FOLIA 110

Annales Universitatis Paedagogicae Cracoviensis

Studia ad Didacticam Mathematicae Pertinentia IV (2012)

Jan Górowski, Adam Łomnicki

O nieskończonych ciągach liczb parami względnie pierwszych raz jeszcze*

Abstract. In the paper the authors, using general formulas, determine and describe a class of infinite sequences of natural numbers, pairs of which are relatively prime. This result was obtained using the theory of Lucas sequences and recurrent equations of the second degree.

Od dawna wiadomo, że ciąg liczb Fermata (F_n), gdzie $F_n = 2^{2^n} + 1, n \in \mathbb{N}_0$ jest ciągiem liczb parami względnie pierwszych. Znane są inne ciągi liczb parami względnie pierwszych (Edwards, 1964; Górowski, Łomnicki, 2009), ale mankamentem najczęściej podawanych w literaturze takich ciągów jest to, że są zdefiniowane rekurencyjnie i zwykle nie potrafimy znaleźć wzoru na wyraz ogólny takiego ciągu. W pracy (Górowski, Łomnicki, 2009) określono wzorami ogólnymi wiele różnych ciągów o wyrazach parami względnie pierwszych.

Będziemy w dalszym ciągu mówili krótko, że nieskończony ciąg liczb naturalnych ma własność *wp*, gdy każde dwa jego różne wyrazy są liczbami względnie pierwszymi. Rozwiniemy pomysł określania ciągów mających własność *wp*, w oparciu o teorię równań rekurencyjnych liniowych rzędu 2.

Niech k oznacza liczbę naturalną dodatnią. Symbolem $\mathbb{N}_k$ oznaczać będziemy w całej pracy zbiór $\mathbb{N} \setminus \{0, 1, 2, \dots, k-1\}$. Niech p, q oznaczają liczby całkowite, takie, że $NWD(p, q) = 1$ i $p^2 + 4q > 0$ i $q \neq 0$.

Rozważmy dwa ciągi $(\mathcal{F}_n), (\mathcal{L}_n)$ spełniające równanie rekurencyjne

$$G_n = p\, G_{n-1} + q\, G_{n-2}, \quad n \in \mathbb{N}_2 \tag{1}$$

oraz odpowiednio warunki początkowe

$$\mathcal{F}_0 = 0, \quad \mathcal{F}_1 = 1, \quad \mathcal{L}_0 = 2, \quad \mathcal{L}_1 = p.$$

*Once again on infinite sequences of natural numbers, pairs of which are relatively prime

2010 Mathematics Subject Classification: Primary: 97F30, Secondary: 97F60

Key words and phrases: infinite sequences of natural numbers pairs of which are relatively prime, general formulas

Ciąg $(\mathcal{F}_n)$ nazywać będziemy ciągiem Fibonacciego, a ciąg $(\mathcal{L}_n)$ – ciągiem Lucasa. Wiadomo, że

$$\mathcal{F}_n = \frac{r^n - s^n}{r - s}, \quad \mathcal{L}_n = r^n + s^n \quad \text{dla } n \geqslant 0, \tag{2}$$

gdzie $r = \frac{p+\sqrt{p^2+4q}}{2}$, $s = \frac{p-\sqrt{p^2+4q}}{2}$ (Koshy, 2001).

Zauważmy, że wzory (2) dla $n \in \mathbb{Z}$ określają funkcje $(\mathcal{F}_n)_{n\in\mathbb{Z}}$ $(\mathcal{L}_n)_{n\in\mathbb{Z}}$, które spełniają równanie rekurencyjne $G_n = p\,G_{n-1} + q\,G_{n-2}$ o dziedzinie $\mathbb{Z}$.

Podstawowe tożsamości dla funkcji $(\mathcal{F}_n)_{n\in\mathbb{Z}}$, $(\mathcal{L}_n)_{n\in\mathbb{Z}}$, to

$$-(-q)^n\mathcal{F}_{-n} = \mathcal{F}_n, \ (-q)^n\mathcal{L}_{-n} = \mathcal{L}_n, \text{ gdzie } n \in \mathbb{Z}, \tag{3}$$

$$\mathcal{F}_{n+m} + (-q)^m\mathcal{F}_{n-m} = \mathcal{L}_m\mathcal{F}_n, \text{ gdzie } n, m \in \mathbb{Z}, \tag{4}$$

$$\mathcal{F}_{n-m} - (-q)^m\mathcal{F}_{n-m} = \mathcal{F}_m\mathcal{L}_n, \text{ gdzie } n, m \in \mathbb{Z}, \tag{5}$$

$$\mathcal{L}_{n+m} + (-q)^m\mathcal{L}_{n-m} = \mathcal{L}_m\mathcal{L}_n, \text{ gdzie } n, m \in \mathbb{Z}, \tag{6}$$

$$\mathcal{L}_{n-m} - (-q)^m\mathcal{L}_{n-m} = (p^2+4q)\mathcal{F}_m\mathcal{F}_n, \text{ gdzie } n, m \in \mathbb{Z}, \tag{7}$$

$$\mathcal{F}_{n+m} = \mathcal{F}_n\mathcal{F}_{m+1} - q\mathcal{F}_{n-1}\mathcal{F}_m, \text{ gdzie } n, m \in \mathbb{Z}. \tag{8}$$

Tożsamości (3) do (8) wynikają bezpośrednio ze wzorów (2). Udowodnimy teraz

Lemat 1

$$\mathcal{F}_{mn} = \mathcal{F}_n \sum_{j=0}^{[\frac{m-1}{2}]} B(m,j)(-1)^j(-q)^{nj}\mathcal{L}_n^{m-1-2j}$$

dla $m \in \mathbb{N}$, $n \in \mathbb{N}_2$, *gdzie* $B(m,j) = \binom{m-1-j}{j}$.

Dowód. Wykorzystamy zasadę indukcji matematycznej prowadzoną ze względu na m.

Dla $m = 0$ oraz $m = 1$ równość podana w Lemacie 1 jest prawdziwa.

Załóżmy teraz, że dla dowolnie ustalonego $m \geqslant 1$ oraz dla każdego $k \in \{0, 1, \ldots, m\}$ i każdego $n \in \mathbb{N}_2$

$$\mathcal{F}_{kn} = \mathcal{F}_n \sum_{j=0}^{[\frac{k-1}{2}]} B(k,j)(-1)^j(-q)^{nj}\mathcal{L}_n^{k-1-2j}.$$

Pokażemy, że dla każdego $n \in \mathbb{N}_2$

$$\mathcal{F}_{(m+1)n} = \mathcal{F}_n \sum_{j=0}^{[\frac{m}{2}]} B(m+1,j)(-1)^j(-q)^{nj}\mathcal{L}_n^{m-2j}.$$

Wykorzystując tożsamość (5), a następnie tożsamość (3) otrzymujemy:

$$\begin{aligned}
\mathcal{F}_{(m+1)n} &= \mathcal{F}_{n+mn} \\
&= (-q)^{mn}\mathcal{F}_{(n-mn)} + \mathcal{F}_{mn}\mathcal{L}_n \\
&= -(-q)^{mn}(-q)^{n-mn}\mathcal{F}_{mn-n} + \mathcal{F}_{mn}\mathcal{L}_n \\
&= -(-q)^n\mathcal{F}_{(m-1)n} + \mathcal{F}_{mn}\mathcal{L}_n.
\end{aligned}$$

Korzystając teraz z założenia indukcyjnego oraz z określenia liczb $B(m,j)$ dostajemy:

$$\begin{aligned}
&\mathcal{F}_{(m+1)n}\\
&= -(-q)^n \sum_{j=0}^{[\frac{m-2}{2}]} B(m-1,j)(-1)^j(-q)^{nj}\mathcal{L}_n^{m-2-2j} + \sum_{j=0}^{[\frac{m-1}{2}]} B(m,j)(-1)^j(-q)^{nj}\mathcal{L}_n^{m-2j}\\
&= \sum_{j=1}^{[\frac{m-2}{2}]+1} B(m-1,j-1)(-1)^j(-q)^{nj}\mathcal{L}_n^{m-2j} + \sum_{j=0}^{[\frac{m-1}{2}]} B(m,j)(-1)^j(-q)^{nj}\mathcal{L}_n^{m-2j}\\
&= \sum_{j=0}^{[\frac{m}{2}]} B(m+1,j)(-1)^j(-q)^{nj}\mathcal{L}_n^{m-2j}.
\end{aligned}$$

Zasada indukcji kończy dowód lematu 1.

Korzystając z tożsamości (6) i (3) analogicznie jak powyżej lemat 1 można udowodnić

Lemat 2

$$\mathcal{L}_{mn} = \sum_{j=0}^{[\frac{m}{2}]} E(m,j)(-1)^j(-q)^{nj}\mathcal{L}_n^{m-2j}$$

dla $m,n \in \mathbb{N}_1$, *gdzie* $E(m,j) = \binom{m-j}{j} + \binom{m-1-j}{m-2j}$ *oraz* $E(m,0) = 1$ *dla* $m \in \mathbb{N}$.

Wnioskiem z lematu 2 jest

Lemat 3
Jeśli $n,m \in \mathbb{N}_1$, $|L_n| \neq 1$ *oraz* $|L_n| \neq 2$, *to:*
$\mathcal{L}_n|\mathcal{L}_{mn}$ *wtedy i tylko wtedy, gdy* m *jest liczbą naturalną nieparzystą.*

Udowodnimy teraz

Twierdzenie 1
$NWD(\mathcal{F}_n,\mathcal{F}_m) = \mathcal{F}_{NWD(n,m)}$ *dla dowolnych* $n,m \in \mathbb{N}_1$.

Dowód. Najpierw wykażemy, że $NWD(\mathcal{F}_n, q) = 1$ dla $n \in \mathbb{N}_1$.

Istotnie, gdyby dla pewnego $n \in \mathbb{N}_1$, $NWD(\mathcal{F}_n, q) = d > 1$, to $n \geqslant 3$, ponieważ $\mathcal{F}_1 = 1$, a $\mathcal{F}_2 = p$. Stąd dalej $\mathcal{F}_n = p$, $\mathcal{F}_{n-1} + q$, $\mathcal{F}_{n-2}$ i $d|\mathcal{F}_{n-1}$.

Powtarzając, to samo rozumowanie, dojdziemy kolejno do wniosków $d|\mathcal{F}_{n-2}$, $d|\mathcal{F}_{n-3}, \ldots, d|\mathcal{F}_1$, co jest niemożliwe, bowiem $\mathcal{F}_1 = 1$. Otrzymana sprzeczność dowodzi, że $NWD(\mathcal{F}_n, q) = 1$ dla $n \in \mathbb{N}_1$.

Teraz wykażemy, że $NWD(\mathcal{F}_n, \mathcal{F}_{n-1}) = 1$ dla $n \in \mathbb{N}_1$.
Gdy $n = 1$ lub $n = 2$, oczywiście $NWD(\mathcal{F}_n, \mathcal{F}_{n-1}) = 1$.
Załóżmy zatem, że $n \geqslant 3$. Wtedy

$$\mathcal{F}_n = p\,\mathcal{F}_{n-1} + q\,\mathcal{F}_{n-2} \text{ i } NWD(\mathcal{F}_n, \mathcal{F}_{n-1}) = NWD(\mathcal{F}_{n-1}, q\mathcal{F}_{n-2})$$

Ponieważ $NWD(\mathcal{F}_m, q) = 1$ dla $m \in \mathbb{N}_1$, zatem

$$NWD(\mathcal{F}_{n-1}, q\mathcal{F}_{n-2}) = NWD(\mathcal{F}_{n-1}, \mathcal{F}_{n-2}).$$

Stąd

$$NWD(\mathcal{F}_n, \mathcal{F}_{n-1}) = NWD(\mathcal{F}_{n-1}, \mathcal{F}_{n-2})$$

dla każdego $n \in \mathbb{N}_3$ oraz

$$NWD(\mathcal{F}_n, \mathcal{F}_{n-1}) = 1 \text{ dla } n \in \mathbb{N}_1.$$

Mamy zatem

$$NWD(\mathcal{F}_n, \mathcal{F}_{n-1}) = NWD(\mathcal{F}_n, q) = 1 \text{ dla } n \in \mathbb{N}_1. \tag{9}$$

Kładąc teraz w tożsamości (8) $m - n$ w miejsce m, gdzie $m \geqslant n \geqslant 1$ otrzymujemy

$$\mathcal{F}_m = \mathcal{F}_n\mathcal{F}_{m-n+1} - q\mathcal{F}_{n-1}\mathcal{F}_{m-n}.$$

Stąd – mając na uwadze (9) – dostajemy

$$NWD(\mathcal{F}_m, \mathcal{F}_n) = NWD(\mathcal{F}_n, \mathcal{F}_{m-n}).$$

Po przyjęciu, że d_1 oznacza resztę z dzielenia liczby m przez n otrzymujemy

$$NWD(\mathcal{F}_m, \mathcal{F}_n) = NWD(\mathcal{F}_n, \mathcal{F}_{d_1}).$$

Przyjmijmy teraz, że do wyznaczenia $NWD(m, n)$ zastosowaliśmy algorytm Euklidesa. Wtedy

$$\begin{gathered} m = k_1 n + d_1 \\ n = k_2 d_1 + d_2 \\ d_1 = k_3 d_2 + d_3 \\ \vdots \\ d_{t-2} = k_t d_{t-1} + d_t \\ d_{t-1} = k_{t+1} d_t, \end{gathered}$$

gdzie d_t jest ostatnią resztą różną od zera.

Wykorzystując odpowiednią ilość razy wykazaną wcześniej własność

$$NWD(\mathcal{F}_m, \mathcal{F}_n) = NWD(\mathcal{F}_n, \mathcal{F}_{d_1})$$

ciągu $(\mathcal{F}_n)$ dostajemy $NWD(\mathcal{F}_m, \mathcal{F}_n) = NWD(\mathcal{F}_n, \mathcal{F}_{d_1}) = NWD(\mathcal{F}_{d_1}, \mathcal{F}_{d_2}) = \ldots = NWD(\mathcal{F}_{d_{t-2}}, \mathcal{F}_{d_{t-1}}) = NWD(\mathcal{F}_{d_{t-1}}, \mathcal{F}_{d_t}) = \mathcal{F}_{d_t}$.

Ostatnia równość wynika z lematu 1. Dowód twierdzenia 1 został zakończony.

Warto zauważyć, że twierdzenie 1 można znaleźć w (Ribenboim, 1997), jednakże przedstawiony tam jego dowód – jak pisze sam autor – nie jest łatwy.

Udowodnimy teraz

TWIERDZENIE 2

$NWD(\mathcal{L}_m, \mathcal{L}_n)$ jest dzielnikiem liczby $\mathcal{L}_{NWD(m,n)}$ dla dowolnych $m, n \in \mathbb{N}_1$.

Dowód. Z określenia liczb $\mathcal{F}_n$ i $\mathcal{L}_n$ bezpośrednio wynika, że $\mathcal{L}_n\mathcal{F}_n = \mathcal{F}_{2n}$ dla $n \in \mathbb{N}$. Stąd oraz z twierdzenia 1 mamy $NWD(\mathcal{L}_m\mathcal{F}_m, \mathcal{L}_n\mathcal{F}_n) = NWD(\mathcal{F}_{2m}, \mathcal{F}_{2n}) = \mathcal{F}_{NWD(2m,2n)} = \mathcal{F}_{2NWD(m,n)} = \mathcal{F}_{NWD(m,n)}\mathcal{L}_{NWD(m,n)}$.

W konsekwencji uzyskujemy tezę twierdzenia 2.

TWIERDZENIE 3

Jeżeli $n, m \in \mathbb{N}_1, d = NWD(m,n)$ oraz $\frac{m}{d}$ i $\frac{n}{d}$ są liczbami nieparzystymi, to $NWD(\mathcal{L}_m, \mathcal{L}_n) = \mathcal{L}_{NWD(m,n)}$.

Dowód. Z lematu 3 wynika, że $\mathcal{L}_d | \mathcal{L}_m$ i $\mathcal{L}_d | \mathcal{L}_n$. Stąd i z twierdzenia 2 bezpośrednio wynika teza twierdzenia 3.

Twierdzenie 3 także można znaleźć w (Ribenboim, 1997), jednakże dowód tam naszkicowany ani nie jest łatwy, ani tak krótki jak ten, który zamieściliśmy powyżej. Wykażemy teraz

TWIERDZENIE 4

Jeśli $q \in 2\mathbb{Z}, p \in \mathbb{Z} \setminus 2\mathbb{Z}, k$ jest dodatnią liczbą naturalną parzystą, to ciąg $(\mathcal{L}_{k^n})_{n \in \mathbb{N}}$ ma własność wp.

Dowód. Kładąc w tożsamości (6) w miejsce m liczbę $m - n$, a następnie opierając się na tożsamości (3) otrzymujemy

$$\mathcal{L}_m = \mathcal{L}_n\mathcal{L}_{m-n} - (-q)^n\mathcal{L}_{m-2n}, \text{ gdzie } m, n \in \mathbb{Z}. \tag{10}$$

Z przyjętych założeń o liczbach p i q wynika, że wszystkie liczby $\mathcal{L}_n$ dla $n \geqslant 1$ są nieparzyste. Ponadto $NWD(\mathcal{L}_n, q) = 1$ dla $n \in \mathbb{N}_1$.

Dowód tego faktu przebiega podobnie jak dowód analogicznej własności dla liczb $\mathcal{F}_n$ (gdzie $n \geqslant 1$) w dowodzie twierdzenia 1.

Niech teraz $m, n \in \mathbb{N}_1$ i $n < m$.

Wykorzystując teraz $\frac{1}{2}k^{m-n}$ razy tożsamość (10), mamy kolejno:

$$\begin{aligned}
\mathcal{L}_{k^m} &= \mathcal{L}_{k^n}\mathcal{L}_{k^m-k^n} - (-q)^{k^n}\mathcal{L}_{k^m-2k^n}, \\
\mathcal{L}_{k^m-2k^n} &= \mathcal{L}_{k^n}\mathcal{L}_{k^m-3k^n} - (-q)^{k^n}\mathcal{L}_{k^m-4k^n}, \\
\mathcal{L}_{k^m-4k^n} &= \mathcal{L}_{k^n}\mathcal{L}_{k^m-5k^n} - (-q)^{k^n}\mathcal{L}_{k^m-6k^n}, \\
&\vdots \\
\mathcal{L}_{k^m-(k^{m-n}-2)k^n} &= \mathcal{L}_{k^n}\mathcal{L}_{k^m-(k^{m-n}-1)k^n} - (-q)^{k^n}\mathcal{L}_{k^m-k^{m-n}\cdot k^n}.
\end{aligned}$$

Z otrzymanych równości i faktu, że $NWD(\mathcal{L}_n, q) = 1$ dla $n \in \mathbb{N}_1$ dostajemy kolejno:

$$\begin{aligned}
NWD(\mathcal{L}_{k^m}, \mathcal{L}_{k^n}) &= NWD(\mathcal{L}_{k^n}, \mathcal{L}_{k^m-2k^n}), \\
NWD(\mathcal{L}_{k^m-2k^n}, \mathcal{L}_{k^n}) &= NWD(\mathcal{L}_{k^n}, \mathcal{L}_{k^m-4k^n}),
\end{aligned}$$

$$NWD(\mathcal{L}_{k^m-4k^n}, \mathcal{L}_{k^n}) = NWD(\mathcal{L}_{k^n}, \mathcal{L}_{k^m-6k^n}),$$

$$\vdots$$

$$NWD(\mathcal{L}_{k^m-(k^{m-n}-2)k^n}, \mathcal{L}_{k^n}) = NWD(\mathcal{L}_{k^n}, \mathcal{L}_0),$$

oraz konkluzję

$$NWD(\mathcal{L}_{k^m}, \mathcal{L}_{k^n}) = NWD(\mathcal{L}_{k^n}, \mathcal{L}_0).$$

Ponieważ $\mathcal{L}_0 = 2$, a $\mathcal{L}_{k^n}$ dla $n \in \mathbb{N}$ są liczbami nieparzystymi, zatem $NWD(\mathcal{L}_{k^m}, \mathcal{L}_{k^n}) = 1$ dla $n \in \mathbb{N}$ i $n \neq m$. Dowód twierdzenia 4 został zakończony.

Twierdzenie 5
Jeśli $p, q \in \mathbb{Z} \setminus 2\mathbb{Z}, k$ jest liczbą naturalną parzystą niepodzielną przez 3, to ciąg $(\mathcal{L}_{k^n})_{n\in\mathbb{N}}$ ma własność wp.

Dowód. Z przyjętych założeń o liczbach p, q wynika, że $\mathcal{L}_n$ dla $n \in \mathbb{N}$ jest liczbą parzystą wtedy i tylko wtedy, gdy $3|n$. Wobec tego $3 | k^n$ dla $n \in \mathbb{N}$ i $(\mathcal{L}_{k^n})_{n\in\mathbb{N}}$ jest ciągiem liczb nieparzystych. Dalej postępujemy analogicznie jak w dowodzie twierdzenia 4 i uzyskujemy

$$NWD(\mathcal{L}_{k^m}, \mathcal{L}_{k^n}) = NWD(\mathcal{L}_0, \mathcal{L}_{k^n}) = NWD(2, \mathcal{L}_{k^n}) = 1$$

dla $n \in \mathbb{N}$ i $n \neq m$, co kończy dowód twierdzenia 5.

Z twierdzenia 4 uzyskujemy

Twierdzenie 6
Ciąg (a_n) określony wzorem $a_n = a^{k^n} + 1$, gdzie a i k są ustalonymi liczbami parzystymi i dodatnimi ma własność wp.

Dowód. Zauważmy, że jeśli w twierdzeniu 4 przyjmiemy, że $p = a+1, q = -a$, to wszystkie założenia tego twierdzenia będą spełnione i ponadto $\mathcal{F}_n = \frac{a^n-1}{a-1}$ oraz $\mathcal{L}_n = a^n + 1$. Stąd i z twierdzenia 4 dostajemy tezę twierdzenia 6.

Przyjmując $a = k = 2$ w twierdzeniu 6 otrzymujemy

Wniosek 1
Ciąg (F_n) liczb Fermata zadany wzorem $F_n = 2^{2^n} + 1$ ma własność wp.

Z twierdzenia 1 wynika bezpośrednio

Twierdzenie 7
Jeśli (c_n) jest ciągiem liczb naturalnych mającym własność wp, to ciąg $(\mathcal{F}_{c_n})_{n\in\mathbb{N}}$ ma własność wp.

Literatura

Edwards, A. W. F.: 1964, Infinite coprime sequences, *Math. Gazette* **48**, 416-422.

Górowski, J., Łomnicki, A.: 2009, O nieskończonych ciągach liczb naturalnych, parami względnie pierwszych, *Annales Academiae Paedagogicae Cracoviensis. Studia ad Didacticam Mathematicae Pertinentia* **II**, 51-69.

Koshy, T.: 2001, *Fibonacci and Lucas numbers with applications*, Iohn Wiley & Sons, Inc.

Ribenboim, P.: 1997, *Mała księga wielkich liczb pierwszych*, Wydaw. Naukowo-Techniczne, Warszawa.

Instytut Matematyki
Uniwersytet Pedagogiczny
ul. Podchorążych 2
PL-30-084 Kraków
e-mail alomnicki@poczta.fm
e-mail jangorowski@interia.pl