Notacja

$\mathbb{Z}$ – zbiór liczb całkowitych,

$\mathbb{N}$ – zbiór liczb naturalnych $1, 2, \ldots$,

$\mathbb{P}$ – zbiór liczb pierwszych: $2, 3, 5, 7, 11, \ldots$.

$x|y$ – x jest dzielnikiem y, tzn. $\exists d \in \mathbb{Z}(d \cdot x = y)$,

$\mathrm{ord}_p(x) \in \mathbb{Z}$ – wykładnik przy p w rozkładzie dodatniej liczby wymiernej x na iloczyn całkowitych potęg liczb pierwszych: $x = \prod_{p\in\mathbb{P}} p^{\mathrm{ord}_p(x)}$;

$\gcd(a, b)$ – największy wspólny dzielnik liczb $a, b \in \mathbb{Z}$.

Wszystkie wyniki w niniejszym artykule są klasyczne i dobrze znane.

Dzielniki Fermata

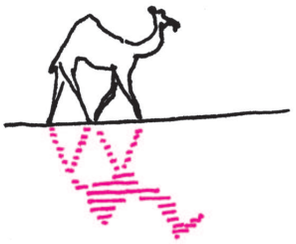
Włodzimierz HOLSZTYŃSKI

1. Wstęp

Dzielniki Fermata to większe od 1 dzielniki liczb Fermata $F(n) := 2^{2^n} + 1$ dla $n = 0, 1, \ldots$. Zatem $F(0) = 3, F(1) = 5, F(2) = 17, \ldots$. Liczby niebędące dzielnikami Fermata nazywamy niedzielnikami Fermata.

Każde dwie różne liczby Fermata są względnie pierwsze (Goldbach). Dlatego dzielnik Fermata jest dzielnikiem tylko jednej liczby Fermata.

Na to, żeby liczba postaci $2^k + 1$ była pierwsza, konieczne jest, żeby k było postaci 2^n. Fermat przypuszczał, iż warunek ten jest także dostateczny, czyli że każda $F(n)$ jest pierwsza. Jest tak dla $n = 0, 1, 2, 3, 4$, ale Euler wykazał (co Fermat przegapił), że $F(5)$ jest złożona. Potem udowodniono złożoność następnych kilku liczb Fermata, a o żadnej nowej nie pokazano, że jest pierwsza. Choćby dlatego warto zająć się dzielnikami Fermata: dawni mistrzowie koncentrowali się na kolejno ustalonej liczbie Fermata, i szukali jej dzielników; w niniejszym artykule będziemy skupiać się na kolejno ustalonej liczbie pierwszej i sprawdzać, czy jest ona dzielnikiem jakiejkolwiek liczby Fermata (większość liczb pierwszych odrzucimy).



2. Okresowość liczb Fermata mod p

Liczby Fermata są nieparzyste. Początkowe dwie nieparzyste liczby pierwsze, 3 i 5 są liczbami Fermata, a więc dzielnikami Fermata. A 7? Należy sprawdzić nieskończenie wiele podzielności $7|F(n)$. A jednak uczynimy to w skończonej liczbie kroków. Skorzystamy ze wzoru rekurencyjnego:

$$F(n) = (F(n-1) - 1)^2 + 1 \quad \text{dla } n = 1, 2 \ldots \tag{1}$$

Rozpatrzmy ciąg liczb Fermata $\bmod 7$, albo ogólniej $\bmod p$, dla dowolnego $p = 2, 3, \ldots$. Jeżeli $k < n$ i $F(k) \equiv F(n) \bmod p$, to $F(k+1) \equiv F(n+1) \bmod p$ (na mocy wzoru rekurencyjnego), więc ciąg $F(k), F(k+1), \ldots$ będzie miał okres $n - k$. Ale klas $\bmod p$ jest tylko p. Więc $F(k) \equiv F(n) \bmod p$ dla pewnego k oraz n, spełniających $0 \leqslant k < n \leqslant p$. Zatem p dzieli jedną z liczb $F(0), \ldots, F(p-1)$, albo nie dzieli żadnej liczby Fermata:

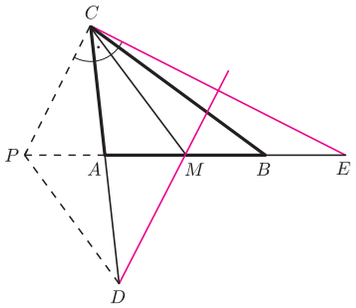
Twierdzenie 1. *Jeżeli $p > 1$ oraz $p|F(n)$, to $p > n$.*

Dla wygody rachunkowej wprowadźmy $B(n) := 2^{2^n}$, skąd $B(n) = (B(n-1))^2$ dla $n = 1, 2, \ldots$, oraz $F(n) = B(n) + 1$ dla $n = 0, 1 \ldots$. Sprawdźmy, czy 7 jest dzielnikiem Fermata:

n	0	1	2
$B(n) \bmod 7$	2	4	2
$F(n) \bmod 7$	3	5	3

– nie jest. (W ten sposób prosty program komputerowy może błyskawicznie znaleźć wszystkie dzielniki Fermata, które przez trzy wieki mozolnie odkrywali matematycy w przedkomputerowych czasach.)

Rozwiązanie zadania M 1220.
Oznaczmy przez P punkt symetryczny do punktu M względem punktu A (rys.).



Wówczas proste DM i CP są równoległe, a punkt M jest środkiem odcinka PE. Na mocy równości $PM = EM = CM$ punkt M jest środkiem okręgu opisanego na trójkącie PEC, skąd wynika, że $\sphericalangle PCE = 90^\circ$. Zatem proste DM i CE są prostopadłe.

3. Dzielniki Fermata mod 4

Niech $p|F(n)$ dla $n > 0$. Wtedy kongruencja $x^2 \equiv -1 \bmod p$ ma rozwiązanie, na przykład $x := B(n-1) = F(n-1) - 1$. Dla p pierwszego oznacza to, na mocy twierdzenia Eulera, że $p \equiv 1 \bmod 4$.

Twierdzenie 2. *Wszystkie pierwsze dzielniki Fermata p przystają do $1 \bmod 4$, z wyjątkiem $p = 3$.*

Tak więc 3 i 5 są liczbami Fermata, 7 oraz $11 \equiv 3 \bmod 4$, więc nie są dzielnikami, i dopiero liczba pierwsza 13 znowu ma szansę być dzielnikiem Fermata – sprawdźmy:

n	0	1	2	3	4
$B(n) \bmod 13$	2	4	3	9	3
$F(n) \bmod 13$	3	5	4	10	4

– nie jest.

Już Euler wiedział, że każdy dzielnik pierwszy liczby Fermata $F(n)$ daje resztę 1 z dzielenia przez 2^{n+1}, a pod koniec XIX wieku E. Lucas pokazał, że jest to prawdziwe także dla modułu 2^{n+2}. Niedawno Kżizek, Luca i Somer (J. Number Theory 97, 2002, 95–112) pokazali, że suma odwrotności dzielników pierwszych wszystkich liczb $F(n)$ jest zbieżna. Wiele dalszych informacji, łącznie z wynikami poszukiwań numerycznych, można znaleźć na stronie internetowej `www.prothsearch.net/fermat.html`

Władysław Narkiewicz

4. Zastosowanie Małego Twierdzenia Fermata (MTF)

Niech $p|F(n)$ dla $p \in \mathbb{P}$, skąd $2^{2^{n+1}} \equiv 1 \bmod p$. Także $2^{p-1} \equiv 1 \bmod p$ (MTF), więc $2^k \equiv 1 \bmod p$ dla $k := \gcd(2^{n+1}, p-1)$; zauważmy, że wówczas $k \mid 2^{\mathrm{ord}_2(p-1)}$.

Twierdzenie 3. *Jeżeli $p \in \mathbb{P}$ jest dzielnikiem Fermata, to $2^{2^t} \equiv 1 \bmod p$ dla $t := \mathrm{ord}_2(p-1)$; więc $p < 2^{2^t}$.*

Czyni to algorytm poszukujący dzielników Fermata znacznie efektywniejszym. Wśród pierwszych $p \equiv 1 \bmod 4$, po niedzielniku 13 i pierwszej liczbie Fermata 17, następnym kandydatem na dzielnik Fermata jest $p := 29 = 7 \cdot 2^2 + 1$. Ale $2^{2^2} = 16 < 29$, więc 29 nie jest dzielnikiem Fermata.

Tezę $2^{2^t} \equiv 1 \bmod p$ (tw. 3) możemy przepisać w postaci $p|F(t) - 2$. Ale z równania (1) otrzymujemy:

$$F(t) - 2 = \prod_{k=0}^{t-1} F(k) \quad \text{dla } t = 1, 2 \ldots \tag{2}$$

Zatem twierdzenie 3 możemy równoważnie napisać tak.

Twierdzenie 4. *Jeżeli $p \in \mathbb{P}$ jest dzielnikiem Fermata, to $p|F(s)$ dla pewnego $s < \mathrm{ord}_2(p-1)$.*

Ponieważ $F(s)$ jest pierwsza dla $s < 5$, to otrzymujemy wniosek.

Twierdzenie 5. *Jedyne pierwsze dzielniki Fermata p, dla których $\mathrm{ord}_2(p-1) < 6$, to liczby Fermata $F(s)$ dla $s < 5$.*

5. Wyliczenia (bez komputera)

W świetle twierdzenia 5 pozostali nam do badania kandydaci ze zbioru $\{p \in \mathbb{P} : p \equiv 1 \bmod 64\}$, czyli liczby pierwsze występujące w ciągu arytmetycznym $64 \cdot a + 1$. Dla $a \equiv 2 \bmod 3$ oraz $a \equiv 1 \bmod 5$ otrzymujemy wyrazy złożone, więc można ograniczyć się do $a \equiv 0, 3, 4, 7, 9, 10, 12, 13 \bmod 15$. Sporo wśród nich jest pierwszych: $193, 257, 449, 577, 641, 769, \ldots$ (dla $a := 13 \equiv -1 \bmod 7$ otrzymujemy wyraz podzielny przez 7; dla $a := 15$ otrzymujemy $961 = 31^2$). Sprawdźmy kolejnych kandydatów p. Dzięki twierdzeniu 3, poniższe tabelki rozciągają się tylko po $s = \mathrm{ord}_2(p-1) - 1$.

Dla $p := 193 = 2^6 \cdot 3 + 1$ mamy:

s	0	1	2	3	4	5
$B(n) \bmod 193$	2	4	16	63	109	108
$F(n) \bmod 193$	3	5	17	64	110	109

Więc 193 jest niedzielnikiem. Następnie $257 = F(3)$. Popatrzmy na $p := 449 = 2^6 \cdot 7 + 1$:

s	0	1	2	3	4	5
$B(n) \bmod 449$	2	4	16	256	431	324
$F(n) \bmod 449$	3	5	17	257	432	325

Liczba pierwsza 449 jest niedzielnikiem.

Kolej na $577 = 2^6 \cdot 9 + 1$:

s	0	1	2	3	4	5
$B(n) \bmod 577$	2	4	16	256	335	287
$F(n) \bmod 577$	3	5	17	257	336	288

Znowu niedzielnik, 577. Pora na $p := 641 = 2^7 \cdot 5 + 1$:

s	0	1	2	3	4	5
$B(n) \bmod 641$	2	4	16	256	154	640
$F(n) \bmod 641$	3	5	17	257	155	0

Dzielnik! Dowiedliśmy przy okazji, że $F(5)$ jest złożona:

Twierdzenie 6. *(Euler)*

$$641 | F(5).$$

Spróbujmy $769 = 2^8 \cdot 3 + 1$; rutynowy początek tabeli ($s = 0, 1, 2$) pomijamy:

s	3	4	5	6	7
$B(n) \bmod 769$	256	171	19	361	360
$F(n) \bmod 769$	257	172	20	362	361

Niedzielnik. Pokazaliśmy, że jedynymi dzielnikami Fermata < 1000 są liczby Fermata $3, 5, 17, 257$ oraz liczba 641.