vec{b}, \vec{d}, \vec{c}) = L(\vec{d}, \vec{e}),$$

co kończy dowód lematu. Wypisanie dokładnych wzorów na współrzędne wektorów $\vec{d}$ i $\vec{e}$ pozostawiamy jako ćwiczenie. ■

W dowodach lematów 3 i 4 jest zawarty opis algorytmu rozwiązania zadania. Rozpoczynamy od zbioru wektorów $\{\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n\}$ i przyjmujemy $\vec{a} = \vec{a}_1$ oraz $\vec{b} = \vec{a}_2$. Następnie rozważamy kolejno $\vec{c} = \vec{a}_i$, dla $i = 3, 4, \ldots, n$. Wiemy już, że krata $L(\vec{a}, \vec{b}, \vec{c})$ ma bazę złożoną z co najwyżej dwóch wektorów. Znajdujemy je jak w dowodach lematów, zastępujemy nimi $\vec{a}$ i $\vec{b}$, a zbiór wektorów redukujemy do $\{\vec{a}, \vec{b}, \vec{a}_{i+1}, \ldots, \vec{a}_n\}$. Na końcu dostajemy poszukiwaną bazę kraty złożoną z co najwyżej dwóch wektorów. Podstawową wadą tej metody jest to, że współrzędne otrzymanych wektorów bazowych szybko rosną, ale korzystając z rozwiązania zadania „Tomki” (por.[11]) możemy znaleźć za każdym razem równoważną bazę złożoną z wektorów krótkich.

Rozwiązanie wzorcowe

Opiszemy teraz drugie rozwiązanie. Jest ono oparte na następującej obserwacji.

Lemat 5 *Dla dowolnych wektorów $\vec{a}$ i $\vec{b}$ istnieją wektory*

$$\vec{c} = [x_c, 0] \quad \textit{oraz} \quad \vec{d} = [x_d, y_d]$$

takie, że $L(\vec{a}, \vec{b}) = L(\vec{c}, \vec{d})$.

Dowód Jeśli $y_a = 0$ lub $y_b = 0$, to lemat jest oczywisty, rozważmy więc przypadek, gdy $y_a \neq 0$ oraz $y_b \neq 0$. Zdefiniujmy

$$m = \mathrm{NWD}(y_a, y_b), \quad k = \frac{y_a}{m} \quad \text{oraz} \quad l = \frac{y_b}{m}.$$

Wówczas $\mathrm{NWD}(k, l) = 1$ i za pomocą rozszerzonego algorytmu Euklidesa znajdujemy liczby p i q takie, że $kp + lq = 1$. Wtedy $y_ap + y_bq = m$. Stąd łatwo wynika, że wektory

$$\vec{c} = l \cdot \vec{a} - k \cdot \vec{b} \quad \text{oraz} \quad \vec{d} = p \cdot \vec{a} + q \cdot \vec{b}$$

są szukanymi wektorami. Mianowicie

$$\vec{c} = [lx_a - kx_b, 0]$$

oraz $\vec{c}, \vec{d} \in L(\vec{a}, \vec{b})$. Ponadto

$$\vec{a} = q \cdot \vec{c} + k \cdot \vec{d} \quad \text{oraz} \quad \vec{b} = -p \cdot \vec{c} + l \cdot \vec{d},$$

skąd wynika, że $\vec{a}, \vec{b} \in L(\vec{c}, \vec{d})$.

Można także łatwo dowieść, że jeśli wektory $\vec{a}$ i $\vec{b}$ są równoległe, to otrzymany wektor $\vec{c}$ jest wektorem zerowym i wtedy $L(\vec{a}, \vec{b}) = L(\vec{d})$. ■

Teraz możemy opisać algorytm oparty na lemacie 5. Rozpoczynamy od zbioru wektorów $\{\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n\}$. Przyjmujemy $\vec{a} = \vec{a}_1$ i rozważamy kolejno pary wektorów $\vec{a}$, $\vec{a}_i$ dla $i = 2, 3, \ldots, n$. Każdą taką parę zastępujemy przez dwa wektory, z których jeden wektor (oznaczymy go $\vec{b}_i$) ma drugą współrzędną zerową (drugi wektor z pary podstawiamy pod $\vec{a}$). W ten sposób otrzymujemy zbiór wektorów $\{\vec{a}, \vec{b}_2, \vec{b}_3, \ldots, \vec{b}_n\}$, gdzie tylko $\vec{a}$ może mieć obie współrzędne niezerowe, a pozostałe wektory mają drugą współrzędną zerową. Teraz zauważmy, że dwa wektory

$$\vec{b}_2 = [x_2, 0] \quad \text{oraz} \quad \vec{b}_3 = [x_3, 0]$$

możemy zastąpić jednym wektorem $\vec{b} = [x, 0]$, gdzie $x = \mathrm{NWD}(x_2, x_3)$. Powtarzając to postępowanie kolejno dla par wektorów $\vec{b}$ i $\vec{b}_i$ dla $i = 4, 5, \ldots, n$ na końcu dostajemy poszukiwaną bazę złożoną z co najwyżej dwóch wektorów. Program wzorcowy był oparty na tym algorytmie.

Uwagi końcowe

Zauważmy, że w algorytmie wzorcowym istotne było to, że wszystkie współrzędne wektorów były liczbami całkowitymi. Natomiast pierwszy z przedstawionych algorytmów jest nieco ogólniejszy. Założenie, iż współrzędne wektorów są całkowite, było w nim wykorzystane tylko do wykazania, że istnieją liczby całkowite p, q i r spełniające równości (1) i (3). Wiele innych krat ma te własności i algorytm pierwszy pozwala znaleźć co najwyżej dwuelementową bazę takiej kraty. Natomiast może okazać się, że w takiej kracie nie istnieje żaden wektor postaci $[x, 0]$, a więc nie można zastosować algorytmu wzorcowego.

Testy

Zadanie było testowane za pomocą 10 testów generowanych losowo. Zawsze najpierw była ustalana baza, a następnie były generowane losowo wektory kraty. Dla utrudnienia dbano o to, by wektory bazowe nie znalazły się wśród wektorów generowanych losowo, a także, by nie istniała baza złożona z wektora poziomego i pionowego.

W poniższej tabeli *n* oznacza liczbę wektorów odpowiadających ruchom skoczka.

Nazwa	**n**	**Opis**
sko1.in	3	test zawierający 2 wektory liniowo zależne
sko2.in	5	test losowy
sko3.in	10	test losowy
sko4.in	20	test losowy
sko5.in	50	test losowy
sko6.in	60	test losowy
sko7.in	70	test losowy
sko8.in	80	test losowy
sko9.in	90	test losowy
sko10.in	100	test losowy

Zawody II stopnia

opracowania zadań