ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE V (1962)

wmptm 1897

Ministerstwo Nauki i Szkolnictwa Wyższego

W. SIERPIŃSKI (Warszawa)

Co osiągnięto w teorii liczb za pomocą maszyn elektronowych?

Odczyt popularny, wygłoszony w Warszawie 6. XII. 1960 r.

Teoria liczb zajmuje się badaniem własności liczb całkowitych. Wszystkie inne rodzaje liczb, z jakimi ma do czynienia współczesna matematyka, sprowadzają się do układów liczb całkowitych albo też do zbiorów takich układów. Dzisiejsza matematyka, jak mówimy, została zarytmetyzowana. Toteż nic dziwnego, że badanie własności tych podstawowych elementów, z których jest zbudowana matematyka, tj. liczb całkowitych, wzbudza wciąż zainteresowanie.

Nierozwiązane dotąd zagadnienia matematyki, a w szczególności teorii liczb, można podzielić na dwa rodzaje. Do pierwszego rodzaju można zaliczyć takie, dla których znamy metodę, która doprowadziłaby do rozwiązania zagadnienia, gdyby wykonane zostały pewne rachunki, ale przeszkodą ich wykonania jest ich długość. Do drugiego rodzaju zaliczymy takie zagadnienia, dla których nie znamy żadnej metody, zapewniającej ich rozwiązanie. Oczywiście, maszyny mogą być stosowane tylko do rozwiązywania zagadnień pierwszego rodzaju.

Podamy tu przede wszystkim przykłady zagadnień pierwszego i drugiego rodzaju.

Takie proste zagadnienie jak to, czy dana liczba całkowita jest podzielna przez inną daną liczbę całkowitą i jaką ewentualnie daje przy dzieleniu przez nią resztę, jest oczywiście zagadnieniem, które potrafimy rozwiązać, albo też zagadnieniem 1-go rodzaju, i może niekiedy wymagać uciążliwych rachunków. Oto weźmy na przykład takie pytanie:

Czy liczba $a = 2^{2^{16}}+1 = 2^{65536}+1$, mająca, jak łatwo obliczyć 19729 cyfr (w układzie dziesiętnym), jest podzielna przez liczbę $m = 825753601$?

Zanim się tym pytaniem zajmiemy bliżej, wyjaśnimy, skąd się ono wzięło.

Do roku 1953 nie było wiadomym, czy prawdziwym jest przypuszczenie, że każda z liczb ciągu nieskończonego

$$2+1,\ 2^2+1,\ 2^{2^2}+1,\ 2^{2^{2^2}}+1,\ 2^{2^{2^{2^2}}}+1,\ldots$$

jest pierwszą. Wiedziano, że pierwsze cztery wyrazy tego ciągu są liczbami pierwszymi, natomiast nie wiedziano, czy wyraz piąty czyli liczba a, jest liczbą pierwszą. Gdyby się okazało, że liczba a jest podzielna przez liczbę m, wynikałoby stąd, że jest ona złożona, a więc, że przypuszczenie, o którym mowa, jest fałszywe. Dlaczego właśnie wzięto tu dziewięciocyfrową liczbę m — wyjaśnimy później.

A teraz zajmiemy się bliżej pytaniem, jak można rozstrzygnąć, czy liczba a, mająca 19729 cyfr, jest podzielna przez liczbę m czy też nie.

Już samo obliczenie liczby a oraz wypisanie wszystkich jej kolejnych cyfr byłoby rzeczą niezmiernie uciążliwą, a cóż dopiero wykonanie jej dzielenia przez dziewięciocyfrową liczbę m. Ale nam nie chodzi tu o wynik tego dzielenia, ani o znalezienie jego ilorazu. Wystarczy dowiedzieć się jaką jest reszta z dzielenia liczby a przez liczbę m. I oto dzięki budowie liczby $a = 2^{2^{16}}+1$ będzie można znajdywanie tej reszty znacznie uprościć. Wystarczy oczywiście znaleźć resztę z z dzielenia liczby $2^{2^{16}}$ przez m.

Niech s oznacza daną liczbę naturalną. Możemy ustalić postępowanie, które pozwoli nam obliczyć resztę z z dzielenia liczby 2^{2^s} przez m, nie obliczając samej liczby 2^{2^s}.

Przypuśćmy, że przy pewnym naturalnym n znamy resztę r_n z dzielenia liczby 2^{2^n} przez m. Oczywiście, będzie tu $r_n < m$, oraz będzie $2^{2^n} = k_n m + r_n$, gdzie k_n jest liczbą całkowitą (całością ilorazu z dzielenia 2^{2^n} przez m). Ponieważ $2^{2^{n+1}} = (2^{2^n})^2$, więc $2^{2^{n+1}} = (k_n m + r_n)^2 = (k_n^2 m + 2k_n r_n)m + r_n^2$, skąd wynika, że reszta r_{n+1} z dzielenia liczby $2^{2^{n+1}}$ przez m jest równa reszcie z dzielenia liczby r_n^2 przez m. Tak więc, jeżeli znamy resztę r_n z dzielenia liczby 2^{2^n} przez m, to, dla znalezienia reszty r_{n+1} z dzielenia liczby $2^{2^{n+1}}$ przez m, wystarczy liczbę r_n (mniejszą od m, a więc mającą co najwyżej 9 cyfr) podnieść do kwadratu i znaleźć resztę z z dzielenia tego kwadratu przez m. Ponieważ $2^{2^4} = 65536 = r_4$, więc, w podany wyżej sposób, trzeba będzie obliczyć kolejno liczby $r_5, r_6, \ldots$, aż do r_{16}, czyli dwanaście razy wykonywać podnoszenie do kwadratu liczb co najwyżej dziewięciocyfrowych, a następnie wyznaczać za każdym razem reszty z dzielenia tych kwadratów przez dziewięciocyfrową liczbę m. Oczywiście rachunki te mogłyby być wykonane i bez pomocy maszyn do liczenia, chociaż byłoby to uciążliwe.

Ale przejdźmy do pytania, skąd wzięła się liczba m, ten przypuszczalny dzielnik liczby a.

Otóż znanym było od dawna twierdzenie, że dzielniki naturalne liczby $F_s = 2^{2^s}+1$ są postaci $2^{s+2}k+1$, gdzie $k = 0, 1, 2\ldots$ Chcąc więc znaleźć najmniejszy, większy od jedności, dzielnik naturalny liczby $a = F_{16}$, musimy go szukać wśród liczb postępu arytmetycznego $2^{18}k+1$,

gdzie $k = 1, 2, 3, \ldots$ Dla danego naturalnego $k \leqslant 3150$, z uwagi na to, że, jak łatwo obliczyć, $2^{18} \cdot 3150 + 1 = m$, stwierdzenie, czy a jest czy nie jest podzielne przez $2^{18}k+1$, będzie więc wymagało rachunków nie dłuższych niż omówione wyżej rachunki potrzebne dla stwierdzenia, czy liczba a jest podzielna przez m czy też nie.

Rachunki te zostały w roku 1953 wykonane za pomocą maszyn elektronowych SWAC, przy czym w ciągu $3\frac{1}{4}$ godziny stwierdzono, że dopiero dla $k = 3150$ otrzymujemy dzielnik m liczby a (1). W ten sposób znaleziono najmniejszy >1 dzielnik liczby a i stwierdzono, że nie jest ona liczbą pierwszą, skąd wynika fałszywość przypuszczenia, o którym mówiliśmy wyżej.

Błędem byłoby jednak sądzić, że metoda, którą tak skutecznie dało się zastosować do liczby F_{16}, daje się tym bardziej zastosować dla każdej liczby naturalnej $s < 16$ do badania, czy liczba F_s jest pierwszą, czy też nie.

Oto weźmy na przykład liczbę F_{17}. W myśl wyżej wspomnianego twierdzenia wiemy, że dzielniki naturalne tej liczby są postaci $2^{19}k+1$ i, dla znalezienia najmniejszego >1 takiego dzielnika liczby F_{17}, badano za pomocą maszyn elektronowych, czy go nie ma dla kilku tysięcy kolejnych wartości liczby naturalnej k, ale go nie znaleziono. Jeżeli najmniejszy >1 dzielnik liczby F_{17} ma na przykład sto lub więcej cyfr, to tą metodą się go nie znajdzie.

Ciekawym jest, że omawianą metodą nie potrafimy też znaleźć najmniejszego >1 dzielnika liczb F_7 ani liczby F_8 i F_{13}, chociaż w inny sposób, jeszcze w pierwszym dziesiątku naszego stulecia, zanim zaczęto stosować maszyny elektronowe, udowodniono, że liczby F_7 i F_8 są złożone. Zachodzi bowiem następujące twierdzenie:

Na to, żeby liczba $F_s = 2^{2^s}+1$, *gdzie s jest liczbą naturalną, była liczbą pierwszą, potrzeba i wystarcza, żeby liczba* $3^{2^{2^s-1}}+1$ *była podzielna przez liczbę* F_s (2).

Dla zbadania czy liczba $3^{2^{2^s-1}}+1$ jest podzielna przez F_s nie ma potrzeby obliczania jej. Można tu bowiem zastosować rozumowanie podobne do tego, które stosowaliśmy wyżej do badania podzielności liczby a przez m, co ogranicza rachunki do wykonania mniej niż 2^s podnoszeń do kwadratu liczb nie większych od F_s oraz dzieleń tych kwadratów przez F_s.

Toteż, jeżeli chodzi o liczby F_7 i F_8, z których pierwsza ma 39, druga zaś 78 cyfr, rachunki te zostały, jak już wspomnieliśmy, wykonane nawet

(1) Zob. J. L. Selfridge, *Mathematical tables and other aids to computation*, 44 (1953), str. 274-275.

(2) Dowód elementarny tego twierdzenia znajduje się w książce W. Sierpiński, *Teoria liczb*, Część II, Warszawa 1959, str. 391-392.

bez użycia maszyn elektronowych. Ponieważ liczba F_{13} ma 2467 cyfr, zaś $2^{13} = 8192$, więc dla zbadania, czy liczba F_{13} jest pierwszą czy nie należałoby wykonać mniej niż 8200 podnoszeń do kwadratu liczb, mających nie więcej niż 2467 cyfr oraz tyleż dzieleń tych liczb przez F_{13}. Rachunki te zostały wykonane w roku 1960 i stwierdzono, że liczba F_{13} jest złożona, ale żadnego jej dzielnika pierwszego nie znamy (zob. G. A. Paxson, *The compositeness of the thirtheenth Fermat number*, Mathematics of Computation 15 No 76, October 1961). Obliczenie za pomocą maszyny trwało 6 godzin i 17 minut.

Już wielki matematyk francuski P. Fermat (który żył w XVII wieku) wiedział, że liczby F_n są pierwsze dla $n = 0, 1, 2, 3$ i 4, i wyraził przypuszczenie, że są one pierwsze dla każdego naturalnego n, ale już w 1732 roku Euler wykazał, że liczba F_5 jest złożona, podzielna przez 641. Później udowodniono, że liczba F_6 też jest złożona i znaleziono jej najmniejszy dzielnik >1. O liczbach F_7 i F_8, jak już wspominaliśmy, wiemy, że są złożone, ale nie znamy żadnego ich rozkładu na iloczyn dwóch liczb naturalnych >1. Dla każdej z liczb F_9, F_{10}, F_{11} i F_{12} metodą, o której mówiliśmy wyżej, znaleziono ich najmniejszy dzielnik >1 i stwierdzono że są złożone. Dla liczby F_{10}, mającej 309 cyfr, znaleziono w r. 1953 przy pomocy maszyn elektronowych jej najmniejszy >1 dzielnik, którym jest liczba $2^{12} \cdot 11131 + 1$. Natomiast najmniejszy >1 dzielnik liczby złożonej F_{12}, którym jest liczba $2^{14} \cdot 7 + 1$, znaleźli jeszcze w roku 1878 Lucas i Pierwuszyn bez pomocy maszyn do liczenia.

Ogółem znamy dotąd 36 liczb złożonych F_n, z których największą jest F_{1945}, mająca więcej niż 10^{580} cyfr, a więc liczba, której nie jesteśmy w możności napisać. Stosując metodę, o której mówiliśmy wyżej, znaleziono za pomocą maszyn elektronowych najmniejszy >1 jej dzielnik, którym jest liczba $2^{1947} \cdot 5 + 1$, mająca 587 cyfr ([3]). Stąd, że p jest najmniejszym >1 dzielnikiem pewnej liczby wynika natychmiast, że p jest liczbą pierwszą. Tak więc mamy tu przykład znalezionej przy pomocy maszyn elektronowych liczby pierwszej o 587 cyfrach.

Nie wiemy czy istnieje liczba pierwsza F_n, gdzie $n > 4$. Pytanie to jest drugiego rodzaju. Podobnie drugiego rodzaju jest pytanie czy wśród liczb F_n istnieje nieskończenie wiele liczb złożonych.

Największą znaną dziś liczbą pierwszą jest liczba $2^{3217} - 1$, mająca 969 cyfr. Że jest ona pierwszą stwierdzono w 1957 roku przy pomocy szwedzkiej maszyny elektronowej cyfrowej BESK, opierając się na twierdzeniu Lucas-Lehmera, podającym warunek konieczny i wystarczający na to, żeby liczba postaci $2^n - 1$ była pierwszą ([4]). Praca maszyny

([3]) Zob. Proc. Amer. Math. Soc. 9 (1958), str. 673-681.

([4]) Bliższe szczegóły o tym twierdzeniu i jego stosowaniu, jak też jego dowód elementarny znajduje się w książce W. Sierpiński *Teoria liczb*, Część II, Warszawa 1959, str. 381-386.

trwała $5\frac{1}{2}$ godziny. W tomie 12 *Mathematical tables and other aids to computation* z r. 1958 na str. 60 podane jest pełne rozwinięcie dziesiętne tej liczby $2^{3217}-1 = 2591170860\ldots 2909315071$. Jak wiadomo, jeżeli (dla pewnego naturalnego n) 2^n-1 jest liczbą pierwszą, to $2^{n-1}(2^n-1)$ jest liczbą doskonałą, czyli liczbą naturalną, równą sumie wszystkich swych mniejszych od niej samej dzielników naturalnych. Tak więc $2^{3216}(2^{3217}-1)$ jest liczbą doskonałą i to największą z dotąd znanych. Dla znalezienia rozwinięcia dziesiętnego tej liczby trzeba więc liczbę $2^{3217}-1$, mającą 969 cyfr, pomnożyć przez liczbę $2^{3216} = 1295585430\ldots 454657536$, również mającą 969 cyfr. Mnożenie to zostało wykonane 17 listopada 1959 roku w Experimental Center w Atlantic City (New Yersey), przy czym praca maszyny trwała 5 minut.

Pełne rozwinięcie liczby

$$2^{3216}(2^{3217}-1) = 3357083\ldots 8525056,$$

mającej 1937 cyfr, podane jest w czasopiśmie *Mathematics of Computation* 14 (1960) na str. 200.

Wszystkie liczby pierwsze, mające sto lub więcej cyfr (a takich znamy już kilkanaście) zostały znalezione za pomocą maszyn elektronowych w ostatnim dziesięcioleciu. Znamy kilka liczb pierwszych, mających dokładnie sto cyfr (na przykład liczba $81\cdot 2^{324}+1$), ale nie znamy żadnej liczby pierwszej, mającej tysiąc lub więcej cyfr, chociaż, jak wiadomo, istnieje nieskończenie wiele takich liczb pierwszych. Zagadnienie znalezienia takiej liczby jest zagadnieniem 1-go rodzaju. Można żywić nadzieję, że za pomocą maszyn elektronowych zostanie ono kiedyś rozwiązane. Nie znamy też dotąd żadnej liczby pierwszej, mającej dokładnie 500 cyfr, chociaż udowodniono, że liczba taka, nawet więcej niż jedna, istnieje.

Co do liczb 2^n-1 wyrażono przypuszczenie, że jeżeli liczba 2^n-1 jest pierwszą, to i liczba $2^{2^n-1}-1$ jest pierwszą. W r. 1953 stwierdzono za pomocą maszyn elektronowych, że przypuszczenie to jest fałszywe, gdyż liczba $2^{13}-1 = 8191$ jest pierwszą, natomiast liczba $2^{8191}-1$ (mająca 2466 cyfr) jest złożoną [5]. Praca maszyny elektronowej trwała tu 100 godzin. Nie znamy jednak żadnego rozkładu tej liczby na iloczyn dwóch liczb naturalnych od niej mniejszych. Zagadnienie znalezienia takiego rozkładu jest oczywiście zagadnieniem 1-go rodzaju. Są więc zagadnienia 1-go rodzaju, których maszyny elektronowe nie są w możności dotąd rozwiązać. Znaleziono natomiast w r. 1957 za pomocą maszyn elektronowych rozkład liczby $2^{2^{17}-1}-1$ na iloczyn dwóch liczb naturalnych od niej mniejszych, która zatem jest złożona, mimo że liczba $2^{17}-1$ jest pierwszą.

---

[5] Zob. Proc. Amer. Math. Soc. 5(1954), str. 844.

Znamy dotąd 20 liczb pierwszych postaci 2^n-1, z których osiem największych znaleziono za pomocą maszyn elektronowych. Zagadnienie czy liczb pierwszych tej postaci jest nieskończenie wiele (a nawet to, czy jest więcej niż 18) jest zagadnieniem 2-go rodzaju.

Podobnie zagadnieniem 2-go rodzaju jest zagadnienie czy liczb pierwszych postaci 2^n-7 (dla $n>3$) jest nieskończenie wiele. Na początku bieżącego roku wiedziano, że dla naturalnych n, takich iż $3<n<39$, liczby 2^n-7 są wszystkie złożone i postawiono pytanie czy liczba $2^{39}-7$ jest pierwszą. Otóż w lutym 1960 r. na posiadanej przez Zakład Konstrukcji Telekomunikacyjnych i Radiofonii Politechniki Warszawskiej elektronowej maszynie cyfrowej EMC mgr T. Kulikowski przebadał tę liczbę i wykazał, że jest pierwszą. Jest to więc najmniejsza liczba pierwsza postaci 2^n-7 (dla naturalnych $n>3$).

W r. 1958 N. L. Gilbreath wyraził następujące przypuszczenie. Wypiszmy ciąg nieskończony wszystkich kolejnych liczb pierwszych. Pod nim wypiszmy w pierwszym wierszu ciąg różnic kolejnych liczb pierwszych. Pod nim wypiszmy w pierwszym wierszu ciąg różnic kolejnych liczb pierwszych. W drugim wierszu wypiszmy ciąg wartości bezwzględnych różnic kolejnych wyrazów pierwszego wiersza. W każdym następnym wierszu wypisujmy ciąg wartości bezwzględnych różnic kolejnych wyrazów danego wiersza. Gilbreath przypuszcza, że pierwszy wyraz każdego wiersza będzie równy 1.

Oto na przykład 10 pierwszych otrzymanych w ten sposób wierszy (poza ciągiem pierwszych jedenastu liczb pierwszych)

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31
1, 2, 2, 4, 2, 4, 2, 4, 6, 2
1, 0, 2, 2, 2, 2, 2, 2, 4
1, 2, 0, 0, 0, 0, 0, 2
1, 2, 0, 0, 0, 0, 2
1, 2, 0, 0, 0, 2
1, 2, 0, 0, 2
1, 2, 0, 2
1, 2, 2
1, 0
1

Przypuszczenie Gilbreatha zostało za pomocą maszyn elektronowych SWAC sprawdzone dla pierwszych 63418 wierszy. Dowodu na to, że przypuszczenie jest prawdziwe dla każdego wiersza, dotąd nie ma.

W związku ze znanym w teorii liczb twierdzeniem Wilsona zajęto się wyznaczaniem reszt z dzielenia przez liczby pierwsze p liczb (jak wiadomo całkowitych) $((p-1)!+1)/p$. Za pomocą maszyny elektronowej SMIL Uniwersytetu w Lund obliczono przed paru laty te reszty dla wszyst-

kich liczb pierwszych p, gdzie $10000 < p < 30000$ i, opierając się na wcześniejszych wynikach, stwierdzono, że tylko dla liczb $p = 5, 13$ i 563 liczba $(p-1)!+1$ jest podzielna przez p^2 ([6]). Zagadnienie, czy są jeszcze inne takie liczby jest 2-go rodzaju.

W związku ze znanym, tzw. małym twierdzeniem Fermata, zajęto się, dla liczb pierwszych p, wyznaczaniem reszt z dzielenia liczby (jak wiadomo całkowitej) $(2^{p-1}-1)/p$ przez p. Za pomocą wymienionej wyżej maszyny obliczono te reszty dla wszystkich liczb pierwszych $p < 50000$ i stwierdzono, że dla takich p są one równe zeru tylko dla $p = 1093$ i $p = 3511$. Pytanie, czy poza tymi dwiema liczbami pierwszymi p są jeszcze inne, dla których liczba $2^{p-1}-1$ jest podzielna przez p^2, jest zagadnieniem 2-go rodzaju. Nie wiemy też czy istnieje nieskończenie wiele liczb pierwszych p, dla których liczba $2^{p-1}-1$ nie jest podzielna przez p^2.

Niech $\Delta(x)$ oznacza różnicę pomiędzy liczbą $\pi_3(x)$ liczb pierwszych $\leqslant x$, które przy dzieleniu przez 4 dają resztę 3, a liczbą $\pi_1(x)$ liczb pierwszych $\leqslant x$, które przy dzieleniu przez 4 dają resztę 1. Już w 1914 roku Littlewood dowiódł, że istnieje nieskończenie wiele takich liczb naturalnych n, dla których $\Delta(n) > 0$, jak też nieskończenie wiele takich n, dla których $\Delta(n) < 0$, ale jeszcze kilka lat temu nie znano żadnej liczby n, dla której $\Delta(n) < 0$. Za pomocą maszyny elektronowej EDSAC J. Leech obliczył $\Delta(n)$, dla wszystkich naturalnych $n \leqslant 3000000$. W ten sposób znalazł on, że najmniejszą liczbą n, dla której $\Delta(n) < 0$ jest $n = 26861$. Mamy tu $\pi_1(n) = 1473$, $\pi_3(n) = 1472$, zatem $\Delta(n) = -1$. Znaleziono też, że $\Delta(623681) = -8$, $\Delta(627859) = \Delta(627860) = \ldots = \Delta(627900) = 0$, $\Delta(2951071) = 256$ ([7]).

Liczby postaci $n \cdot 2^n + 1$, gdzie n jest liczbą naturalną, zwane są liczbami Cullena. Najmniejszą z nich jest liczba $1 \cdot 2^1 + 1 = 3$, która jest pierwszą. Nasunęło się pytanie, czy są jeszcze inne liczby pierwsze Cullena. Za pomocą maszyny elektronowej SWAC znaleziono, że najmniejszą liczbą pierwszą Cullena > 3 jest liczba $141 \cdot 2^{141} + 1$. (Zob. R. M. Robinson, Proc. of the Amer. Math. Soc. 9 (1958), str. 677.)

Za pomocą maszyny SWAC stwierdzono, że liczba

$$M = (18!-1) : 59 = 108514808571661$$

jest złożoną i znaleziono jej rozkład na czynniki pierwsze:

$$M = 226663 \cdot 478749547,$$

(zob. Mathesis 67 (1958), str. 218-220).

([6]) Zob. *Mathematical tables and other aids to computation* 12 (1958), str. 281.

([7]) Zob. *Mathematical tables and other aids to computation* 13 (1959), str. 272-284.

Mówiliśmy dotąd o zastosowaniach maszyn elektronowych do rozwiązania różnych zagadnień dotyczących liczb pierwszych. Podamy teraz przykłady zastosowań innego rodzaju.

Jak wiadomo, Fermat wypowiedział twierdzenie, że jeżeli n jest liczbą naturalną >2, to równanie

$$x^n+y^n=z^n$$

nie ma rozwiązań w liczbach naturalnych x, y, z.

Otóż za pomocą maszyn elektronowych SWAC w Los Angeles w Kalifornii udowodniono, że twierdzenie Fermata jest prawdziwe dla wszystkich wykładników naturalnych n, gdzie $2 < n < 4003$ ([8]).

Zauważymy tu, że nie dla każdego danego naturalnego n pytanie, czy twierdzenie Fermata jest prawdziwe dla wykładnika n, jest zagadnieniem 1-go rodzaju. Natomiast zagadnieniem pierwszego rodzaju jest, dla danych naturalnych n i m, wyznaczenie wszystkich rozwiązań równania $x^n+y^n=z^n$ w liczbach naturalnych x, y, z, gdzie $z \leqslant m$.

Za pomocą maszyny elektronowej EDSAC w Laboratorium Matematycznym Uniwersytetu w Cambridge wyznaczono dla każdej danej liczby całkowitej k, gdzie $0 \leqslant k \leqslant 100$, wszystkie rozwiązania równania

$$x^3+y^3+z^3=k,$$

w liczbach całkowitych x, y, z, gdzie $|z| \leqslant |y| \leqslant |x| \leqslant 3164$ ([9]).

Mgr A. Mąkowski postawił w r. 1959 w czasopiśmie belgijskim *Mathesis* pytanie, czy równanie

$$x^3+y^3+2z^3=113$$

ma rozwiązanie w liczbach całkowitych x, y, z.

Jak podają w tymże czasopiśmie *Mathesis* w t. 69 z r. 1960 na stronie 218 K. Moszyński i J. Swianiewicz, za pomocą maszyny elektronowej „Mercury" Uniwersytetu w Manchester znaleziono, że równanie to ma rozwiązanie $x=-133$, $y=-46$, $z=107$. Za pomocą maszyny elektronowej EDSAC II J. Leech wyznaczył dla $|E| \leqslant 4303$ wszystkie rozwiązania w liczbach naturalnych A, B, C, D równania

$$A^4+B^4+C^4+D^4=E^4\ ([10]).$$

Celem tego odczytu nie jest oczywiście przedstawienie wszystkiego tego, co osiągnięto w teorii liczb za pomocą maszyn elektronowych. Wybrałem tu tylko kilkanaście przykładów, dających pojęcie o tym jakiego to rodzaju są osiągnięcia.

([8]) Zob. *Proc. of the National Academy of Sciences* 41 (1955), str. 970-973.

([9]) Zob. *Journ. London Math. Soc.* 30 (1955), str. 101-110.

([10]) Zob. *Proc. of the Cambridge Phil. Soc.* 54 (1958), str. 554.

Nowoczesne elektronowe maszyny rachunkowe powstały zaledwie kilkanaście lat temu.

Dla każdego zagadnienia, które ma być rozwiązane przez maszyny elektronowe, musi być przygotowany ogólny schemat rozwiązania. Na tej podstawie opracowuje się szczegółowy program rachunku. Zawiera on instrukcje, wyznaczające wszystkie operacje arytmetyczne i logiczne, niezbędne do przeprowadzenia obliczeń. Programowanie jest procesem żmudnym i niezwykle pracochłonnym.

A oto wiadomości o naszych maszynach elektronowych, które otrzymałem od magistra Andrzeja Wąkulicza.

W Polsce pracują obecnie dwie maszyny cyfrowe. Większa z tych maszyn została zbudowana przez Zakład Aparatów Matematycznych Polskiej Akademii Nauk w roku 1958. Aparat ten o nazwie XYZ może wykonać w ciągu sekundy około 800 operacji arytmetycznych na liczbach mających nie więcej niż jedenaście cyfr.

Druga maszyna o nazwie EMC została zbudowana w roku 1959 w Zakładzie Konstrukcji Telekomunikacyjnych i Radiofonii Politechniki Warszawskiej. Może ona wykonać około stu arytmetycznych operacji w ciągu sekundy na liczbach, mających nie więcej niż dziesięć cyfr.

Oba te aparaty mogą być z powodzeniem stosowane do rozwiązywania zagadnień rachunkowych teorii liczb, w których ilość operacji arytmetycznych (na liczbach co najwyżej dziesięciocyfrowych) nie przekracza trzydziestu milionów, które maszyna XYZ wykona w ciągu $8\frac{1}{4}$ godziny. Gdyby chodziło o większą liczbę operacji, możliwość rozwiązania zadania przez maszynę wymagałaby szczegółowej analizy.

W innych krajach istnieją maszyny, mające większe możliwości, względnie mogące szybciej wykonać dane rachunki. Są tam i takie maszyny, które mogą wykonać pół miliona działań arytmetycznych na sekundę. Oto na przykład, gdyby chodziło o znalezienie wszystkich takich dzielników naturalnych liczby F_{16}, które mają nie więcej niż 10 cyfr, to maszyna SWAC wykonała to w ciągu $3\frac{1}{4}$ godziny, natomiast maszyna XYZ potrzebowałaby na to około 18 godzin, a maszyna EMC przeszło 400 godzin.

Osoby, których interesuje urządzenie i funkcjonowanie maszyn rachunkowych, znajdą bliższe szczegóły o tym w książeczce A. B. Empachera *Maszyny liczą same?*, która się właśnie ukazała.

Dodano przy korekcie: Niedawno stwierdzono przy pomocy maszyny elektronowej, że liczby $2^{4253}-1$ i $2^{4423}-1$ są pierwsze: ta ostatnia, mająca 1332 cyfry, jest więc największą znaną obecnie liczbą pierwszą.