Rozwiązanie zadania M-D

Mateusz Kwaśnicki

2 lipca 2008

1 Zadanie

Niech p, q będą liczbami naturalnymi większymi od 1. Określamy *ciąg mnożąco-dzielący* (a_n) dla mnożnika p i dzielnika q w następujący sposób. Rozpoczynamy od $a_1 = 1$. Wyraz a_{n+1} jest równy $\lfloor a_n/q \rfloor$, o ile ta liczba jest dodatnia i nie wystąpiła jeszcze w ciągu, bądź pa_n w przeciwnym przypadku.

Na przykład gdy $p = 3$ oraz $q = 2$, to początkowymi wyrazami ciągu M-D są liczby $1, 3, 9, 4, 2, 6, 18, 54, 27, 13, 39, 19, 57, 28, 14, 7, 21, \ldots$.

Zadanie polega na stwierdzeniu, czy ciąg M-D jest permutacją ciągu liczb naturalnych. Poniżej dowodzimy, że odpowiedź jest twierdząca wtedy i tylko wtedy, gdy $\log_q p$ jest niewymierny, czyli gdy $q^n = p^m$ tylko dla $n = m = 0$. Warunek ten jest spełniony między innymi przez każdą parę liczb względnie pierwszych.

Zadanie pojawiło się na łamach kanadyjskiego czasopisma *Crux Mathematicorum*, w numerze 26 (2000), zadanie 2248.

Łatwo udowodnić implikację w jedną stronę. Niech bowiem $\log_q p$ będzie liczbą wymierną, czyli $q^n = p^m$ dla pewnych względnie pierwszych n, m. Wówczas $d = q^{1/m} = p^{1/n}$ jest liczbą całkowitą większą od 1, a więc każdy wyraz ciągu M-D jest potęgą liczby d. W szczególności liczba $d+1$ nie pojawi się w ciągu M-D.

W dalszej części udowodnimy implikację w drugą stronę.

2 Oznaczenia

Zbiory liczb całkowitych, całkowitych dodatnich i rzeczywistych oznaczamy odpowiednio przez $\mathbb{Z}$, $\mathbb{Z}^+$, $\mathbb{R}$. Grupę ilorazową topologicznych grup addytywnych $\mathbb{R}$ oraz $\mathbb{Z}$ (izomorficzną z odcinkiem $[0,1)$ z dodawaniem „modulo 1") będziemy oznaczać przez $\mathbb{T}$. Elementami $\mathbb{T}$ są warstwy $[a] = a + \mathbb{Z} = \{a + n : n \in \mathbb{Z}\}$, gdzie $a \in \mathbb{R}$. Niech $\kappa : \mathbb{R} \to \mathbb{T}$ będzie kanonicznym homomorfizmem danym wzorem $\kappa(a) = [a]$. Przypomnijmy, że zbiór $U \subset \mathbb{T}$ jest otwarty wtedy i tylko wtedy, gdy $\kappa^{-1}(U)$ jest otwartym podzbiorem $\mathbb{R}$. Ponadto jeśli V jest otwartym podzbiorem $\mathbb{R}$, to $\kappa(V)$ jest otwarty w $\mathbb{T}$, a więc κ jest odwzorowaniem otwartym.

3 Formalna definicja ciągu M-D

Ustalmy $p, q > 1$ takie, że $\log_q p$ jest liczbą niewymierną. Definiujemy ciąg M-D wraz ze zbiorami A_n równaniami:

$$\begin{array}{ll} a_1 = 1, & \\ A_n = \{0\} \cup \{a_m : m \leq n\}, & \\ a_{n+1} = pa_n & \text{jeśli } \lfloor a_n/q \rfloor \in A_n, \\ a_{n+1} = \lfloor a_n/q \rfloor & \text{jeśli } \lfloor a_n/q \rfloor \notin A_n. \end{array}$$

Ponadto określamy:

$$\begin{array}{l} A = \{a_m : m \in \mathbb{Z}^+\}, \\ B = \mathbb{Z}^+ \setminus A. \end{array}$$

Musimy udowodnić dwa stwierdzenia:

$$a_n = a_m \text{ tylko jeśli } n = m, \tag{1}$$

$$B = \emptyset. \tag{2}$$

4 Dwie własności zbiorów A_n, A oraz B

Ustalmy $n \in \mathbb{Z}^+$ i załóżmy, że $\lfloor a_n/q^k \rfloor \in A_n$ dla pewnego $k \in \mathbb{Z}^+$. Jeśli $\lfloor a_n/q^k \rfloor = 0$, to $\lfloor a_n/q^{k+1} \rfloor = 0 \in A_n$. Załóżmy więc, że $\lfloor a_n/q^k \rfloor > 0$, czyli $\lfloor a_n/q^k \rfloor = a_m$ dla pewnego $m \leq n$. Ponieważ $\lfloor a_n/q^k \rfloor < a_n$, więc $m < n$. Zatem albo $\lfloor a_m/q \rfloor \in A_m \subset A_n$ (i wtedy $a_{m+1} = pa_m$), albo $\lfloor a_m/q \rfloor = a_{m+1} \in A_n$. Tak czy inaczej $\lfloor a_n/q^{k+1} \rfloor = \lfloor a_m/q \rfloor \in A_n$. Stąd indukcyjnie:

$$\text{Jeśli } \lfloor a_n/q \rfloor \in A_n, \text{ to } \lfloor a_n/q^k \rfloor \in A_n \text{ dla wszystkich } k \geq 0. \tag{3}$$

Weźmy teraz $a \in A$, czyli $a = a_n$ dla pewnego n. Wówczas albo $\lfloor a_n/q \rfloor = a_{n+1} \in A$, albo $\lfloor a_n/q \rfloor \in A_n \subset A \cup \{0\}$. Zatem $\lfloor a/q \rfloor \in A \cup \{0\}$. Stąd indukcyjnie $\lfloor a/q^k \rfloor \in A \cup \{0\}$. Innymi słowy, jeśli oznaczymy $b = \lfloor a/q^k \rfloor$, to:

$$\text{Jeśli } b \in B, \text{ to } q^k b + l \in B \text{ dla wszystkich } k \in \mathbb{Z}^+, 0 \le l < q^k. \tag{4}$$

5 Prawo skracania pod podłogą

Wykorzystamy następujące łatwe twierdzenie o podłodze. Załóżmy, że $pa = \lfloor px \rfloor$, gdzie $x \in \mathbb{R}$, $a \in \mathbb{Z}$ zaś $p \in \mathbb{Z}^+$. Wówczas:

$$a = \left\lfloor \frac{pa}{p} \right\rfloor = \left\lfloor \frac{\lfloor px \rfloor}{p} \right\rfloor = \left\lfloor \frac{px}{p} \right\rfloor = \lfloor x \rfloor .$$

Zatem:

$$pa = \lfloor px \rfloor \text{ implikuje } a = \lfloor x \rfloor , \tag{5}$$

jeśli $x \in \mathbb{R}$, $a \in \mathbb{Z}$, $p \in \mathbb{Z}^+$.

6 Dowód stwierdzenia (1)

Załóżmy nie wprost, że $a_i = a_j$ dla pewnych $i \neq j$. Niech n będzie najmniejszym indeksem takim, że $a_n = a_m$ dla pewnego m, $0 < m < n$. Oczywiście oznacza to, że $a_n \in A_{n-1}$, a więc $a_n = pa_{n-1}$. Niech $1 < i \le m$ będzie takim indeksem, że:

$$a_m = \lfloor a_{m-1}/q \rfloor , a_{m-1} = \lfloor a_{m-2}/q \rfloor , \ldots , a_{i+1} = \lfloor a_i/q \rfloor , a_i = pa_{i-1}.$$

(Taki indeks istnieje, ponieważ $a_2 = pa_1$.) Wówczas:

$$pa_{n-1} = a_n = a_m = \lfloor a_i/q^{m-i} \rfloor = \lfloor pa_{i-1}/q^{m-i} \rfloor .$$

Na mocy (5) wnioskujemy, że $a_{n-1} = \lfloor a_{i-1}/q^{m-i} \rfloor$. Ponieważ $a_i = pa_{i-1}$, więc $\lfloor a_{i-1}/q \rfloor \in A_{i-1}$. Z własności (3) wynika więc, że:

$$a_{n-1} = \lfloor a_{i-1}/q^{m-i} \rfloor \in A_{i-1}.$$

Innymi słowy $a_{n-1} = a_j$ dla pewnego j spełniającego nierówności $0 < j \le i - 1 \le m - 1 < n - 1$. Stanowi to sprzeczność z wyborem n. Założenie nie wprost musi być zatem fałszywe, czyli dowiedliśmy (1). Warto zauważyć, że nie skorzystaliśmy z założenia o niewymierności $\log_q p$.

7 Dowód stwierdzenia (2)

Ponownie załóżmy nie wprost, że B jest niepusty i niech $a \in B$. Dowiedziemy, że $q^t a + s \notin B$ dla pewnych $t, s \in \mathbb{Z}^+$, $0 \leq s < q^t$, co stoi w sprzeczności z własnością (4). Kluczową obserwacją okaże się to, że różnica między $\log_q a$ oraz $\log_q(q^t a + s)$ jest bliska liczbie całkowitej. Oznacza to, że odległość między warstwami $\left[\log_q a\right]$ i $\left[\log_q(q^t a + s)\right]$ w $\mathbb{T}$ jest bardzo mała. Wystarczy więc pokazać, że zbiór warstw $\left[\log_q a_n\right]$ nie może być oddzielony od $\left[\log_q a\right]$ dla wszystkich n. To zaś wyniknie ze związku między ciągiem $\left[\log_q a_n\right]$ i obrotami niewymiernymi na $\mathbb{T}$.

Z udowodnionego stwierdzenia (1) wynika, że $\lim_{n\to\infty} a_n = \infty$. Oznacza to, że dla nieskończenie wielu indeksów n zachodzi $a_{n+1} = pa_n$. Niech $k_1, k_2, \ldots$ będzie ściśle rosnącym ciągiem wszystkich takich n. Zatem:

$$a_{k_{n+1}} = \left\lfloor \frac{a_{k_n+1}}{q^{k_{n+1}-k_n-1}} \right\rfloor, \quad a_{k_n+1} = pa_{k_n}. \tag{6}$$

Niech $b_n = \log_q a_n$, $\alpha = \log_q p$. Założyliśmy, że α jest liczbą niewymierną. Określamy:

$$\epsilon_n = \log_q \left(\frac{a_{k_n+1}}{q^{k_{n+1}-k_n-1}} \right) - \log_q a_{k_{n+1}} = b_{k_n+1} - b_{k_{n+1}} - k_{n+1} + k_n + 1.$$

Własność (6) i nierówności $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ dla $x \in \mathbb{R}$ implikują:

$$\begin{aligned} 0 \leq \epsilon_n &< \log_q(a_{k_{n+1}} + 1) - \log_q a_{k_{n+1}} = \\ &= \log_q \left(\frac{a_{k_{n+1}} + 1}{a_{k_{n+1}}} \right) < \frac{1}{a_{k_{n+1}} \ln q}. \end{aligned} \tag{7}$$

Z definicji ϵ_n oraz z (6) wynika, że:

$$\begin{aligned} \left[b_{k_{n+1}}\right] &= \left[b_{k_n+1} - \epsilon_n\right], \\ \left[b_{k_n+1}\right] &= \left[\log_q(pa_{k_n})\right] = \left[b_{k_n} + \alpha\right]. \end{aligned} \tag{8}$$

Dokładnie tego oczekiwaliśmy: warstwa $\left[b_{k_{n+1}}\right]$ jest bardzo bliska warstwie $\left[b_{k_n+1}\right]$, która jest obrazem warstwy $\left[b_{k_n}\right]$ przez niewymierny obrót. Zanim przystąpimy do szczegółów rozumowania, przypomnijmy, że szukamy wyrazu a_m takiego, że $a_m = q^t a + s$ dla pewnych $t, s \in \mathbb{Z}^+$, $0 \leq s < q^t$, lub równoważnie $b_m = \log_q a_m \in [\log_q a + t, \log_q(a+1) + t)$.

Określmy:

$$\begin{aligned}\delta &= \log_q(a+\tfrac{1}{2}) - \log_q a,\\ V &= \left(\log_q(a+\tfrac{1}{2}), \log_q(a+1)\right),\\ U &= \kappa(V).\end{aligned}$$

Ponieważ U jest niepustym, otwartym podzbiorem $\mathbb{T}$, zaś α jest liczbą niewymierną, więc (wobec minimalności obrotu niewymiernego) istnieje $L \in \mathbb{Z}^+$ taki, że dla wszystkich $x \in \mathbb{R}$ zachodzi $[x + l\alpha] \in U$ dla pewnego l, $0 \le l \le L$.

Niech M będzie tak duże, że $L < M\delta \ln q$. Ponieważ $\lim_{n\to\infty} a_n = \infty$, więc istnieje N takie, że $a_n > M$ dla $n \ge N$. Ustalmy n takie, że $k_n \ge N$. Dla pewnego l, $0 \le l \le L$, zachodzi $[b_{k_n} + l\alpha] \in U$. Oznacza to, że dla pewnego $i \in \mathbb{Z}$:

$$b_{k_n} + l\alpha + i \in V.$$

Z definicji V:

$$\log_q(a+\tfrac{1}{2}) < b_{k_n} + l\alpha + i < \log_q(a+1) \tag{9}$$

Niech $m = n + l$. Korzystając z własności (8), otrzymujemy:

$$[b_{k_m}] = [b_{k_n} + l\alpha - \epsilon_n - \epsilon_{n+1} - \cdots - \epsilon_{m-1}]$$

lub równoważnie:

$$b_{k_m} = b_{k_n} + l\alpha - \epsilon_n - \epsilon_{n+1} - \cdots - \epsilon_{m-1} + j$$

dla pewnego $j \in \mathbb{Z}$. Teraz jeśli $n \le \nu < m$, to $k_{\nu+1} > k_n \ge N$, a więc $a_{k_{\nu+1}} > M$. Wobec (7) oznacza to, że $0 \le \epsilon_\nu < (a_{k_{\nu+1}} \ln q)^{-1} < (M \ln q)^{-1}$. Zatem:

$$b_{k_n} + l\alpha + j - \frac{l}{M \ln q} < b_{k_m} \le b_{k_n} + l\alpha + j.$$

Lecz M było określone tak, aby $l/(M\ln q) \le L/(M \ln q) < \delta$. Stąd:

$$b_{k_n} + l\alpha + j - \delta < b_{k_m} \le b_{k_n} + l\alpha + j.$$

Wraz z (9) i definicją δ prowadzi to do:

$$\log_q(a+\tfrac{1}{2}) - i + j - (\log_q(a+\tfrac{1}{2}) - \log_q a) < b_{k_m} < \log_q(a+1) - i + j.$$

Ostatecznie otrzymujemy:

$$\log_q a + j - i < b_{k_m} < \log_q(a+1) + j - i.$$

Wyrażając ten warunek za pomocą wyjściowego ciągu, otrzymujemy:

$$q^{j-i}a < a_{k_m} < q^{j-i}(a+1).$$

W szczególności $j - i$ musi być dodatnie. Stąd $a_{k_m} = q^t a + s$ dla $t = i - j$ i pewnego s spełniającego warunek $0 < s < q^t$. Sprzeczność z (4).

Dowiedliśmy zatem, że B jest pusty. To kończy rozwiązanie.