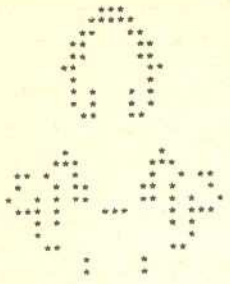
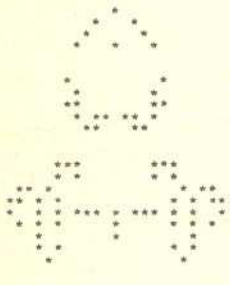


mutacja 35



mutacja 36

# O największej znanej liczbie pierwszej

*Dr hab. Andrzej ROTKIEWICZ*

Wielki polski matematyk, twórca polskiej szkoły matematycznej i genialny badacz, znakomity popularyzator matematyki, autor pięćdziesięciu książek i 720 prac naukowych, doctor honoris causa wielu uniwersytetów, zmarły przed ponad siedmiu laty Profesor dr Wacław Sierpiński w przedmowie do II części swej Teorii Liczb napisał:
„Jako przykład postępu, jaki dokonał się w teorii liczb w ostatnim czasie, wystarczy podać, że największą znaną w roku 1950 liczbą pierwszą była liczba $2^{127}-1$, mająca 39 cyfr, dziś zaś największą znaną liczbą pierwszą jest liczba $2^{3217}-1$, mająca 969 cyfr. Wówczas znaliśmy tylko 12 liczb doskonałych, dziś zaś znamy ich 18". Te słowa były pisane w roku 1958. Liczby pierwsze są to liczby naturalne, które mają dokładnie dwa dzielniki naturalne. Są to więc liczby 2, 3, 5, 7, 11, ... Liczby doskonałe są to liczby, które są równe sumie swych dzielników naturalnych, mniejszych od nich samych. Najmniejszą liczbą doskonałą jest, jak łatwo widzieć, liczba $6 = 1+2+3$. Następną po niej jest liczba $28 = 1+2+4+7+14$.

Można dowieść, że na to, aby liczba parzysta $n$ była liczba doskonałą, potrzeba i wystarcza, by była ona postaci $2^{s-1}(2^s-1)$, gdzie $2^s-1$ jest liczbą pierwszą. Zatem wszystkie liczby doskonałe parzyste są zawarte we wzorze $2^{p-1}(2^p-1)$ z warunkiem, że liczby $p$ oraz $2^p-1$ są pierwsze.
Już Euklides podał następującą metodę wyznaczania liczb doskonałych:
„Obliczamy kolejne sumy składników szeregu

$$1+2+4+8+16+32+\ldots$$

Jeżeli suma taka okaże się liczbą pierwszą, to pomnóżmy ją przez ostatni składnik. Otrzymamy liczbę doskonałą".
Na podstawie przytoczonego poprzednio twierdzenia widzimy, że metoda Euklidesa wyznacza wszystkie parzyste liczby doskonałe. Dla $p = 2, 3, 5, 7$ liczby $2^p-1$ odpowiednio równe 3, 7, 31, 127 są pierwsze, zatem 6, 28, 496, 8128 są liczbami doskonałymi, co zostało zauważone już przez Nicomachusa około 100 roku naszej ery.

Manuskrypt z roku 1456 podaje poprawnie jako piątą liczbę doskonałą liczbę 33550336, która równa się $2^{12}(2^{13}-1)$.

Fermat w 1640 roku zauważył, że $2^{23}-1$ ma dzielnik 47, zaś $2^{37}-1$ ma dzielnik 223, zaś Euler w 1732 r. zauważył, że 1103 jest dzielnikiem liczby $2^{29}-1$. Euler w 1772 roku stwierdził, że liczba $2^{31}-1 = 2147483647$ jest pierwsza i — co za tym idzie — że liczba $2^{30}(2^{31}-1) = 2305843008139952128$ jest doskonała. Jest to ósma z kolei liczba doskonała parzysta. Dziewiąta z kolei liczba doskonała parzysta odpowiada wykładnikowi $p = 61$. Jest to liczba $2^{60}(2^{61}-1)$. Pierwszość liczby $2^{61}-1$ mającej 19 cyfr została stwierdzona przez Pierwuszyna w 1883 r., Seelhoffa w 1886 r. i Hudelota w 1887 r.

Powers w 1911 r. znalazł następną liczbę doskonałą $2^{88}(2^{89}-1)$. Tenże wraz z Fauquemberguem znalazł w 1914 r. liczbę doskonałą $2^{106}(2^{107}-1)$, a Fauquembergue również w 1914 r. znalazł dwunastą liczbę doskonałą $2^{126}(2^{127}-1)$ mającą 77 cyfr. Drugi czynnik tej liczby, $2^{127}-1$, był największą liczbą pierwszą do roku 1950. Ze względów historycznych ważna jest uwaga, że Mersenne w 1644 r. twierdził, że $2^p-1$ jest pierwsze tylko dla 11 wartości $p$, a mianowicie dla $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$, i 257.

Lehmer dowiódł jednak, że liczba $2^{257}-1$ nie jest pierwsza i przeto liczba $2^{256}(2^{257}-1)$ nie jest doskonała. Tak więc w ciągu Mersenne'a należy skreślić 257 i 67 a dopisać 61, 89 i 107. Poza tym istnieją dla $n > 257$ liczby Mersenne'a $M_n$, które są pierwsze. W styczniu 1952 r. przy użyciu maszyny matematycznej SWAC, oraz twierdzenia Lucasa-Lehmera udowodniono, że liczby Mersenne'a $M_{521} = 2^{521}-1$ i $M_{601} = 2^{601}-1$ są pierwsze. Pierwsza z tych liczb ma 157 cyfr, druga 183 cyfry. W tym samym roku, w czerwcu, udowodniono, że liczba $M_{1279} = 2^{1279}-1$ jest pierwsza. Ma ona 376 cyfr. We wrześniu 1952 r. znaleziono, że liczby $M_{2203}$ i $M_{2281}$ są pierwsze. Pierwsza ma 664 cyfry, druga 687 cyfr. Praca maszyny elektronowej dla stwierdzenia, że liczba $M_{2281}$ jest pierwsza, trwała 66 minut.

Aby liczba $2^n-1$ była liczbą pierwszą potrzeba, żeby $n$ było liczbą pierwszą, bowiem $2^{rq}-1$ jest podzielne przez $2^r-1$

Cataldi zauważył to w 1603 roku i sprawdził, że $2^p-1$ jest pierwsze dla $p = 13, 17$ i 19.

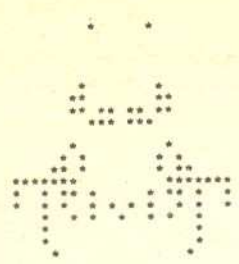
Rozwiązanie zadania M 113
Zauważmy, że liczby $2^n$ i $2^{n+3}$ dają przy dzieleniu przez 7 takie same reszty, gdyż różnica $2^{n+3}-2^n = 2^n(2^3-1) = 7\cdot 2^n$ jest podzielna przez 7. Podobnie liczby $n^2$ i $(n+7)^2$ dają przy dzieleniu przez 7 takie same reszty, co wynika z równości $(n+7)^2-n^2 = 7(2n+7)$.
Ciąg reszt z dzielenia przez 7 liczb $2^n$ $(n = 1, 2, 3, \ldots)$ jest zatem okresowy i okres wynosi 3, jest to więc ciąg

(*) 2, 4, 1, 2, 4, 1, ...

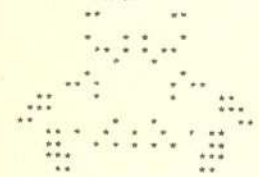
Ciąg reszt z dzielenia przez 7 liczb $n^2$ $(n = 1, 2, 3, \ldots)$ jest też okresowy i okres wynosi 7, jest to więc ciąg

(**) 0, 1, 4, 2, 2, 4, 1, 0, 1, 4, 2, 2, 4, 1, ...

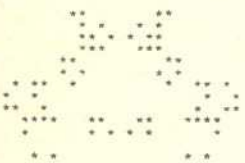
Reszta, jaką daje przy dzieleniu przez 7 liczba $2^n+n^2$, jest sumą reszt, jakie dają liczby $2^n$ i $n^2$ (być może zmniejszoną o 7). Łatwo jednak sprawdzić, że liczba 7 nie jest sumą liczb wziętych po jednej ze zbiorów $\{1, 2, 4\}$ i $\{0, 1, 2, 4\}$, tj. ze zbiorów wartości ciągów (*) i (**).
Wykazaliśmy w ten sposób twierdzenie ogólniejsze:
Dla żadnych liczb naturalnych $m$ i $n$ liczba $2^m+n^2$ nie dzieli się przez 7.



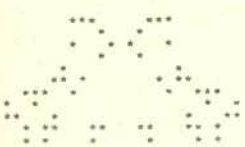
mutacja 37



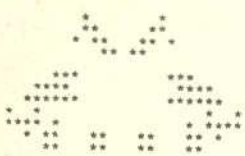
mutacja 38



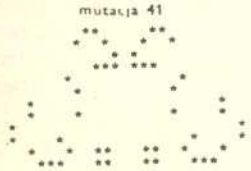
mutacja 39



mutacja 40



mutacja 41



mutacja 42

mutacja 43

W 1958 roku na szwedzkiej maszynie elektronowej BESK stwierdzono, że liczba $M_{3217} = 2591170 \ldots 09315071$, mająca 969 cyfr jest pierwsza. Praca maszyny trwała $5\frac{1}{2}$ godzin. Następnie w 1964 r. znaleziono liczby pierwsze $M_{9689}$, $M_{9941}$ i $M_{11213}$. Używano maszyny ILLAC II na uniwersytecie w Illinois. $M_{11213}$ ma 3381 cyfr. Czas pracy maszyny dla udowodnienia, że jest ona pierwsza wynosił 2 godziny i 14 minut.

Dziś znamy 24 liczby Mersenne'a, które są pierwsze i tyle samo znamy liczb doskonałych.

Największa znana liczba pierwsza wynosi $2^{19437}-1 = 4315424797 \ldots 0968041471$ i ma 6002 cyfry.

Największą znaną liczbą doskonałą jest obecnie $(2^{19937}-1)2^{19936} = 9311445590 \ldots 0271942656$ i ma 12003 cyfry.

Tak więc obecnie znamy 24 liczby Mersenne'a $M_n$, które są pierwsze. Otrzymujemy je dla $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 617, 1279, 2203, 2281, 3217, 4219, 4423, 9689, 9941, 11213, 19937$.

Największa znana liczba pierwsza $M_{19937}$ i największa znana liczba doskonała zostały znalezione 4 marca 1971 roku na maszynie elektronowej IBM 360/91 w Stanach Zjednoczonych Ameryki przez Tuckermanna przy pomocy twierdzenia Lucasa-Lehmera. Czas pracy maszyny wynosił 35.01 min. Dokładniejsze dane można znaleźć w artykule Tuckermanna w 68 tomie czasopisma *The Proceedings of the National Academy of Sciences of the United States of America* na stronach 2319–2320 w artykule pt. „The 24th Mersenne Prime".

Twierdzenie Lucasa-Lehmera można sformułować tak: Liczba $2^p-1$, gdzie $p$ jest liczbą pierwszą $> 2$, jest liczbą pierwszą wtedy i tylko wtedy, gdy

$$(1) \qquad (2^p-1) \mid (1+\sqrt{3})^{2^{p-1}} + (1-\sqrt{3})^{2^{p-1}} = V_{2^{p-1}}.$$

Aby więc stwierdzić, że liczba $2^{19937}-1$ jest dzielnikiem liczby $(1+\sqrt{3})^{2^{19936}} + (1-\sqrt{3})^{2^{19936}}$ można poglądowo powiedzieć, że twierdzenie Lucasa-Lehmera zastępuje biliony, biliony, biliony ... dzieleń jednym dzieleniem.

Z kolei łatwo dowieść, że podzielność (1) zachodzi wtedy i tylko wtedy, gdy $(p-1)$-szy wyraz ciągu

$$S_1 = 4, S_2 = 14, S_3 = 194, \ldots, S_k, \ldots,$$

gdzie

$$S_1 = 4 \text{ zaś } S_k = S_{k-1}^2 - 2 \text{ dla } k = 2, 3, \ldots,$$

jest podzielny przez $M_p = 2^p-1$.

Rzeczywiście, przez indukcję łatwo dowieść, że

$$(2) \qquad V_{2^{n-1}} = 2^{2^{n-2}} S_{n-1}$$

W samej rzeczy, jeżeli $n = 2$ to $V_{2^{n-1}} = V_{2^1} = (1+\sqrt{3})^2 + (1-\sqrt{3})^2 = 8$ oraz $2^{n-2} S_{n-1} = 2^{2^0} \cdot S_1 = 2 \cdot 4 = 8$.

Jeśli zaś zachodzi (2) dla liczby naturalnej $n \geqslant 2$ to

$$S_{n-1} = \frac{V_{2^{n-1}}}{2^{2^{n-2}}}, \text{ skąd } 2^{2^{n-1}} \cdot S_n = 2^{2^{n-1}} \cdot (S_{n-1}^2 - 2) = 2^{2^{n-1}} \left( \frac{V_{2^{n-1}}^2}{2^{2^{n-1}}} - 2 \right) =$$

$$= V_{2^{n-1}}^2 - 2 \cdot 2^{2^{n-1}} = [(1+\sqrt{3})^{2^{n-1}} + (1-\sqrt{3})^{2^{n-1}}]^2 - 2 \cdot 2^{2^{n-1}} =$$

$$= (1+\sqrt{3})^{2^n} + (1-\sqrt{3})^{2^n} = V_{2^n}$$

i na mocy indukcji stwierdzamy, że wzór (2) zachodzi dla każdego $n \geqslant 2$.

Oznaczmy teraz przez $\bar{t}$ resztę jaką otrzymamy dzieląc $t$ przez $M_p = 2^p-1$. Wtedy twierdzenie Lucasa-Lehmera można wypowiedzieć tak: Liczba $M_p = 2^p-1$, gdzie $p$ jest liczbą pierwszą $> 2$, jest liczbą pierwszą wtedy i tylko wtedy, gdy $(p-1)$-szy wyraz ciągu określonego rekurencyjnie przez

$$r_1 = 4, r_2 = 14, \ldots, r_{k+1} = \overline{r_k^2 - 2} \text{ dla } k = 1, 2, \ldots$$

jest podzielny przez $M_p = 2^p-1$.

Aby obliczyć $r_{p-1}$ potrzeba więc wykonać $p-2$ podnoszeń do kwadratu liczb będących resztami z dzielenia przez $M_p$, a więc mających nie więcej cyfr niż liczba $M_p = 2^n-1$, a następnie znajdować resztę z dzielenia przez $M_p$ tych kwadratów zmniejszonych o liczbę 2. Te mnożenia i dzielenia wykonują właśnie maszyny matematyczne.

Do tej pory nie wiemy jednak, czy istnieje nieskończenie wiele liczb pierwszych Mersenne'a.