O pewnym uogólnieniu małego twierdzenia Fermata

Anna LEŚNIAK[*]

Udowodnione ponad trzysta lat temu małe twierdzenie Fermata głosi, że dla każdej liczby całkowitej a i liczby pierwszej p zachodzi podzielność $p \mid a^p - a$. Pragnę przedstawić jego uogólnienie, związane z iteracją funkcji zespolonej $f(z) = z^a$, gdzie $a \geqslant 2$ jest liczbą całkowitą.

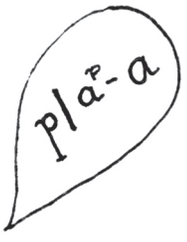
Część wstępna

Jeśli f jest obrotem płaszczyzny względem ustalonego punktu O o kąt 45°, to każdy punkt P spełnia warunek $f^{80}(P) = P$, czy $f^{48}(P) = P$, ale dla $P \neq O$ okresem podstawowym jest 8.

Niech f będzie funkcją określoną na pewnym niepustym zbiorze X, przyjmującą wartości w tym zbiorze. Przyjmijmy oznaczenie $f^0 = \mathrm{id}$ (tzn. $f^0(x) = x$ dla każdego $x \in X$) oraz w sposób indukcyjny zdefiniujmy $f^n = f \circ f^{n-1}$ dla dodatnich liczb naturalnych n. Powiemy, że $n \geqslant 1$ jest *okresem* punktu x_0, jeżeli $f^n(x_0) = x_0$, natomiast *okresem podstawowym* punktu x_0 nazwiemy najmniejszy spośród jego okresów (o ile takie istnieją). Zauważmy, że

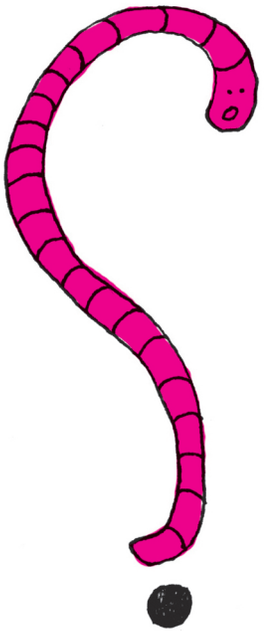
$(*)$ okres podstawowy punktu x_0 jest dzielnikiem każdego z jego okresów.

Rzeczywiście, niech m będzie okresem podstawowym, a n pewnym okresem x_0. Niech $n = km + r$, gdzie $r \in \{0, \ldots, m-1\}$ jest resztą z dzielenia n przez m. Przypuśćmy, że $r \neq 0$. Wtedy $x_0 = f^n(x_0) = f^{km+r}(x_0) = f^r(f^{km}(x_0)) = f^r(x_0)$, co jest sprzeczne z definicją liczby m.



Załóżmy, że dla dowolnej liczby naturalnej n funkcja f ma skończenie wiele punktów o okresie n, a ich liczbę oznaczmy przez a_n. Ponadto niech b_m będzie liczbą punktów o okresie podstawowym m. Wówczas z $(*)$ łatwo wynika

$$a_n = \sum_{m|n} b_m.$$



Rozważmy teraz x_0 o okresie podstawowym m. Wówczas $f(x_0), \ldots, f^{m-1}(x_0)$ również mają okres podstawowy m. W przeciwnym razie, $f^l(f^k(x_0)) = f^k(x_0)$ dla pewnego $1 \leqslant k \leqslant m-1$ i $l < m$. Stąd $f^{k+l}(x_0) = f^k(x_0)$, więc

$$x_0 = f^m(x_0) = f^{m-k}(f^k(x_0)) = f^{m-k}(f^{k+l}(x_0)) = f^l(f^m(x_0)) = f^l(x_0),$$

co prowadzi do sprzeczności, ponieważ x_0 ma okres minimalny m i $l < m$. Ponadto punkty $x_0, f(x_0), \ldots, f^{m-1}(x_0)$ są parami różne, gdyż gdyby $f^k(x_0) = f^l(x_0)$ dla pewnych $0 \leqslant k < l \leqslant m-1$, to

$$f^k(x_0) = f^l(x_0) = f^{k+(l-k)}(x_0) = f^{l-k}(f^k(x_0)),$$

czyli $f^k(x_0)$ miałby okres minimalny nie większy niż $l - k < m$, co (jak pokazaliśmy wcześniej) jest niemożliwe. Z poczynionych obserwacji wynika, że zbiór punktów o okresie podstawowym m jest sumą skończonej liczby rozłącznych, m-elementowych zbiorów postaci $\{x_0, f(x_0), \ldots, f^{m-1}(x_0)\}$, a zatem $m \mid b_m$.

Zauważmy teraz, że jeżeli p jest liczbą pierwszą, to $a_p = b_p + b_1 = b_p + a_1$, zatem $b_p = a_p - a_1$. Analogicznie, jeśli q jest liczbą pierwszą różną od p, to wówczas $a_{pq} = b_{pq} + b_p + b_q + b_1$, a skoro $b_p = a_p - a_1$, $b_q = a_q - a_1$, więc

$$b_{pq} = a_{pq} - a_p - a_q + a_1.$$

Okazuje się, że otrzymywane równości możemy uogólnić, korzystając z *formuły inwersyjnej Möbiusa*, wedle której jeśli $(x_n)_{n=1}^{\infty}$ i $(y_n)_{n=1}^{\infty}$ są ciągami liczb całkowitych oraz $x_n = \sum_{m|n} y_n$, to wówczas $y_n = \sum_{m|n} \mu(m) x_{\frac{n}{m}}$, gdzie

$$\mu(m) = \begin{cases} 1, & \text{dla } m = 1; \\ (-1)^k, & \text{dla } m = p_1 \cdots p_k, \text{ gdzie } p_i \text{ to różne liczby pierwsze;} \\ 0, & \text{w przeciwnym razie.} \end{cases}$$

Jej bezpośrednie zastosowanie prowadzi nas do równości $b_n = \sum_{m|n} \mu(m) a_{\frac{n}{m}}$, co w połączeniu z podzielnością $n \mid b_n$ pozwala stwierdzić, że dla dowolnej liczby naturalnej n

$$n \,\Big|\, \sum_{m|n} \mu(m) a_{\frac{n}{m}}.$$

[*]Państwowa Wyższa Szkoła Zawodowa w Nowym Sączu

Część zasadnicza

Wróćmy do twierdzenia Fermata.

Dla ustalonego $a > 1$ rozważmy funkcję zespoloną $f(z) = z^a$. Złożenie n-krotne funkcji f jest równe

$$f^n(z) = z^{a^n}.$$

Zauważmy, że dla każdego n zbiór wszystkich punktów okresowych o okresie n jest skończony. Rzeczywiście, składa się on z zespolonych pierwiastków równania

$$z^{a^n} = z,$$

Jednym z jego pierwiastków jest $z = 0$, a jeżeli $z \neq 0$, to $z^{a^n-1} = 1$, więc z jest pierwiastkiem zespolonym z jedynki stopnia $a^n - 1$, a tych jest dokładnie $a^n - 1$. Wynika stąd, że w tej sytuacji

$$a_n = a^n, \quad \text{czyli} \quad n \,\Big|\, \sum_{m|n} \mu(m) a^{\frac{n}{m}}.$$

Dla liczby pierwszej $n = p$ otrzymujemy małe twierdzenie Fermata: $p \,|\, a^p - a$.

Czytelnik Uważny zauważy, że dla $a = 1$ nie możemy stosować naszego rozumowania (dlaczego?). Na szczęście zachodzi $\sum_{m|n} \mu(m) = 0$, dla dowolnej liczby naturalnej $n > 1$, zatem nasze twierdzenie pozostaje prawdziwe i w tym przypadku.

Spróbujmy pójść jeszcze krok dalej. Niech $(d_n)_{n=1}^{\infty}$ będzie ciągiem liczb całkowitych. Powiemy, że jest on *ciągiem Dolda*, jeżeli dla każdej liczby naturalnej zachodzi podzielność

$$n \,\Big|\, \sum_{m|n} \mu(m) d_{\frac{n}{m}}.$$

Z wcześniejszych rozważań wynika, że ciąg $(a^n)_{n=1}^{\infty}$ jest ciągiem Dolda dla dowolnej liczby całkowitej a.

Ciągi Dolda mają ciekawą charakteryzację. Niech $(c_n)_{n=1}^{\infty}$ będzie ciągiem liczb całkowitych. Powiemy, że ciąg $(d_n)_{n=1}^{\infty}$ jest generowany przez ciąg $(c_n)_{n=1}^{\infty}$, jeżeli dla $n \geqslant 1$ zachodzi

$$d_n = c_1 d_{n-1} + c_2 d_{n-2} + \cdots + c_{n-1} d_1 + n c_n.$$

Okazuje się, że $(d_n)_{n=1}^{\infty}$ jest ciągiem Dolda wtedy i tylko wtedy, gdy jest generowany przez pewien ciąg $(c_n)_{n=1}^{\infty}$. Zostało to wykazane przez Bau-Sen Du, Sen-Shan Huanga i Ming-Chia Li – ich dowód można znaleźć w artykule *Generalized Fermat, double Fermat and Newton sequences* opublikowanym w czasopiśmie *Journal of Number Theory* w 2003 roku.

Przy okazji

Na pomysł, by uogólnić małe twierdzenie Fermata, wpadł też Leonard Euler. Posłużył się w tym celu funkcją φ noszącą dziś jego nazwisko. Funkcja ta zlicza dla dowolnej liczby naturalnej n liczby z n względnie pierwsze i mniejsze od n (dodatkowo przyjmuje się, że $\varphi(1) = 1$). Nietrudno wykazać, że jeśli w rozkładzie n na liczby pierwsze występują liczby $p_1, p_2, \ldots, p_k$ w dowolnych dodatnich potęgach, to $\varphi(n)$ jest równe

$$n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Euler udowodnił, że

dla względnie pierwszych n i a zachodzi

$$a^{\varphi(n)} \equiv 1 \,(\mathrm{mod}\, n)$$

czy, jak kto woli

$$n \,|\, a^{\varphi(n)} - 1.$$

Małe twierdzenie Fermata jest szczególnym przypadkiem tego twierdzenia, bo dla liczby pierwszej p jest $\varphi(p) = p - 1$. Zatem mamy

$$p \,|\, a(a^{p-1} - 1) \quad [= a^p - a],$$

bo gdy p nie dzieli a, to dzieli $a^{p-1} - 1$.

Twierdzenie Eulera ma tak prosty dowód, że można by zmieścić go na marginesie. Oto on.

Oznaczmy przez $r_1, \ldots, r_{\varphi(n)}$ wszystkie liczby względnie pierwsze z n i mniejsze od n. Gdy a jest względnie pierwsze z n, liczby $ar_1, \ldots, ar_{\varphi(n)}$ też są względnie pierwsze z n i nie ma wśród nich dwóch przystających modulo n, bo

$$ar_i \equiv ar_j \,(\mathrm{mod}\, n) \;\Rightarrow\; a(r_i - r_j) \equiv 0 \,(\mathrm{mod}\, n) \;\Rightarrow\; r_i = r_j \;\Rightarrow\; i = j.$$

Zatem dla każdego k istnieje dokładnie jedno takie l, że $ar_k \equiv r_l \,(\mathrm{mod}\, n)$. Wobec tego

$$a^{\varphi(n)} r_1 \cdot \ldots \cdot r_{\varphi(n)} = ar_1 \cdot \ldots \cdot ar_{\varphi(n)} \equiv r_1 \cdot \ldots \cdot r_{\varphi(n)} \,(\mathrm{mod}\, n),$$

a więc, dzieląc stronami przez $r_1 \cdot \ldots \cdot r_{\varphi(n)}$, otrzymujemy

$$a^{\varphi(n)} \equiv 1 \,(\mathrm{mod}\, n).$$

M. K.