FOLIA 82

Annales Universitatis Paedagogicae Cracoviensis

Studia ad Didacticam Mathematicae Pertinentia III (2010)

Jan Górowski, Adam Łomnicki

Kilka uwag na temat liczb Fermata F_5 i F_6*

Abstract. In this paper we give the necessary and sufficient conditions for the number of the form $d = k \cdot 2^7 + 1$ and $d = k \cdot 2^8 + 1$ to be divisors of the Fermat numbers F_5 and F_6, respectively. Moreover, we present numerous elementary proofs of the complexity of the numbers F_5 and F_6.

Liczby postaci $F_n = 2^{2^n} + 1$, gdzie $n \in \mathbb{N}$, nazywane są liczbami Fermata. Wiele interesujących faktów dotyczących tych liczb można znaleźć m.in. w pracach (Narkiewicz, 2003; Ribenboim, 1997; Sierpiński, 1969; Yan, 2006). W literaturze dydaktycznej powtarzane jest domniemanie, iż Fermat był przekonany, że wszystkie liczby F_n są pierwsze. Liczby Fermata nabrały znaczenia, gdy F. Gauss udowodnił, że konstrukcja n-kąta foremnego ($n \geqslant 3$) środkami klasycznymi jest możliwa wtedy i tylko wtedy, gdy $n = 2^t$ dla $t \in \mathbb{N}_2$ lub $n = 2^m p_1 \cdot p_2 \cdot \ldots \cdot p_s$, gdzie $m \in \mathbb{N}$, a p_j dla $j \in \{1, \ldots, s\}$ są parami różnymi liczbami pierwszymi Fermata. Euler wykazał (zob. Sierpiński, 1959) następujące

Twierdzenie 1
Każdy dzielnik liczby F_n jest postaci $k \cdot 2^{n+2} + 1$, gdzie k jest liczbą naturalną.

Zapewne dzięki temu twierdzeniu odkrył, że liczba $5 \cdot 2^7 + 1$, czyli 641 jest dzielnikiem liczby F_5. Złożoność, a właściwie pełny rozkład liczby F_6 na czynniki pierwsze znaleźli T. Clansen w 1856 r. oraz F. Landry w 1880 r.

W tej pracy pokażemy użyteczność prostych narzędzi matematycznych do uzasadnienia złożoności liczb F_5 i F_6. Udowodnimy najpierw

Twierdzenie 2
Liczba $d = k \cdot 2^7 + 1$, gdzie k jest liczbą naturalną, jest dzielnikiem liczby $F_5 = 2^{32} + 1$ wtedy i tylko wtedy, gdy $d | (2^4 + k^4)$.

Dowód. Ponieważ $d = k \cdot 2^7 + 1$, zatem $1 = d - k \cdot 2^7$. Stąd każdy wspólny dzielnik liczb d i k jest dzielnikiem 1. Zatem $NWD(d, k) = 1$. Wobec tego następujące warunki są równoważne:

$$d | F_5, \quad d | (2^4 (k \cdot 2^7)^4 + k^4), \quad d | (2^4 (k \cdot 2^7)^4 - 2^4 + 2^4 + k^4),$$

*Some comments on the Fermat numbers F_5 and F_6

$$d| \left[2^4(k\cdot 2^7+1)(k\cdot 2^7-1)((k\cdot 2^7)^2+1)+(2^4+k^4)\right],$$

$$d|(2^4+k^4).$$

Wykorzystując twierdzenie 2, bez trudu znajdziemy jeden z dzielników liczby F_5. Dla $k=5$ mamy bowiem $d=5\cdot 2^7+1=641$ oraz $2^4+5^4=641$.

Wyróżnimy teraz jeszcze trzy warunki równoważne warunkowi podanemu w twierdzeniu 2. W tekście poniżej zostały one podkreślone. Niech $d=k\cdot 2^7+1$, gdzie $k\in\mathbb{N}$.

Następujące warunki są równoważne:

$$d|F_5, \quad d|(2^4+k^4), \quad d|2^7(2^4+k^4), \quad d|(2^7k^4+k^3-k^3+2^{11}),$$

$$d|\left[k^3(k\cdot 2^7+1)+(2^{11}-k^3)\right], \quad \underline{d|(2^{11}-k^3)}, \quad d|2^7(k^3-2^{11}),$$

$$d|(2^7k^3+k^2-k^2-2^{18}), \quad d|\left[k^2(k\cdot 2^7+1)-(k^2+2^{18})\right], \quad \underline{d|(k^2+2^{18})},$$

$$d|2^7(k^2+2^{18}), \quad d|(2^7k^2+k-k+2^{25}), \quad d|\left[k(2^7+1)+(2^{25}-k)\right], \quad \underline{d|(2^{25}-k)}.$$

Wobec tego udowodniliśmy

Twierdzenie 3
Niech $d=k\cdot 2^7+1$, gdzie k jest ustaloną liczbą naturalną. Wtedy warunek $d|F_5$ jest równoważny następującym warunkom:

(1) $d|(2^4+k^4)$,

(2) $d|(2^{11}-k^3)$,

(3) $d|(2^{18}+k^2)$,

(4) $d|(2^{25}-k)$.

Zauważmy, że warunek (4) z twierdzenia 3 pozwala odkryć „bez obliczeń” drugi dzielnik liczby F_5. Mamy bowiem

$$2^{25}-5=641\cdot 52347.$$

Stąd

$$2^{25}-52347=640\cdot 52347+5,$$

$$2^{25}-52347=5(52347\cdot 2^7+1).$$

Wobec tego liczba $k=52347$ spełnia warunek (4) z twierdzenia 3, co pozwala stwierdzić, że liczba $d=52347\cdot 2^7+1$ jest dzielnikiem liczby F_5.

Znanych jest kilka dowodów faktu, że $641|F_5$. Dowody te oparte są na twierdzeniach dotyczących relacji przystawania modulo m (zob. Sierpiński, 1959).

W tej części pracy podamy osiem oryginalnych dowodów tego, że $641|F_5$, opartych na wzorach skróconego mnożenia.

Dowód I. Następujące warunki są równoważne:

$$641|F_5, \quad 641|2F_5, \quad 641|((2^{11})^3 - 125^3 + 125^3 + 2).$$

Ponieważ $641|(2^{11} - 125)$ oraz $641|(125^3 + 2)$, zatem $641|F_5$.

Dowód II. Następujące warunki są równoważne:

$$641|F_5, \quad 641|2^4 \cdot 10^6 F_5, \quad 641|(10^6(2^6)^6 + 2^4 \cdot 10^6), \quad 641|\left[(640^6 - 1) + (2^4 10^6 + 1)\right].$$

Ponieważ $641|(640^6 - 1)$ oraz $641|(2^4 \cdot 10^6 + 1)$, zatem $641|F_5$.

Dowód III. Następujące warunki są równoważne:

$$641|F_5, \quad 641|\left[((2^{16})^2 - 154^2) + (154^2 + 1)\right].$$

Ponieważ $641|(2^{16} - 154)$ i $641|(154^2 + 1)$, zatem $641|F_5$.

Dowód IV. Następujące warunki są równoważne:

$$641|F_5, \quad 641|4F_5, \quad 641|((2^{17})^2 - 333^2 + 333^2 + 4).$$

Ponieważ $641 \mid (2^{17} + 333)$ i $641 \mid (333^2 + 4)$, zatem $641 \mid F_5$.

Dowód V. Następujące warunki są równoważne:

$$641|F_5, \quad 641|\left[2^6((2^{13})^2 - 141^2) + (2^6 \cdot 141^2 + 1)\right],$$

$$641|\left[2^6((2^{13})^2 - 141^2) + (2^6 \cdot 141^2 - 640)\right],$$

$$641|\left[((2^{13})^2 - 141^2) + (141^2 - 10)\right].$$

Ponieważ $641|(2^{13} + 141)$ i $641|(141^2 - 10)$, zatem $641|F_5$.

Dowód VI. Następujące warunki są równoważne:

$$641|F_5, \quad 641|5^4 F_5, \quad 641|[5^4(2^8)^4 + 5^4], \quad 641|\left[((5 \cdot 2^8)^4 - 2^4) + (2^4 + 5^4)\right],$$

$$641|\left[2^4((5 \cdot 2^7)^4 - 1) + 641\right].$$

Ponieważ $641 = 5 \cdot 2^7 + 1$, zatem $641|F_5$.

Dowód VII. Następujące warunki są równoważne:

$$641|F_5, \quad 641|2^4 F_5, \quad 641|(2^{36} + 2^4), \quad 641|(64^6 + 2^4), \quad 641|(640^6 + 10^6 2^4),$$

$$641|\left[(640^6 - 640^2) + (10^6 \cdot 2^4 + 640^2)\right], \quad 641|\left[640^2(640^4 - 1) + 10^2 \cdot 2^8(5^4 + 2^4)\right].$$

Ponieważ $641 = 5^4 + 2^4$, zatem $641|F_5$.

Dowód VIII. Następujące warunki są równoważne:

$$641|F_5, \quad 641|2^8(2^{32}+1), \quad 641|(2^{40}+2^8), \quad 641|(2^{40}\cdot 5^4+2^8\cdot 5^4),$$

$$641|\left[((5\cdot 2^{10})^4-8^4)+(8^4+5^4\cdot 2^8)\right], \quad 641|\left[8^4((5\cdot 2^7)^4-1)+2^8(2^4+5^4)\right].$$

Stąd $641|F_5$.

Zajmiemy się teraz badaniem liczby $F_6 = 2^{64}+1$. Udowodnimy najpierw

Twierdzenie 4
Jeśli $d = k\cdot 2^8+1$, gdzie k jest ustaloną liczbą naturalną, to warunkowi $d|F_6$ równoważne są następujące warunki:

(1) $d|(k^8+1)$,

(2) $d|(k^7-2^8)$,

(3) $d|(k^6+2^{16})$,

(4) $d|(k^5-2^{24})$,

(5) $d|(k^4+2^{23})$,

(6) $d|(k^3-2^{40})$,

(7) $d|(k^2+2^{48})$,

(8) $d|(k-2^{56})$.

Dowód. Następujace warunki są równoważne:

$$d|F_6, \quad d|k^8\cdot(2^{64}+1), \quad d|\left[((k\cdot 2^8)^8-1)+(k^8+1)\right], \quad d|(k^8+1).$$

Dowód równoważności pozostałych warunków przebiega analogicznie do dowodu równoważności warunków (2), (3), (4) w twierdzeniu 3.

Z twierdzenia 4 wynika następujący

Wniosek
Liczba F_6 jest liczbą złożoną i jednym z jej dzielników jest liczba $1071\cdot 2^8+1$, czyli 274177.

Dowód. Wystarczy sprawdzić, czy dla liczby $d = 1071\cdot 2^8+1$ spełniony jest jeden z warunków od (1) do (8) twierdzenia 4. Sprawdzimy np., że spełniony jest warunek (1). Należy zatem wykazać, że $d|(1071^8+1)$.

Mamy:

$$d = 274177, \quad 1071^2 = 4d+50333, \quad 1071^4 = 16d^2+8d\cdot 50333+50333^2,$$

$$1071^4 = 16d^2+402664d+9240d+15409, \quad 1071^4 = s\cdot d+15409,$$

gdzie $s = 16d+411904$.

Stąd dostajemy:

$$1071^8 + 1 = (sd + 15409)^2 = s^2d^2 + 2sd \cdot 15409 + 15409^2 + 1.$$

Ponieważ $15409^2 + 1 = 866d$, zatem $d|(1071^8 + 1)$.

Niewielkim wysiłkiem można sprawdzić, że spełniony jest każdy z pozostałych warunków twierdzenia 4. Biorąc np. pod uwagę warunek (6) z twierdzenia 4 mamy:

$$1071^3 - 2^{40} = 1228480911 - 1099511627776 = -1098283146865 = -4005745d.$$

$$\begin{aligned} 1071^2 &\equiv 50333 \pmod{d},\\ 1071^3 &\equiv 167951 \pmod{d},\\ 2^{10} &\equiv 1024 \pmod{d},\\ 2^{20} &\equiv -48132 \pmod{d},\\ 2^{40} &\equiv 167951 \pmod{d}. \end{aligned}$$

Stąd $d|(1071^3 - 2^{40})$.

Ponieważ $2^{56} = 72057594037927936$, więc

$$2^{56} - 1071 = 72057594037926865 \quad \text{oraz} \quad 2^{56} - 1071 = d \cdot 262814145745,$$

gdzie $d = 1071 \cdot 2^8 + 1$.

Stąd też

$$\begin{aligned} 2^{56} - 262814145745 &= 1071 \cdot 2^8 \cdot 262814145745 + 1071,\\ 2^{56} - 262814145745 &= 1071(2^8 \cdot 262814145745 + 1). \end{aligned}$$

Stąd oraz z twierdzenia 4 dostajemy także informację, że liczba $2^8 \cdot 262814145745 + 1$ jest dzielnikiem liczby F_6.

W tej części pracy pokażemy, że dobierając odpowiednio system pozycyjny zapisu liczb można łatwo uzasadnić, że $641|F_5$ oraz $(1071 \cdot 2^8 + 1)|F_6$.

Zajmijmy się najpierw liczbą F_5 i przyjmijmy, że podstawą systemu, w którym będziemy prowadzili rozważania jest liczba $q = 2^7$. Wtedy $d = 641 = 5q + 1$ oraz $F_5 = 16q^4 + 1$. Dla uzasadnienia, że $5q + 1$ dzieli F_5, wystarczy znaleźć $a_1, a_2, a_3 \in \{0, 1, 2, 3, \ldots, 127\}$ takie, by $16q^4 + 1 = (5q + 1)(a_3q^3 + a_2q^2 + a_1q + 1)$.

Po wykonaniu mnożenia mamy

$$16q^4 + 1 = 5a_3q^4 + (5a_2 + a_3)q^3 + (5a_1 + a_2)q^2 + (5 + a_1)q + 1.$$

Stąd otrzymujemy:

$$\begin{aligned} &5 + a_1 = 128, && a_1 = 123,\\ &5 \cdot 123 + a_2 + 1 = 5 \cdot 128, && a_2 = 24,\\ &5 \cdot 24 + a_3 + 5 = 128, && a_3 = 3. \end{aligned}$$

Ponieważ $5 \cdot a_3 + 1 = 16$, zatem $16q^4 + 1 = (5q + 1)(3q^3 + 24q^2 + 123q + 1)$.

W ten sposób przedstawiliśmy liczbę F_5 w postaci iloczynu

$$(5 \cdot 2^7 + 1)(3 \cdot 2^{21} + 24 \cdot 2^{14} + 123 \cdot 2^7 + 1).$$

W przypadku liczby F_6 przyjmijmy, że podstawą systemu, w którym będziemy teraz działać, jest liczba $q = 1071$.

Aby pokazać, że liczba $d = 256q + 1$ dzieli liczbę F_6, wystarczy pokazać, że $d|(q^8+1)$ (zob. tw. 4 warunek (1)). W tym celu wystarczy znaleźć $a_1, a_2, \ldots, a_6 \in \{0, 1, \ldots, 1070\}$ tak, by $q^8+1 = (256q+1)\cdot(a_6q^6+a_5q^5+a_4q^4+a_3q^3+a_2q^2+a_1q+1)$.

Po wykonaniu mnożenia otrzymamy

$$\begin{aligned} q^8 + 1 = 256a_6q^7 + (256a_5 + a_6)q^6 + (256a_4 + a_5)q^5 + (256a_3 + a_4)q^4 \\ + (256a_2 + +a_3)q^3 + (256a_1 + a_2)q^2 + (256 + a_1)q + 1. \end{aligned}$$

Stąd $a_1 = 815,\ a_2 = 204,\ a_3 = 60,\ a_4 = 656,\ a_5 = 196,\ a_6 = 4$.

Zatem $1071^8+1 = (256\cdot1071+1)\cdot(4\cdot1071^6+196\cdot1071^5+656\cdot1071^4+60\cdot1071^3+ +204 \cdot 1071^2 + 815 \cdot 1071 + 1)$. To kończy uzasadnienie, że liczba $d = 1071 \cdot 2^8 + 1$ dzieli liczbę F_6.

Literatura

Narkiewicz, W.: 2003, *Teoria liczb*, PWN, Warszawa.

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

Sierpiński, W.: 1959, *Teoria liczb, cz. 2*, PWN, Warszawa.

Sierpiński, W.: 1969, *Arytmetyka teoretyczna*, PWN, Warszawa.

Yan, S. Y.: 2006, *Teoria liczb w informatyce*, PWN, Warszawa.

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