Z ARCHIWUM M

# Co wiemy a czego nie wiemy o liczbach pierwszych

**1.Co to są liczby pierwsze?**

Do pojęcia, liczb pierwszych doprowadzają już pewne proste zagadnienia które nasuwa nam tak elementarne działanie arytmetyczne takie jak mnożenie liczb naturalnych, czyli całkowitych dodatnich. Jak wiadomo, iloczyn dwóch liczb naturalnych jest zawsze liczbą naturalną. Są więc liczby naturalne, będące iloczynami dwóch liczb naturalnych większych od jedności. Ale są też liczby naturalne większe od jedności które nie są iloczynami dwóch liczb naturalnych większych od jedności, na przykład liczby 2, 3, 5 albo 13. Takie właśnie liczby nazywamy pierwszymi. A więc: Liczbą pierwszą nazywamy każdą liczbę naturalną, większą od jedności, która nie jest iloczynem dwóch liczb naturalnych, większych od jedności. Nasuwa się tu pytanie , czy co do każdej liczby naturalnej $n > 1$ potrafimy się przekonać, czy jest, czy też nie jest liczbą pierwszą. Otóż sama definicja liczb pierwszych nasuwa się spodób przekonania się o tym. Jeżeli bowiem liczba naturalna $n > 1$ nie jest pierwszą, to jest iloczynem liczb naturalnych a i b, większych od jedności. Mamy więc $n = a*b$ ,gdzie $a > 1$ i $b > 1$, skąd wynika natychmiast, że $n > a$ oraz $n > b$. Liczba natnralna $n > 1$, która nie jest pierwszą,jest więc iloczynem dwóch liczb naturalnych od niej mniejszych: Liczby takie nazywamy liczbami złożonymi. Jeżeli liczba n jest złożoną, to mamy $n = a * b$ ,gdzie a i b są liczbami naturalnymi $> 1$ oraz $< n$. Iloraz $n : a = b$ jest liczbą naturalną, zatem a jest dzielnikiem naturalnym liczby n większym od 1 I mniejszym od n. Zatem żeby się przekonać o tym ,że liczba naturalna $n > 1$ jest pierwszą, wystarczy się przekonać ,że nie ma dzielnika naturlanego $n > 1$ oraz $< n$, a do osiągnięcia tego wystarczy wykonać n-2 dzielenia liczby n przez liczby 2,3,...,n-1. Jeżeli przez żadną z tych liczb liczba n nie jest podzielna bez reszty – i tylko wtedy – liczba n jest pierwszą. Tak więc, teoretycznie przynajmniej, potrafimy zawsze (za pomocą skończonej liczby dzieleń) przekonać się, czy dana liczba naturalna n jest, czy nie jest pierwszą. Praktycznie jednak, opisany tu sposób może nastręczać duże trudności, gdy liczba n jest wielką. Nie jesteśmy dotąd w stanie, z powodu długości potrzebnych rachunków, zastosować tego sposobu do liczby $2^{101} - 1$, mającej 31 cyfr (w układzie dziesiętnym), jakkolwiek na innej drodze dowiedziono, że liczba ta jest złożoną. Nie znamy jednak dotąd żadnego jej rozkładu na iloczyn dwóch liczb naturalnych, większych od jedności (chociaż wiemy, że taki rozkład istnieje).

**2. Dzielniki pierwsze liczb naturalnych**

Udowodnimy teraz kilka łatwych twierdzeń o liczbach pierwszych:

Twierdzenie 1. Każda liczba naturalna $n > 1$ ma co najmniej jeden dzielnik pierwszy.

Dowód. Niech n będzie liczbą naturalną $> 1$: ma ona dzielniki większe od jedności, na przykład samo n. Wśród dzielników liczby n większych od jedności istnieje najmniejszy, p. Gdyby p nie było liczbą pierwszą, to w myśl definicji liczb pierwszych p byłoby iloczynem dwóch liczb naturalnych większych od 1, $p = ab > a$ i a byłoby większym od jedności dzielnikiem liczby p, a więc i liczby n, i to mniejszym od p, wbrew definicji liczby p.

Twierdzenie 2. Każda liczba złożona n ma co najmniej jeden dzielnik pierwszy $\leq \sqrt{n}$.

Dowód. Jeżeli n jest liczbą złożoną, to $n = ab$, gdzie a i b są liczby naturalne $< n$. Zmieniając ewentualnie znakowanie, możemy założyć, że $a \leq b$. Stąd $n = ab \geq a^2$, zatem $a \leq \sqrt{n}$. Ale liczba a jest $> 1$, gdyż w razie $a = 1$ byłoby $n = b$, gdy tymczasem $b < n$. W myśl twierdzenia 1 liczba a ma więc dzielnik pierwszy p oczywiście $\leq a$ , a więc $\leq \sqrt{n}$. Liczba p, jako dzielnik a liczby n , jest dzielnikiem liczby n. Liczba n ma więc dzielnik pierwszy $p \leq \sqrt{n}$. Udopwodniliśmy zatem twierdzenie 2.

**3. Ile jest liczb pierwszych?**

Aby odpowiedzieć na to pytanie, udowodnimy następujące .

Twierdzenie 3. Jeżeli n jest liczbą naturalną >2, to między n a n! leży co najamnije jedna liczba pierwsza. (n! oznacza iloczyn 1*2*3*...* n).

Doweód. Ponieważ $n > 2$, więc liczba całkowita $N = n! - 1$ jest $> 1$ i, w myśl twierdzenia 1, ma dzielnik pierwszy p, oczywiście $\leq N$, a więc $< n!$. Nie może tu być $p \leq n$, gdyż wtedy p byłoby jednym z czynników iloczynu $n! = 1 * 2 * 3 * ... * n$, a więc p byłoby dzielnikiem liczby n!, a będąc też dzielnikiem liczby N, byłoby dzielnikiem różnicy tych liczb, czyli liczby $n! - N = 1$, co

niemożliwe.
Niemożliwe. Jest więc p > n, a ponieważ już wiemy, że p <. n!, więc mamy n < p < n! i twierdzenie 3 zostało dowiedzione. Dla każdej więc liczby naturalnej istnieje liczba pierwsza od niej większa , skąd wynika, że liczb pierwszych jest nieskończenie wiele, o czym wiedział już Euklides. W szczególności wynika stąd, że istnieją liczby pierwsze, mające (w układzie dziesiętnym) co najmniej tysiąc cyfr, ale żadnej takiej liczby nie znamy. Największa znana dotąd liczba pierwsza ma 969 cyfr: jest to liczba $2^{3217}$ - 1, co do której w 1957 roku stwierdzono (za pomocą szwedzkiej maszyny elektronowej BESK), że jest pierwsza. Warto podkreślić postęp, jaki się tu dokonał w ciągu ostatniego dziesięciolecia. Na początku 1951 roku największą znaną liczbą pierwszą była liczba $2^{127}$ - 1, mająca 39 cyfr, o której już w 1914roku , udowodniono , że jest pierwszą. W zwiazku z twierdzeniem 3 zauważymy, że w r. 1850 Czebyszew udowodnił mocniejsze twierdzenie (tzw. postulat Bertranda), że dla naturalnych v > 3 między n a 2n - 2 istnieje co najmniej jedna liczba pierwsza. Wynika stąd, że w twierdzeniu 3 liczbę n! można zastąpić przez liczbę 2n. Znamy wprawdzie obecnie elementarne dowody tego twierdzenia, ale są one dosyć długie). Można też dowieść, że dla naturalnych n > 5 między n a 2n leżą co najmniej dwie liczby pierwsze. Z twierdzenia Czebyszewa wynika z łatwością, że dla każdej liczby naturalnej s istnieją co najmniej trzy liczby pierwsze mające każda s cyfr. Każda bowiem z liczb $10^{s-1}$, $2 * 10^{s-1}$, $4 * 10^{s-1}$, i $8 * 10^{s-1}$ ma s cyfr, a w myśl twierdzenia Czebyszewa dla s > 1 istnieją liczby pierwsze p, q i r takie, iż

$$10^{s-1}\ p < 2 * 10^{s-1,} < q\ <\ 4 * 10^{s-1} < r < 8 * 10^{s-1}$$

i jasnym jest, że każda z liczb p, q, r ma s cyfr. Dla s = l zaś mamy cztery liczby pierwsze jednocyfrowe: 2,3,5 i 7. Liczb pierwszych dwucyfrowych jest 21, trzycyfrowych 143. Istnieją więc co najmniej trzy liczby pierwsze, mające każda po sto cyfr. Do niedawna jednak nie znano żadnej takiej liczby pierwszej. R. M. Robinson znalazł trzy liczby pierwsze mające po sto cyfr: $81 \cdot 2^{324} + 1$, $63 \cdot 2^{326} + 1$, $35 \cdot 2^{327} + 1$. Nie znamy dotąd żadnej liczby pierwszej mającej tysiąc cyfr, chociaż wiemy, że istnieją co najmniej trzy takie liczby.

**4.Jak można wyznaczyć wszystkie liczby pierwsze, mniejsze od danej liczby?**

Sposób, o którym będzie mowa, znany był już w starożytności: nosi on nazwę sita Eratostenesa.
Przypuśćmy, że chcemy otrzymać wszystkie liczby pierwsze, nie większe od pewnej liczby naturalnej a. W tym celu wypiszemy wszystkie kolejne liczby naturalne od 1 do a i będziemy z tego ciągu wykreślali wszystkie te liczby, które nie są pierwsze, a więc przede wszystkim liczbę 1, a następnie dla każdej liczby naturalnej n > 1 wszystkie liczby większe od n i podzielne przez n. Jak łatwo widzieć, każda liczba złożona ≤ a zostanie w ten sposób wykreślona i pozostaną tylko liczby pierwsze. A więc z ciągu 1,2,3,4,... a wykreślamy liczbę 1, a następnie liczby większe niż 2 i podzielne przez 2, dalej liczby większe niż 3 i podzielne przez 3. Liczb podzielnych przez 4 nie potrzebujemy już wykreślać, gdyż zostały one wykreślone jako liczby > 2 i podzielne przez 2. ' Dalej więc wykreślamy liczby większe niż 5 i podzielne przez 5 itd. Możemy przy tym już nie wykreślać żadnej liczby > √a,gdyż jeżeli n jest liczbą złożoną ≤ a, to w myśl twierdzenia 2 liczba n ma dzielnik pierwszy p ≤ √n, zatem ≤ √a, i przeto wobec p ≤ √a liczba n została już wykreślona, gdy wykreślaliśmy liczby większe od p i podzielne przez p. Więc na przykład, chcąc otrzymać wszystkie liczby pierwsze ≤ 100 wykreślamy z ciągu 1, 2, 3, . . ., 100 liczbę 1, następnie liczby > 2 podzielne przez 2, dalej liczby > 3 i podzielne przez 3, następnie liczby > 5 i podzielne przez 5 i wreszcie liczby > 7 i podzielne przez 7 . Wszystkie pozostałe w naszym ciągu liczby będą pierwsze. Otrzymujemy w ten sposób następujący ciąg (w którym liczby wykreślone są podkrślone, zatem wszystkie nie podkreślonesą liczby są pierwsze).
1 2 3 4 5 6 7 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100
n – tą z kolei liczbę pierwszą oznaczamy przez $p_n$. Jest więc $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_{10} = 29$, $p_{25} = 97$. Łatwo byłoby obliczyć że $p_{100} = 541$. W 1909 roku wydane zostały drukiem tablice

liczb pierwszych mniejszych od dziesięciu milionów. W tablicach tych podany jest dla każdej liczby naturalnej ≤ 10 170 000, nie podzielnej przez 2,3,5 lub 7, najmniejszy jej dzielnik pierwszy : D. N. Lehmer Factor Table for the First Ten Millions, Washington, Carnegie Institution 1909. W roku 1951 wydano tablice liczb pierwszych dla 11-go miliona: J.P Kulik,L.Poletti, R. J. Porter, Liste des nombres premiers du onzieme million (plus précisément de 10 006 741 à 10 999 997), Amsterdam 1951. Nasz rodak, Jakub Filip Kulik (urodzony we Lwowie w 1793 r., zmarły w Pradze w 1863 r.), pozostawił rękopis (przechowywany w Wiedeńskiej Akademii Nauk), w którym podane są wszystkie liczby pierwsze zawarte w pierwszych stu milionach. Z tych tablic (po sprawdzeniu ich) korzystano przy sporządzaniu wydanych w 1951 r. tablic liczb pierwszych 11-go miliona. Uczeni amerykańscy zapowiadają, że wkrótce będą mieli maszynę elektronową, na której będzie zrobiona taśma zawierająca 500 milionów kolejnych liczb pierwszych (wszystkie liczby $p_n$ dla $n \leq 500\,000\,000$).

**5. Liczby pierwsze bliźniacze**

Co do ciągu nieskończonego kolejnych liczb pierwszych, czyli ciągu
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,....
nasuwa się szereg pytań. Na niektóre tylko z tych pytań łatwo jest dać odpowiedź. Więc na przykład, dwiema najmniejszymi liczbami pierwszymi są liczby 2 i 3. Są to kolejne liczby naturalne. Nasuwa się pytanie, czy są jeszcze inne kolejne liczby naturalne, które obie byłyby pierwsze. Łatwo dowieść, że liczb takich nie ma, gdyż z każdych dwóch kolejnych liczb naturalnych jedna jest parzysta i przeto, jeżeli jest > 2, to jest złożona. Istnieje natomiast dużo par kolejnych liczb nieparzystych, które są obie pierwsze, na przykład pary 3 i 5, 5 i 7, 11 i 13, 17 i 19, 29 i 31, 41 i 43. Pary takie nazywamy parami liczb bliźniaczych. Poniżej 30-tu milionów są 152 892 takie pary. Już dawno postawiono pytanie, czy par liczb pierwszych bliźniaczych jest nieskończenie wiele. Na pytanie to nie znamy odpowiedzi. Nie wiemy więc, czy liczba 2 daje się na nieskończenie wiele sposobów przedstawić jako różnica, dwóch liczb pierwszych. Wyrażono przypuszczenie, że każda liczba parzysta daje się na nieskończenie wiele sposobów przedstawić jako różnica dwóch kolejnych liczb pierwszych. Nie potrafimy dowieść nawet tego, że każda liczba parzysta daje się choćby w jeden sposób przedstawić jako różnica dwóch kolejnych liczb pierwszych, co sprawdzono dla wielu kolejnych liczb parzystych, na przykład 2 = 5 - 3, 4 = 11 - 7, 6 = 29 - 23, 8 = 97 - 89, 10 = 149 - 139, 12 = 211 - 199, 14 = 127-113; 16 = 1847 - 1831,18 = 541 - 523,20 = 907 - 887. Nie potrafiy nawet dowieść, że każda liczba parzysta jest różnicą dwóch liczb pierwszych (choćby niekolejnych). Natomiast potrafimy znaleźć wszystkie liczby nieparzyste będące różnicami dwóch liczb pierwszych. Jeżeli bowiem liczba naturalna nieparzysta n jest różnicą dwóch liczb pierwszych, n = p- q, to jedna z tych liczb pierwszych musi być parzysta, a druga jest nieparzysta, zatem jedna z liczb p i q, jak łatwo widzieć, liczba q,musi być równa 2. Jest więc n = p - 2, gdzie p jest liczbą pierwszą nieparzystą Tak więc wszystkimi liczbami naturalnymi nieparzystymi które są różnicami dwóch liczb pierwszych, są liczby o 2 mniejsze od liczb pierwszych nieparzystych, zatem liczby 1, 3, 5, 9, 11, 15, ... Liczb takich jest więc nieskończenie wiele. Ale jest też nieskończenie wiele liczb nieparzystych, które nie są różnicami dwóch liczb pierwszych, na przykład wszystkie liczby postaci 6k+1, gdzie k jest liczbą naturalną. Nie może tu bowiem być 6k+1 = p - 2, gdzie p jest liczbą pierwszą, gdyż wtedy byłoby p = 6k + 3 = 3(2k+1), a więc p byłoby liczbą złożoną.

**6.Przypuszczenie GOLDBACHA**

W 1742 r. Ch. Goldbach wypowiedział przypuszczenie, że każda liczba parzysta > 2 jest sumą dwóch liczb pierwszych. Przypuszczenie to nie zostało dotąd udowodnione ani też obalone. Zostało ono sprawdzon dla wszystkich liczb parzystych aż do 100 000. Wyrażono też, mocniejsze przypuszczenie, mianowicie, że każda liczba parzysta, > 6 jest sumą dwóch różnych liczb pierwszych,co S.Gołaszewski sprawdził dla liczb ≤ 50 000. Można dowieść, że to ostatnie przypuszczenie jest równoważne, |że każda, naturalna >17 jest sumą trzech różnych liczb pierwszych. Natomiast A. Schinzel dowiódł, że z przypuszczenia Goldbacha wynika, iż każda liczba nieparzysta > 17 jest sumą trzech różnych liczb pierwszych. Z Goldbacha wynika z łatwością, że każda liczba nieparzysta > 7 jest sumą trzech liczb pierwszych nieparzystych. Jeśli

bowiem n jest liczbą naturalną i 2n + 1 > 7, to 2n + 1 – 3 = 2(n-1) . Liczba; parzysta 2(n - 1) > 4 jest, w myśl przypuszczenia Goldbacha, sumą dwóch liczb pierwszych p + q, które nie mogą być parzyste, gdyż liczba nasza jest > 4. Liczby pierwsze p i q są więc nieparzyste i liczba 2n+1 = 3 + p + q jest sumą trzech liczb pierwszych nieparzystych. Czy każda liczba nieparzysta > 7 jest sumą trzech liczb pierwszych nieparzystych, tego nie wiemy, ale w 1937 r. I. Winogradow dowiódł, że każda dostatecznie wielka liczba nieparzysta jest sumą trzech liczb pierwszych nieparzystych. Znamy nawet taką liczbę a, że każda liczba nieparzysta > a jest sumą trzech liczb pierwszych nieparzystych,

$$a = 3^{3^{16}}$$

Można więc powiedzieć, że rozstrzygnięciu pytania, czy każda liczba nieparzysta > 7 jest sumą trzech liczb pierwszych nieparzystych, stoi na przeszkodzie tylko długość potrzebnych na to rachunków, gdyż wystarczyłoby tu zbadać tylko liczby nieparzyste > 7 oraz ≤ a, a dla każdej danej liczby nieparzystej można za pomocą skończonej liczby prostych działań arytmetycznych rozstrzygnąć, czy jest, czy też nie jest sumą trzech liczb pierwszych nieparzystych. Inaczej jest z przypuszczeniem Goldbacha: tu nie możemy powiedzieć, że rozstrzygnięciu pytania, czy przypuszczenie to jest prawdziwe, czy nie, stoi na przeszkodzie jedynie długość potrzebnych na to rachunków. Udowodniono, że każda liczba naturalna > 1 jest sumą dwudziestu lub mniej liczb pierwszych. Udowodniono, że każda liczba naturalna > 11 jest sumą dwóch lub więcej różnych liczb pierwszych. Na przykład 12 = 5 + 7, 13 = 2 + 11, 17 = 2 + 3 + 5 + 7, 29 == 3 + 7 + 19. A. Mąkowski zaś dowiódł, że każda liczba naturalna > 55 jest sumą różnych liczb pierwszych postaci 4k+3, oraz udowodnił trzy analogiczne twierdzenia o sumach liczb pierwszych każdej z postaci 4k + 1, 6k+1 i 6k + 5. Z przypuszczenia Goldbacha wynika z łatwością, że każda liczba całkowita nieparzysta (dodatnia lub ujemna) może być na nieskończenie wiele sposobów przedstawiona w postaci p + q - r, gdzie p, q i r są liczbami pierwszymi nieparzystymi. Istotnie, dla każdej liczby całkowitej k istnieje liczba pierwsza nieparzysta r taka, że 2k - 1 + r > 4 (wystarczy wziąć jako r dostatecznie dużą liczbę pierwszą). Lecz wtedy 2k - 1 + r jest liczbą parzystą > 4, a więc, w myśl przypuszczenia Goldbacha, 2k-1+r = p+q, gdzie p i q są liczby pierwsze nieparzyste. Stąd 2k-1= p + q - r, przy czym liczba pierwsza r może być dowolnie wielka. Stąd wniosek, o którym mowa. Ciekwaym jest, że wniosek ten został w 1923 r. udowodniony przez J.G. van der Corputa. Dowód jest jednak trudny. W związku z przypuszczeniem Goldbacha zauważymy, że łatwo jest dowieść, iż każda liczba naturalna > 11 jest sumą dwóch liczb zło.żonych .Jeżeli bowiem n > 11 jest liczbą parzystą, to n - 4 jest liczbą parzystą > 2, zatem liczbą złożoną i n jest sumą dwóch liczb złożonych: 4 i n - 4. Jeżeli zaś n > 11 jest liczbą nieparzystą, to n-9 jest liczbą parzystą > 2, zatem złożoną i n jest sumą dwóch liczb złożonych: 9 i n - 9. Nie należy stąd jednak wyprowadzać wniosku, że badanie liczb złożonych jest łatwiejsze niż badanie liczb pierwszych. Nie potrafimy na przykład dać odpowiedzi na pytanie, czy wśród liczb

$$F_n = 2^{2^n} + 1$$

gdzie n = 1,2,3, ..., mamy nieskończenier wiele złożonych (dotąd znamy tylko 35 takich liczb złożonych, z których największą jest liczba $F_{1945}$). G.H. Hardy i J. E. Littlewood wypowiedzieli przypuszczenie (dotąd nie udowodnione), że każda dostatecznie wielka liczba naturlana nie będąca kwadratem, jest sumą kwadratu liczby całkowitej oraz liczby pierwszej, natomiast J. W. Linnik dowiódł w 1959r., że każda dostatecznie wielka liczba naturalna jest sumą dwóch kwadratów liczb całkowitych oraz liczby pierwszejW związku z przypuszczeniem Hardy'ego i Littlewooda zauważmy ,że łatwo jest dowieść, iż istnieje nieskończenie wiele kwadratów liczb naturalnych, które są, jak również takich, które nie są sumą kwadratu liczby całkowitej oraz liczby pierwszej. Z jednej bowiem strony, jeżeli p jest liczbą pierwszą nieparzystą, to p+1/2 jest liczbą naturalną I mamy:

$$(p+1/2)^2 = (p-1/2)^2 + p$$

z drugiej zaś strony, jeżeli n = 3k + 2, gdzie k jest liczbą naturalną to nie może być przy całkowitym

nieujemnym x i pierwszym p : $n^2 = x^2 + p$

gdyż byłoby wtedy n > x oraz

$$p = n^2 - x^2 = (n — x)(n + x),$$

skąd, z uwagi na to, że p jest liczbą pierwszą: n - x = 1 n + x = p, zatem

$$p = 2n - 1 = 3(2k + 1),$$

co przy naturalnym k jest niemożliwe.

**7. Przypuszczenie GILBREATHA**

N. L. Gilbreath wyraził (w 1958 r.) następujące przypuszczenie. Jeżeli wypiszemy ciąg kolejnych liczb pierwszych, pod nim, w pierwszym wierszu, ciąg różnic kolejnych liczb pierwszych, w drugim wierszu ciąg bezwzględnych wartości różnic kolejnych wyrazów pierwszego wiersza, w trzecim wierszu ciąg bezwzględnych wartości różnic kolejnych wyrazów drugiego wiersza itd., to w każdym wierszu pierwszym wyrazem będzie 1.

Przypuszczenie Gilbreatha zostało sprawdzone dla pierwszych 63 418 wierszy. Ogólnego dowodu jego prawdziwości jednak prawdziwości jednak nie znaleziono. Oznaczmy dla, naturalnych n, przez $a_n$ najmniejszą liczbę naturalną, taką ,że $a_n$+1-wszy wyraz n-go wiersza jest pierwszym wyrazem tego wiersza, będącym > 2.

Więc na przykład $a_1 = 3$, $a_2 = 8$, $a_3 = 14$. Obliczono, że $a_4 = 14$, $a_5 = 25$, $a_6 = 24$, $a_7 = 23$, $a_8 = 22$, $a_9 = 25$, $a_{10} = 59$, $a_{14} = 97$, $a_{15} = 174$, $a_{22} = 280$, $a_{23} = 740$, $a_{24} = 874$, $a_{34} = 866$, $a_{35} = 2180$, $a_{64} = 5940$, $a_{65} = 23266$, $a_{94} = 31533$. Gdyby można było dowieść, że $a_n > 2$ dla naturalnych n, to stąd wynikałaby z łatwością prawdziwość przypuszczenia Gilbreatha.

**8.Rozkład liczby naturalnej na czynniki pierwsze**

Opierając się na twierdzeniu 1 udowodnimy teraz

Twierdzenie 4. Każda liczba naturalna >1 jest iloczynem, którego czynnik jest liczbą pierwszą. Nie wyłączamy tu iloczynów mających jeden tylko czynnik.

Dowód. Niech n będzie daną liczbą naturalną > 1. W myśl twierdzenia 1 liczba n ma (co najmniej jeden) dzielnik pierwszy p' I możemy założyć, że p' jest najmniejszym dzielnikiem pierwszym liczby n Mamy więc n = p'n', gdzie n' jest liczbą naturalną. Jeżeli n' = 1, to n = p' i n jest iloczynem utworzonym z jednego tylko czynnika pierwszego. Jeżeli zaś n' > 1, to n' ma dzielnik pierwszy p", o którym możemy założyć, że jest najmniejszym dzielnikiem pierwszym liczby n'. Jest to zarazem dzielnik pierwszy liczby n i zdefinicji liczby p' wynika, że musi być p' ≤ p". Mamy więc n' = p"n" i albo n" = 1 i wtedy n' jest iloczynem liczb pierwszych p' i p" (niekoniecznie różnych), albo też n" > 1 i z liczbą n" możemy postąpić jak przedtem z liczbami n i n' " itd.. Wobec n = p'n' oraz p' > 1 mamy n' < n. Podobnie znajdujemy n" , n' itd. Liczby naturalne n, n', n", ... tworzą więc ciąg malejcy który nie może zawierać więcej niż n wyrazów. Zatem przy pewnym naturlanym k będzie $n^{(k)}$ wyrazem ostatnim tego ciągu, to znaczy będzie $n^{(k)} = 1$, gdyż w razie $n^{(k)} > 1$ moglibyśmy położyć

$$n^{(k)} = p^{(k+1)}\, n^{(k+1)}$$

i otrzymalibyśmy dalszy wyraz $n^{(k+1)}$ naszego ciągu. Mamy więc n = p'n', n' = p"n", ...,$n^{(k-1)} = p^{(k)}\, n^{(k)}$ oraz $n^{(k)} = 1$, skąd znajdujemy

1) $$n = p'p"p"'. . .p^{(k)},$$

gdzie p', p", ..., $p^{(k)}$ są liczby pierwsze i możemy założyć, żo p' ≤ p"≤ p"' ≤ .. .≤ $p^{(k)}$ (o ile dla każdej z liczb n, n', :.. będziemy wyznaczali jej najmniejszy dzielnik pierwszy).

Wśród czynników iloczynu (1) mogą być równe. Jeżeli będziemy wypisywali równe czynniki jako potęgę jednego z nich z odpowiednim naturalnym wykładnikiem, to ze wzoru (1) otrzymamy wzór

2) $$n = q_1^{a1} q_2^{a2} ... q_s^{as},$$

gdzie s jest liczbą naturalną, $q_1$ $q_2$, ..., $q_s$ są liczby pierwsze ros nące, zaś $a_1$ $a_2$, ..., $a_s$ wykładniki naturalne. Wzór (2) nazywamy rozwinięciem kanonicznym liczby n na czynniki pierwsze.

Nie tylko więc udowodniliśmy twierdzenie 4, ale nadto podaliśmy też sposób znalezienia dla każdej liczby naturalnej n > 1 jej rozwinięcia kanonicznego na czynniki pierwsze. Znalezienie tego rozwinięcia jest więc, dla każdej danej liczby naturalnej n > 1, teoretycznie zawsze możliwe, ale praktycznie może nastręczać duże trudności z powodu długości potrzebnych rachunków. Dla

niektórych liczb rachunki te są tak długie, że obecnie, nawet przy użyciu największych maszyn do liczenia, nie mamy możności ich wykonania. Nie znamy na przykład rozwinięcia na czynniki pierwsze liczby $2^{101} - 1$ (mającej 31 cyfr); dowiedziono tylko, że jest iloczynem dwóch różnych czynników pierwszych, z których mniejszy (nie znany zresztą dotąd) ma co najmniej 11 cyfr. Nie znamy też rozwinięcia na czynniki pierwsze liczby

$$F_{13} = 2^{2^{13}} + 1$$

, o której nie wiemy, czy jest pierwszą, czy nie. Natomiast dla liczby

$$F_{1945} = 2^{2^{1945}} + 1$$

, która mu więcej niż $10^{582}$ cyfr (gdyż $2^{1945} = 32 * 2^{1940} = 32 \cdot (2^{10})^{194} > 30(10^3)^{194} = 3 * 10^{583}$ , skąd

$$F_{1945} > 2^{3*10^{583}} > (2^{10})^{10^{583}} > 10^{3*10^{583}})$$

a więc której wszystkich cyfr nie jesteśmy w możności wypisać, znaleziono przed kilku laty najmniejszy dzielnik pierwszy, którym jest liczba $5*2^{1947}$ mająca 587 cyfr. Nie znamy natomiast innych dzielników pierwszych liczby $F_{1945}$ ani też jej rozkładu na czynniki pierwsze. Co do rozkładu (2) liczby $n > 1$ na czynniki pierwsze, to nasuwa się pytanie, czy taki rozkład jest tylko jeden (jeżeli liczby $q_1, q_2, .., qs$ tworzą ciąg rosnący). Dowód jednoznaczności rozkładu oprzemy na kilku prostych twierdzeniach o liczbach pierwszych.

Twierdzenie 5. Liczba pierwsza p ma tylko dwa dzielniki naturalne : 1 i p

Dowód.Gdyby liczba p miała jeszcze inny dzielnik a poza 1 i p, to musiałoby oczywiście być $1 < a < p$ oraz $p = a * b$, gdzie b jest liczbą naturalną > 1, gdyż w razie b=1 byłoby p = a, wbrew założeniu co do liczby a. Liczba p byłaby więc iloczynem dwóch liczb natrualnych większych od jedności, wbrew założeniu, że p jest liczbą pierwszą. Udowodniliśmy więc twierdzenie 5. Jak łatwo widzieć, zachodzi też twierdzenie, że jeżeli liczba naturalna p ma dokładnie dwa dzielniki naturalne, to jest liczbą pierwszą. Wtedy bowiem musi być $p > 1$ i gdyby p nie było liczbą pierwszą, byłoby p iloczynem dwóch liczb naturalnych większych od jedności, a i b i, wobec $p = a * b$ oraz $b > 1$, byłoby $1 < a < p$ I a byłoby dzielnikiem liczby p różnym od 1 i p, a więc liczba p miałaby co najmniej trzy różne dzielniki naturalne. Mamy więc też

Twierdzenie 6. Na to, żeby liczba naturalna była pierwszą, potrzeba i wystarcza, żeby miała dokładnie dwa różne dzielniki naturalne (oczywiście jedność i samą siebie).

Udowodnimy teraz

Twierdzenie 7. Jeżeli a i b są liczby naturalne i iloczyn ab jest podzielny przez liczbę pierwszą p, to jedna co najmniej z liczb a i b jest podzielna przez p.

Dowód. Gdyby twierdzenie 7 nie było prawdziwe, istniałaby najmniejsza liczba pierwsza p, dla której nie jest ono prawdziwe, a dla takiej liczby pierwszej p istniałby najmniejszy iloczyn ab dwóch liczb naturalnych a i b podzielny przez p, mimo że żaden z czynników a i b nie jest podzielny przez p. Okażemy, że wówczas liczby a i b są mniejsze od p. W samej rzeczy, gdyby na przykład było $a > p$, mielibyśmy $a = kp + a_1$, gdzie $a_1 < p$ i $a_1 > 0$, gdyż a nie jest podzielne przez p. Stąd $ab = (kp + a_1)b = kpb + a_1b$, a ponieważ ab oraz kpb są podzielne przez p, więc $a_1$ jest podzielne przez p. Lecz $a_1 < p <$ a i $a_1$ nie jest podzielne przez p, przy czym $a_1b < ab$ - co przeczy założeniu co do iloczynu ab. Jest więc $a < p$ i podobnie dowodzimy, że $b < p$, skąd $ab < p^2$. Skoro ab jest podzielne przez p, więc mamy $ab = lp$, gdzie l jest liczbą naturalną, większą od 1, gdyż inaczej byłoby $p = ab$, gdzie $a > 1$ i $b > 1$ (gdyż liczby a i b nie są podzielne przez p). Z drugiej strony wobec $ab < p^2$ mamy $l < p$. Liczba l, jako naturalna > 1, ma dzielnik pierwszy $q \leq l < p$. Wobec $q < p$ i definicji liczby p, skoro iloczyn ab, jako podzielny przez l, jest podzielny przez liczbę pierwszą $q < p$, więc jeden co najmniej z czynników a i b musi być podzielny przez q. Jeżeli na przykład a jest podzielne przez q, to $a = a'q$. Lecz l jest podzielne przez q, zatem $l = tq$, gdzie t jest liczbą naturalną. Wobec $ab = lp$ mamy więc $a'qb = tqp$, skąd $a'b = tp$, przy czym, wobec $a = a'q$, mamy $a' < a$, skąd $a'b < ab$ - wbrew założeniu co do iloczynu ab. Założenie, że twierdzenie 7 nie

jest prawdziwe, doprowadza więc do sprzeczności. Z dowiedzionego twierdzenia wynika łatwo przez indukcję następujący

Wniosek. Jeżeli $a_1,a_2,...,a_m$ jest ciągiem skończonym liczb naturalnych, których iloczyn jest podzielny przez liczbę pierwszą p, to jedna co najmniej z liczb $a_1,a_2,...,a_m$ musi być podzielna przez p.

Dowód. Wniosek jest prawdziwy dla m = 2. Przypuśćmy, że jest prawdziwy dla m liczb i niech $a_1,a_2,...,a_m,a_{m+1}$ będą m + 1 liczbami naturalnymi. Jeżeli iloczyn $a_1a_2,...,a_ma_{m+1}$ jest podzielny przez liczbę pierwszą p, to, w myśl twierdzenia 7, jedna co najmniej z dwóch liczb $a_1a_2,...,a_m$ i $a_{m+1}$ jest podzielna przez p. Jeżeli liczba $a_1a_2,...,a_m$, jest podzielna przez p, to, wobec założenia, że wniosek jest prawdziwy dla m liczb, wnosimy, że jedna co najmniej z liczb $a_1a_2,...,a_m$ jest podzielna przez p. Z prawdziwości wniosku dla m liczb wynika więc jego prawdziwość dla m + 1 liczb.

Przypuśćmy teraz, że istnieją liczby naturalne, które mają dwa różne rozwinięcia kanoniczne na czynniki pierwsze. Wśród takich liczb naturalnych istnieje oczywiście liczba najmniejsza. Niech to będzie liczba n, dająca prócz rozwinięcia kanonicznego

(2) $n = q_1^{a1}q_2^{a2}...q_s^{as}$ ,

jeszcze rozwinięcie

(3) $n = r_1^{b1}r_2^{b2}...r_t^{bt}$ ,

gdzie $r_1,r_2...$, $r_t$ jest ciągiem rosnącym liczb pierwszych, zaś $b_1,b_2...,b_t$ są liczby naturalne. Wobec (2) liczba n jest podzielna przez $q_1$ a więc wobec (3) i w myśl wniosku z twierdzenia 5, jedna co najmniej z liczb $r_1,r_2...$, $r_t$ musi być podzielna przez $q_1$, oczywiście liczba $r_1$, gdyż $q_1$ jest najmniejszym dzielnikiem pierwszym liczby (3). Lecz w myśl twierdzenia 5, liczba pierwsza $r_1$ ma tylko dwa dzielniki naturalne: 1 i $r_1$, skoro zaś liczba pierwsza $q_1$ jest też dzielnikiem liczby $r_1$, to musi być $r_1 = q_1$. Wstawiając do wzoru (3) $q_1$ zamiast $r_1$ otrzymujemy, wobec (2) dla liczby naturalnej n', gdzie $n = q_1n'$, równość

$$n' = q_1^{a1-1}q_2^{a2}....q_s^{as} = q_1^{b1-1}r_{2b2}....r_t^{bt} ,$$

Ponieważ liczba n' jest mniejsza niż n, więc, wobec założenia co do liczby n, liczba n' ma tylko jedno rozwinięcie kanoniczne na czynniki pierwsze, skąd z łatwością wynika, że musi być $s = t$, $r_2 = q_2$ , $r_3 = q_3$, $….r_s = q_s$, $a_1 = b_1$ , $a_2 = b_2$, … $a_s = b_s$ . Rozwinięcia (2) i (3) byłyby więc identyczne, wbrew założeniu. Założenie ,że istnieją liczby naturalne mające dwa różne rozwinięcia kanoniczne na czynniki pierwsze, doprowadza więc do sprzeczności.

Udowodniliśmy więc

Twiedzenie 8. Każda liczba naturalna n > 1 daje tylko jedno rozwinięcie na czynniki pierwsze, jeżeli nie zwracamy uwagi na porządek czynników

**9.Jakie cyfry mogą być na początku i na końcu liczb pierwszych?**

Ostatnia cyfra liczby pierwszej, mającej więcej niż jedną cyfrę, nie może być parzystą,, gdyż wtedy liczba byłaby >2 oraz parzysta, a więc złożona; nie może też ostatnią cyfrą być 5, gdyż wtedy liczba byłaby > 5 i podzielna przez 5, a więc złożona. Tak więc ostatnią cyfrą liczby pierwszej > 10 może być tylko 1, 3, 7 lub 9. Nasuwa się pytanie, czy możemy coś więcej powiedzieć o cyfrach liczb pierwszych większych od 10, na przykład o zespołach kilku ostatnich lub kilku pierwszych cyfr liczb pierwszych. Okazuje się, że więcej nic tu powiedzieć nie można, gdyż zachodzi następujące twierdzenie:

Jeżeli mamy dwa dowolne ciągi skończone cyfr (układu dziesiętnego) $a_1$, $a_2,...$, $a_m$ oraz $b_1$, $b_2,...$, $b_n$, gdzie $b_n$ =1, 3, 7 lub 9, to istnieje dowolnie wielka liczba pierwsza p, której m pierwszymi cyframi są kolejno $a_1$, $a_2,...$, $a_m$, zaś n ostatnimi cyframi są kolejno $b_1$, $b_2,...$, $b_n$

.Dowód tego twierdzenia jest trudny, chociaż może być przeprowadzony elementarnie .

W szczególności z twierdzenia tego wynika, że istnieją liczby pierwsze, mające na początku i na końcu dowolnie wielką liczbę cyfr równych 1 (ale być może - w środku też inne cyfry niż 1).

W związku z tym nasuwa się pytanie, czy istnieje nieskończenie wiele liczb pierwszych, których

wszystkie cyfry są jedynkami. Odpowiedzi na to pytanie nie znamy. Znamy zaledwie kilka liczb pierwszych, których wszystkie cyfry są równe 1, na przykład 11 i 11111111111111111111111 $=10^{23} - 1/9$ .Dowód (który podał M. Kraitchik), że ta ostatnia liczba jest pierwszą, nie jest łatwy. Łatwo natomiast jest dowieść, że jeżeli liczba, której wszystkie cyfry są jedynkami, jest pierwszą, to liczba jej cyfr musi być pierwszą. Warunek ten nie jest jednak wystarczający, gdyż na przykład 111 = 3*37, 11111 = 41*271, 1111111 = 239*4649.
Również liczba $10^{37} - 1 /9$ ,mająca 37 cyfr, jest złożona. Szukano też innych, niż utworzone z samych cyfr 1, liczb pierwszych, które pozostają pierwszymi przy każdej permutacji ich cyfr. Z liczb dwucyfrowych są to liczby 13 i 31, 17 i 71, 37 i 73, 79 i 97, z liczb zaś trzycyfrowych są to liczby 113, 131, 311; 199, 919, 991; 373, 373, 733. Nie znamy innych i nie wiemy, czy jest ich liczba skończona. Nie winny też, czy istnieje nieskończenie wiele liczb pierwszych, któych pierwsza i ostatnia cyfra są = 1, zaś pozostałe są = 0, jak na przykład liczba 101. Łatwo dowieść, że takie liczby pierwsze muszą być postaci

$$10^{2^n} + 1$$

gdzie n jest liczbą naturalną, ale warunek ten nie jest wystarczający, gdyż na przykład

$$10^{2^2} + 1 = 73 * 137$$

**10.Liczba liczb pierwszych, nie większych od danej liczby**
Dla danej liczby x oznaczamy przez $\pi(x)$ liczbę liczb pierwszych nie większych od x. Mamy więc na przykład $\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(4) = 2$, $\pi(5) = 3$, $\pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$, $\pi(10000) = 1229$, $\pi(10^8) = 5761455$, $\pi(10^9) = 50847534$, $\pi(10^{10}) = 455052512$
L.Locher -Ernst zauważył, że dla $n > 50$ wyrażenie

$$f(n) = \frac{n}{\frac{1}{3} + \frac{1}{4} + \frac{1}{5} + ..... + \frac{1}{n}}$$

daje dość dobrze przybliżoną wartość liczby $\pi(n)$. Na przykład $\pi(10^3) = 168$, zaś $f(10^3) = 167{,}1$. Dla $n = 10^9$ iloraz $\pi(n) : f(n)$ wynosi 1,007, zaś dla $n = 10^{10}$ wynosi on 1,005. Można też dowieść elementarnie, chociaż dowód jest długi i skomplikowany, że stosunek $\pi(n) : f(n)$ zmierza do jedności, gdy n wzrasta niograniczenie. Dla wielkich n wyrażenie f(n) trudne jest do obliczenia. Znane są natomiast inne wyrażenia przybliżone dla liczby $\pi(n)$, na przykład wyrażenie n
gdzie lg n oznacza logarytm naturalny liczby n (tj logarytm przy zasadzie e). J. Hadamard i Ch. de la Vallée Poussin dowiedli w 1896 r., że stosunek $\pi(n)$ do n/ lg n zmierza do jedności gdy n wzrasta nieograniczenie. Można dowieść, że miliardowa liczba pierwsza (tj. liczba $p_{109}$) ma 11 cyfr.
Łatwo jest dowieść, że dla naturalnych $n > 1$ mamy $\pi(n -1)/n-1 < \pi(n)/n$, gdy n jest liczbą pierwszą,zaś $\pi(n -1)/n-1 > \pi(n)/n$ liczbą złożoną. Można dowieść, że stosunek $\pi(n)$ do n zmierza do zera, gdy n wzrasta nieograniczenie. Jasnym jest, że$\pi(p_n) = n$ dla naturalnych n. Łatwo jest dowieść, że istnieją dowolnie długie ciągi kolejnych liczb naturalnych, nie zawierające żadnej liczby pierwszej. Ciągiem m kolejnych takich liczb jest na przykład ciąg
(m + 1)! + 2, (m + 1)! + 3, (m + 1)! + 4, ...,(m+ 1)! + (m + 1),
gdyż pierwsza z liczb tego ciągu jest podzielna przez 2, druga przez .3 itd., ostatnia przez m + 1, a więc wszystkie są złożone.
Dla m = 100 byłyby to olbrzymie liczby, ale już między liczbami pierwszymi 370261 a 370373 leży 111 kolejnych liczb złożonych. W setce kolejnych liczb od 1671800 do 1671900 nie ma żadnej liczby pierwszej. Trudniej byłoby dowieść, że istnieją liczby pierwsze, które z obu stron są otoczone dowolnie wielką liczbą liczb złożonych, to znaczy, że dla każdej liczby naturalnej m istnieje liczba pierwsza p taka, że każda z liczb p - k oraz p + k, gdzie k = 1,2, ..., m, jest złożoną.
Trudnym jest też dowód twierdzenia E. Landau'a, że dla dostatecznie wielkich liczb naturalnych n mamy $\pi(2n) < 2\pi(n)$, czyli twierdzenia, że dla takich n jest liczb pierwszych $\leq$ n więcej, niż liczb

pierwszych leżących między n a 2n. Nie wiemy, czy dla wszelkich liczb naturalnych x > 1 i y > 1 mamy $\pi(x+y) \leq \pi(x)+\pi(y)$

**11. Pewne własności n-tej z kolei liczby pierwszej**

Niełatwym jest dowód twierdzenia H. J. Scherka (podanego przez niego w 1830 r.), że dla naturalnych p mamy przy odpowiednim obiorze znaków + lub - wzory

$$p_{2n} = 1 \pm p_1 \pm p_2 \pm ... \pm p_{2n-2} + p_{2n-1}$$

$$p_{2n+1} = 1 \pm p_1 \pm p_2 + ....+p_{2n-1}+2p_{2n}$$

Więc na przykład $p_6 = 1+p_1- p_2 – p_3 + p_4 +p_5$

$$p_7 = 1 + p_1 – p_2 – p_3 + p_4 - p_5 + 2p_6$$

czyli 13 = 1 + 2 -3 -5 + 7 + 11, 17 = 1 + 2 – 3 – 5 +7 – 11 +2*13

Można też dowieść, że dla naturalnych n przy odpowiednim obiorze znaków + lub - mamy

$p_{2n+1} = \pm p_1 \pm p_2 \pm ... \pm p_{2n-1} + p_{2n}$

Na przykład $p_7 = p_1 + p_2 - p_3 - p_4 + p_5 + p_6$, czyli 17 = 2 + 3 - 5 - 7 + 11 + 13.

A. Schinzel dowiódł, że jeżeli a i b są, dwie liczby dodatnie, to istnieją liczby pierwsze p i q takie, iż a < p/q < b. Można dowieść, że dla każdej liczby rzeczywistej dodatniej x , ciąg $P\pi(nx)/n$ zmierza do x, gdy n wzrasta nieograniczenie. Udowodniono, że istnieje nieskończenie wiele liczb pierwszych pyakichi, że następna po p liczba pierwsza jest bliższa do p niż poprzedzająca p liczba pierwsza, a także że istnieje nieskończenie wiele liczb pierwszych p takich, że poprzedzająca p liczba pierwsza jest bliższa, do p niż następująca po p liczba pierwsza. Innymi słowy - udowodniono, że istnieje nieskończenie wiele liczb naturalnych n takich ,że

$$p_{n+1} – p_n < p_n – p_{n-1,} \text{ czyli } p_n > p_{n-1} + p_{n+1} / 2$$

a także istnieje nieskończenie wiele liczb naturalnych n takich, że

$$p_n < p_{n-1} + p_{n+1} / 2$$

Nie wiemy natomiast, czy istnieje nieskończenie wiele takich n, dla których

$$p_n = p_{n-1} + p_{n+1} / 2$$

Wyrażono przypuszczenie, że odpowiedź na to pytanie jest twierdząca. Mamy na przykład

$p_n = p_{n-1} + p_{n+1} / 2$ dla n = 16, 37, 40, 47, 55, 56, 240, 273.

P.Erdós i P. Turan dowiedli też, że istnieje nieskończenie wiele liczb naturlanych n takich, iż $p_n^2 > p_{n-1}p_{n+1}$ oraz nieskończenie wiele takich, iż$p_n^2 > p_{n-1}p_{n+1}$ Udowodniono też, że $p_{n+1} < p_{n-1} + p_n$ dla n = 3, 4, 5, .. . Dla kolejnych liczb pierwszych zachodzi też następujące twierdzenie (którego dowód nie jest trudny, ale dosyć długi):

Dla każdej liczby naturalnej m istnieje liczba naturalna n taka, iż

$$1/p_1 + 1/p_2+...+1/p_n > m$$

Ale już dla m = 10 wyniosłoby n kilkadziesiąt tysięcy. Istnieją czwórki kolejnych liczb pierwszych, dające dwie pary liczb bliźniaczych, na przykład 11, 13, 17, 19 lub 179, 181, 191, 193. Jeżeli taką czwórkę tworzą liczby pierwsze p, p + 2, p + 6 i p + 8, to mówimy, że mamy czworaczki. Pierwsza z podanych tu przez nas czwórek daje czworaczki, druga nie. Inne przykłady czworaczków otrzymujemy dla p =5, 101, 191, 821, 1481, 3251. Wyrażono przypuszczenie, że czworaczków jest nieskończenie wiele. W. A. Gołubiew obliczył w 1959 r., że w pierwszych dziesięciu milionach mamy 899 czworaczków, w pierwszych zaś piętnastu milionach mamy ich 1209. Największe znane dotąd czworaczki, jak podaje A. Ferrier, otrzymujemy dla p = 2 863 308 731.

**12. Wielomiany a liczby pierwsze**

Nasuwa się pytanie, czy istnieje wielomian f(x) zmiennej x o całkowitych współczynnikach, który dla każdej wartości naturalnej x daje liczbę pierwszą f(x). Okażemy, że wielomianu takiego nie ma. Niech

$$f(x) = a_0x^m + a_1x^{m-l} + ... + a_{m-1}x + a_m$$

będzie wielomianem stopnia naturalnego m o całkowitych współczynnikach $a_0, a_1, ..., a_m$, gdzie $a_0 \neq 0$. Gdyby było $a_0 < 0$, to dla dostatecznie wielkich x byłoby f(x) < 0: założymy więc, że $a_0 > 0$. Wówczas, jak wiadomo, istnieje taka liczba całkowita $x_0$, że

$$n = f(x_0) > 1 \text{ oraz że } f(x) > f(x_0) \text{ dla } x > x_0.$$

Okażemy, że przy dowolnym naturalnym k liczba $f(x_0 + kn)$ będzie złożoną. Jeżeli bowiem x i h są

liczby naturalne, to przy wszelkim naturalnym i liczba $(x + h)_i - x_i$ jest podzielna przez $(x + h) - x = h$, skąd wnosimy, że liczby $a_i(x + h)^i — a_i x^i$ dla i = 0, 1, 2, .. ., m są podzielne przez h, zatem też liczba f(x + h) - f(x) jest podzielna przez h. Wynika stąd, że liczba $f(x_0 + kn) - f(x_0)$ jest podzielna przez kn, czyli $f(x_0 + kn) - n = tn$, co dajef$(x_0 + kn) = (t + 1 )n$ i dowodzi, że liczba f(x0 + kn), która, jak wiemy, jest > $f(x_0) = n$, jest podzielna przez liczbę naturalną n > 1, zatem jest złożoną, c.b.d.o.

Dowiedliśmy więc, że jeżeli f(x) jest wielomianem o współczynnikach całkowitych, gdzie współczynnik przy najwyższej potędze x jest dodatni, to dla nieskończenie wielu liczb naturalnych x liczba f(x) jest złożoną.

Znamy natomiast wielomiany, które dla wielu kolejnych liczb naturalnych przybierają wartości będące liczbami pierwszymi. Takim jest na przykład wielomian Eulera $x^2 + x + 41$, który dla x = 0,1,2, ..., 39 daje różne liczby pierwsze. Wyrażono przypuszczenie, że istnieje nieskończenie wiele liczb naturalnych x, dla któych $x^2 + x + 41$ jest liczbą pierwszą. Nie wiemy, czy istnieje taka liczba naturalna a > 41, żeby każda z liczb $x^2 + x + a$ dla x = 0, 1, 2, ..., a - 2 była pierwszą. W każdym razie nie ma takich liczb $a \leq 10^9$.

Wielomian $x^2 - 79x + 1601$ daje liczby pierwsze dla x = 0, 1, ..., 79, ale nie wszystkie różne.

Nasuwa się teraz pytanie, czy istnieją wielomiany, które dla naturalnych wartości zmiennej dają nieskończenie wiele liczb pierwszych. Oczywiście istnieją takie wielomiany pierwszego stopnia, na przykład wielomian 2x + 1. Ale nie znamy żadnego wielomianu stopnia > l,o którym potrafilibyśmy dowieść, że daje nieskończenie wiele liczb pierwszych (dla naturalnych wartości x). Nie wiemy, czy takim jest dwumian $x^2 + 1$. Dwumian ten daje liczby pierwsze dla x = 1, 2, 4, 6, 10. Obliczono, że dla $x \leq 10\,000$ jest 842 liczb pierwszych postaci $x^2 + 1$ (gdzie x jest liczbą naturalną); dla $x < 1\,000\,000$ jest 6656 takich liczb, dla $x < 180\,000$ jest takich liczb pierwszych 11 223. Wyrażono przypuszczenie, że dla każdej liczby naturalnej k istnieje nieskończenie wiele liczb pierwszych postaci $x^2+k$ , gdzie x jest liczbą naturalną. Istnieje oczywiście tylko jedna liczba pierwsza postaci $x^3 + 1$, gdzie x jest liczbą naturalną, ale wyrażono przypuszczenie, że istnieje nieskończenie wiele liczb pierwszych postaci $x^3 + 2$, gdzie x jest liczbą naturalną (liczby pierwsze otrzymujemy tu dla x = 1, 3, 5, 29), a także postaci $x^3 - 2$ (liczby pierwsze mamy tu dla x = 9, 15, 19, 27).

Nie wiemy, czy istnieje nieskończenie wiele liczb pierwszych postaci $x^2 + y^2 + 1$ gdzie x i y są liczby naturalne, natomiast można, dowieść (chociaż jest to rzeczą trudną), że istnieje nieskończenie wiele liczb pierwszych postaci $x^2 + y^2 + z^2$ 1, gdzie x, y i z są, liczby naturalne. Później udowodnimy, że istnieje nieskończenie wiele liczb pierwszych postaci $x^2 + y^2$, gdzie x i y są liczby naturalne. Natomiast nie wiemy, czy istnieje nieskończenie wiele liczb pierwszych, które są sumami sześcianów trzech liczb całkowitych.

**13. Postępy arytmetyczne utworzone z liczb pierwszych**

Udowodniono, że istnieje nieskończenie wiele postępów arytme tycznych utworzonych z trzech różnych liczb pierwszych, ale dowód tego jest trudny. Nie wiemy natomiast, czy istnieje nieskończenie wiele postępów arytmetycznych utworzonych z trzech różnych liczb pierwszych, których pierwszym wyrazem jest liczba 3; znamy dużo takich postępów, na przykład 3, 7, 11; 3, 11, 19; 3, 13, 23; 3, 17, 31 ; 3, 23, 43; 3, 31, 59; 3, 37, 71; 3, 41, 79; 3, 43, 83.

Łatwo dowieść, że nie ma postępu arytmetycznego utworzonego z trzech różnych liczb pierwszych, którego pierwszym wyrazem byłaby liczba 2 (gdyż wtedy trzeci wyraz postępu byłby parzysty > 2). Natomiast wyrażono przypuszczenie, że istnieje nieskończenie wiele postępów arytmetycznych, utworzonych, z trzech liczb pierwszych, których pierwszym wyrazem jest dowolna dana liczba pierwsza nieparzysta.

Istnieje tylko jeden postęp arytmetyczny o różnicy 2, utworzo ny z trzech liczb pierwszych, mianowicie 3, 5, 7 (gdyż z trzech kolejnych liczb nieparzystych zawsze jedna jest podzielna przez 3). Łatwo jest też dowieść, że istnieje tylko jeden postęp arytmetyczny o różnicy 4, utworzony z trzech liczb pierwszych, mianowicie 3, 7, 11. Nie ma oczywiście postępów arytmetycznych o różnicy nieparzystej, utworzonych z trzech liczb pierwszych. Wyrażono przypuszczenie, że istnieje nieskończenie wiele postępów o różnicy (i, utworzonych z trzech liczb pierwszych. Takimi są na

przykład postepy: 5, 11, 17; 11, 17, 23; 17, 23, 29. Mamy tu więc też postęp pięciowyrazowy o różnicy 6, utworzony z pięciu liczb pierwszych: 5,11,17,23,29, ale taki postęp jest tylko jeden, gdyż w każdym postępie o różnicy 6, utworzonym z pięciu liczb naturalnych, jeden z wyrazów musi być podzielny przez 5. Nasuwa się pytanie, czy istnieją postępy arytmetyczne utworzone z dowolnej liczby różnych liczb pierwszych. Najdłuższy ze znany z postępów arytmetycznych utworzonych z różnych liczb pierwszyvh ma 12 wyrazów: jest to postęp o pierwszym wyrazie 23143 i różnicy 30030, znaleziony przez W. A. Gołubiewa. Nie wiemy, czy istnieje postęp arytmetyczny utworzony ze stu różnych liczb pierwszych. V. Thebault dowiódł, że w postępie arytmetycznym, utworzonym z n > 1 liczb pierwszych, większych od n, różnica postępu musi być podzielna przez każdą liczbę pierwszą ≤ n. Wynika stąd, że jeżeli istnieje postęp arytmetyczny utworzonym ze stu różnych liczb pierwszych, to różnica tego postępu musi być olbrzymią liczbą, mającą co najmniej kilkadziesiąt cyfr. Wyrażono przypuszczenie, że jeżeli r jest liczbą naturalną podzielną przez każdą liczbę pierwszą ≤ n (gdzie n jest daną liczbą naturalną > 1), to istnieje nieskończenie wiele postępów arytmetycznych o różnicy r, utworzonych z n kolejnych liczb pierwszych. Na przykład 47, 53, 59 jest postępem arytmetycznym o różnicy 6, utworzonym z trzech kolejnych liczb pierwszych. Innymi takimi postępami są 151, 157, 163; 167, 173, 179. Znamy też postępy arytmetyczne o różnicy 6, utworzone z czterech kolejnych liczb pierwszych, na przykład 251, 257, 263, 269 albo 1741, 1747, 1753, 1759.

**14Małe twierdzenie Fermata**

Twierdzenie 9. Jeżeli p jest liczbą pierwszą, to dla każdej liczby całkowitej a liczba $a^p - a$ jest podzielna przez p.

Dowód. Niech p będzie daną liczbą pierwszą. Twierdzenie jest oczywiście prawdziwe dla liczby a = 1. Niech teraz a będzie daną liczbą naturalną i przypuśćmy ,że twierdzenie jest prawdziwedla liczby a .W myśl wzoru Newtona dal dwumianu mamy:

(4)
$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{p-1}a + 1$$

gdzie dla k = 1, 2, ..., p - 1 mamy

$$\binom{p}{k} = \frac{p(p-1)(p-2)\ldots(p-k+1)}{1.2\ldots k}$$

przy czym, jak wiadomo, liczby $\binom{p}{k}$ są całkowite. Wnosimy stąd, że liczba $1.2\ldots k * \binom{p}{k}$ jest

podzielną przez p, zatem, w myśl wniosku z twierdzenia 7, jedna co najmniej z liczb

$1.2\ldots k * \binom{p}{k}$ musi być podzielną przez p. Lecz, wobec k < p, żadna z liczb 1, 2, ..., k nie jest

podzielną przez p, skąd wnosimy, że liczba $\binom{p}{k}$ musi być podzielną przez p. Stąd, wobec (4), wnosimy, że liczba $(a + l)^p - a^p - 1$ jest podzielną przez p. Dodając do tej liczby liczbę $a^p$ - a, podzielną przez p (gdyż zakładamy, że twierdzenie jest prawdziwe dla liczby a), wnosimy, że liczba $(a + l)^p - (a + 1)$ jest podzielną przez p, czyli że twierdzenie jest prawdziwe dla liczby a + 1.

W ten sposób dowiedliśmy przez indukcję, że twierdzenie jest prawdziwe dla każdej liczby naturalnej a. Dla liczby 0 jest ono też oczywiście prawdziwe. Jeżeli p jest liczbą pierwszą nieparzystą, to mamy $(- a)^p = -a^p$ i przeto $(-a)^p - (- a) = -(a^p - a)$, skąd wnosimy, że twierdzenie jest też prawdziwe dla liczb a całkowitych ujemnych. Jeżeli zaś p = 2, to mamy $a^2 - a = (a - 1)a$, a z dwóch kolejnych liczb całkowitych a - 1 oraz a zawsze jedna jest parzystą i przeto zawsze $2 \mid a^2 - a$.

Twierdzenie 9 zostało więc udowodnione. Jako szczególny przypadek twierdzenia 9, dla a = 2, otrzymujmy twierdzenie, że dla każdej liczby pierwszej p liczba $2^p$-2 jest podzielną przez p. Nasuwa się pytanie, czy na odwrót, jeżeli n jest liczbą naturalną > 1 taką, że $n \mid 2^n - 2$, to czy n musi

być liczbą pierwszą. Do wielu twierdzeń, względnie przypuszczeń, dotyczących liczb pierwszych, doprowadziło badanie dużej liczby poszczególnych przy padków. Gdybyśmy tutaj na przykład badali wszystkie kolejne liczby naturalne > 1 oraz ≤ 300, okazałoby się, że każda liczba naturalna n taka, iż $1 < n \leq 300$ i dla której liczba 2n - 2 jest podziena przez n, jest liczbą pierwszą. Być może ta właśnie droga doprowadziła Chińczyków przed 25 wiekami do wypowiedzenia twierdzenia, że jeżeli dla liczby naturalnej n > 1 liczba $2^n$ - 2 jest podzielna przez n, to liczba n jest pierwszą. Okazało się jednak, że twierdzenie to jest fałszywe, gdyż liczba $2^{341}$ - 2, jak to zaraz okażemy, jest podzielna przez 341, a liczba 341 = 11*31 jest złożoną.

Że liczba $2^{341}$ - 2 jest podzielna przez 341, możemy się przekonać w następujący sposób. Mamy oczywiście $2^{341}$ — 2 = $(2^{31})^{11}$ - 211 + $2^{11}$- 2. Liczba $2^{10}$ - 1 =1023 = 3*341 jest podzielna przez 341 zatem też i liczba $(2^{10})^3$ - 1 jest podzielna przez 341. Liczby $2^{11}$ - 2 = $2(2^{10} - 1)$ i $2^{31}$ - 2 = $2[(2^{10})^3 - 1]$ są więc podzielne przez 341, skąd wynika, że i liczba $(2^{31})^{11}$ - $2^{11}$ jest podzielna przez 341 (gdyż dla naturalnych a, b i k liczba $a^k$ - $b^k$ jest, jak wiadomo, podzielna przez a - b). Stąd, wobec naszej równości dla liczby $2^{341}$ - 2, wynika natychmiast, że jest ona podzielna przez 341, c.b.d.o.

Nasunęło się z kolei pytanie, czy liczb naturalnych n, dla których twierdzenie chińskie jest fałszywe, jest nieskończenie wiele. Aby dowieść, że odpowiedź na to pytanie jest twierdząca, wystarczy (wobec tego że wiemy, iż liczba złożona nieparzysta 341 nie spełnia twierdzenia chińskiego) dowieść, że dla każdej liczby złożonej nieparzystej n, nie spełniającej twierdzenia chińskiego, istnieje liczba złożona nieparzysta większa od n, również nie spełniająca twierdzenia chińskiego. Przypuśćmy więc, że liczba nieparzysta złożona n = ab, gdzie a i b są liczby naturalne > 1, nie spełnia twierdzenia chińskiego, że więc $n \mid 2^n - 2$. Liczba $m = 2^n - 1 = (2^a)^b - 1$ jest nieparzystą, złożoną, gdyż podzielną przez liczbę $2^a$ - 1 większą od 1 (gdyż a > 1), i mniejszą od m (gdyż b > 1), a przy tym m > n (gdyż n > 1). Wystarczy więc jeszcze okazać, że $m|2^m$ - 2. Otóż wobec $n \mid 2^n - 2$ i uwagi, że n jest liczbą nieparzystą, mamy $n \mid 2^{n-1}$ 1, zatem $2^{n-1} - 1 = kn$, gdzie k jest liczbą naturalną. Stąd

$$2^{m-1} = 2^{2(2^{n-1}-1)} = 2^{2kn} = (2^n)^{2k}$$

Liczba $2^{m-1} – 1 = (2^n)^{2k}$ - 1 jest więc podzielna przez liczbę $2^n$- l = m i tym bardziej liczba $2^m$ - 2 jest podzielna przez m, i przeto liczba złożona m nie spełnia twierdzenia chińskiego, c.b.d.o.

Nasunęło się też pytanie, czy istnieją liczby złożone parzyste nie spełniające twierdzenia chińskiego. Dopiero w 1950 r. D. H.Lehmer znalazł taką liczbę: 161 038. Znalezienie tej liczby było rzeczą trudną, ale sprawdzenie, że jest dzielnikiem liczby $2^{161038}$ - 2, nie jest trudne. Łatwo bowiem sprawdzić, że 161038 = 2 • 73 • 1103, 161037 = 32 • 29 • 617, $2^9$ - 1 = 7 • 73, $2^{29}$- 1 = 1103 • 486737. Liczba $2^{161037}$ - 1 jest więc podzielna przez $2^9$ - 1 i przez $2^{29}$ - 1, zatem też przez 73 i przez 1103, a więc liczba $2^{161038}$ -2 jest podzielna przez 2, 73 oraz 1103, a ponieważ liczby te są różnymi liczbami pierwszymi, więc liczba $2^{161038}$ - 2 jest podzielna przez ich iloczyn, czyli przez liczbę 161038, c.b.d.o.

W 1951 r. N. G. W. H. Beeger dowiódł, że istnieje nieskończenie wiele liczb parzystych n, dla których liczba $2^n$ - 2 jest podzielna przez n. Dowiedziono też, że istnieje nieskończenie wiele par różnych liczb pierwszych p i q takich, że liczba $2^{pq}$ - 2 jest podzielna przez pq, zaś A. Schinzel dowiódł w 1958 r., że dla każdej liczby całkowitej a i każdej liczby naturalnej m istnieją różne liczby pierwsze p > m i q > m takie, iż $pq \mid a^{pq} – a$. W związku z fałszywością twierdzenia chińskiego nasunęło się pytanie, czy istnieją liczby złożone n takie, że dla każdej liczby całkowitej a liczba $a^n$ - a jest podzielna przez n. Takie liczby złożone n nazywamy bezwzględnie pseudopierwszymi. Wyrażono przypuszczenie (dotąd nie udowodnione), że takich liczb jest nieskończenie wiele. Najmniejszą liczbą bezwzględnie pseudopierwszą jest liczba 561 = 3 • 11 • 17. Aby dowieść, że liczba 561 jest bezwzględnie pseudopierwszą, wystarczy dowieść, że dla wszelkich całkowitych a liczba $a^{561}$ - a jest podzielna przez każdą z liczb pierwszych 3, 11 i 17.

Liczba $a^{561}$ - a jest oczywiście podzielna przez 3, jeżeli a jest podzielne przez 3. Jeżeli zaś a nie jest podzielne przez 3, to a jest postaci 3k ± 1, skąd $a^2$ - 1 = $(3k \pm l)^2$ - 1 = 3(3k ± 2) k, zatem $3 \mid a^2 - 1$, skąd $3 \mid a^{2*280} - 1$ i tym bardziej $3 \mid a^{561} - a$.

Liczba $a^{561}$ - a jest oczywiście podzielna przez 11, jeżeli liczba a jest podzielna przez 11. W myśl twierdzenia Fermata mamy dla wszelkich całkowitych a, 11 | $a^{11}$ - a = a ($a^{10}$ - 1) i, jeżeli liczba a nie jest podzielna przez 11, to stąd wynika, że 11 | $a^{10}$ - 1, skąd 11 | $a^{10*56}$ 1 i, tym bardziej 11 | $a^{561}$ – a. Liczba $a^{561}$ - a jest podzielna przez 17, jeżeli liczba a jest podzielna przez 17. W myśl twierdzenia Fermata mamy dla wszelkich całkowitych a, 17 | $a^{17}$ - a i jeżeli liczba a nie jest podzielna przez 17, to stąd wynika, że 17 ] $a^{16}$ - 1, skąd 17 | $a^{16*35}$ - 1, i tym bardziej 17 | $a^{561}$ - a (gclyż 16 * 35 + 1 = 561). Dowiedliśmy więc, że liczba 561 jest bezwzględnie pseudopierwszą.
Liczbami bezwzględnie pseudopierwszymi są też
5*29*73, 7 * 13 * 31, 7*23*31, 7 * 31 * 73, 13 * 37 * 61, 5 * 17 * 29 * 113 * 337 * 673 * 2689;
znamy też wiele innych. Z małego twierdzenia Fermata wynika, że jeżeli p jest liczbą pierwszą > 2, to liczba $2^{p-1}$ - 1 jest podzielna przez p. Nasunęło to pytanie, czy istnieją liczby pierwsze p,dla których liczba $2^{p-1}$ - 1 byłaby podzielna przez $p^2$. Znamy tylko dwie takie liczby pierwsze p, mianowicie 1093 i 3511, i wiemy, że nie ma innych takich liczb pierwszych p ≤ 100 000; nie wiemy natomiast, czy są większe od tej liczby ani też czy ich ilość jest skończona.
Z twierdzenia Fermata wynika też z łatwością, że jeżeli p jest liczbą pierwszą, to liczba $1^{p-1}$+ $2^{p-1}$+$3^{p-1}$+...+$(p-1)^{p-1}$ +1 jest podzielna przez p. G. Giuga wyraził w 1950 r. przypuszczenie, że podzielność ta zachodzi jedynie dla liczb pierwszych, co sprawdził dla wszystkich liczb ≤ $10^{1000}$.

**15. Dowód, że w postępach 4k + 1, 4k + 3 i 6k + 5 jest nieskończenie wiele liczb pierwszych**

Niech teraz n oznacza dowolną liczbę naturalną > 1. Liczba n! jest więc liczbą parzystą i liczba nieparzysta $(n!)^2$ + 1, jako większa od 1 ma w myśl twierdzenia 1, dzielnik pierwszy p, oczywiście nieparzysty, a więc będący postaci 4k + 1 lub 4k + 3 (gdzie k jest liczbą, całkowitą), przy czym większy od n. Przypuśćmy, że p = 4k +3. Mamy oczywiście $(n!)^2$+1 | $(n!)^{2(2k+1)}$, gdyż jak wiadomo,dla naturalnych a i nieparzystych m liczba $a^m$ + 1 jest podzielna przez a+ l (wtedy bowiem $a^m$ + 1 = (a + 1) ($a^{m-1}$ - $a^{m-2}$ + … + a+1). Ponieważ 2(2k + 1) = 4k +. 2 = p - 1, więc wobec
p | $(n!)^2$ + 1, mielibyśmy p | (n!)p-1 +1, zatem p | $(n!)^p$ + n!. Lecz w myśl twierdzenia Fermata mamy p | $(n!)^p$ - n\. Stąd p | 2 • n!, co jest niemożliwe, gdyż p jest liczbą nieparzystą > n. Zatem p musi być liczbą postaci 4k + 1. Dowiedliśmy w ten sposób, że dla każdej liczby naturalnej n > 1 istnieje liczba pierwsza > n, będąca postaci 4k + 1 (i że taką liczbą będzie każdy dzielnik pierwszy liczby $(n!)^2$ + 1). Udowodniliśmy więc
Twierdzenie 10. Liczb pierwszych postaci 4k + 1 jest nieskończenie wiele.
W związku z naszym dowodem nasuwa się pytanie, czy dla każdej liczby pierwszej p postaci 4k + 1 istnieje liczba naturalna n taka, że p | $(n!)^2$ + 1. (Mamy na przykład 5 | $2!^2$ + 1, 13 | $6!^2$ + 1), Otóż można okazać , że jeżeli p jest liczbą pierwszą postaci 4k + 1, to p | $[(p-1/2)!]^2$ + 1 .A więc będzie
17 | $(8!)^2$ + 1, 29 | $(14!)^2$ + 1, 37 | $(18!)_2$ + 1. W związku z twierdzeniem 10 nasuwa się pytanie, ile jest liczb pierwszych postaci 4k + 3. Tu dowód, że ich jest nieskończenie wiele, jest znacznie łatwiejszy. Opiera się on na następującym lemacie.
Lemat. Każda liczba naturalna postaci 4k + 3 ma co najmniej jeden dzielnik pierwszy tejże postaci.
Dowód. Niech n = 4k + 3. Liczba ta ma oczywiście dzielniki naturalne postaci 4t + 3 (gdzie t jest liczbą całkowitą), gdyż sama jest jednym z nich. Oznaczmy przez p najmniejszy z takich dzielników. Jest więc p > 1. Gdyby p było liczbą złożoną, mielibyśmy p = ab, gdzie a i b byłyby liczbami naturalnymi > 1 i mniejszymi od p, przy tym nieparzystymi, gdyż p, jako liczba postaci 4k+ 3 jest nieparzysta. Obie liczby a i b nie mogą być postaci 4t+1, gdyż wtedy ich iloczyn p = ab = ($4t_1$ + 1) ($4t_2$ + 1) = $4(4t_1t_{i_2} + t_1 + t_2)$ + 1 byłby postaci 4t + 1, co jest niemożliwe. Zatem co najmniej jedna z liczb a i b jest postaci 4t + 3. Ponieważ dzielniki liczby p są zarazem dzielnikami liczby n, więc liczba n miałaby dzielnik naturalny postaci 4t + 3 mniejszy od p, wbrew definicji liczby p. Liczba p jest więc pierwszą. Udowodniliśmy więc nasz lemat.

Niech teraz n oznacza dowolną liczbę naturalną. Liczba 4 • n! - 1 jest oczywiście naturalną, postaci 4k + 3. W myśl lematu ma ona co najmniej jeden dzielnik pierwszy p postaci 4t + 3. Musi tu być p > n, gdyż liczba 4n! - 1 jest podzielna przez p, a nie jest oczywiście podzielna przez żadną liczbę naturalną > 1 i n. Dowiedliśmy więc, że dla każdej liczby naturalnej n istnieje liczba pierwsza > n, będąca postaci 4k + 3. Udowodniliśmy więc

Twierdzenie 11. Liczb pierwszych postaci 4k + 3 jest nieskończenie wiele.
Oznaczmy, dla liczby rzeczywistej x, przez $\pi_1(x)$ liczbę liczb pierwszych postaci 4k + 11 nie większych od x, zaś przez $\pi_3(x)$ liczbę liczb pierwszych postaci 4k + 3 nie większych od x. Jest więc na przykład $\pi_1(10) = 1$, $\pi_3(10) = 2$; $\pi_1(17) = \pi_3(17) = 3$, $\pi_1(100) = 11$, $\pi_3(100) = 13$. Obliczono, że $\pi_1(x) \leq \pi_3(x)$ dla $x < 26\ 861$. Błędem jednak byłoby na podstawie tak wielkiej liczby przypadków wysnuwać wniosek, że zawsze jest $\pi_1(x) \leq \pi_3(x)$, bo jak obliczył J. Leech w 1957 r., dla $x = 26\ 861$ mamy $\pi_1(x) = 1473$, zaś $\pi_3(x)$, = 1472. Już w 1914 r. Littlewood dowiódł, że istnieje nieskończenie wiele liczb naturalnych x, dla których $\pi_1(x) > \pi_3(x)$, jako też nieskończenie wiele liczb naturalnych x, dla których $\pi_1(x) < \pi_3(x)$. Widzimy więc, jak zawodne mogą być przypuszczenia co do liczb pierwszych wysnuwane na podstawie badania wielkiej liczby przypadków. Twierdzenia 10 i 11 można wypowiedzieć w następujący sposób:
Każdy z postępów arytmetycznych
1, 5, 9, 13, 17, 21, ...
oraz
3, 7, 11, 15, 19, 23, ...
zawiera nieskończenie wiele liczb pierwszych. W związku z tym nasuwa się pytanie, jakie postępy arytmetyczne nieskończone, utworzone z liczb naturalnych, zawierają nieskończenie wiele liczb pierwszych. Niech będzie dany postęp arytmetyczny nieskończony a, a + r, a + 2r, ...
o pierwszym wyrazie naturalnym a i różnicy naturalnej r. Jeżeli liczby a i r mają dzielnik wspólny d > 1, to oczywiście każda z liczb naszego postępu będzie podzielna przez d i, jak łatwo widzieć, żaden wówczas wyraz postępu, poza być może pierwszym wyrazem, nie będzie liczbą pierwszą. Wynika stąd, że warunkiem koniecznym na to, żeby postęp arytmetyczny o pierwszym wyrazie a i różnicy r zawierał nieskończenie wiele liczb pierwszych, jest, aby liczby a i r nie miały dzielnika wspólnego większego od 1. Otóż jeszcze w 1837 r. P. G. Lejeune Dirichlet dowiódł, że warunek ten jest zarazem wystarczający. Dowód tego twierdzenia, choć upraszczany później przez różnych autorów, jest jednak skomplikowany i długi. Nie byłby prostszy dowód twierdzenia, że w każdym postępie arytmetycznym, którego pierwszy wyraz i różnica są liczbami naturalnymi nie mającymi wspólnego dzielnika większego od jedności, znajduje się co najmniej jedna liczba pierwsza. Łatwo bowiem dowieść, że twierdzenie to, chociaż wydaje się, że jest słabszym od twierdzenia Lejeune Dirichleta, jest mu równoważne. Niektóre przypadki szczególne twierdzenia Lejeune Dirichleta (zwanego też twierdzeniem o postępie arytmetycznym) są łatwe do udowodnienia. Podamy tu dowód dla a = 5, r = 6. W tym celu udowodnimy następujący
Lemat. Każda liczba naturalna postaci 6k + 5 ma co najmniej jeden dzielnik pierwszy tejże postaci.
Dowód tego lematu jest całkiem podobny do dowodu lematu o liczbach postaci 4k + 3, z tą różnicą, że zamiast postaci 4k + 3 bierzemy postać 6k + 5, a dalej opieramy się na uwadze, że liczba postaci 6t + 5, jako niepodzielna przez 2 ani przez 3, może mieć dzielniki tylko postaci 6t + 1 lub 6t + 5, oraz że iloczyn dwóch liczb postaci 6t + 1 jest liczbą tejże postaci. Dla dowodu samego twierdzenia bierzemy, dla danej liczby naturalnej n, liczbę 6*n! - 1, która oczywiście jest postaci 6k + 5 i, w myśl lematu, ma dzielnik pierwszy p tejże postaci, przy czym łatwo dowieść, że p > n. Dla każdej więc liczby naturalnej n istnieje liczba pierwsza p > n, będąca postaci 6k + 5. Stąd
Twierdzenie12. Liczb pierwszych postaci 6k + 5 jest nieskończenie wiele
Zatem postęp arytmetyczny 5, 11, 17, 23, 29, 35, ... zawiera nieskończenie wiele liczb pierwszych. Tym bardziej więc postęp arytmetyczny
2, 5, 8, 11, 14, 17, 20, ...
zawiera, nieskończenie wiele liczb pierwszych, gdyż zawiera on wszystkie wyrazy postępu 5, 11, 17, 23, ....
Istnieje więc też nieskończenie wiele liczb pierwszych postaci 3k+2.Są jeszcze niektóre inne postępy arytmetyczne, o których dość łatwo jest dowieść, że zawierają nieskończenie wiele liczb pierwszych. Takim jest na przykład postęp 8 k + 1 (gdzie k= 1,2, 3, . . .).

**16. Pewne przypuszczenia co do liczb pierwszych**

Niech teraz n będzie daną liczbą naturalną > 1. Ustawmy liczby naturalne 1, 2, 3, . . ., $n^2$ w n wierszy, po n liczb w każdym wierszu, czyli utwórzmy tablicę

1, 2, 3, k, ….., n,
n + 1, n + 2, …..... n + k. ..., 2n,
2n + 1, 2n + 2, …..... , 2n + k, ..., 3n,
….....
….....
(n - 1) n + 1,..... (n - 1) n + k, . .., $n^2$

Kolumny tej tablicy tworzą postępy arytmetyczne (o n wyrazachi) A. Schinzel wyraził przypuszczenie, że jeżeli k jest liczbą naturalną < n , nie mającą wspólnego z n dzielnika > 1, to k-ta kolumna naszej tablicy zawiera co najmniej jedną liczbę pierwszą. A. Gorzelewski sprawdził to przypuszczenie dla wszystkich liczb naturalnych ≤ 100.
Ja wyraziłem przypuszczenie, że każdy wiersz wypisanej tablicy (gdzie n > 1) zawiera co najmniej jedną liczbę pierwszą. Przypuszczenie to zostało sprawdzone przez A. Schinzla przy pomomocy tablic A Westerna i D. H. Lehmera dla wszystkich n ≤ 4400. Pierwszy wiersz naszej tablicy (dla n > 1) zawiera zawsze liczbę pierwszą 2. Twierdzenie, że drugi wiersz naszej tablicy zawiera co najmniej jedną liczbę pierwszą, jest, jak łatwo widzieć, równoważne twierdzeniu Czebyszewa, a więc jest prawdziwe. Udowodniono też, że dla n ≥ 3 trzeci wiersz naszej tablicy zawiera co najmniej jedną liczbę pierwszą, innymi słowy, że (dla n ≥ 3) między 2n a 3n leży co najmniej jedna liczba pierwsza (co jest prawdziwym również dla n = 2). Ogólniej udowodniono, że dla n ≥ 9 każdy z dziewięciu pierwszych wierszy naszej tablicy zawiera co najmniej jedną liczbę pierwszą.
Ponieważ dwoma ostatnimi wierszami naszej tablicy są :

$(n - l)^2$, $(n – l)^2 + 1$,..... $n^2 - n$,
$n^2 - n + 1$, $n^2 - n + 2$, . . ., $n^2$,

więc z naszego przypuszczenia wynika, że między każdymi dwoma kolejnymi kwadratami liczb naturalnych leżą co najmniej dwie liczby pierwsze. Ponieważ łatwo jest dowieść, że jeżeli m jest liczbą naturalną, to istnieje liczba naturalna n taka, iż

$m^3 \leq (n - l)^2$ oraz $n^2 \leq (m + l)^3$,

więc z przypuszczenia naszego wynika, że między każdymi dwoma kolejnymi sześcianami liczb naturalnych leżą co najmniej dwie liczby pierwsze. Nie wiemy, czy to jest prawdą, natomiast udowodniono, że dla dostatecznie wielkich liczb naturalnych m między $m^3$ a $(m + l)^3$ leży dowolnie wiele liczb pierwszych. Wspomnimy tu jeszcze o tym, że jak zauważył Ladislav Skuła, z przypuszczenia co do naszej tablicy (dla n = 2, 3, . . .) wynika, iż zarówno jej n + 1-szy, jako też jej n + 2-gi wiersz zawierają co najmniej po jednej liczbie pierwszej (czyli że dla naturalnych n > 1 każdy z ciągów $n^2 + 1$, $n^2 + 2$, . .., $n^2 + n$ oraz $n^2 + n + 1$, $n^2 + n + 2$, ..., $n^2 + 2n$ zawiera co najmniej jedną liczbę pierwszą). Nie jest to na ogół prawdą dla n + 3-go wiersza, na przykład dla n = 2 lub dla n = 4 (gdzie ciągi 9, 10 oraz 25, 26, 27, 28 nie zawierają żadnej liczby pierwszej).
Z przypuszczenia co do naszej tablicy łatwo byłoby też wyprowadzić wniosek, że jeżeli wszystkie liczby naturalne będziemy wypisywali kolejno w wierszach, n liczb w n-tym wierszu, więc jeżeli utworzymy nieskończoną tablicę trójkątną:
1
2, 3
4, 5, 6
7, 8, 9, 10
11, 12, 13, 14, 15
….....
….....
in w każdym wierszu tej tablicy, poczynając od drugiego, znajdzie się co najmniej jedna liczba pierwsza. Niewiey, czy to jest prawdą.

**17. Twierdzenie LAGRANGE'A**

Twierdzenie 13. Jeżeli p jest liczbą pierwszą, zaś

(i) $f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$

wielomianem stopnia naturalnego n o współczynnikach całkowitych, gdzie współczynnik przy najwyższej potędze x, $a_0$, jest niepodzielny przez p, to wśród liczb

(ii) $x = 0, 1, 2, 3, ..., p - 1$

istnieje nie więcej niż n takich, dla których liczba f(x) jest podzielna przez p.

Dowód. Twierdzenie jest prawdziwe dla wielomianów stopnia 1. W samej rzeczy, gdyby wśród liczb (ii) były co najmniej dwie różne $x_1$ i $x_2 > x_1$ takie, że $p \mid f(x_1)$ i $p \mid f(x_2)$, to mielibyśmy $p \mid f(x_1) - f(x_2)$, a ponieważ $f(x) = a_0x + a_1$, więc mielibyśmy $p \mid a_0(x_2 - x_1)$ , przy czym $x_2 - x_1$, jako różnica dwóch różnych liczb ciągu (ii), a, więc mniejszych od p, nie jest podzielna przez p, więc p byłoby dzielnikiem iloczynu dwóch liczb naturalnych niepodzielnych przez p wbrew twierdzeniu 7.

Niech teraz n oznacza daną liczbę naturalną > 1. Przypuśćmy,że twierdzenie jest prawdziwe dla wielomianów stopnia n - 1. Przypuśćmy ,że twierdzenie Langrage'a nie jest jednak prawdziwe dla pewnego wielomianu (i) stopnia n, a więc że istnieje n + 1 liczb całkowitych $\geq 0$, $x_1 < x_2 < ... < x_{n+1} < p$ takich, iż $p \mid f(x_i)$ dla i = 1,2,..., n + 1.)

Mamy $f(x) - f(x_l) = a_0(x^n - x^n_1) + a_1 (x^{n-1} - x_1^{n-1}) + ... + + a^{n-1} - (x - x_1)$. Stąd, ponieważ $x^k - x_1^k = (x - x_1) +(x^{k-1} + x_1x^{k-2} + ... + x_1^{k-2} x + x_1^{k-1})$ dla k = 2, 3,.....n ,znajdujemycz łatwością

(iii) $f(x) - f(x_1) = (x - x_1)f_l(x)$,

gdzie $f_l(x)$ jest wielomianem całkowitym stopnia n - 1 o całkowitych współczynnikach (zależnych od $a_0$, $a_1$ ..., $a_n$ oraz $x_1$), przy czym współczynnikiem przy $x^{n-1}$ będzie $a_0$, zatem liczba niepodzielna przez p.

Wobec tożsamości (iii) znajdujemy

(iv) $f(x_i) - f(x_1) = (x_i - x_l) f_l(x_i)$ dla i = 2, 3, ….. n+1.

Lecz z $p \mid f(x_i)$ dla i = 1, 2,...,n + 1 wynika, że

$$p \mid f(x_i) - f(x_1) \qquad \text{dla } i = 2, 3, ...,n+ 1,$$

zatem wobec (iv),

$$p \mid (x_i - x_1) f_l(x_i) \qquad \text{dla } i = 2, 3, ..n + 1,$$

a ponieważ liczby $x_i - x_1$ dla i = 2, 3, ..., n+1 nie są podzielne przez p, więc, w myśl twierdzenia 7, musi być

$$p \mid f_l(x_i) \qquad \text{dla } i = 2, 3,..n + 1,$$

wbrew założeniu, że twierdzenie jest prawdziwe dla wielomianów stopnia n - 1.

Wniosek. Jeżeli p jest liczbą pierwszą, zaś (i) wielomianem stopnia n o współczynnikach całkowitych, i jeżeli istnieje więcej niż n liczb naturalnych x < p, dla których f(x) jest podzielne przez p, to wszystkie współczynniki wielomianu (i) muszą być podzielne przez p.

Dowód. Przypuśćmy, że wielomian (i) spełnia warunki wniosku, ale nie wszystkie współczynniki jego są podzielne przez p. Niech $a_{n-k}$ oznacza pierwszy z kolei współczynnik niepodzielny przez p i przypuśćmy, że k > 0. Dla każdej liczby naturalnej x, dla której f(x) jest podzielne przez p, będzie też

$$g(x) = a_{n-k}x^k + a_{n-k+1}x^{k-l} + ...+a_n$$

podzielne przez p. Dla wielomianu g(x), stopnia k, istniałoby więc więcej niż n i, wobec $k \leq n$, więcej niż k liczb naturalnych x < p, dla których $p \mid g(x)$, wbrew twierdzeniu Lagrange'a (gdyż $a_{n-k}$ nie jest podzielne przez p). Musi więc być k = 0, czyli wszystkie współczynniki wielomianu (i),

poza być może $a_n$, są podzielne przez p. Lecz, skoro istnieje liczba x, dla której f(x) jest podzielne przez p, to z (i) wnosimy natychmiast, że musi być też $p|a_n$. W każdym więc razie założenie, że wniosek nasz nie jest prawdziwy, doprowadza do sprzeczności.

**18.Twierdzenie WILSONA**

Podamy teraz pewne ważne zastosowanie udowodnionego wniosku. Niecli p będzie liczbą pierwszą i niech

$$f(x) = (x - 1)\ (x - 2)\ .\ .\ .\ (\ x - p + 1) - x^{p-1} + 1$$

będzie to wielomian stopnia p - 2 o całkowitych współczynnikach. Dla .x = l, 2, ..., p-l mamy, w myśl twierdzenia Fermata, $p \mid x^p - x = x(x^{p-1} -1)$, skąd $p \mid x^{p-1} - 1$.

Lecz dla x = 1, 2, ..., p - 1 mamy też oczywiście $p \mid (x - 1)\ (x - 2)\ ...\ (x - p + 1)$,

gdyż dla takich x jeden z czynników tego iloczynu jest zerem. Wobec wzoru na f(x) (i uwagi, że różnica dwóch liczb podzielnych przez p jest podzielna przez p) wnosimy, że $p \mid f(x)$ dla x = 1, 2, ..., p – 1. W myśl wniosku z twierdzenia Lagrange'a (dla n = p - 2) wnosimy więc, że wszystkie współczynniki naszego wielomianu, zatem też i jego wyraz wolny, są podzielne przez p. Lecz dla nieparzystych p (wobec $(-1)^{p-1} = 1$) wyrazem wolnym wielomianu f(x) jest liczba 1 * 2 * 3 ... (p- 1) + 1 czyli (p - 1)! + 1. Zatem jeżeli p jest liczbą pierwszą nieparzystą, to $p \mid (p - 1)! + 1$, co jest prawdą i dla p = 2, gdyż 1! + 1 = 2. Udowodniliśmy więc

Twierdzenie 14 (Wilsona). Dla każdej liczby pierwszej p liczba (p-1)!+1 jest podzielna przez p.

Godnym uwagi jest, że jeżeli dla liczby naturalnej n > 1 liczba (n - 1)! + 1 jest podzielna przez n, to n musi być liczbą pierwszą. Gdyby bowiem n było liczbą złożoną, byłoby n = a • b, gdzie a i b są liczby naturalne > 1 oraz < n i liczba a byłaby jednym z czyników iloczynu 1*2 ... (n - 1), a więc liczba (n - 1)! + 1 przy dzieleniu przez a dawałaby resztę 1, gdy tymczasem, będąc podzielna przez n, musi być tym bardziej podzielna przez a. Stąd sprzeczność, co dowodzi, że liczba n musi być pierwszą. A więc na to, żeby liczba naturalna n > 1 była pierwszą, potrzeba i wystarcza, żeby liczba (n - 1)! + 1 była podzielna przez n. Tak więc, teoretycznie, za pomocą jednego tylko dzielenia możemy się przekonać, czy liczba jest czy nie jest pierwszą. Praktycznie jednak stosować tego niepodobna, gdyż już dla trzycyfrowych n liczba (n - 1)! + 1 ma przeszło sto cyfr. W związku z twierdzeniem Wilsona nasunęło się pytanie, czy są takie liczby pierwsze p, dla których liczba (p - 1)! + 1 jest podzielna przez $p^2$. Dla $p \leq 30000$ są tylko trzy takie liczby: 5, 13 i 563. Nie wiemy, czy takich liczb p jest nieskończenie wiele.

Twierdzenia Fermata i Wilsona można połączyć w jedno następujące twierdzenie:

Jeżeli p jest liczbą pierwszą, to dla każdej liczby całkowitej a liczba $a^p + (p – 1)!a$ jest podzielna przez p.

W samej rzeczy, jeżeli p jest liczbą pierwszą, a dowolną liczbą całkowitą, to w myśl twierdzenia Fermata liczba $a^p$ - a jest podzielna przez p, a ponieważ, w myśl twierdzenia Wilsona liczba a + (p - l)!a = [1 + (p - 1)!]a jest podzielna przez p, więc i suma tych liczb, czyli liczba $a_p$ + (p - l)!a jest podzielna przez p. Z drugiej strony, jeżeli ta liczba jest podzielna przez p przy wszelkim całkowitym a, to dla a = 1 otrzymujemy stąd twierdzenie Wilsona, z którego wynika, że przy dowolnym całkowitym a mamy $p \mid (p - l)!a + a$, co, wobec $p|a^p$ +(p - l)!a daje $p \mid a^p + (p - 1)!a$ -[(p - l)!a + a], czyli $p \mid a^p$ - a, co daje twierdzenie Fermata. Łatwo też byłoby dowieść, że twierdzenia Fermata i Wilsona można połączyć w jedno twierdzenie:

Jeżeli p jest liczbą pierwszą, zaś a liczbą całkowitą, to liczba (p -1)! $a^p$ + a jest podzielna przez p (Leo Moser). Z twierdzenia Wilsona łatwo jest wyprowadzić następujące

Twierdzenie 15 (Leibniza): Na to, żeby liczba naturalna p > 2 była pierwszą, potrzeba i wystarcza, żeby liczba (p-2)!-1 była podzielna przez p.

Dowód. Jeżeli liczba p > 2 jest pierwszą, to w myśl twierdzenia Wilsona liczba (p - 1)! + 1 jest podzielna przez p. Lecz wobec (p-1)! = (p - 2)!(p-1) mamy (p - 1)! + 1= (p – 2)!p – [(p - 2)! - 1], skąd wobec podzielności lewej strony przez p wnosimy o podzielności przez p liczby (p - 2)! - 1.

Z drugiej strony, jeżeli p | (p- 2)! - 1, to p | (p - 1)! - (p - l) i przeto p | (p - 1)! + 1, skąd (wobec p > 2), jak już dowiedliśmy wyżej, wynika, że p musi być liczbą pierwszą. Udowodniliśmy więc twierdzenie Leibniza. Jeżeli p jest liczbą pierwszą > 3, to (p - 1)! > p, gdyż wtedy (p-1)! ≥ 2(p-1) = p+(p - 2) > p i przeto liczba (p - 1)! + 1 jest większą od p i, w myśl twierdzenia Wilsona, podzielna

przez p: jest więc liczbą złożoną.
Zatem: jeżeli $p > 3$ jest liczbą pierwszą, to liczba $(p - 1)! + 1$ jest złożoną. Wynika stąd, że istnieje nieskończenie wiele liczb naturalnych n, dla których liczba n!+1 jest złożoną. Nasuwa się tu pytanie, czy istnieje też nieskończenie wiele liczb naturalnych n, dla których liczba n! + 1 jest pierwszą. Odpowiedzi na to pytanie nie znamy.Pierwszymi są liczby 1!+1 = 2, 2! + 1 = 3, 3! + l = 7; następną liczbą pierwszą tej postaci jest 11! -j- 1 = 39916801. Nie wiemy, czy liczba 27! + 1 jest pierwszą. Z twierdzenia Leibniza wynika z łatwością, że istnieje nieskończenie wiele liczb naturalnych n, dla których liczba n!-1 jest złożoną. Niee wiemy natomiast, czy istnieje nieskończenie wiele naturalnych n, dla których liczba n!-1 jest pierwszą. Pierwszymi są liczby 3! - 1 = 5, 4! - 1 = 23, 6! - 1 = 719. Nie wiemy też, czy wśród liczb p!+ 1, gdzie p jest liczbą pierwszą, istnieje nieskończenie wiele liczb złożonych. Podobnie dla liczb p! - 1. Nie znamy też odpowiedzi na pytanie, czy istnieje nieskończenie wiele liczb naturalnych n, dla których liczba $p_1p_2...p_n + 1$ jest pierwszą (gdzie $p_n$ jest n-tą liczbą pierwszą), ani też czy jest nieskończenie wiele takich liczb naturalnych n, dla których liczba $p_1p_2...p_n + 1$ jest złożoną. Liczby $p_1 + 1 = 3$, $p_1p_2 + 1 = 7$, $p_1p_2p_3 + 1 = 31$,$p_1p_2p_3p_4 + 1 = 211$, $p_1p_2p_3p_4p_5 + 1 = 2311$ są pierwsze, ale liczby $p_1p_2...p_n + 1$ są złożone dla n = 6, 7 i 8, podzielne odpowiednio przez 59, 19 i 347. Udowodnimy tu jeszcze (według pomysłu A. Schinzla), że dla naturalnych $x > 3$ iloczyn $Q_n$ wszystkich liczb pierwszych mniejszych od n jest > n. Przypuśćmy, że przy pewnym naturalnym $n > 3$ mamy $Q_n \leq n$. Byłoby więc $Q_n - 1 < n$. Lecz $Q_n - 1$ nie jest podzielne przez żadną liczbę pierwszą < n (gdyż liczby takie są dzielnikami liczby $Q_n$), a ponieważ $n \geq 4$, więc liczba $Q_n - 1 \geq Q4 - 1 = 5 > 1$ ma dzielnik pierwszy p, który zatem musi być $\geq$ n. Tym bardziej więc $Q_n - 1 \geq n$, co daje sprzeczność. Jest więc $Q_n > n$ dla $n > 3$, c.b.d.o.
O iloczynie $P_n$ wszystkich liczb pierwszych $\leq n$ można dowieść, że dla naturalnych n jest $P_n < 4^n$, zaś dla naturalnych $n \geq 29$ jest $P_n > 2^n$. Udowodniono też, że dla naturalnych $n > 2$ suma wszystkich liczb pierwszych $\leq n$ jest > n.

**19. Rozkłady liczb pierwszych na sumę dwóch kwadratów**

Niech teraz p będzie liczbą pierwszą postaci 4k + 1.
Wobec parzystości liczby p-1/2 = 2k będzie
1*2*3 … p-1/2 = (-1)(-2)....(-(p-1)/1),
co przy dzieleniu przez p daje oczywiście taką samą resztę jak liczba
(p - 1) (p-2) ... (p- p-1/2),
która, jeżeli odwrócimy porządek jej czynników, może być napisana w postaci
p+1/2(p+1/2 + 1)...(p-2)(p-1),
skąd, mnożąc przez (p-1/2)! i zważywszy ,że p+1/2 = p-1/2+1 wnosimy ,że liczba $(p-1/2)!^2$ daje przy dzieleniu przez p taką samą resztę, jak (p - 1)!. Ponieważ zaś ta ostatnia liczba, zwiększona o l, jest w myśl twierdzenia Wilsona podzielna przez p, więc również liczba $(p-1/2)!^2 + 1$ jest podzielną przez p. Udowodniliśmy więc
Twierdzenie 16. Jeżeli p jest liczbą pierwszą postaci 4k + 1, liczba $(p – 1)!^2 + 1$ jest podzielna przez p. Aby z tego twierdzenia wyprowadzić dalszy wniosek, udowodnimy następujący
Lemat. Jeżeli p jest liczbą pierwszą, zaś a liczbą całkowitą niepodzielną przez p, to istnieją liczby naturalne x i y, $x < \sqrt{p}$ i $y < \sqrt{p}$ takie, że przy odpowiednim znaku + lub - liczba $ax \pm y$ jest podzielna przez p.
Dowód. Niech p będzie daną liczbą pierwszą i niech m oznacza największą liczbę naturalną $\leq \sqrt{p}$: będzie więc $m + 1 > \sqrt{p}$, zatem $(m + l)^2 > p$. Weźmy pod uwagę liczby całkowite ax - y, gdzie x i y przybierają wartości 0, 1, 2, . .., m. Liczb takich, jest $(m + 1)^2 > p$, a ponieważ różnych reszt z ich dzielenia przez p jest tylko p, więc przy dwóch różnych układach $x_1$, $y_1$ i $x_2$, $y_2$, gdzie na przykład $x_1 \geq x_2$, liczby $ax_1 - y_1$ i $ax_2 - y_2$ muszą przy dzieleniu przez p dawać tę samą resztę, zatem liczba $ax_1 - y_1 - (ax_2 – y_2) = a(x_1-x_2) – (y_1-y_2)$ jest podzielna przez p. Nie może tu być $x_1 = x_2$, gdyż wtedy liczba $y_1 - y_2$ byłaby podzielna przez p, co wobec $0 \leq y_1 < m \leq \sqrt{p} < p$ i podobnie $0 \leq y_2 < p$, jest niemożliwe, skoro układy $x_1$, $y_1$ i $x_2$, $y_2$ są, jak zakładamy, różne. Nic może tu też być $y_1 = y_2$, gdyż wtedy liczba $a(x_1 - x_2)$ byłaby podzielna przez p i, wobec niepodzielności liczby a przez p, wynikałoby, że liczba $x_1 - x_2$ jest podzielna przez p, co, jak wyżej dla $y_1 - y_2$, dowodzimy, że jest niemożliwe. Wobec $x_1 \geq x_2$ i $x_1 \neq x_2$ liczba $x_1 – x_2$ jest więc naturalną, zaś liczba $y_1 - y_2$ całkowitą,

różną od zera, zatem, przy odpowiednim znaku, liczba $y = \pm (y_1 - y_2)$ jest naturalną i mamy $x = x_1 - x_2 \leq x1 \leq m \leq \sqrt{p}$ a więc $x < \sqrt{p}$, gdyż równość $p = x^2$ nie jest możliwą, skoro liczba p jest pierwszą. Podobnie znajdujemy, że $y < \sqrt{p}$. Przy tym liczba $ax \pm y$ która przy odpowiednim znaku jest równa liczbie $a(x_l - x_2) -(y_1 - y_2)$, jest podzielna przez p. Lemat został więc udowodniony.
Niech teraz p będzie liczbą pierwszą postaci $4k + 1$ i niech $a = (p-1/2)!$: będzie to liczba niepodzielna przez p (jako iloczyn pewnych liczb naturalnych mniejszych od p i w myśl wniosku z twierdzenia 7): w myśl naszego lematu istnieją więc liczby naturalne x I y takie, iż $x < \sqrt{p}$, $y < \sqrt{p}$ i że przy odpowiednim znaku + lub - liczba $ax \pm y$ jest podzielna przez p. W każdym więc razie liczba $a^2x^2 - y^2 = (ax + y)(ax - y)$ będzie podzielna przez p. Lecz, w myśl twierdzenia 16, liczba $a^2 + 1$ jest podzielna przez p, a więc też i liczba $a^2x^2 + x^2$ jest podzielna przez p. Skoro liczby $a^2x^2 + x^2$ oraz $a^2x^2 - y^2$ są podzielne przez p, to i ich różnica $x^2+y^2$ jest podzielna przez p, zatem $x^2 + y^2 = kp$, gdzie k jest liczbą naturalną. Ponieważ $x < \sqrt{p}$ oraz $y < \sqrt{p}$ , więc $x^2 + y^2 < 2p$, czyli $kp < 2p$, skąd $k < 2$, a ponieważ k jest liczbą naturalną, więc dowodzi to, że $k = 1$, czyli że $x^2 + y^2 = p$. Udowodniliśmy więc
Twierdzenie 17 (Fermata o liczbach pierwszych). Każda liczba pierwsza postaci $4k + 1$ jest sumą dwóch kwadratów liczb naturalnych.
Oto na przykład $5 = l^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = l^2 + 4^2$, $29 = 2^2 + 5^2$, $37 = l^2 + 6^2$, $41 = 4^2 + 5^2$, $53 = 2^2 + 7^2$, $61 = 5^2 + 6^2$, $73 = 3^2 + 8^2$.
Udowodnimy teraz, że rozkład liczby pierwszej na sumę dwóch, kwadratów liczb naturalnych, jeżeli nie zwracać uwagi na porządek składników, może być tylko jeden. Udowodnimy nawet ogólniejsze
Twierdzenie 18. Jeżeli a i b są danymi liczbami naturalnymi, to żadna liczba pierwsza p nie daje się dwoma różnymi sposobami przedstawić w postaci $p = ax^2 + by^2$, gdzie x i y są liczbami naturalnymi, o ile, w razie $a = b = 1$, nie zwracamy uwagi na porządek składników.
Dowód. Przypuśćmy, że liczba pierwsza p daje dwa rozkłady

$$p = ax^2 + by^2 = ax_1^2 + by_1^2,$$

gdzie $x, y, x_1, y_1$ są liczby naturalne. Mamy stąd

$$p^2 = (axx_1 + byy_1)^2 + ab\,(xy_1 - yx_1)^2 = (axx_l - byy_1)^2 + ab(xy_1 + yx_1)^2$$

Lecz $(axx_1 + byy_1)(xy_1 + yx_1) = (ax^2 + by^2)x_1y_1 + (ax_1^2 + by_1^2)xy = p(x_1y_1 + xy)$. Jeden więc co najmniej z czynników lewej strony musi być podzielny przez liczbę pierwszą p.
Jeżeli $p \mid axx_1 + byy_1$, to z pierwszego ze wzorów na $p^2$ wynika, że, musi być $xy_1 – yx_1 = 0$, zatem $xy_1 = yx_1$ i ,że mamy $p = axx_1+byy_1$, skąd $px = (ax^2+by^2)x_1 = px_1$, skąd $x = x_1$, zatem też $y = y_1$
Jeżeli zaś $p \mid xy_1 + yx_1$, to z drugiego ze wzorów na $p^2$ wynika, że axx1 — byy1 = 0 oraz $p^2 = ab(xy_1 +yx_1)^2$, co, z uwagi na to, że liczby $x, y, x_1$ i $y_1$ są naturalne, jest możliwe tylko gdy $a = b = 1$, a wtedy mamy stąd $p = xy_1 + yx_1$ oraz $xx_1 - yy_1 = 0$, co daje $px = (x^2 + y^2)y_1 = py_1$, skąd $x = y_1$, zatem, wobec $p = x^2 + y^2 = x_1^2 + y_1^2$ ,$y = x_1$ i rozkłady nasze różnią się tylko porządkiem składników. Twierdzenie 18 zostało udowodnione.
Z twierdzenia 18 wynika natychmiast, że jeżeli liczba naturalna n daje się co najmniej na dwa sposoby przedstawić jako suma dwóch kwadratów liczb naturalnych (jeżeli nie uważać za różne rozkładów różniących się tylko porządkiem składników), to n nie jest liczbą pierwszą.
Więc na przykład stąd, że $2501 = l^2 + 50^2 = 10^2 + 49^2$, wnosimy, że liczba 2501 nie jest pierwszą.
Jeżeli m i n są liczbami naturalnymi, to mamy $m^4 + 4n^4 = (m^2)^2 + (2n^2)^2 = (m^2 – 2n^2)^2 + (2mn)^2|$
Jeżeli $m = n$ lub to $= 2n$, to nasze rozkłady na sumę kwadratów są jednakowe, ale wtedy mamy albo $m^4 + 4n^4 = 5n^4$, co jest liczbą pierwszą tylko dla $m = n = 1$, albo też $m^4 + 4n^4 = 20n^4$, co jest liczbą złożoną. Jeżeli zaś $m \neq n$ i to $m \neq 2n$, to jak łatwo dowieść, rozkłady nasze różnią się nie tylko porządkiem składników, a więc liczba $m^4 + 4n^4$ jest złożoną. Zatem:
Jeżeli m i n są liczbami naturalnymi, z których co najmniej jedna jest różna od jedności, to liczba $m^4 + 4n^4$ jest złożoną.
W szczególności (dla $m = 1$) wynika stąd, że liczby $4n^4 + 1$, gdzie n jest liczbą naturalną > 1, są wszystkie złożone. Jeżeli znamy dwa rozkłady danej liczby naturalnej na sumę dwóch kwadratów

(różniące się nie tylko porządkiem składników), to można okazać, że potrafimy znaleźć rozkład tej liczby na iloczyn dwóch liczb naturalnych większych od jedności. W szczególności, dla naturalnych $n > 1$ mamy rozkład

$$4n^4 + 1 - (2n^2 + 2n + 1)(2n^2 - 2n + 1),$$

gdzie czynniki po prawej stronie są > 1.
Zauważymy tu jednak, że jeżeli liczba naturalna daje jeden tylko rozkład na sumę dwóch kwadratów liczb naturalnych, to stąd jeszcze nie wynika, że musi być liczbą pierwszą. Na przykład, jak łatwo się o tym przekonać, liczba 10 daje jeden tylko taki rozkład: $10 = 1^2 + 3^2$; liczba 18 daje jeden tylko taki rozkład: $18 = 3^2 + 3^2$. Podobnie liczba 45 daje jeden tylko rozkład: $45 = 3^2 + 6^2$.
Można jednak dowieść, że jeżeli liczba naturalna nieparzysta n daje jeden tylko rozkład na sumę dwóch kwadratów liczb całkowitych $\geq 0$ (o ile nie uważać za różne rozkładów, różniących się tylko porządkiem składników), i w tym rozkładzie składniki nie mają wspólnego dzielnika >1, to n jest liczbą pierwszą. Opierając się na tym, stwierdzono na elektronowej maszynie cyfrowej EMC (w Zakładzie Konstrukcji Telekomunikacyjnych i Radiofonii Politechniki Warszawskiej), że liczba $2^{39} - 7$ jest pierwszą, gdyż badanie wykazało istnienie jednego tylko rozkładu tej liczby, $2^{39} - 7 = 64045^2 + 738684^2$, na sumę dwóch kwadratów, przy czym w tym rozkładzie liczby nie mają. wspólnego dzielnika > 1.
O liczbach $2^n - 7$ dla n = 4, 5, ..., 38 wiadomo, że są złożone. Pytanie, czy wszystkie liczby $2^n - 7$ są dla naturalnych n > 3 złożone, postawił w 1956 r. P. Erdos. Odpowiedź jest tu więc przecząca. Liczby $2^n - 7$ są złożone dla n = 40, 41, .., 50, gdyż są one, jak stwierdzono, podzielne odpowiednio przez 3, 5, 3, 107, 3, 5, 3, 11, 3, 61, 3. Tak więc wśród liczb $2^n - 7$ dla naturalnych n, gdzie $3 < n \leq 50$, jest tylko jedna pierwsza(dla n = 39). Łatwo jest dowieść, że wśród liczb $2^p - 7$, gdzie p jest liczbą pierwszą, jest nieskończenie wiele złożonych. W myśl bowiem twierdzenia 10 mamy nieskończenie wiele liczb pierwszych postaci 4k + 1, a dla każdej takiej liczby pierwszej p, wobec $5 \mid 2^4 - 1$, mamy $5 \mid 2^{4k} - 1$, skąd $5 \mid 2^{4k+1} - 2$, zatem też $5 \mid 2^p - 7$.
Nie wiemy, czy istnieje nieskończenie wiele liczb naturalnych n, dla których liczba $2^n - 7$ jest pierwszą. W związku z twierdzeniem 17 nasuwa się pytanie, co można powiedzieć o rozkładach innych liczb pierwszych na sumę dwóch kwadratów. Liczba 2 daje oczywiście jeden tylko rozkład na sumę dwóch kwadratów liczb naturalnych: $2 = 1^2 + 1^2$. Pozostają więc jeszcze do zbadania liczby pierwsze postaci 4k + 3 (gdzie k= 0, 1, 2, ...). Otóż łatwo jest dowieść, że żadna liczba naturalna tej postaci nie rozkłada się na sumę dwóch kwadratów liczb całkowitych. Bo skoro jest nieparzystą, to w razie $4k + 3 = x^2 + y^2$, gdzie x i y są liczbami całkowitymi, liczby x i y nie mogłyby być obie parzyste, ani też obie nieparzyste. A więc jedna z liczb x, y musi być parzystą, a druga nieparzystą. Ale kwadrat liczby parzystej przy dzieleniu przez 4 daje resztę 0, zaś kwadrat liczby nieparzystej - resztę 1. Suma $x^2 + y^2$, dawałaby więc przy dzieleniu przez 4 resztę 1, gdy tymczasem liczba 4k + 3 daje resztę 3. Wzór $4k + 3 = x^2 + y^2$ nie jest więc przy całkowitych k, x i y możliwy.
Tak więc, z liczb pierwszych tylko liczba 2 oraz liczby pierwsze postaci 4k + 1 rozkładają się na sumę dwóch kwadratów liczb naturalnych, dając każda po jednym tylko takim rozkładzie (jeżeli nie uważać za różne rozkładów różniących się tylko porządkiem składników). Trudniejszą byłaby odpowiedź na pytanie, jakie liczby naturalne są sumami dwóch kwadratów liczb naturalnych. Sam już warunek konieczny i dostateczny na to, żeby liczba naturalna była sumą dwóch kwadratów liczb naturalnych, jest dosyć skomplikowany. Można mianowicie dowieść, że na to, żeby liczba naturalna n była sumą dwóch kwadratów liczb naturalnych, potrzeba i wystarcza, żeby w jej rozkładzie na czynniki pierwsze, czynniki postaci 4k + 3, o ile występują, występowały w potęgach o wykładnikach parzystych I ponadto żeby albo liczba 2 wchodziła z wykładnikiem nieparzystym, albo też żeby liczba n miała co najmniej jeden dzielnik pierwszy postaci 4k +1.
Badano też, ile dana liczba naturalna n daje rozkładów na sumę dwóch kwadratów liczb naturalnych. Zależy to od jej rozkładu na czynniki pierwsze. Można dowieść, że istnieją liczby naturalne dające dowolnie wiele rozkładów na sumę dwóch kwadratów liczb naturalnych. Liczba 65 claje dwa rozkłady na sumę dwóch kwadratów liczb naturalnych: $65 = 1^2 + 8^2 = 4^2 + 7^2$; liczba

1105 daje cztery takie rozkłady: $1105 = 4^2 + 33^2 = 9^2 + 32^2 = 12^2 + 31^2 = 23^2 + 24^2$.

**20. Rozkłady liczb pierwszych na różnicę dwóch kwadratów i inne**

Nasuwa się teraz pytanie, jakie liczby pierwsze i iloma sposobami dają się przedstawić jako różnice dwóch kwadratów liczb naturalnych. Przypuśćmy, że liczba pierwsza p rozkłada się na różnicę dwóch kwadratów liczb naturalnych, że więc mamy $p = x^2 - y^2$, gdzie x i y są liczby naturalne, oczywiście $x > y$. Stąd $p = (x - y)(x + y)$ i $x - y$ oraz $x + y$ są dwoma dzielnikami naturalnymi liczby p, pierwszy mniejszy od drugiego. Ponieważ p jest liczbą pierwszą, więc wnosimy stąd, że $x - y = 1$, $x + y = p$ zatem $x = p+1/2$ , $y = p-1/2$ . Liczba p musi więc być liczbą nieparzystą i wtedy mamy jedyny rozkład

$$p = (p+1/2)^2 – (p-1/2)^2$$

Mamy więc

Twierdzenie 19. Każda liczba pierwsza nieparzysta jest różnicą dwóch kwadratów liczb naturalnych, i to tylko na jeden sposób. Łatwo jest dowieść, że na to, żeby liczba naturalna $n > 1$ była różnicą dwóch kwadratów liczb naturalnych, potrzeba i wystarcza, żeby przy dzieleniu przez 4 nie dawała reszty 2. Można dowieść, że istnieją liczby, dające dowolnie wielką liczbę rozkładów na różnicę dwóch kwadratów. Z twierdzenia 19 wynika, że liczba naturalna, mająca więcej niż jeden rozkład na różnicę dwóch kwadratów liczb naturalnych, nie jest pierwszą.

Ale łatwo jest też dowieść, że jeżeli liczba nieparzysta daje jeden tylko rozkład na różnicę dwóch kwadratów liczb całkowitych, to jest. liczbą pierwszą. Przypuśćmy bowiem, że liczba nieparzysta n jest złożoną: mamy więc $n = ab$, gdzie a i b są liczby naturalne $> 1$. Mamy oczywiście

$$n = (n+1/2)^2 = (n-1/2)^2 = (a+b/2)^2 – (a-b/2)^2$$

przy czym, jeżeli na przykład $a \geq b$, to $n - 1 = ab - 1 > a - b$ (gdyż $b > 1$): rozkłady nasze są więc różne. Liczba nieparzysta złożona daje więc co najmniej dwa różne rozkłady na różnicę dwóch kwadratów liczb całkowitych. Są jednak liczby nieparzyste złożone, rozkładające się w jeden tylko sposób na różnicę dwóch kwadratów liczb naturalnych, na przykład liczba 9. (Można dowieść, że takimi są kwadraty liczb pierwszych nieparzystych.).

Przejdziemy z kolei do pytania, jak jest z rozkładami liczb pierwszych na sumę trzech kwadratów liczb naturalnych. Można dowieść, że istnieje nieskończenie wiele liczb pierwszych, będących sumami trzech kwadratów liczb naturalnych, jako też nieskończenie wiele liczb pierwszych, nie będących takimi sumami. Z liczb pierwszych < 100 sumami trzech kwadratów liczb naturalnych są tylko następujące:

$3= 1^2 + 1^2 + 1^2$, $11 = 1^2 + 1^2 + 3^2$, $17 = 2^2 + 2^2 + 3^2$, $19 = 1^2 + 3^2 + 3^2$, $29 = 2^2 + 3^2 + 4^2$, $41 = 1^2 + 2^2 + 6^2 = 3^2 + 4^2 + 4^2$, $43 = 3^2 + 3^2 + 5^2$, $53 = 1^2 + 4^2 + 6^2$, $59 = 1^2 + 3^2 + 7^2$, $61 = 3^2 + 4^2 + 6^2$, $67 = 3^2 + 3^2 + 7^2$, $73 = 1^2 + 6^2 + 6^2$, $83 = 1^2 + 1^2 + 9^2 = 3^2 + 5^2 + 7^2$, $89 = 2^2 + 2^2 + 9^2 = 2^2 + 6^2 + 7^2 = 3^2 + 4^2 + 8^2$, $97 = 5^2 + 6^2 + 6^2$.

Widzimy też stąd, że są liczby pierwsze, które mają więcej niż jeden rozkład na sumę trzech kwadratów liczb naturalnych, na przykład liczby 41, 83 i 89. Łatwo jest natomiast dowieść, że każda liczba całkowita daje się na nieskończenie wiele sposobów przedstawić w postaci x2 + y2 - z2, gdzie x, y i z są liczbami naturalnymi. Wystarczy w tym celu zauważyć, że dla całkowitych k i t mamy tożsamości

$$2k - 1 = (2t)^2 + (k - 2t^2)^2 - (k - 2t^2 – 1)^2$$
$$2k = (2t + 1)^2 + (k - 2t^2 – 2t) – (k - 2t^2 - 2t - 1)^2.$$

Co się tyczy rozkładów liczb pierwszych na sumę czterech kwadratów liczb naturalnych, to można dowieść, że rozkłady takie mają wszystkie liczby pierwsze z wyjątkiem liczb 2, 3, 5, 11, 17, 29 i 41. Dowód jest jednak trudny.

Można też dowieść, że jedynymi liczbami pierwszymi, które nie są sumami pięciu kwadratów liczb naturalnych, są liczby 2, 3 i 7, oraz że dla każdej liczby naturalnej m > 3 istnieje tylko skończona liczba liczb pierwszych, nie będących sumami m kwadratów liczb naturalnych.

I. Chowla wyraził przypuszczenie, że jeżeli liczbę 1 uważać za liczbę pierwszą (jak to dawniej niektórzy czynili), to każda liczba naturalna jest sumą ośmiu lub mniej kwadratów liczb pierwszych. Zostało to sprawdzone dla liczb naturalnych ≤ 240 000. W związku z twierdzeniem 17 nasuwa się pytanie, jakie liczby pierwsze dają się przedstawić w postaci $x^2 + 2y^2$, względnie $x^2 + 3y^2$, gdzie x i y są liczbami naturalnymi. Zachodzą tu następujące twierdzenia.

Na to, żeby liczba pierwsza p była postaci $x^2 + 2y^2$, gdzie x i y są liczby naturalne, potrzeba i wystarcza, żeby p było postaci 8k + 1 lub 8k + 3. Każda liczba pierwsza tych postaci daje tylko jeden rozkład postaci $x^2 + 2y^2$ (co wynika z twierdzenia 18).

Więc na przykład

$$3 = 1^2 + 2 \cdot 1^2,\ 11 = 3^2 + 2 \cdot 1^2,\ 17 == 3^2 + 2 \cdot 2^2,\ 19 = 1^2 + 2 \cdot 3^2.$$

Wyrażono przypuszczenie, że istnieje nieskończenie wiele liczb pierwszych p postaci 8k + 1 jako też postaci 8k + 3 takich, że $p = 1^2 + 2y^2$, gdzie y jest liczbą naturalną, a także nieskończenie wiele takich, że $p = x^2 + 2 \cdot 1^2$, gdzie x jest liczbą naturalną. Na przykład $73 = 1^2 + 2 * 6^2$, $83 = 9^2 + 2 \cdot 1^2$.

Na to, żeby liczba pierwsza p była postaci $p = x^2 + 3y^2$, gdzie x i y są liczbami naturalnymi, potrzeba i wystarcza, żeby p było postaci 6k + 1. Każda liczba pierwsza tej postaci daje jeden tylko rozkład postaci $x^2 + 3y^2$.

Więc na przykład $7 = 2^2 + 3 \cdot 1^2$, $13 = 1^2 + 3 \cdot 2^2$, $19 = 4^2 + 3 \cdot 1^2$, $31 = 2^2 + 3 \cdot 3^2$, $37 = 5^2 + 3 \cdot 2^2$.

Wyrażono przypuszczenie, że istnieje nieskończenie wiele liczb pierwszych p postaci 6k + 1 takich, że $p = 1^2 + 3y^2$, gdzie y jest liczbą naturalną, jako też nieskończenie wiele takich, że $p = x^2 + 3 \cdot 1^2$, gdzie x jest liczbą naturalną. Mamy na przykład $67 = 8^2 + 3 * 1^2$, $103 = 10^2 + 3 \cdot 1^2$, $109 = 1^2 + 3 \cdot 6^2$.

Z twierdzenia 17 wynika natychmiast, że na to, żeby liczba pierwsza, p była postaci $x^2 + 4y^2$, gdzie x i y są liczby naturalne, potrzeba i wystarcza, żeby p było postaci 4k + 1.

Udowodniono też następujące twierdzenie:

Na to, żeby liczba pierwsza nieparzysta p była postaci $x^2 - 2y^2$, gdzie x i y są, liczbami naturalnymi, potrzeba i wystarcza, żeby p było liczbą postaci 8k +1 lub 8k + 7.

Zajmiemy się teraz pytaniem, jakie liczby pierwsze są sumami dwóch sześcianów liczb naturalnych. Łatwo tu jest dać odpowiedź, jeżeli bowiem liczba pierwsza p jest sumą dwóch sześcianów liczb naturalnych, $p = x^3 + y^3$, to $x + y \mid p$ i jeżeli co najmniej jedna z liczb x, y jest >1, to $x + y < x^3 + y^3 = p$: liczba p miałaby więc dzielnik naturalny $x + y > 1$, i mniejszy od p, co niemożliwe. Musi więc być x = y = 1, zatem p == 2. Zatem:

Żadna liczba pierwsza, poza liczbą $2 = 1^3 + 1^3$ , nie jest sumą dwóch sześcianów liczb naturalnych.

A jakie liczby pierwsze są różnicami dwóch sześcianów liczb naturalnych? Jeżeli p jest liczbą pierwszą i $p = x^3 - y^3$, gdzie x i y są liczbami naturalnymi, to x > y i mamy $p = x^3 - y^3 = (x - y)(x^2 + xy + y^2)$, a ponieważ drugi czynnik jest większy od pierwszego, więc musi być $x - y = 1$ oraz $x^2 + xy + y^2 = p$, skąd $p = x^3 - (x - 1)^3 = 3x^2 - 3x + 1$.

Liczba pierwsza p wtedy więc i tylko wtedy jest różnicą dwóch sześcianów liczb naturalnych, jeżeli jest postaci 3x(x -I) + 1 gdzie x jest liczbą naturalną > 1, i wtedy p jest różnicą sześcianów dwóch kolejnych liczb naturalnych. Nie wiemy, czy takich liczb pierwszych jest nieskończenie wiele. Wyrażono przypuszczenie, że jest ich nieskończenie wiele. Dla x = 2, 3, 4, 5 otrzymujemy tu liczby pierwsze $7 = 2^3 - 1^3$, $19 = 3^3 - 2^3$, $37 = 4^3 - 3^3$, $61 = 5^3 - 4^3$; dla x = 6 otrzymujemy liczbę złożoną $91 = 7 \cdot 13$, dla x = 7 mamy liczbę pierwszą $127 = 7^3 - 6^3$, dla x = 8 i x=9 mamy liczby złożone $169 = 13^2$ i $217 = 7 \cdot 31$ ; dla x = 10, 11, 12 mamy liczby pierwsze $271 = 10^3 - 9^3$, $331 = 11^3 - 10^3$, $397 = 12^3 - 11^3$; dla x = 13 mamy liczbę złożoną 469 = 7*67; dla x = 14 i 15 mamy liczby pierwsze $547 = 14^3 - 13_3$ i $631 = 15^3 - 14^3$; dla x = 18 mamy liczbę pierwszą $919 = 18^3 - 17^3$.

Wszystkimi liczbami pierwszymi < 1000, będącymi różnicami dwóch sześcianów liczb naturalnych, są więc liczby: 7, 19, 37, 61, 127, 271, 331, 397, 547, 631 i 919.

Łatwo jest natomiast dowieść, że istnieje nieskończenie wiele liczb pierwszych, nie będących różnicami dwóch sześcianów liczb naturalnych. Dowiedliśmy bowiem, że każda liczba pierwsza,

która jest różnicą dwóch sześcianów liczb naturalnych, jest postaci 3x(x - 1) + 1, gdzie x jest liczbą naturalną > 1. Ale z dwóch kolejnych liczb naturalnych x - 1 i x zawsze jedna jest parzysta. Nasza liczba pierwsza musi więc być postaci 6k + 1. Lecz w myśl twierdzenia 12, istnieje nieskończenie wiele liczb pierwszych postaci 6k + 5, a żadna taka liczba nie jest oczywiście postaci 6k + 1, a więc nie jest różnicą dwóch sześcianów liczb naturalnych. Są jednak liczby złożone postaci 6k + 5, będące różnicami dwóch sześcianów liczb naturalnych, na przykład liczba $215 = 6 \bullet 35 + 5 = 6^3 - 1^3$. Można też dowieść, choć byłoby to trudniejsze, że istnieje nieskończenie wiele liczb pierwszych postaci 6k + 1, nie będących różnicami dwóch sześcianów liczb naturalnych: takimi są na przykład liczby pierwsze 31, 67, 103, 139, 157. Co do liczb pierwszych, będących sumami trzech sześcianów liczb naturalnych, to wypowiedziano przypuszczenie, że liczb takich jest nieskończenie wiele. Wyrażono nawet mocniejsze przypuszczenie, że już liczb pierwszych postaci $x^3 + 2 = x^3 + 1^3 + 1^3$, gdzie x jest liczbą naturalną, jest nieskończenie wiele. Takimi są na przykład liczby $3 = 1^3 + 2$, $29 = 3^3 + 2$, $127 = 5^3 + 2$, $24391 = 29^3 + 2$. Można dowieść, że istnieje nieskończenie wiele liczb pierwszych, nie będących sumami trzech sześcianów liczb całkowitych. Wyrażono też przypuszczenie, że dla każdej liczby parzystej n istnieje nieskończenie wiele liczb pierwszych, będących sumami dwóch n-tych potęg liczb naturalnych (co udowodniono tylko dla n = 2, ob. twierdzenie 17). Natomiast (podobnie jak to wyżej dowiedliśmy dla n = 3) łatwo jest dowieść, że żadna liczba pierwsza > 2 nie jest sumą dwóch n-tych potęg liczb naturalnych, gdzie n jest liczbą nieparzystą > 1. Zauważymy tu jeszcze, że K. F. Roth dowiódł (w 1951 r.) iż każda dostatecznie wielka liczba naturalna jest sumą ośmiu sześcianów liczb naturalnych, z których co najmniej siedem jest sześcianami liczb pierwszych.

**21. Reszty kwadratowe**

Jeżeli p jest liczbą pierwszą, to resztą kwadratową dla liczby p nazywamy każdą liczbę całkowitą r, dla której istnieje liczba całkowita x taka, iż liczba $x^2 - r$ jest podzielna przez p. Innymi słowy, liczbę całkowitą r nazywamy resztą kwadratową dla p, jeżeli istnieje kwadrat liczby całkowitej, dającej przy dzieleniu przez p taką samą resztę jak r. Liczby całkowite, nie będące resztami kwadratowymi dla p, nazywamy nieresztami kwadratowymi dla p.

Dla liczby 2 oczywiście każda liczba całkowita jest resztą kwadratową, gdyż jeżeli r jest liczbą nieparzystą, to $2 \mid 1^2 - r$, jeżeli zaś r jest liczbą parzystą, to $2 \mid 0^2 - r$. Niech teraz p będzie liczbą pierwszą nieparzysta. Zbadamy, ile w ciągu 1, 2, 3, .. ., p - 1 jest reszt kwadratowych dla p.

Oznaczmy ogólnie przez $r_x$ resztę z dzielenia liczby $x^2$ przez p. Dla całkowitych x liczby $r_x$ oczywiście będą wszystkie resztami kwadratowymi dla p (gdyż będzie $p \mid x^2 - r_x$). W szczególności więc resztą kwadratową dla p będzie każda z liczb

$$(i)\ r_1, r_2, \ldots . r_{p-1}/2$$

(p-1/2) jest liczbą naturalną, gdyż założyliśmy, że p jest liczbą pierwszą nieparzystą. Liczby ciągu (i) są oczywiście różne od zera (gdyż żadna z liczb $1^2, 2^2, \ldots, (p-1/2)^2$ nie jest podzielna przez p): są to więc liczby ciągu 1, 2, 3, ..., p - 1. Okażemy, że liczby (i) są wszystkie różne. Przypuśćmy, że dla pewnych naturalnych i i j, gdzie $i < j \leq p-1/2$ ,mamy $r_i = rj$. Znaczyłoby to, że liczby $i^2$ i $j^2$ dają przy dzieleniu przez p jednakowe reszty, a więc liczba $j^2 - i^2 = (j - i)(j + i)$ byłaby podzielna przez p. Lecz, wobec nierówności, które mamy dla i oraz j, liczby j - i oraz j + i są naturalne i obie mniejsze od p (gdyż $j + i < 2j \leq p - 1 < p$), a liczba pierwsza p nie może być dzielnikiem iloczynu dwóch liczb naturalnych mniejszych od p. Dowiedliśmy więc, że $ri \neq rj$ dla $i < j \leq p-1/2$. Mamy więc co najmniej p-1/2 reszt kwadratowych dla p wśród liczb ciągu 1, 2,...p - 1. Okażemy teraz, że w tym ciągu nie ma więcej reszt kwadratowych dla p poza liczbami (i). Przypuśćmy dla dowodu, że r jest liczbą z ciągu 1, 2, ..., p - 1, będącą resztą kwadratową dla p. Istnieje więc liczba całkowita a taka, że $p \mid a^2 - r$. Wynika stąd ,że $p \mid (a^2)^{p-1/2} - r^{p-1/2}$. Ponieważ liczba r nie jest podzielna przez p, więc i liczba a nie jest podzielna przez p. W myśl twierdzenia Fermata mamy więc $p \mid a^{p-1} - 1$. Lecz przedtem otrzymaliśmy $p \mid a^{p-1} - - r^{p-1/2}$ . Liczba p dzieli więc różnicę prawych stron obu naszych wzorów, czyli $p \mid r^{p-1/2} - 1$. Mamy więc $p \mid r_i^{p-1/2} - 1$ dla i= 1, 2, ..., p-1/2. W myśl twierdzenia Lagrange'a, wielomian $x^{p-1/2} - 1$ nie może być podzielny przez p dla więcej niż p-1/2 różnych

wartości x z ciągu 0, 1, 2, ..., p - 1. Wynika stąd, że poza p-1/2 liczbami (i) nie ma w ciągu 1,2, ..., p - 1 innych liczb r, dla których p | $r^{p-1/2}$ - 1, czyli nie ma w tym ciągu innych reszt kwadratowych dla p. Udowodniliśmy więc

Twierdzenie 20. Jeżeli p jest liczbą pierwszą nieparzystą, to w ciągu 1, 2, 3, ..., p-1 mamy dokładnie p-1/2 reszt kwadratowych dla p (i oczywiście tyleż niereszt kwadratowych dla p, gdyż p - 1 - (p – ½) = p-1/2

Z dowodu naszego twierdzenia wynika też natychmiast, że dla otrzymania wszystkich liczb ciągu 1,2, .. ., p - 1, będących resztami kwadratowymi dla liczby pierwszej nieparzystej p, wystarczy wyznaczyć reszty z dzielenia przez p liczb

$$1^2,2^2,3^2,.....(p-1/2)^2$$

W ten sposób znajdujemy na przykład, że wszystkimi resztami kwadratowymi dodatnimi dla modułu 13, mniejszymi od 13, są liczby 1, 4, 9, 3, 12, 10, a więc (wśród liczb > 0 oraz < 13) nieresztami dla 13 będą liczby 2, 5, 6, 7, 8 i 11. Jak dowiedliśmy wyżej, liczba r z ciągu 1, 2, ..., p -1 jest wtedy i tylko wtedy resztą kwadratową dla liczby pierwszej nieparzystej p, jeżeli liczba $r^{p-1/2}$ -1 jest podzielna przez p. Jeżeli więc liczba a z naszego ciągu jest nieresztą kwadratową dla p, to liczba $a^{p-1/2}$ - 1 nie jest podzielna przez p. Lecz, w myśl twierdzenia Fermata, liczba $a^{p-1}$ - 1, jest podzielna przez p, a ponieważ $a^{p-1}$- 1 = ($a^{p-1/2}$ -1)($a^{p-1/2}$ + 1), więc skoro p nie dzieli pierwszego czynnika prawej strony to musi dzielić drugi czynnik, czyli musi być p | $a^{p-1/2}$. Zatem : liczba a z ciagu 1,2,...p-1 jest resztą kwadratową dla liczby pierwszej nieparzystej p jeżeli p | $a^{p-1/2}$ -1 ,i nieresztą, jeżeli p | $a^{p-1/2}$+1 .Zauważmy ,że dla liczb złożonych jest inaczej. Na przykład dla n = 15 spośród liczb naturlanych < 15 tylko pięć (a więc mniej niż n-1/2 = 7) jest resztami kwadratowymi dla lioczby 15, mianowicie liczby 1,4,6,9 i 10, a pozostałe 9 liczb jest nieresztami kwadratowymi dla liczby 15 .Spośród liczb naturalnych < 8 tylko dwie, mianowicie liczby 1 i 4, są resztami kwadratowymi dla liczby 8. Zauważmy tu jeszcze ,że A. Vale Vins znalazł twierdzenie ,że liczba nieparzysta n jest wtedy i tylko wtedy pierwszą , gdy żadna z liczb $2^2,3^2,4^2,....$ $(n-1/2)^2$ przy dzieleniu przez n nie daje reszty 0 ani 1. Badano też dla liczb pierwszych reszty sześcienne, bikwadratowe i wyższych stopni. Można dowieść, że dla każdej liczby nieparzystej n istnieje nieskończenie wiele liczb pierwszych p, dla których każda liczba całkowita jest resztą n-tego stopnia. Na przykład dla liczb 5 i 11 każda liczba całkowita jest resztą sześcienną, zaś dla liczb 5 i 7 każda liczba całkowita jest resztą 5-go stopnia. Dowód, że każda liczba całkowita jest resztą 5-go stopnia dla liczby pierwszej 7, wynika natychmiast z następujących wzorów, które sprawdzamy z łatwością:

$$7 \mid 0^5 - 0,\ 7 \mid 1^5 - 1,\ 7 \mid 4^5 - 2,\ 7 \mid 5^5 - 3,\ 7 \mid 2^5 - 4,\ 7 \mid 3^5 - 5,\quad 7 \mid 6^5 - 6.$$

Można dowieść, że dla liczb pierwszych 5 i 17 każda liczba całkowita jest resztą każdego nieparzystego stopnia. Można też dowieść, że na to, żeby cłła liczby pierwszej p każda liczba całkowita była resztą każdego nieparzystego stopnia, potrzeba i wystarcza, żeby liczba pierwsza p była postaci

$2^{2^k}+1$ czyli żeby była liczbą pierwszą Fermata.

**22. Liczby FERMATA**

Liczby Fermata są to liczby postaci $F_k = 2^{2^k}+1$ gdzie k = 0, 1, 2, ... Słynny matematyk XVII

wieku, P. Fermat, przypuszczał, że wszystkie te liczby są pierwsze. Jest to prawdą dla k = 0, 1, 2, 3, 4, lecz L. Euler w 1772 r. okazał, że liczba

$$F_5 = 2^{2^5}+1 = 4294967297$$

mająca 10 cyfr, jest złożoną, podzielną przez 641. Dziś (w roku 1960) znamy już 35 liczb złożonych $F_k$, mianowicie dla k = 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 18, 23, 36, 38, 39, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 260, 267, 268, 284, 316, 452, 1945.
Wśród tych 35-ciu liczb złożonych $F_k$ są takie, dla których znamy ich rozkład na czynniki pierwsze (na przykład $F_5$ i $F_6$), są takie, dla których tego rozkładu nie znamy, ale znamy rozkład na iloczyn dwóch liczb całkowitych > 1 (do liczb takich należy $F_{1945}$), a są i takie, dla których nie znamy żadnego rozkładu na iloczyn dwóch liczb całkowitych > 1, chociaż wiemy, że taki rozkład istnieje ($F_7$ i $F_8$). Zacznijmy od największej ze znanych liczb złożonych Fermata, od liczby $F_{1945}$. Liczba cyfr tej liczby jest > $10^{582}$, a więc niepodobna jej wszystkich cyfr wypisać. A jednak, jak już wspominaliśmy, znamy najmniejszy dzielnik pierwszy tej liczby, którym jest liczba $m = 5 \cdot 2^{1947} + 1$. Nasuwają się tu dwa pytania: 1) jak znaleziono ten dzielnik i 2) jak można się przekonać, że liczba m, mająca 587 cyfr, jest dzielnikiem liczby $F_{1945}$, której cyfr nie jesteśmy w możności wypisać. Oczywiście nie będziemy tu wykonywali dzielenia liczby $F_{1945}$ przez liczbę to ani też znajdowali ilorazu z tego dzielenia, lecz na innej drodze przekonamy się, a raczej wyjaśnimy, jak się przekonano, że liczba $F_{1945}$ przy dzieleniu przez m daje resztę zero.
Oznaczmy, dla liczby całkowitej t, przez t^ resztę z dzielenia t przez m. Z definicji liczby t^ wynika, że dla każdej liczby całkowitej l będzie m | t – t^. Określimy teraz ciąg $r_k$ (k = 1,2,...) przez warunki

(i) r1 = 22, $r_{k+1} = r_k^{2\wedge}$ dla k= 1,2....

Udowodnimy przez indukcję, że będzie

(ii) $m \mid 2^{2k} - r_k$ dla k = 1, 2, … dla k = 1,2....

Wzór (ii) jest oczywiście prawdziwy dla k = 1, gdyż $2^{2^1} - r_1 = 0$. Przypuśćmy, że jest on prawdziwy dla pewnej liczby naturalnej k. Wobec (ii) mamy tym bardziej $m \mid 2^{2^{k+1}} - r_k^2$, a ponieważ, wobec m | t - t^, dla $t = r_k^2$, mamy $m \mid r_{k2} - r_k^{2\wedge}$, więc

$m \mid 2^{2^{k+1}} - r_k^{2\wedge}$ zatem; wobec (i), $m \mid 2^{2^{k+1}} - r_{k+1}$ Wzór (ii) został więc udowodniony przez indukcję. Dla k = 1945 znajdujemy

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

skąd wynika, że liczba $F_{1945}$ daje przy dzieleniu przez m taką samą resztę, jak liczba $r_{1945} + 1$. Dla zbadania, czy liczba $F_{1945}$ jest podzielna przez to, wystarczy więc zbadać, czy liczba $r_{1945} + 1$ jest podzielna przez m. Zastanowimy się teraz, jakie działania trzeba będzie wykonać, aby obliczyć liczbę $r_{1945}$. Ze wzorów (i) wynika, że liczby $r_2, r_3, ...$, jako reszty z dzielenia przez m, są wszystkie < m, zatem mają każda nie więcej niż 587 cyfr. Ze wzorów (i) wynika więc, że dla obliczenia liczby $r_{1945}$ trzeba wykonać 1944 podnoszenia do kwadratu liczb, mających nie więcej niż 587 cyfr, i taką samą liczbę dzieleń tych kwadratów (a więc liczb, mających nie więcej niż 1175 cyfr) przez liczbę to, mającą 587 cyfr. Są to działania, które obecne maszyny elektronowe były w stanie wykonać. W ten sposób stwierdzono, że liczba $F_{1945}$ jest podzielna przez liczbę to = $5 \cdot 2^{1947} + 1$, a ponieważ, jak łatwo dowieść, $F_{1945} > m$, więc liczba $F_{1945}$ jest złożoną. Przejdziemy teraz do pytania, jak znaleziono dzielnik pierwszy m liczby $F_{1945}$. Otóż znane było twierdzenie, że każdy dzielnik naturalny liczby $F_n$ musi mieć postać $2^{n+2}k + 1$, gdzie k jest liczbą całkowitą nieujemną. Dla n = 1945 wynika stąd, że dzielnikami liczby $F_{1945}$ mogą być tylko liczby postępu arytmetycznego $2^{1947}k + 1$, gdzie k = 0, 1, 2, ... Dla k = 0 otrzymujemy dzielnik trywialny 1. Dla k = 1 liczba $2^{n+2} + 1 = 2^{1947} + 1$ jest oczywiście podzielna przez 3, a więc nie jest pierwszą. Dla k = 2 liczba $2^{n+2}2 + 1 = 2^{1948} + 1 = (2^4)^{487} + 1$ jest podzielna przez $2^4 + 1$, a więc nie jest pierwszą. Dla k= 3 liczba $2^{n+2} \cdot 3 + 1 = 2^{1947} *3 + 1$ jest złożoną, podzielną przez 5, gdyż $5 \mid 2^4 - 1$, skąd $5 \mid 2^{1944} - 1$ oraz, mnożąc prawą stronę przez $2^3 \cdot 3$, $5 \mid 2^{1947} *3 - 24$ skąd też $5 \mid 2^{1947} * 3 + 1$. Dla k = 4 liczba $2^{n+2} \cdot 4 + 1 = 2^{1949} + 1$ jest podzielna przez 3, zatem złożona. Szukając więc dzielnika pierwszego liczby $F_{1945}$, musimy ją dzielić przez $2^{1947} \cdot 5 + 1 = m$. Ponieważ dzielenie wypadło bez reszty, więc skonstatowano, że

liczba $F_{1945}$ jest złożoną. Łatwo też, jak zauważył A. Schinzel, dowieść, że liczba m jest pierwszą. Gdyby bowiem liczba m była złożoną, m = ab, gdzie a i b są liczby naturalne > 1, to liczby a i b musiałyby, jako dzielniki liczby $F_{1945}$, być wyrazami postępu $2^{1947}k + 1$ dla naturalnych k > 0, skąd a > $2^{1947}$ oraz b > $2^{1947}$, zatem m = ab > $2^{3894}$ > 5 • $2^{1947}$ + 1 = m, co niemożliwe. Liczba to jest więc pierwszą. Podobnie można badać inne liczby Fermata. Dla liczby $F_5$, co do której Fermat był przekonany, że jest pierwszą, badanie jest tu bardzo proste. Dzielniki liczby $F_5$ muszą, jak wiemy, mieć postać $2^7$ • k +1, czyli 128k + 1. Dla k = 1 otrzymujemy tu liczbę 129, podzielna przez 3, a więc złożoną; dla k = 2 otrzymujemy liczbę pierwszą 257, która nie jest dzielnikiem liczby $F_5$, o czym łatwo się przekonać dzieląc dziesięciocyfrową liczbę $F_5$ przez liczbę 257. Dla k = 3 otrzymujemy liczbę 385, podzielną przez 5, a więc złożoną. Dla k = 4 otrzymujemy liczbę 513 = $2^9$ + 1, podzielną przez 3, a więc złożoną. Dla k = 5 otrzymujemy liczbę pierwszą 641, o której łatwo się przekonać, że jest dzielnikiem liczby $F_5$. Ponieważ liczba $2^{32} = 4^{16} = (3 + l)^{16} = (5 - l)^{16}$ przy dzieleniu przez 3 jako też przez 5 daje resztę 1, zatem $F_5$ daje resztę 2, więc liczba $F_5$ nie jest podzielna przez 3 ani przez 5 i przeto nie jest też podzielna przez żadną z liczb 129, 385 i 513. Zatem, za pomocą dwóch tylko dzieleń przekonywamy się, że 641 jest najmniejszym dzielnikiem pierwszym liczby $F_5$. Dzieląc liczbę $F_5$ = 4294967297 przez 641 otrzymujemy iloraz 6700417. Dzielniki tej liczby, będącej dzielnikiem liczby $F_5$, muszą mieć postać $2^7$ • k + 1 i, jeżeli jest ona złożoną, musi posiadać dzielnik pierwszy nie większy od jej pierwiastka kwadratowego, i tym bardziej < 2600. Mamy tu więc dla k nierówność 128k + 1 < 2600, skąd k < 21, a z drugiej strony wiemy, że musi być k > 4, gdyż najmniejszym dzielnikiem pierwszym liczby $F_5$ jest 641. W ten sposób, za pomocą niewielu dzieleń stwierdzono, że liczba 6700417 jest pierwsza, i otrzymano rozkład liczby $F_5$ na iloczyn dwóch różnych czynników pierwszych.Dla liczby $F_6$ znaleziono dzielnik $2^8$ • 1071 + 1 i w ten sposób stwierdzono, że jest złożoną.

Szukanie dzielników pierwszych liczby $F_n$ wśród liczb postępu arytmetycznego $2^{n+2}$ • k + 1 tylko wtedy doprowadza do wykrycia takiego dzielnika, jeżeli istnieje niezbyt wielki dzielnik pierwszy liczby $F_n$. W przeciwnym razie, podstawiając za k nawet bardzo wiele kolejnych liczb naturalnych, nie natrafimy na taki dzielnik. Zachodzi to na przykład dla liczb $F_7$ i $F_8$, z których pierwsza ma 39, zaś druga 78 cyfr. Nie znamy żadnego dzielnika pierwszego żadnej z tych liczb, ani też żadnego ich rozkładu na iloczyn dwóch liczb naturalnych większych od 1, a jednak J. C. Morehead dowiódł w 1905 r,, że liczba $F_7$ jest złożoną, zaś tenże oraz A. E. Western dowiedli w 1909 r., że liczba $F_8$ jest złożoną. Dowiedli oni tego dzięki następującemu twierdzeniu.

Twierdzenie 21. Jeżeli liczba $F_n$ jest pierwszą, to liczba $3^{2^{2^n-1}}+1$ jest podzielna przez Fn.

Udowodnimy najpierw następujący

Lemat. Jeżeli k jest liczbą całkowitą nieujemną i jeżeli liczba p = 12k + 5 jest pierwszą, to liczba $3^{6k+2}$ + 1 jest podzielna przez p.

Dowód lematu. Lemat jest oczywiście prawdziwy dla liczby k = 0, możemy więc dalej zakładać, że k jest liczbą naturalną. Niech p = 12k + 5. Weźmy iloczyn pierwszych 6k + 2 liczb naturalnych podzielnych przez 3 i rozbijmy czynniki tego iloczynu na trzy grupy, zaliczając do pierwszej grupy pierwsze 2k czynniki, do drugiej następne 2k + 1 czynników, zaś do trzeciej pozostałe 2k + 1 czynniki.

Czynniki pierwszej grupy dają iloczyn 3*6*9.. . 6k. Czynniki drugiej grupy dają, po odwróceniu porządku czynników, iloczyn

(12k + 3) • 12k • (12k - 3)... (6k + 6) (6k + 3),

który wobec p = 12k + 5 możemy napisać w postaci

(p - 2) (p - 5) (p - 8).. .[p-(6k + 2)].

Ponieważ liczba czynników jest tu nieparzysta (równa 2k + 1), więc iloczyn nasz, po rozwinięciu i zebraniu składników podzielnych przez p, da nam liczbę pu - 2*5*8. . .(6k + 2), gdzie u jest pewną liczbą całkowitą. Czynniki trzeciej grupy dają iloczyn

(12k + 6) (12k + 9) (12k + 12).. .(18k + 6) = (p + 1) (p + 4)... (p + 7).. .(p + 6k + 1) = pv + 1 • 4 • 7.. ,(6k + 1), gdzie v jest liczbą naturalną.

Mamy więc 3 • 6 • 9.. .(18k + 6) = 3*6*9...6k. (pu - 2*5*8.... (6k.+-2)) (pv + 1*4*7. . .(6k + 1)) = pw - 1*2*3*4*5*6.. .(6k + 1). (6k + 2) = pw - (6k + 2)!, gdzie w jest liczbą całkowitą.

Lecz 3*6*9... (18k + 6) = (6k + 2)!$3^{6k+2}$ . Wnosimy stąd, że liczba pw jest podzielna przez (6k + 2)!, zatem pw = (6k + 2)!t, gdzie t jest liczbą całkowitą. Lecz 6k + 2 < 12k + 5 = p i przeto liczba (6k +2)! nie jest podzielna przez p. Skoro iloczyn (6k + 2)!t jest podzielny przez p, to musi t być podzielne przez p, t = pu, skąd w = (6k + 2)!u, gdzie u jest liczbą całkowitą. Mamy więc $3^{6k+2}$ = pu - 1, skąd wynika, że liczba $3^{6k+2}$ + 1 jest podzielna przez p, c.b.d.o.

Udowodniliśmy więc nasz lemat.

Dowód twierdzenia 21. Niech n będzie daną liczbą naturalną. Mamy więc $2^n$ = 2m, gdzie m jest liczbą naturalną: stąd $F_n$ - 1 = $4^m$, skąd wynika, że liczba $F_n$ - 5 jest podzielna przez 4. Z drugiej strony mamy $F_n$ - 1 = $4^m$ = (3 + l)$^m$ = 3t +1, gdzie t jest liczbą naturalną. Stąd $F_n$ - 5 = 3(t - 1), co dowodzi, że liczba $F_n$ - 5 jest podzielna przez 3, a ponieważ, jak dowiedliśmy, jest podzielna przez 4, więc jest podzielna przez 12, zatem $F_n$ = 12k + 5, gdzie k jest liczbą całkowitą. Z lematu naszego wynika więc, że jeżeli liczba $F_n$ jest pierwsza, to liczba $3^{6k+2}$ + 1 = $3^{(Fn-1)/2}$ + 1 = $3^{2^{2^n-1}}+1$ jest podzielna przez $F_n$.

Udowodniliśmy więc twierdzenie 21. Zauważymy też, że można dowieść (co nie będzie nam zresztą dalej potrzebne), że i twierdzenie odwrotne do twierdzenia 21 jest prawdziwe. Zastosujemy teraz twierdzenie 21 do dowodu, że liczba $F_7$ jest złożoną. Wystarczy w tym celu okazać, że liczba $3^{2^{127}}+1$ nie jest podzielna przez liczbę $F_7$ = 340282366920938463463374607431768211457.

W tym celu wystarczy obliczyć resztę z dzielenia liczby $3^{2^{127}}$ przez liczbę $F_7$. Liczba $3^{2^{127}}$ jest tak olbrzymią, że nie potrafimy jej wypisać za pomocą cyfr, ale dla obliczenia, jaką daje resztę przy dzieleniu przez $F_7$, możemy tak postąpić. Liczba $3^{2^7}$ ma 61 cyfr, a więc możemy ją wypisać i obliczyć resztę r z dzielenia jej przez liczbę $F_7$ (Dzisiaj nie jest to rzeczą trudną przy pomocy maszyn elektronowych do liczenia, ale w 1905 roku, gdy robił to Morehead, było to rzeczą uciążliwą, ale możliwą). Reszta $r_l$ z dzielenia liczby $r^2$ przez liczbę $F_7$ będzie oczywiście resztą z dzielenia liczby $3^{2^8}$ przez liczbę $F_7$ Podobnie reszta $r_3$ z dzielenia liczby $r^2_1$ przez liczbę $F_7$, będzie resztą z dzielenia liczby $3^{2^9}$ przez $F_7$, zaś reszta $r_3$ z dzielenia liczby $r^2_2$ przez $F_7$ będzie resztą z dzielenia liczby $3^{2^{10}}$ przez $F_7$ Postępując w ten sposób dojdziemy do reszty $r_{120}$ z dzielenia liczby $3^{2^{127}}$ przez F7. W ten sposób znaleziono, że $r_{120} \neq 2^{2^7}-1$ skąd wynika, że liczba $3^{2^{127}}+1$ nie jest podzielna przez $F_7$,

zatem, w myśl twierdzenia 21, że liczba $F_7$ nie jest pierwszą. W podobny sposób przekonano się też, że liczba $F_8$ nie jest pierwszą. Dla każdej zaś z liczb $F_n$ (n = 9, 10, 11,12), które są złożone, znamy ich dzielniki pierwsze, mianowicie:

$2^{16}$*37 + 1 |$F_9$, $2^{19}$ * 11131 + 1 | $F_{10}$,213*39 +1 |$F_{11}$,$2^{14}$*7 + 1 |$F_{12}$

Liczby $F_{13}$ = $2^{8192}$ + 1 dotąd nie zbadano i nie wiemy, czy jest pierwszą, czy nie. Ma ona 2467 cyfr i dla przekonania się, czy liczba $m = 3^{2^{8191}}+1$ jest przez nią podzielna, trzeba by wykonać około dziesięciu tysięcy podnoszeń do kwadratu liczb, mających nie więcej niż 2467 cyfr, i dzieleń przez liczbę o 2467 cyfrach.

Wielkie maszyny elektronowe dają sobie radę nawet z większymi rachunkami. Gdyby się okazało, że liczba m nie jest podzielna przez $F_{13}$ - mielibyśmy nowy przykład liczby złożonej Fermata. Ponieważ, jak wspominaliśmy, zachodzi twierdzenie odwrotne do twierdzenia 21, więc w razie podzielności liczby m przez $F_{13}$ mielibyśmy nową liczbę pierwszą Fermata, większą od $F_4$.

Podobną jest sytuacja dla liczby $F_{14}$, mającej 4933 cyfry, o której nie wiemy, czy jest pierwszą, czy nie. Natomiast dowiedziono, że liczby $F_{15}$ i $F_{16}$ są złożone i znaleziono ich dzielniki pierwsze: $2^{21}$ • 573 + 1 | $F_{15}$, $2^{18}$• 3150 + 1 | $F_{16}$.

Natomiast liczba $F_{17}$ ma przeszło 30 tysięcy cyfr, a istniejące obecnie maszyny do liczenia nie są w stanie wykonać dziesiątków tysięcy dzieleń liczb o kilkudziesięciu tysiącach cyfr przez liczbę mającą przeszło 30 tysięcy cyfr. Tak więc twierdzenie 21 mogłoby, poza znanymi już liczbami $F_7$ i $F_8$, być zastosowane obecnie jedynie do zbadania liczb $F_{13}$ i $F_{14}$.

Dla liczby $F_{16}$ znaleziono w 1953 r. najmniejszy dzielnik pierwszy $2^{18}$ • 3150 + 1 i obalono w ten sposób przypuszczenie, że wszystkie liczby ciągu nieskończonego

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

są pierwsze, gdyż liczba złożona $F_{16}$ jest piątym wyrazem tego ciągu. Nie wiemy jednak, czy w tym ciągu jest nieskończenie wiele liczb pierwszych ani też czy jest w nim nieskończenie wiele liczb złożonych. Zauważymy, że żadna z liczb

$$2^{2^{n}+1}+1$$

gdzie n jest liczbą naturalną, nie jest pierwszą, gdyż są one > 3 i podzielne przez 3.
Można dowieść, że wśród liczb

$$2^{2^{n}+1}-3$$

gdzie n = 1,2, . . ., jest nieskończenie wiele złożonych, gdyż

$$7 \mid 2^{2^{2k+1}}+3$$

dla k = 0, 1, 2, …

## 23.Liczby pierwsze postaci $n^n+1, n^{n^n}+1$ i inne

W związku z liczbami Fermata nasuwa się pytanie, ile jest liczb pierwszych postaci $n^n + 1$, gdzie n jest liczbą naturalną. Przypuśćmy, że n jest liczbą naturalną i że liczba $n^n + 1$ jest pierwszą. Każda liczba naturalna n jest, jak wiadomo, postaci $n = 2^k * m$, gdzie k jest liczbą całkowitą > 0, zaś m jest liczbą nieparzystą. Gdyby m było liczbą > 1, $nn+1=(n^{2^k})^m+1$ to liczba $n^{2^k}+1$ byłaby > oraz podzielną przez , $n^{2^k}+1$ zatem złożoną. Musi więc być m = 1, zatem n = $2^k$
Jeżeli k = 0, to n = 1 i liczba $n^n + 1 = 2$ jest pierwszą. Jeżeli k > 0, to $k = 2^r s$, gdzie r jest liczbą całkowitą ≥ 0, zaś s liczbą nieparzystą. Gdyby było s > 1, to liczba $n^n + 1 = 2^{2rsn}+1 = (2^{2m})^s + 1$, jako > $2^{2m} + 1$ i podzielną przez tę liczbę, byłaby złożona. Musi więc być s=1, zatem $k = 2^r$ oraz $n = 2^{2r}$ a więc

$$n^n+1=2^{2^r 2^{2^r}}+1=2^{2^{r+2^r}}+1=F_{r+2^r}$$

A więc liczba $n^n + 1$, gdzie n jest liczbą naturalną > 1, jest wtedy i tylko wtedy pierwszą, gdy $n = 2^{2r}$, gdzie r jest liczbą całkowitą ≥ 0 i jeżeli liczba $F_{r+2r}$ jest pierwszą.
Dla r = 0, ponieważ liczba $F_1 = 3$ jest pierwszą, otrzymujemy liczbę pierwszą $2^2 + 1 = 5$. Dla r = 1, ponieważ liczba $F_3 = 257$ jest pierwszą, otrzymujemy liczbę pierwszą $4^4+1 = 257$. Dla r = 2, ponieważ liczba $F_6$ jest jak wiadomo złożoną, podzielną przez 28 • 1071 + 1, nie otrzymujemy liczby pierwszej. Dla r = 3 również nie otrzymujemy liczby pierwszej, gdyż liczba $F_{11}$ jest złożoną, podzielną przez $2^{13}$ • 39 + 1. Jeżeli więc poza liczbami 2, 5 oraz 257 istnieje jeszcze liczba pierwsza postaci $n^n + 1$, to musi być

$$\geq F_{20} > 2^{2^{20}} > 2^{10^6} > 10^{3*10^5}$$

czyli musi to być liczba mająca więcej niż trzysta tysięcy cyfr. Zatem: wśród liczb postaci $n^n +1$ (gdzie n jest liczbą naturalną), mających nie więcej niż trzysta tysięcy cyfr, są tylko trzy liczby pierwsze: $1^1 + 1 = 2$, $2^2 + 1 = 5$ i $4^4 + 1 = 257$.Można by wobec tego zaryzykować przypuszczenie, że nie ma innych liczb pierwszych postaci $n^n+1$, gdzie n jest liczbą naturalną, poza trzema: 2, 5 i 257. Należy jednak wziąć pod uwagę, że z takiego przypuszczenia wynikałoby, że istnieje nieskończenie wiele liczb Fermata złożonych: takimi bowiem byłyby liczby $F_{r+2^r}$ dla r = 4, 5, 6, ..., zatem liczby $F_{20}$, $F_{37}$, $F_{70}$, $F_{135}$, $F_{264}$, $F_{521}$, $F_{1034}$, . . . O żadnej z tych liczb nie udowodniono jednak

dotąd, że jest złożoną. Zapytamy z kolei, co wiemy o liczbach pierwszych postaci

$$n^{n^n}+1$$

Otóż mamy $1^{1^1}+1=2^{2^2}+1=17$ Łatwo jest dowieść, że jeżeli liczba $n^{n^n}+1$ gdzie n jest liczbą naturalną > 1, jest pierwszą, to przy pewnym całkowitym r ≥ 0 musi być n = $2^{2^r}$, zatem

$$n^{n^n}+1=F_{r_{+2^{n+2^r}}}$$

Dla r = 0 otrzymujemy liczbę pierwszą $F_2$ = 17, dla r = 1 liczbę $F_9$, o której wiadomo, że jest złożoną, podzielną przez 216 • 37 + 1. Dla r = 2 otrzymujemy liczbę $F_{66}$, o której łatwo dowieść, że ma więcej niż 1018 cyfr. Stąd wniosek, że Wśród liczb, mających nie więcej niż miliard miliardów cyfr, istnieją tylko dwie liczby pierwsze postaci

$$n^{n^n}+1$$

, gdzie n jest liczbą naturalną, mianowicie 2 i 17. Badano też, które z liczb postaci n • $2^n$+1 gdzie n = 1, 2, 3, ..., są pierwsze (są to tak zwane liczby Cullena). Poza liczbą 3 (dla n = 1) znamy jeszcze tylko jedną taką liczbę pierwszą, dla n = 141. Pytanie, ile jest takich liczb pierwszych, pozostaje otwarte. Jak łatwo dowieść, nie ma innych liczb pierwszych postaci $2^n$ + 1 poza liczbami pierwszymi Fermata. Jeżeli bowiem n = $2^r$* m, gdzie m jest liczbą nieparzystą > 1, to liczba

$$2^n+1=(2^{2^r})^m+1$$

jest podzielną przez mniejszą od niej liczbę $2^{2^r}+1>1$ a więc złożoną. Z liczb pierwszych postaci $2^n$+ 1, gdzie n = 1, 2, znamy więc tylko pięć: dla n = 1, 2, 4, 8, 16, zaś najmniejszą liczbą tej postaci, o której nie wiemy, czy jest pierwszą, czy nie, jest liczba $2^{8192}$ +1. Znamy więc też tylko cztery liczby pierwsze postaci 2 • $2^n$ + 1, gdzie n jest liczbą naturalną, mianowicie dla n = 1, 3, 7 i 15. Natomiast znamy 19 liczb pierwszych postaci 3 • $2^n$ + 1, mianowicie dla n= 1, 2, 5, 6, 8, 12, 18, 30, 36, 41, 66, 189, 201, 209, 276, 353, 408, 438, 534. Liczb pierwszych postaci 4 • $2^n$ + 1, gdzie n = 1, 2, ... znamy tylko trzy: dla n= 2, 6 i 14. Natomiast liczb pierwszych postaci 5 • $2^n$ + 1 (gdzie n = 1, 2, . ..) znamy 12: dla n = 1, 3, 7, 13, 15, 25, 39, 55, 75, 85, 127, 1947.
Dla każdej liczby naturalnej k ≤100, z wyjątkiem k = 47 i k = 94, znamy co najmniej jedną liczbę naturalną n taką, że liczba k• $2^n$+ 1 jest pierwszą. Można jednak dowieść, że istnieje nieskończenie wiele takich liczb naturalnych k, dla których każda z liczb k • $2^n$ + 1 (n =1,2, . . .) jest złożoną.
Badano też liczby pierwsze postaci $2^m + 2^n + 1$, gdzie m i n są liczbami naturalnymi, m > n. Znamy takie liczby pierwsze, na przykład $2^2 + 2 + 1 = 7$, $2^3 + 2 + 1 = 11$, $2^3 + 2^2 + 1 = 13$, $2^4 + 2 + 1 = 19$.
Nie wiemy, czy takich liczb pierwszych jest nieskończenie wiele. Natomiast łatwo jest dowieść, że istnieje nieskończenie wiele liczb złożonych postaci $2^m + 2^n + 1$, gdzie m i n są liczbami naturalnymi, m > n. Wynika to na przykład natychmiast z równości $2^{2n} + 2^{n+1}+1 = (2^n+ 1)^2$ dla n= 2, 3, ..., albo z uwagi, że dla k = 1, 2, ... liczba $2^{4k+1}$ + 2+1 jest zawsze podzielna przez 5, zaś liczba $2^{2k}$ + $2^{2l}$ + 1 jest dla naturalnych k i l zawsze podzielna przez 3. Mamy też rozkład $2^{4k} + 2^{2k} + 1 = (2^{2k} + 2^k + 1) (2^{2k} - 2^k + 1)$. A. Richner obliczył, że liczby $2^n$ + 3 dla n < 24 są pierwsze tylko dla n = 1,2, 3, 4, 6, 7, 12, 15, 16, 18. Łatwo jest dowieść, że wśród liczb

$$2^{2^{2n}}+3$$

jest nieskończenie wiele złożonych, mianowicie, że liczby

$2^{2^{(3k+1)}}+3$ są dla k = 0, 1, 2, ... wszystkie podzielne przez 19. Natomiast liczby

$2^{2^{2k+1}}+3$ są dla k = 0, 1, 2, ... wszystkie podzielne przez 7.

Mamy też

$13 \mid 2^{2^{2^k}}-3$ dla k = 1, 2, 3, ..., skąd wynika, że każda z liczb

$$2^{2^{2^2}}-3, 2^{2^{2^{2^2}}}-3, \ldots.$$

jest podzielna przez 13, zatem złożona.
Nie wiem natomiast, czy wśród liczb

$$2+3, 2^2+3, 2^{2^2}+3, 2^{2^{2^2}}+3, \ldots$$

jest tylko skończona liczba pierwszych.

Natomiast wśród liczb

$$\left| 2^{2^2}+5, 2^{2^{2^2}}+5, \ldots \right.$$

nie ma żadnej pierwszej, gdyż każda z tych liczb jest podzielna przez 7
Dowód tego jest łatwy. Dla naturalnych k liczba $2^{2k} = (3 + l)^k$ przy dzieleniu przez 3 daje resztę 1, zatem $2^{2k} = 3t + 1$, gdzie t jest liczbą naturalną. Stąd

$2^{2^{2k}}+5 = 2^{3t+1}+5 = (7+1)^t * 2+5$ co oczywiście jest podzielne przez 7.

Nie wiadomo, czy istnieje taka liczba naturalna k, dla której istniałoby nieskończenie wiele liczb pierwszych postaci

$2^{n_1}+2^{n_2}+\ldots 2^{n_{k+1}}$ gdzie $n_1, n_2, \ldots, n_k$ są liczby naturalne. Nie wiemy, czy istnieje nieskończenie wiele liczb pierwszych postaci $2^n + n^2$, gdzie n jest liczbą naturalną. Czterema najmniejszymi takimi liczbami pierwszymi są $3 = 2^1 + 1^2$, $17 = 2^3 + 3^2$, $593 = 2^9 + 9^2$ i $32993 = 2^{15} + 15^2$.

**24. Trzy błędne twierdzenia FERMATA**

P. Fermat wypowiedział (w swym liście do Mersenne'a z 1641 r.) trzy następujące twierdzenia:
1.Żadna liczba pierwsza postaci 12k + 1 nie jest dzielnikiem żadnej z liczb postaci $3^n + 1$.
2.Żadna liczba pierwsza postaci l0k + 1 nie jest dzielnikiem\ żadnej z liczb postaci $5^n + 1$.
3.Żadna liczba pierwsza postaci 10k - 1 nie jest dzielnikiem żadnej z liczb postaci $5^n + 1$.
Dopiero w 1959 r. udowodniono, że żadne z tych trzeh twierdzeń nie jest prawdziwe. Pierwsze dlatego, że na przykład $61 \mid 3^5 + 1$, $241 \mid 3^{60} + 1$, drugie dlatego, że $521 \mid 5^5 + 1$, trzecie dlatego, że $29 \mid 5^7 + 1$. A. Schinzel podał dla każdego z tych trzech twierdzeń dowód, że istnieje nieskończenie wiele liczb pierwszych, dla, których jest ono fałszywe.
Tu więc sytuacja jest nieco inna niż z twierdzeniem Fermata o tym, że każda z liczb $2^{2^n+1}+1$

(gdzie n = 1, 2, .. .) jest pierwszą, gdzie znamy tylko skończoną liczbę przykładów fałszywości tego twierdzenia. Poza twierdzeniami 1, 2 i 3 Fermat wypowiedział też twierdzenie, że żadna liczba pierwsza postaci 12k - 1 nie jest dzielnikiem żadnej z liczb postaci $3^n + 1$, które później zostało udowodnione.

**25 Liczby MERSENNE'A**

Liczby Mersenne'a są to liczby postaci $M_n = 2n - 1$, gdzie n = 1, 2, 3, ... Są one ciekawe z dwóch względów. Po pierwsze, największe znane liczby pierwsze są liczbami Mersenne'a, a po drugie,

przy pomocy liczb Mersenne'a znajdujemy wszystkie tak zwane liczby parzyste doskonale, tj. równe sumie wszystkich swych, mniejszych od nich samych, dzielników naturalnych. (Liczbami doskonałymi interesowano się jeszcze w starożytności).
Można też określić n-tą liczbę Mersenne'a jako sumę n pierwszych wyrazów postępu geometrycznego 1, 2, $2^2$, $2^3$, $2^4$, ... Mamy więc
$M_1 = 1$, $M_2 = 3$, $M_3 = 7$, $M_4 = 15$, $M_5 = 31$, $M_6 = 63$, $M_7 = 127$,...
Jak łatwo dowieść, jeżeli wskaźnik n liczby $M_n$ jest liczbą złożoną, to i liczba $M_n$ jest złożoną. Jeżeli bowiem n = ab, gdzie .œ i b są liczbami naturalnymi > 1, to $2^a - 1 > 1$, oraz $2^n - 1 = 2^{ab} - 1 > 2^a - 1$, zaś liczba $2^{ab} - 1$ jest podzielna przez $2^a - 1$, zatem złożona.
Jeżeli więc liczba $M_n$, gdzie n > 1, jest pierwszą, to liczba n musi być pierwszą, ale niekoniecznie na odwrót, gdyż na przykład $M_{11} = 2^{11} - 1 = 2047 = 23 \bullet 89$.
Udowodniono, że jeżeli p jest liczbą pierwszą, to każdy dzielnik naturalny liczby $M_p$ musi być postaci 2kp + 1, gdzie k jest liczbą całkowitą ≥ 0. Więc na przykład dzielnikami liczby $M_{11}$ są liczby 22k + 1, gdzie k = 0, 1, 4 i 93. W szczególności więc wynika stąd, że dzielniki liczby $M_{101} = 2^{101} - 1$ muszą być postaci 202k + 1. Niestety żadnego dzielnika pierwszego liczby $M_{101}$ nie znaleziono dotąd (widocznie liczba k jest tu bardzo wielka), chociaż na innej drodze (o czym będzie mowa później) stwierdzono, że liczba $M_{101}$ jest złożona. Dowiedziono też, że jeżeli q jest liczbą pierwszą postaci 8k + 7, to $q \mid M_{(q-1)/2}$. Pozwoliło to stwierdzić, że wiele spośród liczb $M_p$, gdzie p jest liczbą pierwszą, jest złożonych. Na przykład
$47 \mid M_{23}$, $167 \mid M_{83}$, $263 \mid M_{131}$, $359 \mid M1_{79}$ ,$383 \mid M_{191}$, $479 \mid M_{239}$.
Wypowiedziano przypuszczenie (dotąd nie udowodnione), że wśród liczb $M_p$ , gdzie p jest liczbą pierwszą, istnieje nieskończenie wiele złożonych. Liczb pierwszych Mersenne'a znamy dotąd tylko 18: są to liczby $M_n$ dla n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 617, 1279, 2203, 2281 i 3217. Sześć największych liczb pierwszych Mersenne'a znaleziono (przy pomocy maszyn elektronowych) w ostatnim dziesięcioleciu. Wyjaśnimy teraz, w jaki sposób można było stwierdzić, że te tak wielkie liczby Mersenne'a są pierwsze. Stało się to możliwe dzięki następującemu twierdzeniu, które przedtem udowodniono:
Twierdzenie Lucas - D. H. Lehmera. Liczba $M_p$, gdzie, p jest liczbą pierwszą nieparzystą, wtedy i tylko wtedy jest liczbą pierwszą, gdy liczba $M_p$ jest dzielnikiem, (p - 1 )-go wyrazu ciągu $u_n$(n = 1, 2, ...) określonego przez warunki:

$u_1 = 4$, zaś $u_{n+1} = u_n^2 - 2$ dla n = 1, 2, ...

(a więc ciągu, którego początkowymi wyrazami są liczby 4, 14, 194, 37634,...).
Łatwo jest dowieść, że na to, żeby było $M_p \mid u_{p-1}$ potrzeba i wystarcza, żeby $M_p$ było dzielnikiem (p - l)-go wyrazu ciągu $r_n$(n = 1, 2, ...,) zależnego od $M_p$, określonego przez warunki:

$r_1 = 4$, zaś $r_{n+1}$ jest resztą z dzielenia liczby $r_n^2 - 2$ przez $M_p$ .

Tak więc dla stwierdzenia, czy liczba $M_p$ jest pierwszą, czy nie, mamy tylko do czynienia z podnoszeniem do kwadratu i następnie dzieleniem przez $M_p$ liczb mniejszych od $M_p$. W szczególności dla stwierdzenia, czy $M_{101}$ jest liczbą pierwszą, trzeba się przekonać, czy zachodzi podzielność $M_{101} \mid r_{100}$, a liczba $M_{101}$ ma 31 cyfr. Rachunki te wykonano i stwierdzono, że liczba $r_{100}$ nie jest podzielna przez $M_{101}$, skąd wniosek, że $M_{101}$ jest liczbą złożoną. Dla stwierdzenia, że liczba $M_{3217}$ mająca 969 cyfr, jest pierwszą, należało wykazać, że (odpowiadająca $M_{3217}$) liczba $r_{3216}$ jest podzielna przez $M_{3217}$. Wymagało to kilku tysięcy podnoszeń do kwadratu, a potem dzieleń przez $M_{3217}$ liczb, mających nie więcej niż 969 cyfr, co istniejące maszyny elektronowe były w stanie wykonać. Wypiszemy tu tylko początkowe i końcowe cyfry tej liczby. Jest więc $M_{3217}$ = 2591170.....09315071. Wszystkie 969 cyfr tej liczby podane są w czasopiśmie Mathematical Tables and other Aids to Computation 12(1958) na str. 60. Podano tam też, że na stwierdzenie, że liczba $M_{3217}$ jest pierwszą, szwedzka maszyna elektronowa BESK zużyła 5,5godziny. Wypowiedziano przypuszczenie, że jeżeli liczba Mersenne'a $M_n$ jest pierwszą, to i liczba $M_{M_N}$

jest pierwszą. Sprawdza się to dla czterech najmniejszych liczb pierwszych Mersenne'a, ale już dla piątej z kolei liczby pierwszej Mersenne'a, tj. dla liczby $M_{13} = 8191$, jak obliczył w 1953 r. D. J. Wheeler, nie jest to prawdą, gdyż liczba $M_{M_{13}} = 2^{8191} - 1$ (mająca 2466 cyfr) jest złożoną.

Stwierdzenie tego (na mocy twierdzenia Lucas-Lehmera) wymagało stu godzin pracy maszyny elektronowej. Żadnego dzielnika pierwszego tej liczby złożonej nie znamy. Natomiast, w 1957 r. znaleziono, że mimo iż liczba $M_{17}$ jest pierwszą, liczba $M_{M_{17}}$ jest złożoną, podzielną przez $1768(2^{17} - 1)+ 1$, a także, że mimo, iż liczba $M_{19}$ jest pierwszą, liczba $M_{M_{19}}$ jest złożoną, podzielną przez $120(2^{19} - 1) + 1$

Wypowiedziano też przypuszczenie (dotąd nie obalone), że liczby $q_0, q_1, q_2 \ldots$ gdzie $q_0 = 2$, zaś $q_{n+1} = 2^{qn} - 1$ dla n = 0, 1, 2, ... są wszystkie pierwsze. Jest to prawdą dla liczb $q_n$, gdzie $n \leq 4$, ale liczba $q_5$ ma, jak łatwo obliczyć, więcej niż 1037 cyfr i przeto nie jesteśmy w możności jej wypisać, i tym bardziej sprawdzić, czy jest pierwszą, czy nie. Wspominaliśmy o związku liczb Mersenne'a z szukaniem liczb doskonałych parzystych. Otóż jeszcze Euklides podał następujący sposób otrzymywania wszystkich liczb doskonałych parzystych: Obliczajmy kolejne sumy wyrazów postępu geometrycznego 1, 2, $2^2$, $2^3$, ... Jeżeli suma taka okaże się liczbą pierwszą, to pomnożymy ją przez ostatni składnik. Otrzymamy liczbę doskonałą. Innymi słowy znaczy to, że wszystkie liczby doskonałe parzyste są postaci $2^{p-1} M_p$, gdzie $M_p$ jest liczbą pierwszą. (Prawdziwość tego twierdzenia została później udowodniona). Wynika stąd, że znamy tyle liczb doskonałych parzystych, ile znamy liczb pierwszych Mersenne'a, a więc obecnie 18. Najmniejszą liczbą doskonałą jest $2M_2 = 6$, największą znaną liczbą doskonałą jest $2^{3216}(2^{3217} - 1)$. Liczb doskonałych nieparzystych nie znamy: wiemy tylko, że jeżeli istnieją, to są bardzo wielkie. Co do liczb Mersenne'a, to wspomnimy jeszcze o tym, że F. Jakóbczyk wyraził przypuszczenie, że jeżeli p jest liczbą pierwszą, to liczba $M_p$ nie jest podzielna przez żaden kwadrat liczby pierwszej. A. Schinzel zaś postawił pytanie, czy istnieje nieskończenie wiele liczb Mersenne'a, które są iloczynami samych różnych liczb pierwszych.

**26. Liczby pierwsze w różnych ciągach nieskończonych**

Pytanie, czy dany ciąg nieskończony, nawet w prosty sposób określony, zawiera nieskończenie wiele liczb pierwszych, jest na ogół bardzo trudne. Jak już mówiliśmy o tym, nie wiemy, czy takie ciągi, jak $n^2 + 1$, $n! + 1$, $n! - 1$, $2^n + 1$, $2^n - 1$ (dla n= 1, 2, ...), zawierają nieskończenie wiele liczb pierwszych. Nie wiemy też, czy ciąg nieskończony 1, 11, 111, 1111, ... zawiera nieskończenie wiele liczb pierwszych. Podobnie jest z tak zwanym ciągiem Fibonacciego, $u_n(n = 1, 2, . ..)$, określonym przez warunki

$$u_1 = u_2 = 1, \text{ zaś } u_{n+2} = u_n + u_{n+1} \text{ (dla } n = 1, 2, 3, . ..)$$

Początkowymi wyrazami tego ciągu są liczby

$u_1 = 1$ ,$u_2 = 1$, $u_3 = 2$, $u_4 = 3$, $u_5 = 5$, $u_6 = 8$, $u_7 = 13$, $u_8 = 21$, .. .

Stwierdzono, że liczby $u_n$ są pierwsze dla n = 3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 71. Innych liczb pierwszych $u_n$ dotąd nie znamy. Największa ze znanych ma 15 cyfr: jest to liczba $u_n$ = 308061521 170129. Można dowieść, że jeżeli $n \neq 4$ i liczba $u_n$ jest pierwszą, to liczba n musi być pierwszą, ale niekoniecznie na odwrót, bo na przykład

$$u_2 = 1, u_{19} = 4181 = 37 \cdot 113, u_{31} = 1346269 = 557 \cdot 2417.$$

Nie wiemy, czy wśród liczb $u_p$, gdzie p jest liczbą pierwszą, jest nieskończenie wiele złożonych.

Badano też ciąg $v_n(n = 1, 2, ...)$, określony przez warunki

$$v_1 = 1, v_2 = 3, v_{n+2} = v_n + v_{n+1} \text{ dla } n = 1, 2,...$$

którego początkowymi wyrazami są liczby 1, 3, 4, 7, 11, 18, ... Liczby $v_n$ są pierwszymi dla n = 2, 4, 5, 7, 8, 11, 13, 17, 19, 31, 37, 41, 47, 53, 61. Największą ze znanych liczb pierwszych $v_n$ jest liczba $v_{61}$ = 5600748293801, mająca 13 cyfr. Nie wiemy, czy liczb pierwszych $v_n$ jest nieskończenie wiele. Podamy tu jeszcze jeden ciąg, którym w ostatnich latach zajmowało się kilku matematyków. Wyjdźmy z ciągu wszystkich kolejnych liczb nieparzystych: 1, 3, 5, 7, 9, 11, 13, 15, ... Oznaczmy $u_1 = 1$; w ciągu tym najmniejszą liczbą > $u_1$ jest $u_2 = 3$. Wykreślimy z naszego ciągu co trzecią liczbę (tj. liczby znajdujące się na miejscach, trzecim, szóstym, dziewiątym itd.). Otrzymamy w ten sposób nowy ciąg: 1, 3, 7, 9, 13, 15, 19, 21, 25, 27, ... Najmniejsza, liczbą naszego ciągu > 3 jest 7, którą oznaczymy $u_3$: wykreślimy teraz co siódmą liczbę w ostatnim ciągu, co da nam ciąg 1, 3, 7, 9, 13, 15, 21, 25, 27, ... Najmniejszą liczbą tego ciągu większą od $u_3$ jest 9, którą oznaczymy $u_4$.

Będziemy teraz wykreślali z ostatnio otrzymanego ciągu co dziewiątą liczbę. Jeżeli będziemy tak postępowali dalej, to otrzymamy ciąg nieskończony $u_1$, $u_2$, ..., którego wyrazami mniejszymi od stu będą 1, 3, 7, 9, 13, 15, 21, 25, 31, 33, 37, 43, 49, 51, 63, 67, 69, 73, 75, 79, 87, 93, 99. Liczby naszego ciągu nazwano szczęśliwymi. Nie wiemy, czy wśród tych liczb jest nieskończenie wiele pierwszych. Obliczono, że wśród liczb szczęśliwych, mniejszych od 98600, jest 715 liczb pierwszych.

**27. Rozwiązywanie równań w liczbach pierwszych**

Znamy wiele prostych równań (nawet stopnia 1-go), co do których nie wiemy, czy mają nieskończenie wiele rozwiązań w liczbach pierwszych. Takim, jest na przykład równanie $x + y = z$. Łatwo jest dowieść, że pytanie, czy równanie to ma nieskończenie wiele rozwiązań w liczbach pierwszych x, y, z, jest równoważne pytaniu, czy istnieje nieskończenie wiele par liczb pierwszych bliźniaczych. Jeżeli bowiem p, q i r są liczby pierwsze takie, iż $p + q = r$, to oczywiście liczby p i q nie mogą być obie nieparzyste (gdyż wtedy suma ich byłaby liczbą parzystą > 2, a więc złożoną). Jedna więc z liczb p i q, na przykład liczba q, jest parzystą, zatem = 2. Liczby p i $r = p + 2$ stanowiłyby więc parę liczb pierwszych bliźniaczych. Z drugiej strony, jeżeli liczby p i $r = p + 2$ stanowią parę liczb pierwszych bliźniaczych, to liczby $x = p$, $y = 2$, $z = p + 2$ są pierwsze i dają rozwiązanie równania $x + y = z$. Nie wiemy, czy równanie $2x + 1 = y$, albo równanie $2x - 1 = y$ ma nieskończenie wiele rozwiązań w liczbach pierwszych x, y, chociaż znamy dużo takich rozwiązań, na przykład dla równania $2x + 1 = y$, (x, y) = (2, 5), (3, 7), (5, 11), (11, 23), zaś dla równania $2x - 1 = y$, (x, y) = (2, 3), (3, 5), (7, 13), (19, 37).

Wypowiedziano przypuszczenie, że każde z naszych równań ma ich nieskończenie wiele.

Nie wiemy też, czy równanie $x + y + 1 = z$, ma nieskończenie wiele rozwiązań w liczbach pierwszych x, y, z, co wynika z przypuszczenia Goldbacha. Natomiast udowodniono, że równanie $x + y = z + t$ ma nieskończenie wiele rozwiązań w różnych liczbach pierwszych x, y, z, t, i podobnie równanie $x^2 + y^2 = z^2 + t^2$. Na przykład $7^2 + 19^2 = 11^2 + 17^2$. Łatwo jest natomiast dowieść, że równanie $x^2 + y^2 + z^2 = t^2$ nie ma żadnego rozwiązania w liczbach pierwszych x, y, z, t. Nie wiemy, czy istnieje nieskończenie wiele trójkątów prostokątnych o bokach naturalnych, z których dwa byłyby liczbami pierwszymi. Można dowieść, że pytanie to jest równoważne pytaniu, czy równanie $p^2 = 2q - 1$ ma nieskończenie wiele rozwiązań w liczbach pierwszych p i q. Przykładami takich trójkątów są trójkąty o bokach (3, 4, 5), (5, 12, 13), (11, 60, 61), (19, 180, 181), (29, 240, 241), (61, 1860, 1861).

Łatwo jest znaleźć wszystkie rozwiązania równania $x^2 - 2y^2 = 1$ w liczbach pierwszych x, y. Jeżeli bowiem liczby naturalne x, y spełniają równanie $x^2 = 2y^2 + 1$, to x jest oczywiście liczbą nieparzystą, $x = 2k + 1$, gdzie k jest całkowite, skąd $x^2 = 4k^2 + 4k + 1$, zatem $y^2 = 2k(k + 1)$ i y jest parzyste. Jeżeli więc y jest liczbą pierwszą, to $y = 2$, skąd wnosimy, że równanie nasze ma jedno tylko rozwiązanie w liczbach pierwszych: $x = 3$, $y = 2$. Nie wiemy natomiast, ile jest rozwiązań w liczbach pierwszych. x, y ma równanie $x^2 - 2y^2 = -1$. Znamy takie rozwiązania, na przykład $x = 7$, $y = 5$ lub $x = 41$, $y = 29$. Łatwo jest dowieść, że jeżeli n jest liczbą naturalną > 1, to równanie $p^n + q^n = r^n$ nie ma rozwiązań w liczbach pierwszych p, q, r.

Natomiast nie udowodniono dotąd przypuszczenia Fermata, że jeżeli p jest liczbą pierwszą nieparzystą, to równanie $x^p + y^p = z^p$ nie ma rozwiązań w liczbach naturalnych x, y, z (Udowodniono to dla liczb pierwszych nieparzystych $p < 4002$).

**28. Kwadraty magiczne utworzone z liczb pierwszych**

Kwadratem magicznym (w znaczeniu szerszym) o n wierszach nazywamy tablicę utworzoną z $n^2$ różnych liczb naturalnych wypisanych w n wierszy (i mającą tyleż kolumn), taką że suma liczb każdego wiersza, suma liczb każdej kolumny i suma liczb, znajdujących się na każdej z dwóch przekątnych głównych, są równe. Znamy kwadraty magiczne o trzech i o czterech wierszach, utworzone z samych liczb pierwszych.

Są to kwadraty

| | | |
|---|---|---|
| 569 | 59 | 449 |
| 239 | 359 | 479 |
| 269 | 659 | 149 |

| | | | |
|---|---|---|---|
| 17 | 317 | 397 | 67 |
| 307 | 157 | 107 | 227 |
| 127 | 277 | 257 | 137 |
| 347 | 47 | 37 | 367 |

W pierwszym z tych kwadratów sumy, o których mowa, są wszystkie = 1077, zaś w drugim są = 798. Wyrażono przypuszczenie, że dla każdej liczby naturalnej $n \geq 3$ istnieje nieskończenie wiele kwadratów magicznych (w znaczeniu szerszym), utworzonych z $n^2$ różnych liczb pierwszych.

**29. Kilka nie rozwiązanych zagadnień dotyczących liczb pierwszych**

1)

Nie wiemy, czy istnieje nieskończenie wiele par kolejnych liczb naturalnych, z których każda ma tylko jeden dzielnik pierwszy (jak na przykład pary 2 i 3, 3 i 4, 4 i 5, 7 i 8, 8 i 9, 16 i 17, 31 i 32). Znamy dotąd tylko 24 takie pary, z których największą jest para $2^{3217}$ -1 i $2^{3217}$ (Porówn. dalej 6). Potrafimy natomiast dowieść, że równanie $p^m - q^n = 1$, gdzie p i q są liczby pierwsze, zaś m i n - liczby naturalne > 1, ma tylko jedno rozwiązanie: p = 3, q = 2, m = 2, n= 3.

2)

Nie wiemy, czy istnieje nieskończenie wiele trójek kolejnych liczb naturalnych, z których każda jest iloczynem dwóch różnych liczb pierwszych. (Trójką taką jest na przykład 33 = 3 • 11, 34 = 2*17, 35 = 5 • 7, a także 93 = 3 • 31, 94 = 2 • 47, 95 = 5 • 19). Wypowiedziano przypuszczenie, że takich trójek jest nieskończenie wiele.

3)

Nie wiemy, czy istnieje nieskończenie wiele liczb pierwszych p takich, że dla każdego naturalnego $n < p - 1$ liczba $2^n$ przy dzieleniu przez p daje resztę różną od 1 (Takimi są na przykład liczby pierwsze 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83). Wypowiedziano przypuszczenie, że takich liczb pierwszych p jest nieskończenie wiele.

4)

Nie wiemy, czy z każdej liczby naturalnej $n \geq 10$, przez zmianę dwóch jej cyfr można otrzymać liczbę pierwszą. (Dla liczb dwucyfrowych jest to oczywiste. Dla liczb trzycyfrowych wynika to na przykład stąd, że pierwszymi są liczby 101, 211, 307, 401, 503, 601, 701, 809, 907).

5)

Nie wiemy, czy prawdziwe jest przypuszczenie A. Schinzla, że dla każdej liczby rzeczywistej $x \geq 117$ istnieje co najmniej jedna liczba pierwsza p, leżąca między x a $x + \sqrt{x}$. Przypuszczenie to A. Scliinzel sprawdził dla wszystkich liczb x takich, iż $117 \leq x < 2 \cdot 10^7$.

6)

Łatwo jest dowieść, że wśród każdych sześciu kolejnych liczb naturalnych co najmniej jedna ma co najmniej dwa różne dzielniki pierwsze (gdyż zawsze jedna jest podzielna przez 6, a więc ma dzielniki pierwsze 2 i 3). Można też dowieść, iż spośród każdych trzech kolejnych liczb naturalnych > 7 co najmniej jedna ma co najmniej dwa różne dzielniki pierwsze. Nie wiemy natomiast, czy spośród każdych dwóch dostatecznie wielkich kolejnych liczb naturalnych co najmniej jedna ma co najmniej dwa różne dzielniki pierwsze. Innymi słowy, nie wiemy, czy istnieje liczba naturalna m taka, że dla $n \geq m$ co najmniej jedna z liczb naturalnych n i n + 1 ma co najmniej dwa różne

dzielniki pierwsze. Wiemy tylko, że jeżeli takie m istnieje, to musi być $m \geq 2^{3217}$, gdyż z liczb $2^{3217} - 1$ i $2^{3217}$ każda ma tylko jeden dzielnik pierwszy. Udowodniono też, że z przypuszczenia, że taka liczba to istnieje, wynikałoby, że istnieje tylko skończona liczba liczb pierwszych Fermata i tylko skończona liczba liczb pierwszych Mersenne'a.

**30. Przypuszczenie A. SCHINZLA**

Wielomian zmiennej x o współczynnikach całkowitych nazywamy nieprzywiedlnym, jeżeli nie jest iloczynem dwóch wielomianów (niższych od niego stopni) o współczynnikach całkowitych.

Co do wielomianów o współczynnikach całkowitych zmiennej x, f(x), nasuwa się pytanie, kiedy taki wielomian dla naturalnych wartości x daje nieskończenie wiele liczb pierwszych. Łatwo jest dowieść, że warunkiem koniecznym jest tu, żeby wielomian był nieprzywiedlny. Warunek ten nie jest jednak wystarczający, bo jak łatwo dowieść, wielomian $x^2 + x + 2$ jest nieprzywiedlny, a dla żadnej liczby naturalnej x nie daje liczby pierwszej, gdyż dla każdej liczby naturalnej x wartość jego jest liczbą parzystą > 2. Łatwo też dowieść, że oprócz nieprzywiedlności, wielomian f(x) musi spełniać jeszcze następujący warunek:

Niee ma żadnej liczby naturalnej > 1, która by była dzielnikiem liczby f(x) dla każdej wartości całkowitej x. Czy warunki te są wystarczające na to, żeby wielomian f(x) o współczynnikach całkowitych, gdzie współczynnik przy najwyższej potędze x jest dodatni, dawał nieskończenie wiele liczb pierwszych dla naturalnych x ? W ubiegłym stuleciu W. Buniakowski wyraził przypuszczenie, że tak jest. Z przypuszczenia tego wynika natychmiast, że istnieje nieskończenie wiele liczb pierwszych postaci $x^2 + 1$, gdzie x jest liczbą naturalną, i ogólniej, dla każdych danych liczb naturalnych m nieparzystego i k istnieje nieskończenie wiele liczb pierwszych postaci $x^{2m} + k$, gdzie x jest liczbą naturalną.

Z omawianego przypuszczenia wynika też natychmiast, że istnieje nieskończenie wiele liczb naturalnych x, dla których $x^2 + x + 41$ jest liczbą pierwszą.A. Schinzel wypowiedział następujące ogólniejsze przypuszczenie **P**.

**P.** Jeżeli s jest liczbą naturalną, zaś $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ są wielomiany o całkowitych współczynnikach, mające współczynnik dodatni przy najwyższych potęgach x, nieprzywiedlne i spełniające następujący warunek **S**:

**S**. Nie ma liczby naturalnej > 1, która by była dzielnikiem iloczynu $f_1(x)\ f_2(x)...f_s(x)$ dla każdej wartości całkowitej x,to istnieje nieskończenie wiele liczb naturalnych x, dla których każda z liczb $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ jest pierwszą.

Niech w szczególności s = 2, $f_1(x) = x$, $f_2(x) = x + 2k$, gdzie 2k jest daną liczbą naturalną parzystą. Mamy tu

/x(l) /2(l) = l + 2k, zaś/x(— 1) /2(— 1) = 1 - 2k. Gdyby istniała liczba naturalna d > 1 taka, iż d | $f_1(x)\ f_2(x)$ dla każdej liczby całkowitej x, to musiałoby być d | 2k - 1 oraz d | 2k + 1, co niemożliwe, gdyż jak wiadomo, dwie kolejne liczby nieparzyste 2k - 1 i 2k + 1 nie mają żadnego dzielnika wspólnego większego od jedności. Warunek S jest tu więc spełniony i z przypuszczenia P wynika, że istnieje nieskończenie wiele liczb naturalnych x takich, że liczby $f_l(x)$ oraz $f_2(x)$ są pierwsze, że więc x = p, x + 2k = q, gdzie p i q są liczby pierwsze, skąd 2k = q -p. Z przypuszczenia P wynika więc, że każda liczba naturalna parzysta daje się na nieskończenie wiele sposobów przedstawić jako różnica dwóch liczb pierwszych. W szczególności dla k = 1 wynika stąd istnienie nieskończenie wielu par liczb pierwszych bliźniaczych. Wiele jeszcze innych twierdzeń o liczbach pierwszych (których dotąd nie udowodniono) daje się wyprowadzić z przypuszczenia P A. Schinzla.