ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE IX (1966)

Ministerstwo Nauki i Szkolnictwa Wyższego

W. SIERPIŃSKI (Warszawa)

O podzielności liczb

Odczyt popularny, wygłoszony w Warszawie 11 listopada 1964 r.

Z pojęciem podzielności liczb spotykamy się już w arytmetyce elementarnej. Jednym z podstawowych działań arytmetycznych jest dzielenie jednej liczby całkowitej przez drugą i wyznaczanie odpowiedniej reszty. Jeżeli dzielenie liczby a przez liczbę b wypada bez reszty, mówimy, że liczba a jest podzielna przez b, albo że liczba b jest dzielnikiem liczby a, albo wreszcie, że liczba a jest wielokrotnością liczby b. Wyrażamy to wzorem $b|a$, który czytamy: b jest dzielnikiem a. Na to więc żeby ten wzór zachodził, potrzeba i wystarcza, żeby istniała liczba całkowita k, taka iż $a = kb$.

Ponieważ $0 = 0 \cdot b$ dla każdej liczby całkowitej b, więc każda liczba całkowita jest dzielnikiem liczby 0. Natomiast 0 jest dzielnikiem tylko liczby 0, gdyż przy wszelkim całkowitym k mamy $k \cdot 0 = 0$.

Ponieważ wzór $a = kb$ jest równoważny każdemu ze wzorów: $-a = (-k) \cdot b$, $a = (-k) \cdot (-b)$, $-a = k \cdot (-b)$, więc wzór $b \mid a$ jest równoważny każdemu ze wzorów: $b \mid -a$, $-b \mid a$ oraz $-b \mid -a$. Wynika stąd, że przy badaniu podzielności liczb całkowitych różnych od zera wystarczy się ograniczyć do badania podzielności liczb całkowitych dodatnich, czyli naturalnych.

Łatwo jest wyznaczyć wszystkie wielokrotności naturalne danej liczby naturalnej n: będą to wszystkie wyrazy ciągu nieskończonego

$$n, 2n, 3n, 4n, \ldots$$

Trudniej natomiast jest znaleźć wszystkie dzielniki naturalne liczby naturalnej n, chociaż liczba ich jest zawsze skończona, gdyż dzielnik liczby naturalnej n jest oczywiście zawsze nie większy od n. Dla znalezienia wszystkich dzielników naturalnych danej liczby naturalnej n nie ma zresztą konieczności dzielić ją kolejno przez wszystkie liczby naturalne $\leqslant n$. Jeżeli liczba naturalna a jest dzielnikiem liczby naturalnej n, to iloraz $n:a = b$ jest liczbą naturalną: jest to tak zwany *dzielnik dopełniający* dla a (ze względu na n). Jeżeli $b \leqslant a$, to mamy $n = ab \geqslant b^2$, skąd $b \leqslant \sqrt{n}$; jeżeli zaś $b > a$, to mamy $n = ab > a^2$, skąd $a < \sqrt{n}$. Z każdych więc dwóch dopełniających

się dzielników liczby n jeden co najmniej jest zawsze $\leqslant \sqrt{n}$. Dla wyznaczenia wszystkich dzielników naturalnych liczby naturalnej n wystarczy więc znaleźć wszystkie jej dzielniki naturalne $\leqslant \sqrt{n}$ i następnie dołączyć do nich dzielniki dopełniające. Na przykład dla $n = 100$ wystarczy wyznaczyć dzielniki naturalne liczby 100 nie większe od $\sqrt{100}$ czyli od liczby 10 i następnie dołączyć do nich dzielniki dopełniające. Z liczb naturalnych $\leqslant 10$, jak łatwo sprawdzić, tylko liczby 1, 2, 4, 5 i 10 są dzielnikami liczby 100. Ich dzielnikami dopełniającymi będą liczby 100, 50, 25, 20 i 10. Tak więc liczba 100 ma 9 dzielników naturalnych: 1, 2, 4, 5, 10, 20, 25, 50 i 100. Liczba 101, jak łatwo sprawdzić, nie ma żadnego >1 dzielnika naturalnego $\leqslant \sqrt{101}$, czyli $\leqslant 10$ (gdyż $\sqrt{101} < \sqrt{121} = 11$). Liczba 101 ma więc tylko dwa dzielniki naturalne: 1 i 101. Liczby naturalne, które mają tylko dwa dzielniki naturalne, nazywamy *liczbami pierwszymi*. Aby się więc przekonać, że dana liczba naturalna $n > 1$ jest liczbą pierwszą, wystarczy się przekonać, że nie ma żadnego dzielnika > 1 oraz $\leqslant \sqrt{n}$.

Dla niewielkich liczb naturalnych n znalezienie wszystkich dzielników naturalnych liczby n nie nastręcza trudności. Inaczej jest jednak, gdy liczba naturalna n jest wielka, mająca na przykład kilkadziesiąt cyfr w układzie dziesiętnym. Na przykład dopiero w tym roku znaleziono wszystkie dzielniki naturalne liczby $n = 2^{101}-1$, mającej 31 cyfr. Przy pomocy maszyny elektronowej stwierdzono, że prócz dzielników oczywistych 1 i n ma ona jeszcze dwa inne dzielniki: trzynastocyfrowy dzielnik $d = 7432339208719$ oraz dzielnik dopełniający $n:d$, mający 18 cyfr.

Dla niektórych jednak wielkich liczb znalezienie wszystkich ich dzielników jest rzeczą łatwą. Na przykład dla każdej danej liczby naturalnej s, wszystkimi dzielnikami naturalnymi liczby 2^{s-1} są, jak łatwo dowieść, liczby $1, 2, 2^2, \ldots, 2^{s-1}$. Ma ona więc s dzielników. Wynika stąd, że istnieją liczby naturalne mające dowolną daną liczbę dzielników naturalnych.

W myśl tego, co mówiliśmy wyżej, dla przekonania się, czy dana liczba naturalna n jest liczbą pierwszą czy nie, wystarcza pewna liczba dzieleń, tym większa, im większa jest liczba n. Teoretycznie jednak wystarczyłoby tu jedno dzielenie, jak to zaraz wyjaśnimy.

Jeżeli liczba naturalna $n > 1$ nie jest liczbą pierwszą, to ma ona dzielnik naturalny a, różny od niej samej i od jedności, a więc taki, iż $1 < a < n$. Wówczas dzielnik dopełniający $b = n:a$ będzie oczywiście > 1 oraz $< n$ i będzie $n = ab$. Każda więc liczba naturalna $n > 1$, która nie jest liczbą pierwszą, jest iloczynem dwóch liczb naturalnych > 1 i, jak łatwo widzieć, odwrotnie. Liczby takie nazywamy liczbami *złożonymi*.

Udowodnimy teraz, że *na to, żeby liczba naturalna $n > 4$ była liczbą pierwszą, potrzeba i wystarcza, żeby nie była dzielnikiem liczby* $(n-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1)$, *czyli żeby było* $n \nmid (n-1)!$. (Wzór $k \nmid l$ oznacza, że iczba k nie jest dzielnikiem liczby l).

Gdyby liczba $n > 4$ była liczbą złożoną, to, jak dowiedliśmy przed chwilą, mielibyśmy $n = ab$, gdzie a i b są liczbami naturalnymi $< n$, zatem $\leqslant n-1$. Jeżeli $a \neq b$, to a i b są różnymi czynnikami iloczynu $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1)$, zatem $n = ab \mid (n-1)!$. Gdyby zaś było $a = b$, czyli $n = a^2$, to wobec $n > 4$ byłoby $a > 2$, skąd $2a < a^2 = n$, zatem $2a \leqslant n-1$ i przeto liczby a i $2a$ byłyby różnymi czynnikami iloczynu $(n-1)!$, skąd $a \cdot 2a \mid (n-1)!$ i tym bardziej $n = a^2 \mid (n-1)!$. Dowiedliśmy więc, że jeżeli liczba $n > 4$ jest liczbą złożoną, to $n \mid (n-1)!$. Jeżeli więc $n > 4$ oraz $n \nmid (n-1)!$, to liczba n musi być liczbą pierwszą.

Z drugiej strony, znane jest twierdzenie, że liczba pierwsza, dzieląca iloczyn skończonej liczby liczb naturalnych, dzieli jeden co najmniej z czynników tego iloczynu: gdyby więc n było liczbą pierwszą i dzieliło liczbę $(n-1)!$, to musiałoby dzielić jedną co najmniej z liczb $1, 2, \ldots, n-1$, co jest niemożliwe, gdyż są one mniejsze od n. Jeżeli więc n jest liczbą pierwszą, to $n \nmid (n-1)!$.

Teoretycznie więc, żeby się przekonać, czy liczba całkowita $n > 4$ jest liczbą pierwszą czy nie, wystarczy wykonać jedno dzielenie: $(n-1)! : n$; jeżeli to dzielenie wypadnie bez reszty, to liczba n nie jest liczbą pierwszą, jeżeli natomiast reszta z tego dzielenia jest $\neq 0$, to liczba n jest liczbą pierwszą. Sposób ten nie mógłby jednak być stosowany w praktyce, gdyż już dla niewielkich n, na przykład dla $n = 17$, liczba $(n-1)!$ jest bardzo wielka.

W związku z udowodnionym przez nas twierdzeniem, że liczba naturalna $n > 4$ jest wtedy i tylko wtedy liczbą pierwszą, gdy $n \nmid (n-1)!$, warto zauważyć, że z tak zwanego twierdzenia Wilsona wynika, że liczba naturalna $n > 1$ jest wtedy i tylko wtedy liczbą pierwszą, gdy $n \mid (n-1)! + 1$. Dowód twierdzenia Wilsona jest jednak nieco trudniejszy.

Opowiemy teraz o tym, jak się przekonano, że liczba $F_{1945} = 2^{2^{1945}} + 1$ jest podzielna przez liczbę $5 \cdot 2^{1947} + 1$. Przedtem jednak wyjaśnimy dlaczego stwierdzenie tej podzielności było rzeczą ciekawą.

Otóż żyjący w XVII wieku matematyk francuski Pierre Fermat twierdził, że wszystkie liczby postaci $F_n = 2^{2^n} + 1$, gdzie $n = 1, 2, \ldots$, są pierwsze. Istotnie, tak jest dla $n = 1, 2, 3$ i 4, ale już dla $n = 5$ liczba $F_5 = 2^{32} + 1$, mająca dziesięć cyfr, nie jest, jak okazał Euler, liczbą pierwszą, gdyż ma dzielnik 641. Możemy się tylko dziwić dlaczego Fermat, wypowiadając swe twierdzenie o wszystkich liczbach F_n, które sprawdził tylko dla $n = 1, 2, 3$ i 4, nie próbował dzielić liczby F_5 przez liczby nie większe od tysiąca. Dzielenie takie w czasach Fermata, gdy nie było maszyn do liczenia, było może rzeczą uciążliwą, ale możliwą, i gdyby je Fermat wykonał, byłby znalazł dzielnik 641 liczby F_5. Później udowodniono, że liczby $F_6, F_7, \ldots$, aż do F_{16} nie są pierwsze. Najmniejszą liczbą Fermata, o której dotąd nie wiemy, czy jest pierwszą czy nie, jest liczba F_{17}. Specjaliści od maszyn elektronowych obliczyli niedawno, że stwierdzenie, czy liczba F_{17} jest pierwszą czy nie,

wymagałoby 128 tygodni pracy maszyny elektronowej. Natomiast o liczbie F_{18} wiemy, że nie jest pierwszą i że ma dzielnik $13\cdot 2^{20}+1$. O liczbie F_{19} dopiero w tym roku stwierdzono, że nie jest pierwszą, gdyż ma dzielnik $308385\cdot 2^{21}+1$. Największą z liczb Fermata, o której wiemy, że nie jest liczbą pierwszą, jest liczba F_{1945}, mająca dzielnik $m = 5\cdot 2^{1947}+1$. Dlatego też przekonanie się, że liczba F_{1945} jest podzielna przez m było rzeczą ciekawą.

Liczba F_{1945} ma więcej niż 10^{582} cyfr (w układzie dziesiętnym), a więc nie mamy możności wszystkich jej cyfr wypisać, gdyż na to nie starczyłoby miejsca na świecie, ani czasu. Wspomniana wyżej liczba m ma 587 cyfr, a więc (przy dużej stracie czasu) potrafimy ją obliczyć i wypisać wszystkie jej cyfry.

Skoro liczby F_{1945} nie potrafimy wypisać, to tym bardziej nie potrafimy dzielić jej przez liczbę m i znaleźć odpowiedni iloraz oraz resztę z tego dzielenia. Jakże więc przekonano się o tym, że $m \mid F_{1945}$? Oznaczmy, dla każdej liczby całkowitej t, przez $\bar{t}$ resztę z dzielenia liczby t przez m. Będzie więc $t = km+\bar{t}$, gdzie k jest liczbą całkowitą, a $0 \leqslant \bar{t} < m$, skąd $t-\bar{t} = km$, zatem $m \mid t-\bar{t}$.

Określimy teraz ciąg liczb r_k $(k = 1, 2, \ldots)$ w następujący sposób:

$$r_1 = 2^2, \quad \text{a} \quad r_{k+1} = \overline{r_k^2} \quad \text{dla} \quad k = 1, 2, \ldots \tag{1}$$

Udowodnimy przez indukcję, że

$$m \mid 2^{2^k} - r_k \quad \text{dla} \quad k = 1, 2, \ldots \tag{2}$$

Wzór (2) zachodzi oczywiście dla $k = 1$, gdyż $2^2 - r_1 = 0$. Przypuśćmy teraz, że wzór (2) zachodzi dla pewnej liczby naturalnej k. Wówczas, ponieważ, jak wiadomo, $a-b \mid a^2-b^2 = (a-b)(a+b)$ dla każdych liczb całkowitych a i b, ze wzoru (2) wynika, że $m \mid 2^{2^{k+1}} - r_k^2$. Lecz wobec $m \mid t-\bar{t}$ dla $t = r_k^2$, mamy $m \mid r_k^2 - \overline{r_k^2}$. Lecz jeżeli m jest dzielnikiem dwóch liczb, to jest też dzielnikiem sumy tych liczb i wzory $m \mid 2^{2^{k+1}} - r_k^2$ oraz $m \mid r_k^2 - \overline{r_k^2}$ dają $m \mid 2^{2^{k+1}} - \overline{r_k^2}$, zatem wobec (1), $m \mid 2^{2^{k+1}} - r_{k+1}$, co dowodzi, że we wzorze (2) możemy zastąpić k przez $k+1$. W ten sposób wzór (2) został dla wszelkich naturalnych k udowodniony przez indukcję. Dla $k = 1945$ mamy stąd

$$m \mid F_{1945} - r_{1945} - 1,$$

skąd wynika, że przy dzieleniu przez m liczba F_{1945} daje tę samą resztę, co liczba $r_{1945}+1$. Aby więc się przekonać, czy liczba F_{1945} jest podzielna przez m, wystarczy zbadać, czy liczba $r_{1945}+1$ jest podzielna przez m. Zastanowimy się nad tym jakie działania arytmetyczne należy wykonać, aby obliczyć liczbę r_{1945}. Ze wzorów (1) wynika, że dla obliczenia liczby r_{1945} trzeba 1944 razy podnosić do kwadratu liczby $< m$, a więc mające nie więcej niż 587 cyfr i tyleż razy dzielić te kwadraty (a więc liczby, mające nie więcej niż 1174 cyfry) przez liczbę m, mającą 587 cyfr. Są to mnożenia

i dzielenia, które obecne maszyny elektronowe są w możności wykonać. W ten sposób zostało stwierdzone, że liczba F_{1945} jest podzielna przez m, a więc że nie jest liczbą pierwszą.

Należałoby tu może jeszcze wyjaśnić, skąd się wzięła ta liczba m, co do której postawiono pytanie, czy jest czy też nie jest dzielnikiem liczby F_{1945}. Otóż znane było twierdzenie, że każdy >1 dzielnik liczby F_n musi być postaci $k\cdot 2^{n+2}+1$, gdzie k jest liczbą naturalną. Wobec tego większych od jedności dzielników liczby F_{1945} należy szukać wśród liczb $k\cdot 2^{1947}+1$ dla $k = 1, 2, \ldots$ Dla $k = 1$ mamy tu liczbę $2^{1947}+1$, która jest podzielna przez $2+1 = 3$, a liczba 3, jako nie będąca postaci $k\cdot 2^{1947}+1$, nie może (w myśl twierdzenia, na które powołaliśmy się) być dzielnikiem liczby F_{1947}, a więc tym bardziej i liczba $2^{1947}+1$ nie może być jej dzielnikiem. Liczba $2\cdot 2^{1947}+1 = 2^{8\cdot 247}+1$ jest podzielna przez liczbę $2^8+1 = 257$, która nie jest postaci $k\cdot 2^{1947}+1$, wobec czego, jak wyżej, wnosimy, że liczba $2\cdot 2^{1947}+1$ nie jest dzielnikiem liczby F_{1945}. Udowodnimy, że liczba $3\cdot 2^{1947}+1$ jest podzielna przez 5. Liczba $2^4-1 = 15$ jest podzielna przez 5, skąd, wobec $2^{1944}-1 = 2^{4\cdot 487}-1$ wynika, że $5 \mid 2^{1944}-1$ i przeto liczba 2^{1944} przy dzieleniu przez 5 daje resztę 1, a więc liczba $3\cdot 2^{1947}+1 = 24\cdot 2^{1944}+1$ jest podzielna przez 5. Ponieważ liczba 5 nie jest postaci $k\cdot 2^{1947}+1$, więc jak wyżej, wnosimy, że liczba $3\cdot 2^{1947}+1$ nie jest dzielnikiem liczby F_{1945}. Liczba $4\cdot 2^{1947}+1 = 2^{1949}+1$ jest podzielna przez 3 i, jak wyżej, wnosimy, że nie może być dzielnikiem liczby F_{1945}. Z kolei mamy więc do zbadania liczbę $m = 5\cdot 2^{1947}+1$ o której udowodniono, jak mówiliśmy wyżej, że jest dzielnikiem liczby F_{1945}. Jest to więc najmniejszy >1 dzielnik naturalny tej liczby, a jak wiadomo, każdy najmniejszy >1 dzielnik liczby naturalnej jest zawsze liczbą pierwszą (gdyż gdyby był liczbą złożoną, nie byłby najmniejszym >1 dzielnikiem uważanej liczby). W ten sposób liczba m mająca 587 cyfr jest liczbą pierwszą. Nie jest to jednak największa ze znanych dziś liczb pierwszych (takich, których wszystkie cyfry rozwinięcia dziesiętnego potrafimy wypisać). Największą znaną dziś liczbą pierwszą jest liczba $2^{11213}-1$, mająca 3376 cyfr. Jeżeli uwzględnimy, że jeszcze kilkanaście lat temu największą znaną liczbą pierwszą była liczba $2^{127}-1$, mająca 39 cyfr, to widać stąd, jak wielki postęp w znajdowaniu wielkich liczb pierwszych dokonany został w ostatnich czasach dzięki maszynom elektronowym.

Omówimy tu jeszcze, jak przekonano się, że liczby Fermata F_7, F_8, F_{13} i F_{14} nie są pierwsze. Ciekawe jest, że udowodniono, że liczby te są złożone, chociaż nie znamy dla żadnej z nich żadnego nietrywialnego ich dzielnika. Otóż udowodniono twierdzenie, że na to, żeby liczba Fermata F_n była pierwsza, potrzeba i wystarcza, żeby $F_n \mid 3^{(F_n-1)/2}+1$. Jeżeli więc dla danej liczby naturalnej n stwierdzimy, że $F_n \nmid 3^{(F_n-1)/2}+1$, to na mocy tego twierdzenia będziemy wiedzieli, że F_n jest liczbą złożoną, ale nie będziemy jeszcze znali żadnego nietrywialnego (tj. różnego od 1 i od F_n) dzielnika tej liczby.

Dla $n = 14$ liczba F_n ma 4933 cyfry, a więc z trudem potrafimy ją obliczyć i wypisać, natomiast liczba $3^{(F_n-1)/2}+1$ już dla $n = 7$ ma więcej niż 10^{30} cyfr, a więc nie jesteśmy w możności ich wypisać. Jakże więc stwierdzono, że nie jest ona podzielna przez F_n (dla $n = 7, 8, 13, 14$)?

Oznaczmy dla danego n przez $\bar{t}$ resztę z dzielenia liczby t przez F_n i określmy ciąg r_k ($k = 1, 2, \ldots$) w następujący sposób:

$$r_1 = 3, \text{ a } r_{k+1} = \overline{r_k^2} \text{ dla } k = 1, 2, \ldots$$

Przez indukcję dowodzimy z łatwością, że $F_n \mid 3^{2^{k-1}} - r_k$ dla $k = 1, 2, \ldots$, skąd dla $k = 2^n$ znajdujemy, że $F_n \mid 3^{2^{2^n-1}} - r_{2^n}$, skąd wynika, że liczba $3^{2^{2^n-1}}+1 = 3^{(F_n-1)/2}+1$ przy dzieleniu przez F_n daje tę samą resztę co liczba $r_{2^n}+1$.

Dla obliczenia liczby $r_{2^{14}}$ trzeba więc mniej niż $2^{14} = 16336$ razy podnosić do kwadratu liczby, mające mniej niż 5000 cyfr i tyleż razy dzielić te kwadraty przez liczbę F_n, mającą 4933 cyfry, co istniejące obecnie maszyny elektronowe mogły wykonać. Natomiast dla $n = 7$ i $n = 8$ już w 1905 roku, bez pomocy maszyn elektronowych, stwierdzono, że $F_n \nmid 3^{2^{2^n-1}}+1$. Nasuwa się pytanie, dlaczego Fermat zajął się liczbami tak, bądź co bądź, skomplikowanej budowy, jak liczby $2^{2^n}+1$. Zapewne badał on przedtem liczby prostszej postaci 2^n+1, ale łatwo jest dowieść, że jeżeli taka liczba jest pierwsza, to musi być liczbą Fermata, gdyż n musi być potęgą dwójki. Istotnie, gdyby liczba n nie była postaci 2^k, to, oznaczając przez 2^s największą potęgę liczby 2, dzielącą n (gdzie mogłoby być i $s = 0$), mielibyśmy $n = 2^s l$, gdzie l jest liczbą nieparzystą > 1 (skoro n nie jest liczbą postaci 2^k) i byłoby $2^n+1 = 2^{2^s l}+1$, a więc podzielne przez liczbę $2^{2^s}+1$, która jest > 1 i $< 2^n+1$, (gdyż $l > 1$) i przeto liczba 2^n+1 nie byłaby liczbą pierwszą.

Zauważymy tu, że zajmowano się też liczbami postaci $M_n = 2^n-1$, tak zwanymi *liczbami Mersenne'a*, wśród których znaleziono dotąd 23 liczby pierwsze. Największe znane liczby pierwsze są liczbami Mersenne'a, jak na przykład liczba M_{11213}, o której była już mowa.

Można dowieść, że nie ma liczb naturalnych $n > 1$, dla których $n \mid 2^n-1$. Dowód tego jest elementarny, choć nie jest łatwy (1).

Można natomiast dowieść, że dla każdej liczby całkowitej $a > 1$ istnieje nieskończenie wiele liczb naturalnych n takich, że $n \mid a^n+1$.

Zajmowano się wiele liczbami n, dla których $n \mid 2^n-2$. W myśl znanego twierdzenia Fermata wzór ten zachodzi dla każdej liczby pierwszej n. Chińczycy przed 25 wiekami sądzili, że wzór ten poza liczbą 1 zachodzi tylko dla liczb pierwszych. Godne uwagi jest, że i Leibniz w latach 1680-81 podzielał ich zdanie. Było to jednak twierdzenie fałszywe, gdyż wzór $n \mid 2^n-2$

(1) Patrz moją książeczkę *200 zadań z elementarnej teorii liczb*, Biblioteczka Matematyczna 17, Warszawa 1964, str. 35, zadanie 16°.

może zachodzić też dla liczb złożonych, na przykład $11 \cdot 31 = 341 \mid 2^{341}-2$, co można by okazać elementarnie, nie obliczając liczby $2^{341}-2$, mającej 103 cyfry. Liczby złożone n, dla których $n \mid 2^n-2$, noszą nazwę *liczb pseudopierwszych*. Najmniejszą z nich jest liczba $n = 341$. Udowodniono elementarnie, że liczb takich jest nieskończenie wiele. Liczbę parzystą $n > 2$, dla $n \mid 2^n-2$ znalazł D. H. Lehmer dopiero w 1950 roku: jest to liczba $n = 161038$. Później udowodniono, że liczb parzystych pseudopierwszych jest nieskończenie wiele, ale dowód tego nie jest łatwy.

Łatwo jest dowieść, że liczby Fermata F_n spełniają wzór $F_n \mid 2^{F_n}-2$. Istotnie, ponieważ $2^n \geqslant n+1$ dla naturalnych n (czego dowodzimy z łatwością, na przykład przez indukcję), to $2^{n+1} \mid 2^{2^n}$ dla $n = 1,2,\ldots$, skąd wynika, że

$$F_n = 2^{2^n}+1 \mid 2^{2^{n+1}}-1 \mid 2^{2^{2^n}}-1 \mid 2^{2^{2^n+1}}-2 = 2^{F_n}-2,$$

zatem $F_n \mid 2^{F_n}-2$. Wynika stąd, że liczby Fermata są albo pierwsze, albo pseudopierwsze. T. Banachiewicz sądził, że ponieważ Fermat wierzył w prawdziwość twierdzenia Chińczyków, że nie ma liczb pseudopierwszych, więc stąd wyprowadził (błędne, jak się okazało) twierdzenie, że wszystkie liczby F_n $(n = 1, 2,\ldots)$ są pierwsze.

Szukano też liczb naturalnych $n > 1$, dla których $n^2 \mid 2^n-2$, skąd wynika też, że $n^2 \mid 2^{n^2}-2$; są to więc liczby pseudopierwsze kwadratowe. Dotąd znaleziono dwie takie liczby: 1093 i 3511. Zajmowano się też liczbami złożonymi n, dla których $n \mid a^n-a$ dla każdej liczby całkowitej a. Liczby takie nazwano *bezwzględnie pseudopierwszymi*. Najmniejszą z nich jest liczba $561 = 3 \cdot 11 \cdot 17$. Znamy dużo takich liczb, ale nie wiemy, czy jest ich nieskończenie wiele.

Nie wiemy, czy istnieje nieskończenie wiele liczb złożonych n takich, iż $n \mid 2^n-2$ oraz $n \mid 3^n-3$. Potrafimy natomiast z łatwością dowieść, że dla każdej liczby naturalnej a istnieje liczba złożona n taka, iż $n \mid a^n-a$. W samej rzeczy, jeżeli $a = 1$, to mamy $4 \mid 1^4-1$. Jeżeli $a = 2$, to, jak już mówiliśmy o tym, mamy $11 \cdot 13 = 341 \mid 2^{341}-2$. Jeżeli $a > 2$ i a jest liczbą pierwszą, to możemy przyjąć $n = 2a$, gdyż wtedy liczba a jest nieparzysta i liczba $a^{2a}-a$ jest parzysta, a, jako podzielna przez liczbę nieparzystą a, oraz przez liczbę 2, jest podzielna przez $2a$. Jeżeli wreszcie a jest liczbą złożoną, to możemy przyjąć $n = a$, gdyż oczywiście $a \mid a^a-a$. Udowodniono też, że dla każdej liczby naturalnej a istnieje nieskończenie wiele liczb złożonych n, takich iż $n \mid a^n-a$.

Liczbę wszystkich dzielników naturalnych liczby naturalnej n oznaczamy przez $d(n)$. Dla otrzymania, przy danym naturalnym a, wszystkich wartości funkcji $d(n)$ dla $n \leqslant a$ można stosować następujący sposób. Wypisujemy wszystkie kolejne liczby naturalne od 1 do a i podkreślamy wszystkie wypisane liczby, potem podkreślamy jeszcze raz wszystkie wypisane liczby podzielne przez 2, następnie wszystkie liczby podzielne

przez 3 itd., wreszcie, samą już liczbę a. Liczbą dzielników naturalnych liczby naturalnej $n \leqslant a$ będzie liczba jej podkreśleń. Na przykład dla $a \leqslant 20$ będziemy mieli

$$\underline{1}, \underline{\underline{2}}, \underline{\underline{3}}, \underline{\underline{\underline{4}}}, \underline{\underline{5}}, \underline{\underline{\underline{6}}}, \underline{\underline{7}}, \underline{\underline{\underline{8}}}, \underline{\underline{\underline{9}}}, \underline{\underline{\underline{\underline{10}}}}, \underline{\underline{11}}, \underline{\underline{\underline{\underline{12}}}}, \underline{\underline{13}}, \underline{\underline{\underline{14}}}, \underline{\underline{\underline{15}}}, \underline{\underline{\underline{\underline{16}}}}, \underline{\underline{17}}, \underline{\underline{\underline{\underline{18}}}}, \underline{\underline{19}}, \underline{\underline{\underline{\underline{20}}}}.$$

Stąd znajdujemy $d(1) = 1$, $d(2) = 2$, $d(3) = 2$, $d(4) = 3$, $d(5) = 2$, $d(6) = 4$, $d(7) = 2$, $d(8) = 4$, $d(9) = 3$, $d(10) = 4$, $d(11) = 2$, $d(12) = 6$, $d(13) = 2$, $d(14) = 4$, $d(15) = 4$.

Z otrzymanej tablicy wynika, że $d(2) = d(3)$, $d(14) = d(15)$. Wyrażono przypuszczenie, dotąd nie udowodnione, że istnieje nieskończenie wiele liczb naturalnych n, dla których $d(n) = d(n+1)$. Znaleziono przykłady trzech, czterech, a nawet pięciu kolejnych liczb naturalnych, mających jednakową liczbę dzielników. Mamy na przykład $d(33) = d(34) = d(35) = 4$, $d(242) = d(243) = d(244) = d(245) = 6$, wreszcie $d(n) = d(n+1) = d(n+2) = d(n+3) = d(n+4) = 8$ dla $n = 40311$. Nie wiemy, czy dla każdej liczby naturalnej k istnieje k kolejnych liczb naturalnych o tej samej liczbie dzielników.

W roku 1940 zostały wydane w Cambridge w Anglii tablice liczb $d(n)$ dla $n \leqslant 10000$. Jak wynika z tych tablic, mamy $d(n) \leqslant 64$ dla $n \leqslant 10000$, przy czym $d(n) = 64$ tylko dla $n = 7560$ i 9240. Można jednak dowieść, że dla każdej liczby naturalnej $s > 1$ istnieje nieskończenie wiele liczb naturalnych n, dla których $d(n) = s$.

Z tego krótkiego przeglądu widzimy, jak wiele jest ciekawych zagadnień, dotyczących podzielności liczb całkowitych i jak wiele prostych z nich nie jest dotąd rozwiązanych albo też zostało rozwiązanych dopiero w ostatnich latach.

W tym krótkim artykule nie mogliśmy oczywiście powiedzieć wszystkiego, co dotyczy podzielności liczb całkowitych; nie poruszaliśmy tu na przykład sprawy wspólnych dzielników dwóch lub więcej liczb, ich wspólnych wielokrotnych, ani też tak zwanych cech podzielności. Istnieje jednak specjalna, książeczka Aleksandra Białasa, pt. *O podzielności liczb* (70 stron), Warszawa 1960, gdzie sprawy te są szczegółowo omówione.