ĆWICZENIA DO RÓŻNYCH ROZDZIAŁÓW

1. Dowieść następującego twierdzenia D. Pompeiu [1]): Na to żeby liczba naturalna n była złożona, potrzeba i wystarcza, żeby była sumą czterech liczb naturalnych:

$$(*) \quad n=a+b+c+d, \qquad \text{gdzie} \qquad (**) \quad a:b=c:d.$$

Dowód. Jeżeli n jest liczbą złożoną, to istnieją takie liczby naturalne r i s, że $n=(r+1)(s+1)$. Liczby

$$a=rs, \quad b=r, \quad c=s, \quad d=1$$

spełniają wzory (*) i (**). Warunek jest więc konieczny.

Na odwrót, jeżeli liczby naturalne a, b, c i d spełniają wzory (*) i (**), to ze wzorów tych znajdujemy

$$bn=ab+bb+cb+db=ab+bb+ad+db=(a+b)(b+d).$$

Nadto ze wzoru (*) wynika, że $n>a+b$ i $n>b+d$. Liczba n nie jest więc dzielnikiem żadnej z liczb $a+b$ i $b+d$, których iloczyn bn jest podzielny przez n. Wynika stąd, że n nie jest liczbą pierwszą, a że na mocy (*) jest $n>1$, więc liczba n jest złożona. Warunek jest zatem wystarczający.

2. Dowieść, że na to, by liczba naturalna a była złożona, potrzeba i wystarcza, żeby istniały takie liczby naturalne b i c, że

$$(*) \quad c|ab \qquad \text{i} \qquad (**) \quad a>c>b.$$

Dowód. Jeżeli a jest liczbą złożoną, to istnieją takie liczby naturalne $m>1$ i $n>1$, że $a=mn$. Liczby $c=m$ i $b=1$ spełniają wzory (*) i (**), gdyż $a=mn>m=c>1=b$. Warunek jest więc konieczny.

Na odwrót, przypuśćmy, że a jest liczbą pierwszą. Gdyby było $(a,c)=1$, to wobec (*) byłoby $c|b$, wbrew (**). Jest więc $(a,c)>1$ i, skoro a jest liczbą pierwszą, musi być $a|c$, znowu wbrew (**). Warunek jest więc dostateczny.

---

[1]) Zostało mi ono nadesłane w liście z pozwoleniem umieszczenia w niniejszej książce.

3. Korzystając z cech podzielności przez 7, 11 i 13, dowieść, że $7\cdot 11\cdot 13 \mid 10^{15}+1$.

4. Rozłożyć na czynniki pierwsze liczbę 99999999.

Odpowiedź: $10^8-1=3^2\cdot 11\cdot 73\cdot 101\cdot 137$.

5. M. Boll i J. Reinhart [1]) piszą, że każda liczba postaci $1+p_1p_2\ldots p_n$ (gdzie p_n oznacza n-tą z kolei liczbę pierwszą) jest pierwsza. Dowieść na trzech różnych przykładach, że jest to błędne.

Odpowiedź. Łatwo sprawdzić, że

$$59 \mid 1+p_1p_2\ldots p_6, \qquad 19 \mid 1+p_1p_2\ldots p_7, \qquad 347 \mid 1+p_1p_2\ldots p_8.$$

6. Dowieść, że jeżeli do dowolnej liczby czterocyfrowej (napisanej w układzie dziesiętnym) dopisać tę samą liczbę, to otrzymana w ten sposób liczba ośmiocyfrowa jest podzielna przez 137.

Dowód wynika z tożsamości $10^4n+n=137\cdot 73\cdot n$.

7. Dowieść, że liczby 2, 3, 5 i 7 oraz wszystkie liczby naturalne x pierwszej setki, niepodzielne przez żadną z tych czterech liczb, są wszystkimi liczbami pierwszymi pierwszej setki.

Dowód wynika stąd, że 2, 3, 5 i 7 są wszystkimi liczbami pierwszymi niewiększymi od $\sqrt{100}$ (Ob. twierdzenie 10, str. 15).

8. Dowieść, że jeżeli najmniejszy dzielnik pierwszy p liczby naturalnej n spełnia nierówności $\sqrt[3]{n}<p<n$, to liczba n/p jest pierwsza [2]).

Dowód. Wobec $p<n$ jest $n/p>1$. Gdyby liczba n/p była złożona, byłoby $n=pab$, gdzie $a>1$ i $b>1$. Oznaczając przez q i r odpowiednio dzielniki pierwsze liczb a i b, mielibyśmy $q\geqslant p$ i $r\geqslant p$ na mocy założenia, że p jest najmniejszym dzielnikiem pierwszym liczby n; stąd zaś wobec $a\geqslant q$ i $b\geqslant r$ otrzymalibyśmy $n=pab\geqslant pqr\geqslant p^3$, wbrew nierówności $\sqrt[3]{n}<p$.

9. Dowieść, że jeżeli $p>2$ jest liczbą pierwszą i p liczb pierwszych różnych od p tworzy postęp arytmetyczny, to różnica tego postępu jest podzielna przez każdą liczbę pierwszą niewiększą od p.

---

[1]) Ob. cytowaną już na str. 167 książkę *Les grands courants de la pensée mathématique, présentés par F. Le Lionnais*, Cahiers du Sud, 1948, str. 353.

[2]) Ob. O. Ore, *Number Theory and its History*, New York-Toronto-Londyn 1948, str. 52.

Dowód. Niech liczby pierwsze $q, q+d, \ldots, q+(p-1)d$ tworzą postęp arytmetyczny. Gdyby różnica d tego postępu nie była podzielna przez p, mielibyśmy $(p,d)=1$ i wobec założenia, że $q\neq p$, istniałaby w ciągu $1,2,\ldots,p-1$ w myśl twierdzenia 2 z Rozdziału III (§ 5, str. 52) taka liczba k, że $kd\equiv -q \pmod p$, skąd $p \mid q+kd$ i liczba $q+kd>p$ nie byłaby pierwsza.

Niech teraz $r<p$ będzie liczbą pierwszą. Gdyby d nie było podzielne przez r, mielibyśmy $(r,d)=1$ i istniałaby w ciągu $0,1,2,\ldots,r-1$ taka liczba k, że $kd\equiv -q \pmod r$, skąd $r \mid q+kd$ i liczba $q+kd\geqslant p>r$ nie byłaby pierwsza. Liczba d jest więc podzielna przez każdą liczbę pierwszą $r\leqslant p$, c. b. d. o.

Uwaga. Moritz Cantor przypuszczał (w 1861 r.) że poza trójką liczb 3, 5, 7, nie ma kolejnych liczb pierwszych, tworzących postęp arytmetyczny. Nie kolejne istnieją: np.

31, 37, 43; 41, 47, 53, 59; 61, 67, 73, 79.

10. Niech $m>1$ i $s>m/2$ będą liczbami naturalnymi oraz $a_1, a_2, \ldots, a_s$ — ciągiem różnych reszt modulo m. Dowieść, że każda liczba całkowita przystaje według modułu m do sumy dwu liczb z ciągu $a_1, a_2, \ldots, a_s$ (niekoniecznie różnych).

Dowód. Niech k będzie liczbą całkowitą. Reszty modulo m liczb ciągu $k-a_1, k-a_2, \ldots, k-a_s$ są wszystkie różne. Gdyby były one różne od każdej z liczb $a_1, a_2, \ldots, a_s$, mielibyśmy razem $2s>m$ różnych reszt modulo m, co niemożliwe. Istnieją zatem takie liczby naturalne $i\leqslant s$ i $j\leqslant s$, że $k-a_i\equiv a_j \pmod m$, skąd $k\equiv a_i+a_j \pmod m$, c. b. d. o.

11. Niech n będzie liczbą naturalną. Ile co najwyżej liczb może zawierać zbiór Z liczb naturalnych nie większych od $2n$, z których żadna nie jest podzielna przez żadną inną?

Odpowiedź: n.

Dowód. Oznaczmy dla $k=1,2,\ldots,n$ przez G_k zbiór wszystkich liczb naturalnych niewiększych od $2n$, które są postaci $2^{r-1}(2k-1)$, gdzie r jest liczbą naturalną. Żadne dwa ze zbiorów $G_1, G_2, \ldots, G_n$ nie mają — jak łatwo widzieć — elementów wspólnych. Łatwo też widzieć, że zbiór $G_1+G_2+\ldots+G_n$ jest zbiorem wszystkich liczb naturalnych niewiększych od $2n$, gdyż jeżeli $2k-1$ jest największym dzielnikiem nieparzystym liczby $l\leqslant 2n$, to l należy do zbioru G_k.

Dla każdego $k=1,2,\ldots,n$ z dwu różnych liczb zbioru G_k zawsze większa jest podzielna przez mniejszą. Skoro więc na mocy określenia zbioru Z żadna z jego liczb nie jest podzielna przez żadną inną, to dla każdego $k=1,2,\ldots,n$ zbiór Z może zawierać co najwyżej jedną liczbę ze zbioru G_k. Ponieważ zbiór Z jest zawarty w zbiorze $G_1+G_2+\ldots+G_n$, który — jak widzieliśmy — jest zbiorem wszystkich liczb naturalnych niewiększych od $2n$, więc zbiór Z może się składać co najwyżej z n elementów.

Z drugiej strony, zbiór n liczb naturalnych

$$n+1,\quad n+2,\quad \ldots,\quad 2n,$$

ma oczywiście tę własność, że żadna z należących do niego liczb nie jest podzielna przez żadną inną liczbę tego zbioru.

Uwaga. Dla $n=100$ otrzymujemy stąd wniosek: jeżeli z dwustu liczb $1,2,3,\ldots,200$ wybrano dowolnie 101 liczb, to wśród wybranych liczb znajdują się zawsze takie dwie, z których jedna jest podzielna przez drugą [1]).

Inny łatwy wniosek: każdy zbiór Z liczb naturalnych niewiększych od $2n+1$, z których żadna nie jest podzielna przez żadną inną, zawiera co najwyżej $n+1$ liczb. Że zaś może ich zawierać $n+1$, wynika stąd, że z $n+1$ liczb

$$n+1,\quad n+2,\quad \ldots,\quad 2n,\quad 2n+1$$

żadna nie jest podzielna przez żadną inną.

12. Niech n będzie liczbą naturalną. Dowieść, że zbiór Z liczb naturalnych niewiększych od n, z których każde dwie są względnie pierwsze, zawiera co najwyżej $\pi(n)+1$ liczb i dać przykład takiego zbioru Z o $\pi(n)+1$ elementach.

Dowód wynika stąd, że dwie liczby względnie pierwsze, o ile są obie większe od 1, muszą posiadać różne dzielniki pierwsze. Żądanym przykładem jest zbiór Z złożony z liczby 1 i wszystkich liczb pierwszych niewiększych od n.

13. Wypisać wszystkie zbiory o $\pi(10)+1$ elementach, utworzone z liczb naturalnych pierwszej dziesiątki, z których każde dwie są względnie pierwsze.

Odpowiedź: $1,\ 2,\ 3,\ 5,\ 7,\quad 1,\ 2^2,\ 3,\ 5,\ 7,\quad 1,\ 2^3,\ 3,\ 5,\ 7.$
$1,\ 2,\ 3^2,\ 5,\ 7,\quad 1,\ 2^2,\ 3^2,\ 5,\ 7,\quad 1,\ 2^3,\ 3^2,\ 5,\ 7.$

[1]) Daje to rozwiązanie zadania 20, umieszczonego w czasopiśmie „Matematyka", zeszyt 1, 1948, str. 61 (por. też uwagę w zeszycie 2, 1948, str. 53, oraz rozwiązanie w zeszycie 2, 1949, str. 53).

14. Ile jest różnych zbiorów o $\pi(100)+1$ elementach, utworzonych z liczb naturalnych pierwszej setki, z których każde dwie są względnie pierwsze?

Odpowiedź: $6\cdot4\cdot2\cdot2=96$.

15. Dowieść, że dla każdej liczby naturalnej $m>2$ istnieje nieskończenie wiele liczb pierwszych, które nie są postaci $mk+1$ (dla $k=0,1,2,\ldots$).

Dowód. Niech n będzie dowolną liczbą naturalną. Ponieważ $m>2$, więc $m\cdot n!-1>1$; liczba ta może zatem być przedstawiona jako iloczyn samych czynników pierwszych większych od n, gdyż jest ona niepodzielna przez żadną z liczb pierwszych $p\leqslant n$ (bo przy dzieleniu przez $p\leqslant n$ daje resztę $p-1$). Gdyby każdy z tych czynników pierwszych był postaci $mk+1$, to również ich iloczyn byłby tej postaci i mielibyśmy $mn!-1=mk+1$, skąd wynikałoby, że $m|2$, co niemożliwe wobec $m>2$. Dowiedliśmy więc, że dla $m>2$ liczba $m\cdot n!-1$ ma dla każdej liczby naturalnej n co najmniej jeden czynnik pierwszy większy od n i nie będący postaci $mk+1$. Stąd już wynika istnienie nieskończenie wielu liczb pierwszych, nie będących tej postaci, c. b. d. d.

16. Dowieść, że dla wszelkich liczb naturalnych a, b, l i m, spełniających warunki

$$(*)\quad (l,m)=1 \qquad \text{i} \qquad (**)\quad a^l=b^m,$$

istnieje taka liczba naturalna n, że $a=n^m$ i $b=n^l$.

Dowód. Jest to oczywiste dla $a=1$ (gdyż wówczas też $b=1$). Załóżmy więc, że $a>1$, skąd wynika też wobec $a^l=b^m$, że i $b>1$. Wobec (**) liczby a i b mają te same czynniki pierwsze. Niech

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k} \qquad \text{i} \qquad b=p_1^{\beta_1}p_2^{\beta_2}\ldots p_k^{\beta_k}.$$

Jest zatem wobec (**)

$$p_1^{l\alpha_1}p_2^{l\alpha_2}\ldots p_k^{l\alpha_k}=p_1^{m\beta_1}p_2^{m\beta_2}\ldots p_k^{m\beta_k},$$

skąd $p_i^{l\alpha_i}=p_i^{m\beta_i}$ dla $i=1,2,\ldots,k$, a przeto $l\alpha_i=m\beta_i$. Wobec (*) mamy stąd $\alpha_i=m\gamma_i$, gdzie γ_i jest liczbą naturalną; zatem $lm\gamma_i=m\beta_i$, skąd $\beta_i=l\gamma_i$. Dla $n=p_1^{\gamma_1}p_2^{\gamma_2}\ldots p_k^{\gamma_k}$ wynika stąd z łatwością, że $a=n^m$ i $b=n^l$, c. b. d. o.

17. Znaleźć wszystkie liczby naturalne n, dla których liczba 2^n+1 jest podzielna przez 9.

Odpowiedź. Są to liczby naturalne postaci $6k+3$, gdzie k jest liczbą całkowitą. Jest bowiem $2^6 \equiv 1 \pmod 9$, skąd $2^{6k} \equiv 1 \pmod 9$. Liczby postaci

$$2^{6k+1}, \quad 2^{6k+2}, \quad 2^{6k+3}, \quad 2^{6k+4} \quad \text{i} \quad 2^{6k+5}$$

przystają więc modulo 9 odpowiednio do

$$2, \quad 4, \quad -1, \quad -2 \quad \text{i} \quad -4.$$

Zatem dla liczb naturalnych $n=6k+3$ i tylko dla nich zachodzi kongruencja $2^n \equiv -1 \pmod 9$, c. b. d. o.

18. Biorąc pod uwagę, że $7381 = 11^2 \cdot 61$, dowieść, że

$$3^{7380} \equiv 1 \pmod{7381}.$$

Dowód. $3^5 = 243 \equiv 1 \pmod{11^2}$, skąd $3^{7380} = (3^5)^{1476} \equiv 1 \pmod{11^2}$, a w myśl małego twierdzenia Fermata jest $3^{60} \equiv 1 \pmod{61}$, skąd $3^{7380} = (3^{60})^{123} \equiv 1 \pmod{61}$. Liczba $3^{7380}-1$ jest zatem podzielna przez 11^2 i przez 61, a więc wobec $(11, 61) = 1$ również przez ich iloczyn 7381, c. b. d. o.

19. Rozwiązać kongruencję

$$(*) \quad 2^x = x^2 \pmod 3.$$

Rozwiązanie. Wobec $2^2 \equiv 1 \pmod 3$ jest $2^{x+2k} \equiv 2^x \pmod 3$ dla wszelkich $x \geqslant 0$ całkowitych i dla $k = 0, 1, 2, \ldots$, a ponieważ $(x+3l)^2 \equiv x^2 \pmod 3$ dla wszelkich l całkowitych, więc jeżeli x jest pierwiastkiem kongruencji $(*)$, to jest nim też każda liczba postaci $x+6t$, gdzie $t = 0, 1, 2, \ldots$

Spośród liczb $0, 1, 2, \ldots, 5$ pierwiastkami kongruencji $(*)$ są tylko liczby 2 i 4. Wszystkimi jej pierwiastkami są więc liczby postaci $2+6t$ i $4+6t$, gdzie $t = 0, 1, 2, \ldots$

Uwaga. Liczba, przystająca do pierwiastka kongruencji $(*)$ według jej modułu, może więc nie być pierwiastkiem tej kongruencji, np. liczba 5.

20. Rozwiązać kongruencję $2^x \equiv x^2 \pmod 5$.

Odpowiedź: $x \equiv a+20t$, gdzie a jest którąkolwiek z liczb 2, 4, 16 i 18, a $t = 0, 1, 2, \ldots$

21. Rozwiązać kongruencję $2^x \equiv 3^x \pmod 7$.

Odpowiedź: $x = 6t$, gdzie $t = 0, 1, 2, \ldots$

22. Dowieść, że jeżeli liczby naturalne a i b spełniają kongruencję $a \equiv b \pmod 6$, to $a^a \equiv b^b \pmod 6$.

23. Znaleźć wszystkie pierwiastki naturalne kongruencji $x^x \equiv 3 \pmod 7$.

Odpowiedź: $x = 5+42t$ i $x = 31+42t$, gdzie $t = 0, 1, 2, \ldots$

24. Znaleźć wszystkie pierwiastki naturalne kongruencji $x^x \equiv 5 \pmod 7$.

Odpowiedź: $x = 17+42t$ i $x = 19+42t$, gdzie $t = 0, 1, 2, \ldots$

25. Dowieść, że na to, by liczba naturalna x spełniała kongruencję $x^x+1 \equiv 0 \pmod 7$, potrzeba i wystarcza, żeby liczba ta przystawała modulo 42 do jednej z liczb 13, 27, 33 i 41.

26. Znaleźć wszystkie rozwiązania kongruencji $x \equiv a \pmod x$ w liczbach naturalnych, gdzie a jest daną liczbą naturalną.

Odpowiedź. Są to wszystkie dzielniki naturalne liczby a.

27. Dowieść, że kongruencja $x^2 \equiv 1 \pmod x$ nie ma rozwiązań w liczbach naturalnych większych od 1.

28. Znaleźć wszystkie rozwiązania kongruencji $2^x \equiv x^2 \pmod x$ w liczbach naturalnych.

Odpowiedź: $x = 2^k$, gdzie $k = 0, 1, 2, \ldots$

29. Ile rozkładów na sumę dwu liczb pierwszych ma liczba 48 (jeżeli nie uważać za różne rozkładów, różniących się tylko porządkiem składników)?

Odpowiedź: 5; są to rozkłady:

$$48 = 5+43 = 7+41 = 11+37 = 17+31 = 19+29.$$

30. Dowieść, że liczba $n = 1729$ jest złożona, a jednak ma tę własność, że $a^{n-1} \equiv 1 \pmod n$ dla $(a, n) = 1$.

Wskazówka: $1729 = 7 \cdot 13 \cdot 19$; zastosować rozumowanie ze str. 60.

31. Dowieść, że jeżeli p jest liczbą pierwszą nieparzystą, to $p \mid (p-3)! + 2^{p-2}$.

Wskazówka. Zastosować twierdzenia Wilsona i Fermata.

32. Dowieść, że istnieje nieskończenie wiele liczb złożonych postaci $n!+1$ jako też postaci $n!-1$.

Dowód. Z twierdzenia Wilsona wynika, że dla liczb pierwszych p jest $(p-1)!+1 \equiv 0 \pmod p$, a więc liczba $(p-1)!+1$ jest złożona dla każdej liczby pierwszej $p > 3$. Z tego zaś, że $(p-2)!(p-1)+1 \equiv 0 \pmod p$, wynika, że $(p-2)!-1 \equiv 0 \pmod p$, a więc liczba $(p-2)!+1$ jest złożona dla każdej liczby pierwszej $p \geqslant 7$.

33. Dać przykład wielomianu $W(x)$ o współczynnikach całkowitych, który jest *podzielny arytmetycznie* przez daną liczbę pierwszą p, tj. dla wszelkich wartości całkowitych x ma wartość podzielną przez p, ale który nie jest *podzielny algebraicznie* przez p, tj. nie jest tożsamościowo równy iloczynowi liczby p przez wielomian o współczynnikach całkowitych.

Odpowiedź: $W(x)=x^p-x$.

Na mocy małego twierdzenia Fermata jest bowiem $p|x^p-x$ dla wszelkich x całkowitych, natomiast — jak wiadomo z Algebry — nie może być tożsamościowo $x^p-x=pW_1(x)$, gdzie $W_1(x)$ jest wielomianem o współczynnikach całkowitych, gdyż współczynnik przy najwyższej potędze x po stronie prawej jest podzielny przez p, a po lewej nie.

34. Dowieść, że liczba a, która w układzie dziesiętnym wyraża się za pomocą 91 jedynek napisanych jedna po drugiej, jest liczbą złożoną.

Dowód. Po pomnożeniu liczby a przez 9 i dodaniu jedności otrzymujemy oczywiście 10^{91}. Zatem $a=\frac{10^{91}-1}{9}$. Lecz liczba $10^{91}-1=10^{7\cdot 13}-1$ jest podzielna przez 10^7-1. Zatem a jest podzielne przez $\frac{10^7-1}{9}=1111111$.

35. Dowieść, że liczba 11111 jest złożona.

Dowód: jest ona podzielna przez 41.

36. Zbadać, które z wyrazów ciągu nieskończonego

$$101, \quad 10101, \quad 1010101, \quad \ldots$$

są pierwsze.

Odpowiedź. Tylko pierwszy.

Dowód. 101 jest liczbą pierwszą. Niech a_n będzie n-tym wyrazem ciągu. Jak łatwo widzieć, jest $a_n=\frac{10^{2(n+1)}-1}{99}$ Dla $n>1$ nieparzystych liczba $10^{n+1}-1$ jest podzielna przez 9 i przez 11, zatem przez 99 i

$$a_n=\frac{10^{n+1}-1}{99}\cdot(10^{n+1}+1)$$

jest rozkładem liczby a_n na iloczyn dwu liczb naturalnych większych od jedności. Jeżeli zaś n jest liczbą parzystą, to $9|10^{n+1}-1$, $11|10^{n+1}+1$, a zatem $a_n=\frac{10^{n+1}-1}{9}\cdot\frac{10^{n+1}+1}{11}$ jest rozkładem liczby a_n na iloczyn dwu liczb naturalnych większych od 1.

37. Dowieść, że wszystkie wyrazy ciągu nieskończonego

$$1001, \quad 1001001, \quad 1001001001, \quad \ldots$$

są liczbami złożonymi.

Dowód. Niech a_n będzie n-tym wyrazem tego ciągu; zatem

$$a_n=\frac{10^{3(n+1)}-1}{10^3-1}=\frac{(10^{n+1}-1)(10^{2(n+1)}+10^{n+1}+1)}{10^3-1}.$$

Jeżeli $n>2$, to $10^{n+1}-1>10^3-1$ i przeto $\frac{10^{n+1}-1}{(10^{n+1}-1,10^3-1)}$ jest dzielnikiem liczby a_n większym od 1, a mniejszym od a_n. Liczby a_n są więc złożone dla $n>2$. Lecz i liczby $a_1=1001$ oraz $a_2=1001001$ są złożone, gdyż pierwsza z nich jest podzielna przez 7, druga zaś — przez 3.

38. Dowieść, że wszystkie wyrazy ciągu nieskończonego

$$10001, \quad 100010001, \quad 1000100010001, \quad \ldots$$

są złożone.

Dowód: $a_1=73\cdot 137$, $3|a_2$ i $a_3=10001\cdot 100000001$, a dla $n>3$ dowodzimy podobnie jak w ćwiczeniu 37, że a_n jest liczbą złożoną.

39. Wyrazić za pomocą funkcji liczbowej $E(t)$ liczbę $f(x)$ liczb naturalnych niewiększych od x i mających co najmniej jeden dzielnik pierwszy mniejszy od 10, oraz obliczyć granicę

$$\lim_{x=\infty}\frac{f(x)}{x}.$$

Odpowiedź: $$f(x)=E\left(\frac{x}{2}\right)+E\left(\frac{x}{3}\right)+E\left(\frac{x}{5}\right)+E\left(\frac{x}{7}\right)-$$
$$-E\left(\frac{x}{6}\right)-E\left(\frac{x}{10}\right)-E\left(\frac{x}{14}\right)-E\left(\frac{x}{15}\right)-E\left(\frac{x}{21}\right)-E\left(\frac{x}{35}\right)+$$
$$+E\left(\frac{x}{30}\right)+E\left(\frac{x}{42}\right)+E\left(\frac{x}{70}\right)+E\left(\frac{x}{105}\right)-E\left(\frac{x}{210}\right).$$

$$\lim_{x=\infty}\frac{f(x)}{x}=\frac{27}{35}.$$

40. Dowieść wzoru

$$\pi(x)=1+\sum_{n=3}^{E(x)}\left\{1-\lim_{m=\infty}\left[1-\prod_{k=2}^{n-1}\left(\sin\frac{n\pi}{k}\right)^2\right]^m\right\}$$

dla liczb rzeczywistych $x\geqslant 2$.

41. Dowieść niewymierności liczby $\log_{10}2$.

Dowód. Gdyby liczba $\log_{10}2$ była ułamkiem nieprzywiedlnym l/m (gdzie l i m są liczbami naturalnymi, gdyż $\log_{10}2>0$), to byłoby $10^l=2^m$, co niemożliwe, gdyż lewa strona jest podzielna przez 5, a prawa nie.

42. Wyznaczyć wszystkie liczby wymierne dodatnie x, dla których $\log_{10}x$ jest liczbą wymierną.

Odpowiedź: $x=10^k$, gdzie k jest liczbą całkowitą.

43. Znaleźć wszystkie rozwiązania równania

$$(\overset{*}{**})\quad 3^n-2^m=1$$

w liczbach naturalnych m i n (por. ćwiczenie 9, str. 44) [1].

Rozwiązanie. Niech liczby naturalne m i n spełniają równanie $(\overset{*}{**})$.

Jeżeli $n=2k+1$, to wobec $3^{2k}\equiv 1 \pmod 4$ jest $3^{2k+1}\equiv 3 \pmod 4$, skąd $2^m=3^n-1=3^{2k+1}-1\equiv 2 \pmod 4$, a zatem $2^m\equiv 2 \pmod 4$, co dowodzi, że $m\leqslant 1$ czyli $m=1$.

Jeżeli zaś $n=2k$, to $2^m=3^n-1=3^{2k}-1=(3^k-1)(3^k+1)$, skąd wynika, że $3^k+1\mid 2^n$; liczba 3^k+1 jest więc potęgą dwójki.

Niech $3^k+1=2^l$; wynika stąd (p. str. 44, ćwiczenie 9), że $k=1$; zatem $n=2$ i $m=3$.

Równanie $(\overset{*}{**})$ ma więc w liczbach naturalnych m i n tylko rozwiązania: $m=1$, $n=1$ i $m=3$, $n=2$.

44. Dowieść, że jeżeli x, y i z są liczbami wymiernymi nieujemnymi, to dla wymierności liczby $\sqrt{x}+\sqrt{y}+\sqrt{z}$ potrzeba i wystarcza, żeby każda z liczb x, y i z była kwadratem liczby wymiernej.

[1]) Por. G. Berger i E. Trost, *Elemente der Mathematik*, tom 4 (1949), str. 17, zadanie 36.

Dowód. Dostateczność warunku jest oczywista. Aby dowieść jego konieczności, załóżmy, że $\sqrt{x}+\sqrt{y}+\sqrt{z}=w\geqslant 0$, gdzie w jest liczbą wymierną. Zatem $\sqrt{x}+\sqrt{y}=w-\sqrt{z}$, skąd

$$(*)\qquad x+y+2\sqrt{xy}=w^2+z-2w\sqrt{z},$$

a więc $2\sqrt{xy}=w^2+z-x-y-2w\sqrt{z}$, skąd

$$(**)\qquad 4xy=(w^2+z-x-y)^2+4w^2z-4w(w^2+z-x-y)\sqrt{z}.$$

Gdyby było $w=0$, mielibyśmy $x=y=z=0=0^2$. Gdyby zaś było $w^2+z-x-y=0$, mielibyśmy $2\sqrt{xy}=-2w\sqrt{z}$ wobec $(*)$, co w razie $w\neq 0$ daje $xy=0$ i $z=0$, zatem albo $x=z=0$, skąd $y=w^2$, albo $y=z=0$, skąd $x=w^2$. Możemy więc przyjąć, że $w\neq 0$ i $w^2+z-x-y\neq 0$. Lecz wówczas ze wzoru $(**)$ wynika, że $\sqrt{z}$ jest liczbą wymierną, a przeto że z jest kwadratem liczby wymiernej. W ten sam sposób dowodzimy, że liczby x i y są kwadratami liczb wymiernych. Warunek jest więc konieczny.

45. Dowieść, że jeżeli x, y i z są liczbami naturalnymi, to dla wymierności liczby $\sqrt{x}+\sqrt{y}+\sqrt{z}$ potrzeba i wystarcza żeby liczby x, y i z były kwadratami liczb naturalnych.

Dowód opiera się na ćwiczeniu 44 i na wniosku ze str. 7, w myśl którego liczba naturalna, która jest kwadratem liczby wymiernej, jest kwadratem liczby naturalnej.

46. Dowieść, że jeżeli x i y są liczbami naturalnymi, a liczba $\sqrt[3]{x}+\sqrt[3]{y}$ jest wymierna, to liczby x i y są sześcianami liczb naturalnych.

Dowód. Niech $d=(x,y)$. Zatem $x=da$ i $y=db$, gdzie a i b są liczbami naturalnymi oraz $(a,b)=1$. Jeżeli $\sqrt[3]{x}+\sqrt[3]{y}=w$, gdzie w jest liczbą wymierną, to $x+y+3d(\sqrt[3]{a^2b}+\sqrt[3]{ab^2})=w^3$, skąd wynika, że liczba $\sqrt[3]{a^2b}+\sqrt[3]{ab^2}=u$ jest wymierna dodatnia. Niech więc $u=l/m$, gdzie l i m są liczbami naturalnymi, i niech $(l,m)=1$. Gdyby było $m>1$, mielibyśmy

$$m^3\left[a^2b+ab^2+3ab\left(\sqrt[3]{ab^2}+\sqrt[3]{a^2b}\right)\right]=l^3;$$

zatem wobec $\sqrt[3]{a^2b}+\sqrt[3]{ab^2}=l/m$ byłoby

$$m^2\{ab[(a+b)m+3l]\}=l^3,$$

co jest niemożliwe wobec $(l, m)=1$ i $m>1$. Musi więc być $m=1$; zatem

(i) $$ab(a+b+3l)=l^3.$$

Łatwo widzieć, że

(ii) $$(a,\ a+b+3l)=1,$$

ponieważ w przeciwnym razie istniałaby taka liczba pierwsza p, że $p|a$ i $p|a+b+3l$, a wtedy wobec $p|a$ i (i) byłoby $p|l^3$, skąd $p|l$ i przeto wobec $p|a$ i $p|a+b+3l$ mielibyśmy $p|b$, co niemożliwe, gdyż $(a, b)=1$. Podobnie dowodzimy, że

(iii) $$(b,\ a+b+3l)=1.$$

Z $(a, b)=1$, (ii) oraz (iii) wnosimy z łatwością na mocy (i), że liczby a i b są sześcianami liczb naturalnych:

$$a=m^3, \qquad b=n^3.$$

Ale z wymierności liczby $\sqrt[3]{x}+\sqrt[3]{y}=\sqrt[3]{d}(m+n)$ wynika, że liczba $\sqrt[3]{d}$ jest wymierna; zatem — w myśl wniosku ze str. 7 — naturalna, skąd $d=s^3$, gdzie s jest liczbą naturalną. Jest więc $x=da=(sm)^3$ i $y=db=(sn)^3$, czyli liczby x i y też są sześcianami liczb naturalnych, c. b. d. o.

47. Dowieść, że liczba $\sqrt[3]{2}+\sqrt[3]{3}$ jest niewymierna.

48. Znaleźć wszystkie rozwiązania równania $x^y=y^x$ w liczbach wymiernych dodatnich $x\neq y$ [1]).

Rozwiązanie. Niech x, y będzie takim rozwiązaniem i niech np. $y>x$. Liczba $w=\frac{x}{y-x}$ jest wymierna dodatnia. Zarazem $y=\left(1+\frac{1}{w}\right)x$ i przeto $x^y=x^{\left(1+\frac{1}{w}\right)x}$, a że $x^y=y^x$, więc $x^{\left(1+\frac{1}{w}\right)x}=y^x$, co daje $x^{1+\frac{1}{w}}=y=\left(1+\frac{1}{w}\right)x$, skąd $x^{\frac{1}{w}}=\left(1+\frac{1}{w}\right)$, a zatem

$$x=\left(1+\frac{1}{w}\right)^w, \qquad y=\left(1+\frac{1}{w}\right)^{w+1}.$$

[1]) Zagadnieniem tym zajmowało się wielu matematyków z Eulerem na czele; ob. L. E. Dickson, *History of the Theory of Numbers*, tom 2, New York 1934, str. 687.

Niech $w=n/m$, gdzie $(m, n)=1$, i $x=r/s$, gdzie $(r, s)=1$. Wobec $x=\left(1+\frac{1}{w}\right)^w$ jest więc $\left(\frac{m+n}{n}\right)^{\frac{n}{m}}=\frac{r}{s}$, skąd $\frac{(m+n)^n}{n^n}=\frac{r^m}{s^m}$. Obie strony tej równości są ułamkami nieprzywiedlnymi, gdyż wobec $(m, n)=1$ jest $(m+n, n)=1$, skąd $((m+n)^n, n^n)=1$, a wobec $(r, s)=1$ jest $(r^m, s^m)=1$. Wynika stąd, że $(m+n)^n=r^m$ i $n^n=s^m$. Równości te dają wobec $(m, n)=1$ (ob. ćwiczenie 16, str. 493) $m+n=k^m$ i $r=k^n$ oraz $n=l^m$ i $s=l^n$, gdzie k i l są liczbami naturalnymi. Zatem $m+l^m=k^m$, skąd $k\geqslant l+1$. Gdyby było $m>1$, mielibyśmy $k^m\geqslant(l+1)^m\geqslant l^m+ml^{m-1}+1>l^m+m$, a więc $k^m>l^m+m$, wbrew temu, że $m+l^m=m+n=k^m$. Jest więc $m=1$, skąd $w=n/m=n$. Ostatecznie więc

(*) $$x=\left(1+\frac{1}{n}\right)^n, \qquad y=\left(1+\frac{1}{n}\right)^{n+1},$$

gdzie n jest liczbą naturalną.

Na odwrót, łatwo sprawdzić, że tak wyznaczone liczby x i y spełniają równanie $x^y=y^x$.

Zachodzi więc następujące twierdzenie:

Wszystkie rozwiązania równania $x^y=y^x$ w liczbach wymiernych x, y, gdzie $y>x>0$, zawarte są we wzorach (*), gdzie n jest dowolną liczbą naturalną.

Ze wzorów tych wynika natychmiast, że tylko dla $n=1$ otrzymujemy rozwiązanie w liczbach naturalnych, mianowicie $x=2$, $y=4$. Równanie $x^y=y^x$ ma więc tylko jedno rozwiązanie w liczbach naturalnych x, y, gdzie $y>x$ [1]). Natomiast w liczbach wymiernych x, y, *gdzie* $y>k$, równanie $x^y=y^x$ ma nieskończenie wiele rozwiązań, mianowicie:

$$2,\ 4, \qquad 3^2/2^2,\ 3^3/2^3, \qquad 4^3/3^3,\ 4^4/3^4, \qquad 5^4/4^4,\ 5^5/4^5, \qquad \ldots$$

Tak np.

$$\left(\frac{9}{4}\right)^{\frac{27}{8}}=\left(\frac{27}{8}\right)^{\frac{9}{4}}.$$

[1]) Wynik ten, można też otrzymać na innej drodze, np. wykazując, że

$$\sqrt[3]{3}>\sqrt[2]{2}=\sqrt[4]{4}>\sqrt[5]{5}>\sqrt[6]{6}>\sqrt[7]{7}>\ldots>\sqrt[1]{1}.$$

Ob. W. Sierpiński, *Działania nieskończone*, Monografie Matematyczne, Warszawa-Wrocław 1948, str. 139.

Można też dowieść, że równanie $x^y = y^x$ ma nieskończenie wiele rozwiązań w różnych liczbach x, y, które są obie niewymierne, jako też z których jedna tylko jest wymierną. Wreszcie, ma ono też nieskończenie wiele rozwiązań w różnych liczbach porządkowych pozaskończonych.

49. Dowieść, że liczba $s_n^{(3)}$ wszystkich różnych rozkładów liczby naturalnej n na sumę trzech liczb naturalnych niemalejących wynosi $\mathrm{E}\left(\frac{n^2+6}{12}\right)$.

Dowód. Liczba $s_n^{(2)}$ wszystkich różnych rozkładów liczby naturalnej n na sumę dwu liczb naturalnych, z których druga jest niemniejsza od pierwszej, wynosi $\mathrm{E}\left(\frac{n}{2}\right)$. Lecz, jak łatwo widzieć,

$$s_n^{(3)} = s_{n-1}^{(2)} + s_{n-2}^{(2)} - 1 + s_{n-3}^{(2)} - 2 + \ldots + s_{n-\mathrm{E}\left(\frac{n}{3}\right)}^{(2)} - \left[\mathrm{E}\left(\frac{n}{3}\right) - 1\right],$$

bo dzieląc wszystkie rozkłady $n = k + l + m$, gdzie $k \leqslant l \leqslant m$, na klasy według pierwszego składnika k, otrzymujemy w k-tej klasie oczywiście $s_{n-k}^{(2)} - (k-1)$ rozkładów. Stąd

$$s_n^{(3)} = \mathrm{E}\left(\frac{n-1}{2}\right) + \mathrm{E}\left(\frac{n-2}{2}\right) + \ldots + \mathrm{E}\left(\frac{n - \mathrm{E}\left(\frac{n}{3}\right)}{2}\right) - \frac{1}{2}\mathrm{E}\left(\frac{n}{3}\right)\left[\mathrm{E}\left(\frac{n}{3}\right) - 1\right].$$

Badając kolejno 6 przypadków $n = 6k, 6k+1, \ldots, 6k+5$, sprawdzamy w każdym z nich wzór $s_n^{(3)} = \mathrm{E}\left(\frac{n^2+6}{12}\right)$.

50. Dowieść, że na to, by liczby naturalne n i $n+2$ stanowiły parę liczb bliźniaczych, potrzeba i wystarcza, żeby zachodziła kongruencja

$$(**) \qquad 4[(n-1)!+1] + n \equiv 0 \pmod{n(n+2)} \text{ [1]}.$$

Dowód. Załóżmy, że liczby n i $n+2$ są obie pierwsze. W myśl twierdzenia Wilsona jest więc $(n-1)!+1 \equiv 0 \pmod{n}$; zatem lewa strona kongruencji $(**)$ jest podzielna przez n.

Zarazem $(n+1)!+1 \equiv 0 \pmod{n+2}$, a że $n \equiv -2 \pmod{n+2}$ i $n+1 \equiv -1 \pmod{n+2}$, skąd $(n+1)! \equiv 2(n-1)! \pmod{n+2}$,

[1]) P. A. Clement, American Mathematical Monthly, tom 56 (1949), str. 23-25.

więc $4(n-1)! \equiv -2 \pmod{n+2}$; zatem wobec $n \equiv -2 \pmod{n+2}$ lewa strona kongruencji $(**)$ jest też podzielna przez $n+2$.

Jako podzielna przez liczby pierwsze n i $n+2$, lewa strona kongruencji $(**)$ jest też podzielna przez ich iloczyn $n(n+2)$. Kongruencja ta jest więc spełniona, co dowodzi, że warunek jest konieczny.

Załóżmy teraz, że dla liczby naturalnej n zachodzi kongruencja $(**)$. Gdyby liczba n była parzysta, $n = 2k$, mielibyśmy $n-1 \geqslant k$, skąd $k \mid (n-1)!$ i przeto $2k \mid 4(n-1)!$, skąd wynikałoby $4(n-1)! \equiv 0 \pmod{n}$. Na mocy $(**)$ byłoby więc $4 \equiv 0 \pmod{n}$, co dowodzi wobec $n = 2k$, że $n = 2$ lub $n = 4$. Lecz — jak łatwo sprawdzić — kongruencja $(**)$ nie zachodzi dla żadnej z tych dwu liczb. Liczba n musi więc być nieparzysta.

Z $(**)$ wynika, że $4[(n-1)!+1] \equiv 0 \pmod{n}$, co wobec nieparzystości liczby n daje $(n-1)!+1 \equiv 0 \pmod{n}$, a zatem (ob. Rozdział IV, § 1, str. 57) liczba n jest pierwsza.

Z drugiej strony, wobec

$$n \equiv -2 \pmod{n+2} \quad \text{i} \quad 2(n-1)! \equiv (n+1)! \pmod{n+2},$$

kongruencja $(**)$ daje

$$2[(n+1)!+1] \equiv 0 \pmod{n+2},$$

co wobec nieparzystości liczby n, a więc i liczby $n+2$, daje $(n+1)!+1 \equiv 0 \pmod{n+2}$, skąd wnosimy jak poprzednio, że liczba $n+2$ jest pierwsza. Warunek jest więc zarazem dostateczny.

51. Oznaczmy przez B postulat Bertranda (ob. Rozdział I, § 9, str. 14), a przez T — twierdzenie następujące:

Każdy ciąg skończony kolejnych liczb naturalnych, który zawiera co najmniej jedną liczbę pierwszą, zawiera też co najmniej jedną liczbę pierwszą względem każdego z pozostałych wyrazów tego ciągu [1]).

Dowieść, że twierdzenie T jest równoważne postulatowi B.

Dowód. Z B wynika T. Istotnie, niech

$$(*) \qquad k, k+1, \ldots, l$$

będzie ciągiem skończonym kolejnych liczb naturalnych, p zaś — największą liczbą pierwszą, zawartą w tym ciągu. Gdyby było $2p \leqslant l$, istniałaby w myśl postulatu B taka liczba pierwsza q,

[1]) Por. J. P. Zahlen, *Euclides*, tom 8, Madryt 1948, str. 115-121.

że $p<q<2p\leqslant l$ wbrew określeniu liczby p jako największej liczby pierwszej ciągu (*). Jest więc $l<2p$ i — jak łatwo widzieć — liczba p jest pierwsza względem każdej z liczb $1, 2, \ldots, l$ różnej od p, w szczególności więc względem każdej liczby ciągu (*) różnej od p.

Z T wynika B. Istotnie niech $n>1$ będzie liczbą naturalną. W myśl twierdzenia T w ciągu

$$(\overset{*}{*}) \qquad 2, 3, \ldots, 2n,$$

który zawiera liczbę pierwszą 2, istnieje co najmniej jedna liczba p, pierwsza względem każdej z pozostałych liczb tego ciągu. Liczba p musi być liczbą pierwszą, gdyż w razie $p=ab$, gdzie $a>1$ i $b>1$, liczba $a\neq p$ należałaby do ciągu $(\overset{*}{*})$ i nie byłaby pierwsza względem p. Gdyby było $p\leqslant n$, mielibyśmy $2p\leqslant 2n$ i liczba $2p\neq p$ należałaby do ciągu $(\overset{*}{*})$, nie będąc pierwszą względem p. Jest więc $p>n$, a że $p\leqslant 2n$, gdyż p należy do ciągu $(\overset{*}{*})$, i $p\neq 2n$, gdyż p jest liczbą pierwszą, więc $n<p<2n$.

52. Opierając się na postulacie Bertranda, dowieść, że jeżeli $n>1$ jest liczbą naturalną, to w ciągu (rosnącym) wszystkich liczb naturalnych większych od 1 i pierwszych względem $n!$ pierwsze *trzy* wyrazy są liczbami pierwszymi.

Dowód. Niech największa liczba pierwsza $p\leqslant n$ będzie s-tą z kolei liczbą pierwszą, p_s. Wystarczy oczywiście okazać, że w ciągu (rosnącym) wszystkich liczb naturalnych pierwszych względem $n!$ pierwszymi trzema wyrazami są liczby p_{s+1}, p_{s+2} i p_{s+3}. W tym zaś celu wystarczy okazać, że żadna liczba $k<p_{s+3}$ różna od p_{s+1} i od p_{s+2} nie jest pierwsza względem $n!$

Przypuśćmy, że jest przeciwnie. Niech:

$$(k, n!)=1, \qquad k<p_{s+3}, \qquad k\neq p_{s+1} \quad \text{i} \quad k\neq p_{s+2}.$$

Wobec $(k, n!)=1$ jest $(k, p_i)=1$ dla $i=1, 2, \ldots, s$ (gdyż $p_s\leqslant n$, a więc $p_1p_2\ldots p_s \mid n!$). Stąd $k\neq p_i$ dla $i=1, 2, \ldots, s+1$ i wobec $k<p_{s+2}$ liczba k jest złożona. Zatem $k=ab$, gdzie $a>1$ i $b>1$, a wobec $(k, n!)=1$ jest też $(a, n!)=1$ i $(b, n!)=1$.

Niech p będzie najmniejszym czynnikiem pierwszym liczby a. Wobec $(a, p_i)=1$ dla $i=1, 2, \ldots, s$ jest więc $p\geqslant p_{s+1}$. Podobnie, jeżeli q jest najmniejszym czynnikiem pierwszym liczby b, to $q\geqslant p_{s+1}$. Zatem $k=ab\geqslant pq\geqslant p_{s+1}^2$, a że $k<p_{s+3}$, więc musi być $p_{s+1}^2<p_{s+3}$. Lecz w myśl postulatu Bertranda jest $p_{s+2}\leqslant 2p_{s+1}$ i $p_{s+3}\leqslant 2p_{s+2}$, a przeto, $p_{s+3}\leqslant 4p_{s+1}$. Zarazem dla $n>2$ jest $p_s\geqslant 3$ i $p_{s+1}\geqslant 5$, skąd $4<p_{s+1}$ i $4p_{s+1}<p_{s+1}^2$. Mielibyśmy więc nierówność $p_{s+3}\leqslant 4p_{s+1}<p_{s+1}^2<p_{s+3}$, co niemożliwe. Tym samym twierdzenie jest dowiedzione dla $n>2$. Zachodzi ono również dla $n=2$, gdyż kolejnymi liczbami naturalnymi pierwszymi względem 2! są liczby 3, 5 i 7, które są pierwsze i większe od 1.

Uwaga. W dowiedzionym twierdzeniu nie można liczby *trzy* zastąpić przez liczbę *cztery*, gdyż czwarta z kolei większa od 1 liczba nieparzysta, czyli liczba 9, jest złożona.

53. Opierając się na postulacie Bertranda, dowieść, że dla liczb naturalnych k i n, gdzie $n\geqslant 2^{k-1}$, w ciągu wszystkich liczb naturalnych większych od 1 i pierwszych względem $n!$ pierwsze k wyrazów są liczbami pierwszymi.

54. Dowieść, że jeżeli $(a, m)=1$, to istnieje co najmniej jedno takie rozwiązanie kongruencji $ax\equiv y \pmod m$, iż $0<x\leqslant\sqrt{m}$ i $0<|y|\leqslant\sqrt{m}$.

Dowód. Możemy oczywiście założyć, że $m>1$. Niech $q=\mathrm{E}(\sqrt{m})$. Weźmy pod uwagę liczby $ax-y$ dla $x, y=0, 1, \ldots, q$. Jest ich $(q+1)^2>m$. Istnieją więc różne układy x_1, y_1 i x_2, y_2, spełniające kongruencję $ax_1-y_1\equiv ax_2-y_2 \pmod m$. Gdyby tu było $x_1=x_2$, mielibyśmy $y_1\equiv y_2 \pmod m$, skąd wobec

$$0\leqslant y\leqslant \mathrm{E}(\sqrt{m})<m$$

znaleźlibyśmy $y_1=y_2$, wbrew założeniu, że układy x_1, y_1 i x_2, y_2 są różne. Jest więc $x_1\neq x_2$, np. $x_1>x_2$. Z drugiej strony,

$$a(x_1-x_2)\equiv y_1-y_2 \pmod m$$

i wobec $x, y=0, 1, \ldots, q$ jest $0<x_1-x_2\leqslant q\leqslant\sqrt{m}$ oraz

$$|y_1-y_2|\leqslant q\leqslant\sqrt{m}.$$

Uwaga. Twierdzenie to znalazł Thue [1]). Ore stosuje je do dowodu, że każda liczba pierwsza p postaci $4k+1$ jest sumą dwu kwadratów. Dla liczb pierwszych p postaci $4k+1$ jest bowiem $\left(\frac{-1}{p}\right)=1$ i istnieje taka liczba całkowita a, że $a^2+1\equiv 0 \pmod p$. Jeżeli teraz

$$ax\equiv y \pmod p, \qquad 0<x\leqslant\sqrt{p} \quad \text{i} \quad |y|\leqslant\sqrt{p},$$

[1]) A. Thue, Archiv für Mathematik und Naturwissenschaft, tom 34 (1914) nº 15. Ob. też O. Ore, *Number Theory and Its History*, New York 1948, str. 268.

to $a^2x^2+x^2\equiv y^2+x^2\equiv 0 \pmod p$ czyli $x^2+y^2=tp$, gdzie t jest liczbą naturalną. Lecz $x^2+y^2\leqslant 2[E(\sqrt{p})]^2<2p$, gdyż $E(\sqrt{p})<\sqrt{p}$. Zatem $0<t<2$, skąd $t=1$, a więc $x^2+y^2=p$.

55. Dowieść, że 2047 jest liczbą złożoną, dla której

$$2^{2047}\equiv 2 \pmod{2047} \qquad \text{(K. Matulewicz).}$$

Dowód. $2047=23\cdot 89$. Ponieważ $2^{11}=2048\equiv 1 \pmod{2047}$ i $2046=186\cdot 11$, więc $2^{2046}\equiv 1 \pmod{2047}$, skąd $2^{2047}\equiv 2 \pmod{2047}$ (por. str. 61).

56. Znaleźć wszystkie liczby całkowite podzielne przez 7, które przy dzieleniu przez każdą z liczb naturalnych mniejszych od 7 dają resztę 1. Znaleźć najmniejszą taką liczbę dodatnią.

Odpowiedź. Są to liczby formy $420t-119$, gdzie t jest liczbą całkowitą. Najmniejszą taką liczbą dodatnią jest 301.

57. Niech x będzie dowolną jedno- lub dwucyfrową liczbą naturalną (w układzie dziesiętnym). Dowieść, że jeżeli do reszty z dzielenia liczby x przez 3, pomnożonej przez 70, dodamy resztę z dzielenia liczby x przez 5, pomnożoną przez 21, oraz resztę z dzielenia liczby x przez 7, pomnożoną przez 15, to resztą z dzielenia otrzymanej sumy przez 105 jest liczba x [1]).

Dowód. Niech r_1, r_2 i r_3 będą odpowiednio resztami z dzielenia liczby x przez 3, 5 i 7 i niech $s=70r_1+21r_2+15r_3$. Mamy przy pewnych całkowitych t_1, t_2 i t_3

$$x=r_1+3t_1=r_2+5t_2=r_3+7t_3,$$

skąd $106x=s+105(2t_1+t_2+t_3)$.

Jeżeli $x<105$, to stąd wynika, że x jest resztą z dzielenia liczby s przez 105, c. b. d. o.

58. Dowieść, że każda liczba naturalna ma wielokrotność, wyrażającą się w układzie dziesiętnym za pomocą samych jedynek, po których następują ewentualnie same zera [2]).

Dowód. Każda liczba naturalna n może być przedstawiona w postaci $n=n_1\cdot 2^\alpha 5^\beta$, gdzie $(n_1,10)=1$, a α i β są całkowite nieujemne. Na mocy twierdzenia, dowiedzionego w ćwiczeniu 1, str. 171, liczba n_1 jest dzielnikiem liczby m, wyrażającej się

[1]) Por. *Number Curiosities*, The Lucknow University Mathematical Association, 1949, str. 16 (wydanie litografowane).

[2]) Twierdzenie to zostało zakomunikowane w tym brzmieniu B. Knasterowi przez śp. profesora Włodzimierza Stożka w 1939 r. we Lwowie.

w układzie dziesiętnym za pomocą samych jedynek. Zarazem $2^\alpha 5^\beta \mid 10^\gamma$, gdzie $\gamma=\max(\alpha,\beta)$. Jest więc $n \mid m\cdot 10^\gamma$.

59. Dowieść następującego twierdzenia Fermata:

Jeżeli p jest liczbą pierwszą większą od 3, to każdy dzielnik naturalny liczby $(2^p+1)/3$ jest postaci $2kp+1$.

Dowód. Niech d będzie dzielnikiem naturalnym liczby $(2^p+1)/3$, która jest całkowita, gdyż przy nieparzystym p jest $(2+1) \mid 2^p+1$. Jeżeli $d>1$, to niech q będzie dzielnikiem pierwszym liczby d. Gdyby było $q=3$, mielibyśmy $2^p+1\equiv 0 \pmod 9$, skąd wynika (ob. ćwiczenie 17, str. 493-494), że $p=6k+3$, co niemożliwe, skoro p jest liczbą pierwszą większą od 3.

Zatem $q\neq 3$. Wobec $2^p+1\equiv 0 \pmod q$ mamy $2^{2p}\equiv 1 \pmod q$. Niech δ będzie wykładnikiem, do którego należy liczba 2 modulo q. Nie może tu być $\delta=1$ ani $\delta=2$, gdyż $q\neq 3$. Jest więc $\delta>2$. Lecz $\delta \mid q-1$ (ob. str. 173), jako też $\delta \mid 2p$ wobec $2^{2p}\equiv 1 \pmod q$. Liczby $2p$ i $q-1$ mają zatem wspólny dzielnik większy od 2, co dowodzi, że liczby p i $q-1$ mają wspólny dzielnik większy od 1. Ponieważ p jest liczbą pierwszą więc $p \mid q-1$, czyli $q=pt+1$, oraz $q=2kp+1$, gdyż $2 \mid q-1$, a $(p,2)=1$. Każdy dzielnik pierwszy q liczby d jest więc postaci $2kp+1$, zatem też i liczba d, która jest ich iloczynem, jest tej postaci, c. b. d. o.

60. Niech $q_1,q_2,\ldots,q_s$ będą wszystkimi dzielnikami pierwszymi liczby naturalnej $n-1>1$. Dowieść, że jeżeli istnieje liczba całkowita a, dla której

$$\text{(i)}\quad a^{n-1}\equiv 1 \pmod n, \qquad \text{(ii)}\quad a^{\frac{n-1}{q_i}}\not\equiv 1 \pmod n \quad \text{dla } i=1,2,\ldots,s,$$

to liczba n jest pierwsza.

Dowód. Gdyby liczba n nie była pierwsza, to (ob. Rozdział VIII, § 5, twierdzenie 7, str. 186 i ćwiczenie 5, str. 172) istniałaby taka liczba naturalna $k<n-1$, że

$$\text{(iii)}\quad a^k\equiv 1 \pmod n.$$

Niech k będzie najmniejszą z takich liczb naturalnych. Oczywiście $k\neq 1$, gdyż w razie $k=1$ byłoby $a\equiv 1 \pmod n$ wbrew (ii). Niech r będzie resztą z dzielenia liczby $n-1$ przez k. Dla pewnego całkowitego $t\geqslant 0$ jest więc $n-1=kt+r$, skąd wnosimy wobec (i) oraz (ii), że $a^r\equiv 1 \pmod n$. Wobec $r<k$ i w myśl określenia liczby k dowodzi to, że $r=0$. Jest więc $n-1=kt$ i wobec $k<n-1$ znajdujemy $t>1$. Liczba t, jako większy od jed-

ności dzielnik liczby $n-1$, musi być podzielna przez jedną co najmniej z liczb $q_1, q_2, \ldots, q_s$. Niech np. $t=q_m u$; stąd $n-1=kt=kq_m u$ oraz $a^{ku}=a^{\frac{n-1}{q_m}}\not\equiv 1 \pmod n$, wbrew (iii). Liczba n musi więc być pierwsza, c. b. d. o.

61. Zastosować dowiedzione twierdzenie do dowodu, że liczba 700001 jest pierwsza, obierając $a=3$ [1]), oraz do dowodu, że liczba 373831 jest złożona, obierając $a=2$.

62. Obliczyć średnią geometryczną wszystkich dzielników naturalnych liczby naturalnej n.

Odpowiedź: $\sqrt{n}$. Wynika to ze wzoru dla iloczynu wszystkich dzielników naturalnych liczby n (ob. (18), str. 124).

63. Dowieść, że iloczyn średniej arytmetycznej wszystkich dzielników naturalnych liczby naturalnej n przez ich średnią harmoniczną jest równy liczbie n [2]).

64. Dowieść, że dla wszelkich naturalnych n i k zachodzi równość $\varphi(n^k)=n^{k-1}\varphi(n)$.

65. Dowieść, że jeżeli $p_1, p_2, \ldots, p_n$ są wszystkimi kolejnymi liczbami pierwszymi niewiększymi od $\sqrt{x}$, gdzie $x>1$ jest liczbą rzeczywistą, to

$$\pi(x)=\pi(\sqrt{x})+\psi(p_1, p_2, \ldots, p_n, x)-1,$$

gdzie ψ jest funkcją określoną wzorem (8), str. 138. Zastosować ten wzór do obliczenia liczby $\pi(100)$.

Uwaga. Wzór ten był punktem wyjścia w obliczaniu wartości $\pi(x)$ dla wielkich x, np. dla $x=10^8$ (Meisel) i dla $x=10^9$ (Bertelsen) [3]).

66. Dowieść, że istnieje nieskończenie wiele par różnych liczb naturalnych x, y, dla których $\sigma(x^2)=\sigma(y^2)$.

Dowód. Równość ta zachodzi dla $x=4m$, $y=5m$, jeżeli $(m, 10)=1$.

67. Dowieść, że $\sigma(p)=p+1$ dla liczb pierwszych p i tylko dla nich.

68. Dowieść, że jeżeli liczba n jest złożona, to $\sigma(n)>n+\sqrt{n}$.

Dowód. Liczba n, jako złożona, ma taki dzielnik d, że $1<d<n$, skąd $1<n/d<n$. Jeżeli $d\leqslant\sqrt{n}$, to $n/d\geqslant\sqrt{n}$, a że n/d

[1]) Ob. O. Ore, *Number Theory and Its History*, New York 1948, str. 332.
[2]) Tamże, str. 91.
[3]) Tamże, str. 69.

też jest dzielnikiem liczby n (niekoniecznie zresztą różnym od d), dla którego $1<n/d<n$, więc $\sigma(n)\geqslant n+\sqrt{n}+1$.

69. Dowieść, że dla każdej liczby naturalnej k istnieje taka liczba naturalna n, dla której $\sigma(n)-\sigma(n+1)\geqslant k$.

Dowód. Jeżeli $n+1$ jest liczbą pierwszą i $n+1>k^2+1$, to $\sigma(n+1)=n+2$ i n jest wtedy liczbą złożoną, skąd

$$\sigma(n)\geqslant n+\sqrt{n}+1$$

(p. ćwiczenie 68). Jest więc $\sigma(n)-\sigma(n+1)\geqslant\sqrt{n}-1\geqslant k$.

70. Znając rozkłady liczb naturalnych l i m na sumę dwu kwadratów liczb całkowitych, rozłożyć liczbę l/m na sumę dwu kwadratów liczb wymiernych.

Odpowiedź. Jeżeli $l=a^2+b^2$ i $m=c^2+d^2$, to

$$\frac{l}{m}=\left(\frac{ac+bd}{c^2+d^2}\right)^2+\left(\frac{ad-bc}{c^2+d^2}\right)^2.$$

71. Dowieść, że na to, by liczba naturalna n była sumą kwadratów dwu liczb naturalnych, potrzeba i wystarcza, żeby w jej rozkładzie na czynniki pierwsze każdy czynnik pierwszy postaci $4k+3$ występował w potędze o wykładniku parzystym i żeby, o ile liczba n nie jest podwójnym kwadratem, była ona podzielna przez jedną co najmniej liczbę pierwszą postaci $4k+1$.

72. Wyznaczyć wszystkie liczby naturalne $n\leqslant 100$, które są sumami kwadratów dwu liczb naturalnych.

Odpowiedź: 2, 5, 8, 10, 13, 17, 18, 20, 25, 26, 29, 32, 34, 37, 40, 41, 45, 50, 52, 53, 58, 61, 65, 72, 73, 74, 80, 82, 85, 89, 90, 97, 98.

73. Dowieść, że iloczyn dwu liczb nieparzystych, z których każda jest sumą kwadratów dwu liczb naturalnych, jest sumą kwadratów dwu liczb naturalnych.

Dowód. Zachodzi tożsamość

$$(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2=(ad+bc)^2+(ac-bd)^2.$$

Nie może być $ad=bc$ i $ac=bd$, ponieważ wówczas byłoby $a^2dc=b^2cd$, skąd dla c i d naturalnych wynikałoby $a^2=b^2$, co niemożliwe, skoro liczba a^2+b^2 jest nieparzysta. Dalszy dowód nie nastręcza trudności.

74. Dowieść, że dla każdej liczby naturalnej n równanie $x^2+y^2=z^n$ ma nieskończenie wiele rozwiązań w liczbach naturalnych x, y, z.

Dowód wynika z poprzedniego twierdzenia (ćwiczenie 73) i z równości $5^2=1^2+2^2$; liczby $(5^k)^n$ dla $k=1,2,\ldots$ są sumami kwadratów dwu liczb naturalnych.

75. Sprawdzić, że każda liczba naturalna $n\leqslant 100$, o ile nie jest sumą kwadratów trzech liczb całkowitych, jest postaci $x^2+y^2+2z^2$, gdzie x, y i z są liczbami całkowitymi. Napisać rozkłady takich liczb n.

76. Dowieść, że istnieje nieskończenie wiele takich liczb naturalnych n, że ani n, ani $n+1$ nie jest sumą trzech kwadratów.

Dowód wynika z twierdzenia 14, Rozdziału IV (§ 9, str. 90) i stąd, że jeżeli $n=8(16k+13)+7$, to $n+1=16(8k+7)$.

77. Niech a, b, c i n będą takimi liczbami naturalnymi, że $an=bc$, $n>b$ i $n>c$. Wyznaczyć efektywnie rozkład liczby n na iloczyn dwu liczb naturalnych mniejszych od n.

Rozwiązanie. Liczba $b_1=b/(a,b)$ jest naturalna i $b_1\leqslant b<n$. Zarazem $b_1>1$, gdyż w razie $b_1=1$ mielibyśmy $b=(a,b)$, skąd $b|a$, a zatem $a=kb$, gdzie k jest liczbą naturalną; wobec $an=bc$ byłoby więc $kbn=bc$, skąd $c=kn\geqslant n$ wbrew założeniu. Lecz b_1 jest dzielnikiem liczby n, gdyż dla $a_1=b/(a,b)$ mamy $(a_1,b_1)=1$ i $a_1n=b_1c$, a przeto $b_1|n$. Stąd rozkład $n=b_1\cdot n/b_1$.

78. Dowieść, że każda liczba naturalna, która jest dzielnikiem iloczynu dwu liczb naturalnych od niej mniejszych, jest złożona.

Dowód oprzeć można na ćwiczeniu 77, albo też na twierdzeniu, że każda liczba pierwsza, która jest dzielnikiem iloczynu dwu liczb naturalnych, musi być dzielnikiem co najmniej jednej z nich.

79. Dowieść, że każdy sześcian liczby naturalnej jest różnicą dwu kwadratów liczb całkowitych, z których co najmniej jeden jest podzielny przez 9.

Dowód wynika natychmiast z tożsamości

$$n^3=\left[\frac{n(n+1)}{2}\right]^2-\left[\frac{n(n-1)}{2}\right]^2.$$

80. Dowieść, że $2^{3^n}\equiv 5^{3^n}\equiv -1 \pmod{3^{n+1}}$ dla $n=0,1,2,\ldots$

Dowód wynika przez indukcję na mocy tożsamości

$$a^3+1=(a+1)[(a+1)(a-2)+3].$$

81. Dowieść, że $3^{n+2}|(4^{3^n}+5^{3^n})$ dla $n=0,1,2,\ldots$

Dowód wynika przez indukcję na mocy tożsamości

$$a^3+b^3=(a+b)^3-3ab(a+b).$$

82. Dowieść przez indukcję następującego twierdzenia Van den Broecka [1]):

$$3^{n+2}|10^{3^n}-1 \qquad \text{dla } n=0,1,2,\ldots$$

Dowód wynika przez indukcję na mocy tożsamości

$$a^3-1=(a-1)[(a-1)(a+2)+3].$$

83. Dowieść, że jeżeli p jest liczbą pierwszą, to każda liczba całkowita przystaje modulo p do sumy dwu kwadratów.

Dowód. Dla $p=2$ jest to oczywiste. Jeżeli p jest liczbą pierwszą nieparzystą, to — jak wiemy (ob. str. 70) — żadne dwie z liczb ciągu

$$0^2,\quad 1^2,\quad 2^2,\quad \ldots,\quad \left(\frac{p-1}{2}\right)^2$$

nie przystają do siebie według modułu p. Podobnie, jeżeli k jest liczbą całkowitą, to żadne dwie z liczb ciągu

$$k-0^2,\quad k-1^2,\quad \ldots,\quad k-\left(\frac{p-1}{2}\right)^2$$

nie przystają do siebie według modułu p.

Ponieważ każdy z dwu wypisanych ciągów zawiera po $\frac{p+1}{2}$ liczb, a różnych reszt według modułu p jest tylko $p<p+1$, więc co najmniej jedna z liczb pierwszego ciągu przystaje do pewnej liczby drugiego ciągu; istnieją więc takie liczby całkowite x i y, że $x^2\equiv k-y^2 \pmod p$, skąd $k\equiv x^2+y^2 \pmod p$, c. b. d. o.

84. Wyznaczyć najmniejszą liczbę naturalną m o tej własności, że nie każda liczba całkowita przystaje modulo m do sumy dwu kwadratów.

Odpowiedź: $m=4$, gdyż w razie $3\equiv x^2+y^2 \pmod 4$ byłoby $4k+3=x^2+y^2$, co niemożliwe.

85. Wyznaczyć najmniejszą liczbę złożoną m o tej własności, że każda liczba całkowita przystaje modulo m do sumy dwu kwadratów. Dowieść, że istnieje nieskończenie wiele takich m.

---

[1]) Ob. Mathesis 6 (1886), str. 70.

Odpowiedź: $m=6$, co wynika z kongruencji:

$$0\equiv 0^2+0^2 \pmod 6,\quad 1\equiv 1^2+0^2 \pmod 6,\quad 2\equiv 1^2+1^2 \pmod 6,$$
$$3\equiv 3^2+0^2 \pmod 6,\quad 4\equiv 2^2+0^2 \pmod 6,\quad 5\equiv 2^2+1^2 \pmod 6.$$

Że takich liczb m jest nieskończenie wiele, wynika z łatwością stąd (por. ćwiczenie 83), że jeżeli $m=2p$, gdzie p jest liczbą pierwszą nieparzystą, to liczby ciągu

$$0^2,\quad 1^2,\quad 2^2,\quad \ldots,\quad (p-1)^2$$

dają przy dzieleniu przez m same różne reszty. Istotnie, jeżeli r i $s>r$ są dwiema liczbami z ciągu $0, 1, 2, \ldots, p-1$, to $s-r\leqslant p-1$ i $s+r<2p-2$, a przeto gdyby było $s^2\equiv r^2 \pmod{2p}$ czyli $2p \mid (s-r)(s+r)$, to musiałoby być $s+r=p$, wobec czego liczby $s+r$ i $s-r$ byłyby nieparzyste wbrew $2p \mid (s^2-r^2)$.

86. Wyznaczyć najmniejszą liczbę naturalną m o tej własności, że nie każda liczba całkowita przystaje modulo m do sumy trzech kwadratów.

Odpowiedź: $m=8$, gdyż w razie $7\equiv x^2+y^2+z^2 \pmod 8$ byłoby $8k+7=x^2+y^2+z^2$, co niemożliwe (ob. str. 90).

87. Wyznaczyć wszystkie reszty sześcienne dla modułu 13.

Odpowiedź: 0, 1, 5, 8 i 12.

88. Dowieść, że każda liczba całkowita przystaje modulo 13 do sumy dwu sześcianów.

Dowód wynika z kongruencyj:

$$0\equiv 0^3+0^3 \pmod{13},\quad 1\equiv 1^3+0^3 \pmod{13},\quad 2\equiv 1^3+1^3 \pmod{13},$$
$$3\equiv 2^3+2^3 \pmod{13},\quad 4\equiv 4^3+7^3 \pmod{13},\quad 5\equiv 0^3+7^3 \pmod{13},$$
$$6\equiv 1^3+7^3 \pmod{13},\quad 7\equiv 2^3+4^3 \pmod{13},\quad 8\equiv 0^3+2^3 \pmod{13},$$
$$9\equiv 1^3+2^3 \pmod{13},\quad 10\equiv 7^3+7^3 \pmod{13},\quad 11\equiv 4^3+4^3 \pmod{13},$$
$$12\equiv 0^3+4^3 \pmod{13}.$$

89. Dowieść, że nie każda liczba całkowita przystaje modulo 7 do sumy dwu lub mniej sześcianów.

Dowód wynika stąd, że liczba 4 nie przystaje modulo 7 do sumy dwu lub mniej sześcianów, gdyż sześcian każdej liczby całkowitej jest postaci $7k$ lub $7k\pm 1$.

90. Dowieść, że każda liczba całkowita przystaje modulo 13 do sumy trzech lub mniej bikwadratów, ale nie każda przystaje modulo 13 do sumy dwu lub mniej bikwadratów.

91. Znaleźć wszystkie liczby naturalne $m>1$ o tej własności, że każda liczba całkowita jest resztą sześcienną dla modułu m.

Odpowiedź. Są to wszystkie liczby naturalne, będące iloczynami skończenie wielu różnych liczb pierwszych, z których żadna nie jest postaci $3k+1$ [1]).

Dowód. Załóżmy, że liczba naturalna $m>1$ nie jest iloczynem samych różnych liczb pierwszych. Istnieje wówczas taka liczba pierwsza p, że $m=p^2l$, gdzie l jest liczbą naturalną. Niech $x=pl$. Zatem $0<x<m$ i $x^3=p^3l^3=pl^2m\equiv 0 \pmod m$. Gdyby każda liczba całkowita była resztą sześcienną dla modułu m, to reszty z dzielenia liczb

$$(*)\qquad 0^3,\quad 1^3,\quad 2^3,\quad \ldots,\quad (m-1)^3$$

przez m musiałyby być wszystkie różne, gdy tymczasem jest $x^3\equiv 0 \pmod m$. Liczba m musi więc być iloczynem samych różnych liczb pierwszych.

Gdyby wśród czynników pierwszych liczby m był czynnik $p=3k+1$, to mielibyśmy $0<k={}^1/_3(p-1)<p-1$ i, oznaczając przez g pierwiastek pierwotny dla modułu p, mielibyśmy $g^k\not\equiv 1 \pmod p$, skąd pisząc $m=pm_1$, otrzymalibyśmy

$$g^km_1\not\equiv m_1 \pmod m.$$

Natomiast, wobec $g^{p-1}\equiv 1 \pmod p$ jest $m=pm_1 \mid (g^{p-1}-1)m_1^3$, co wobec $p-1=3k$ daje $(g^km_1)^3\equiv m_1^3 \pmod m$, wbrew temu, że liczby (*) dają przy dzieleniu przez m same różne reszty. Warunek jest więc konieczny.

Na odwrót, załóżmy że liczba naturalna m spełnia ten warunek. Jest więc $m=p_1p_2\ldots p_s$, gdzie $p_1, p_2, \ldots, p_s$ są różnymi czynnikami pierwszymi, z których żaden nie jest postaci $3k+1$. Niech $P=(p_1-1)(p_2-1)\ldots(p_s-1)$. Oczywiście $(P, 3)=1$ i istnieje taka liczba naturalna t, że $Pt\equiv -1 \pmod 3$, skąd $Pt+1=3l$, gdzie l jest liczbą naturalną.

Każda liczba całkowita x spełnia kongruencję

$$(**)\qquad x\equiv x^{Pt+1} \pmod{p_i}\qquad \text{dla } i=1, 2, \ldots, s.$$

Istotnie, niech i będzie jedną z liczb $1, 2, \ldots, s$. Jeżeli $x\equiv 0 \pmod{p_i}$, to kongruencja (**) jest oczywiście prawdziwa. Jeżeli $x\not\equiv 0 \pmod{p_i}$, to w myśl małego twierdzenia Fermata

[1]) Ob. W. Sierpiński, Rocznik Polskiego Towarzystwa Matematycznego, tom 22 (1949), str. 269.

$x^{p_i-1} \equiv 1 \pmod{p_i}$ i wobec $(p_i-1)|P$ znajdujemy $x^{P_i} \equiv 1 \pmod{p_i}$, skąd (*).

Ponieważ m jest iloczynem samych różnych liczb pierwszych $p_1, p_2, \ldots, p_s$ więc z (*) wynika wobec $Pt+1=3l$ kongruencja $x \equiv (x^l)^3 \pmod{m}$ dla każdej liczby całkowitej x. Warunek jest więc dostateczny.

Zauważmy, że liczba l nie zależy od liczby x.

92. Wyznaczyć wszystkie liczby naturalne m, gdzie $1 < m \leqslant 100$, dla których każda liczba całkowita jest resztą sześcienną.

Odpowiedź: 2, 3, 5, 6, 10, 11, 15, 17, 22, 23, 29, 30, 33, 34, 41, 46, 47, 51, 53, 55, 58, 59, 66, 67, 69, 71, 82, 83, 85, 87, 89, 94.

93. Wyznaczyć wszystkie liczby naturalne $m>1$ o tej własności, że $x \equiv x^3 \pmod{m}$ dla wszystkich x całkowitych.

Odpowiedź. Są trzy takie liczby: 2, 3 i 6.

94. Wyznaczyć wszystkie liczby naturalne $m>1$ o tej własności, że $x \equiv x^9 \pmod{m}$ dla każdego x całkowitego.

Odpowiedź. Są to liczby: 2, 3, 5, 6, 10, 15 i 30.

95. Wyznaczyć wszystkie liczby naturalne $m>1$ o tej własności, że $x \equiv x^5 \pmod{m}$ dla każdego x całkowitego.

Odpowiedź. Są to liczby: 2, 3, 5, 6, 10, 15 i 30.

96. Dowieść, że istnieje nieskończenie wiele liczb pierwszych p, dla których każda liczba całkowita jest resztą sześcienną modulo p.

Wskazówka. Oprzeć się na ćwiczeniu 91 i na tym, że liczb pierwszych postaci $3k+2$ jest nieskończenie wiele (ob. str. 79).

97. Dowieść, że na to, by liczba naturalna $m>1$ miała tę własność, że każda liczba całkowita przystaje modulo m do piątej potęgi pewnej liczby całkowitej, potrzeba i wystarcza, żeby liczba m była iloczynem samych różnych liczb pierwszych, z których żadna nie jest postaci $5k+1$ [1]).

98. Wyznaczyć wszystkie liczby naturalne $m>1$ o tej własności, że każda liczba całkowita przystaje modulo m do dziewiątej potęgi pewnej liczby całkowitej.

Odpowiedź ta sama co w ćwiczeniu 91. Wynika to z łatwością stąd, że jeżeli dla każdego x całkowitego istnieje takie y

[1]) Rocznik Polskiego Towarzystwa Matematycznego, tamże.

całkowite, że $x \equiv y^3 \pmod{m}$, to jest też $y \equiv z^3 \pmod{m}$, skąd $x \equiv z^9 \pmod{m}$.

99. Dowieść, że nie istnieje żadna liczba naturalna $m>2$ o tej własności, że każda liczba całkowita przystaje modulo m do szóstej potęgi pewnej liczby całkowitej.

100. Znaleźć wszystkie liczby naturalne $m>1$, dla których istnieją tylko dwie różne reszty sześcienne modulo m (mianowicie reszty 0 i 1).

Odpowiedź: $m=2$.

101. Znaleźć wszystkie liczby naturalne $m>1$, dla których istnieją dokładnie trzy różne reszty sześcienne modulo m.

Odpowiedź. Są tylko trzy takie liczby: 4, 7 i 9.

102. Wyznaczyć wszystkie reszty dwukwadratowe dla modułu 10.

Odpowiedź: 0, 1, 5 i 6.

103. Znaleźć wszystkie liczby naturalne $m>1$, dla których istnieją tylko dwie różne reszty dwukwadratowe modulo m (mianowicie reszty 0 i 1).

Odpowiedź. Jest pięć takich liczb: 2, 3, 5, 8 i 16.

104. Dowieść, że dla każdej liczby naturalnej $n>1$ równanie $x^n+y^n=z^{n-1}$ ma nieskończenie wiele rozwiązań w różnych liczbach naturalnych.

Dowód wynika natychmiast z tożsamości

$$[(1+k^n)^{n-2}]^n+[k(1+k^n)^{n-2}]^n=[(1+k^n)^{n-1}]^{n-1},$$

zachodzącej dla wszelkich liczb naturalnych $n>1$ i $k>1$.

Uwaga. Trudniejsze jest zbadanie, dla jakich $n>3$ naturalnych równanie $x^n+y^n=z^{n-1}$ ma rozwiązania w liczbach naturalnych x, y, z, gdzie $(x, y)=1$. Dla $n=3$ jest

$$1^3+2^3=3^2, \qquad 11^3+37^3=228^2, \qquad 56^3+65^3=671^2.$$

105. Znaleźć wszystkie rozwiązania równania $2x^n=z^{n-1}$ w liczbach naturalnych x i z.

Odpowiedź: $x=2^{n-2}k^{n-1}$ i $z=2^{n-1}k^n$, gdzie k jest liczbą naturalną.

106. Dowieść, że dla każdej liczby naturalnej n równanie $x^n+y^n=z^{n+1}$ ma nieskończenie wiele rozwiązań w różnych liczbach naturalnych.

Dowód wynika natychmiast z tożsamości

$$(1+k^n)^n+[k(1+k^n)]^n=(1+k^n)^{n+1}.$$

107. Dowieść, że równanie $x^3+y^3=z^5$ ma nieskończenie wiele rozwiązań w różnych liczbach naturalnych.

Dowód wynika natychmiast z tożsamości

$$[(1+k^3)^3]^3+[k(1+k^3)^3]^3=[(1+k^3)^2]^5.$$

Np. $(3^6)^3+(2\cdot 3^6)^3=(3^6)^5$.

108. Znaleźć wszystkie rozwiązania równania $2x^3=z^5$ w liczbach naturalnych.

Odpowiedź: $x=2^3m^5$, $z=2^2m^3$, gdzie m jest dowolną liczbą naturalną.

109. Dowieść, że każda liczba kwadratowa jest sumą dwu liczb trójkątnych (p. definicję na str. 92).

Dowód wynika z tożsamości $n^2=\frac{(n-1)n}{2}+\frac{n(n+1)}{2}$.

110. Dowieść, że ciąg ostatnich cyfr kolejnych liczb trójkątnych (w układzie dziesiętnym) jest okresowy (o okresie 20) i wywnioskować stąd, że ostatnią cyfrą liczby trójkątnej może być tylko 0, 1, 3, 5, 6 lub 8 [1]).

111. Dowieść, że dla $n=1,2,\ldots$ liczby $(2^{4n+1}-2^{2n}-1)/9$ są trójkątne.

112. Dowieść, że każda liczba doskonała parzysta $d>6$ jest sumą sześcianów kolejnych liczb nieparzystych:

$$d=1^3+3^3+5^3+\ldots+(2n-1)^3.$$

Dowód wynika stąd, że $1^3+3^3+\ldots+(2n-1)^3=n^2(2n^2-1)$ i że liczby doskonałe parzyste $d>6$ są postaci $2^{p-1}(2^p-1)$, gdzie p jest liczbą nieparzystą, a zatem $n=2^{\frac{p-1}{2}}$ jest liczbą całkowitą, dla której $2^{p-1}(2^p-1)=n^2(2n^2-1)$.

113. Dowieść, że każda liczba doskonała parzysta jest trójkątna.

Wskazówka. Oprzeć się na ćwiczeniu 112 oraz na tym, że $n^2(2n^2-1)=2n^2(2n^2-1)/2$ i $6=3\cdot 4/2$.

[1]) Por. K. Zarankiewicz, Matematyka, zeszyt 6 (1949), str. 3 i 4.

114. Dowieść następującego twierdzenia K. Zarankiewicza: *istnieje nieskończenie wiele liczb naturalnych, które są zarazem trójkątne i kwadratowe.*

Dowód. Jedną z takich liczb jest liczba 1, gdyż $1\cdot 2/2=1^2$. Zakładając, że n jest taką liczbą, że więc $n(n+1)/2=k^2$, łatwo obliczyć, że taką jest również liczba $m=4k+3n+1>n$.

Istotnie:

$$\frac{m(m+1)}{2}=8k^2+2(6n+3)k+9\frac{n(n+1)}{2}+1,$$

co wobec $\frac{n(n+1)}{2}=k^2$ czyli $9\frac{n(n+1)}{2}=k^2+4n(n+1)$ daje

$$\frac{m(m+1)}{2}=9k^2+2\cdot 3(2n+1)k+(2n+1)^2=(3k+2n+1)^2.$$

Tak np. dla $n=1$ otrzymujemy $m=8$; dalej znajdujemy kolejno:

$$m=49,\quad m=288,\quad m=1681,\quad \ldots,$$

co daje liczby:

$$\frac{1\cdot 2}{1}=1^2,\qquad \frac{8\cdot 9}{2}=6^2,\qquad \frac{49\cdot 50}{2}=35^2,$$

$$\frac{288\cdot 289}{2}=204^2,\qquad \frac{1681\cdot 1682}{3}=1189^2,\qquad \ldots$$

Można okazać — co jest jednak trudniejsze — że w ten sposób otrzymamy wszystkie kolejne liczby naturalne, które są trójkątne i kwadratowe zarazem.

Uwaga. Już Euler wykazał, że dla każdego naturalnego n liczba $\frac{(3+2\sqrt{2})^n-(3-2\sqrt{2})^n}{4\sqrt{2}}$ jest naturalna, a jej kwadrat jest liczbą trójkątną.

115. Dowieść, że na to, by liczba naturalna n była sumą dwu liczb trójkątnych, potrzeba i wystarcza, żeby liczba $4n+1$ była sumą dwu kwadratów.

Dowód wynika z równoważności wzorów

$$n=\frac{x(x+1)}{2}+\frac{y(y+1)}{2}\quad \text{i}\quad 4n+1=(x-y)^2+(x+y+1)^2.$$

116. Dowieść, że 1 jest jedyną liczbą trójkątną, która jest sumą kwadratów dwu kolejnych liczb całkowitych.

117. Dowieść następującego twierdzenia K. Zarankiewicza: *każda liczba naturalna, której kolejne cyfry (w układzie dziesiętnym) składają się z dowolnej liczby dwójek, po których następuje ta sama liczba jedynek, jest trójkątna.*

Dowód wynika natychmiast z tożsamości

$$2\cdot\frac{(10^n-1)(2\cdot 10^n+1)}{9}=\frac{2\cdot 10^n-2}{3}\cdot\left(\frac{2\cdot 10^n-2}{3}+1\right)\ ^{1)}.$$

118. Dowieść, że dla wszelkiego naturalnego m liczba $m+1$ należy według modułu m^2 do wykładnika m.

Dowód wynika stąd, że dla każdego k naturalnego zachodzi kongruencja $(m+1)^k\equiv 1+mk \pmod{m^2}$, którą łatwo udowodnić przez indukcję lub za pomocą dwumianu Newtona.

119. Dowieść, że na to, by liczba naturalna n spełniała kongruencję $a^{n-1}\equiv 1 \pmod n$ dla $(a,n)=1$, potrzeba i wystarcza, żeby spełniała ona kongruencję $n\equiv 1 \pmod{\lambda(n)}$, gdzie $\lambda(n)$ jest najmniejszym wykładnikiem naturalnym m, spełniającym kongruencję $a^m\equiv 1 \pmod n$ dla $(a,n)=1$ [2].

120. Dowieść, że jeżeli m jest liczbą naturalną, to warunek

(i) $\qquad m \mid x^9-x \quad$ dla każdego x całkowitego

jest równoważny warunkowi

(ii) $\qquad m \mid 30.$

Dowód. Jeżeli liczba naturalna m spełnia warunek (i), to $m \mid 2^9-2$ czyli $m \mid 510$, jako też $m \mid 3^9-3$ czyli $m \mid 19680$. Zatem $m \mid (510, 19680)$, skąd warunek (ii).

Na odwrót, na mocy małego twierdzenia Fermata mamy $x^9\equiv x \pmod{30}$ dla x całkowitych i tym bardziej $x^9\equiv x \pmod m$ dla $m \mid 30$. Zatem z (ii) wynika (i). (Por. także ćwiczenie 94).

121. Zastąpić w ćwiczeniu 120 warunek (i) przez warunek

$$m \mid x^5-x \quad \text{dla } x \text{ całkowitych.}$$

Dowód jest wówczas nieco inny niż w ćwiczeniu 120.

---

[1]) Ob. też K. Zarankiewicz, Matematyka, zeszyt 6 (1949), str. 4.

[2]) Ob. O. Ore, *Number Theory and its History*, New York 1948, str. 332.

122. Udowodnić twierdzenie Waringa dla ósmych potęg, opierając się na twierdzeniu 16 z Rozdziału IV (§ 11, str. 103), wniosku ze str. 100 oraz na następującej tożsamości A. Hurwitza:

$$5040(a^2+b^2+c^2+d^2)^4=$$
$$=6\sum_4(2a)^8+60\sum_{12}(a\pm b)^8+\sum_{48}(2a\pm b\pm c)^8+6\sum_8(a\pm b\pm c\pm d)^8,$$

gdzie $\sum_4(2a)^8$ oznacza sumę czterech składników

$$(2a)^8+(2b)^8+(2c)^8+(2d)^8,$$

$\sum_{12}(a\pm b)^8$ oznacza sumę dwunastu składników

$$(a+b)^8+(a-b)^8+(a+c)^8+(a-c)^8+\ldots+(c+d)^8+(c-d)^8$$

itd.

123. Dowieść następującego twierdzenia Jacobiego:

Każda liczba naturalna jest postaci $x^2+2y^2+3z^2+6t^2$, gdzie x, y, z, t są całkowite.

Dowód. Niech n będzie liczbą naturalną. W myśl twierdzenia Lagrange'a (str. 93) istnieją takie liczby całkowite a, b, c, d, że

(*) $\qquad n=a^2+b^2+c^2+d^2.$

Rozróżnimy trzy przypadki:

1° Co najmniej trzy spośród liczb a, b, c, d, np. a, b i c, są podzielne przez 3.

2° Tylko dwie spośród liczb a, b, c, d, np. c i d, są podzielne przez 3; wówczas $a\equiv\pm 1 \pmod 3$ i $b\equiv\pm 1 \pmod 3$, a więc jeżeli znaki są w obu kongruencjach zgodne, to możemy w (*) zastąpić a przez $-a$; wobec $-a\equiv\mp 1 \pmod 3$ znaki w kongruencjach dla $-a$ i b będą różne, zatem suma tych liczb, a więc i suma $-a+b+c$ będzie podzielna przez 3.

3° Co najwyżej jedna z liczb a, b, c, d jest podzielna przez 3, np. liczby a, b i c nie są podzielne przez 3; wówczas podobnie jak w przypadku 2° możemy przez ewentualną zmianę znaków niektórych spośród liczb a, b i c osiągnąć to, żeby suma otrzymanych w ten sposób nowych liczb była podzielna przez 3.

Tak więc możemy zawsze założyć równość (*) o a, b, c i d całkowitych i przy tym takich, że

(**) $$a+b+c=3z,$$

gdzie z jest liczbą całkowitą.

Lecz z każdych trzech liczb całkowitych co najmniej dwie przystają modulo 2, np. $a\equiv b \pmod 2$, czyli że $a+b=2k$, gdzie k jest liczbą całkowitą. Stąd $a-b=2(k-b)=2y$, gdzie y jest liczbą całkowitą. Ale — jak łatwo sprawdzić —

$$3(a^2+b^2+c^2)=(a+b+c)^2+2(k-c)^2+6y^2,$$

co dowodzi wobec (**), że liczba $k-c$ jest podzielna przez 3. Niech $k-c=3t$. Stąd $a^2+b^2+c^2=3z^2+6t^2+2y^2$, zatem

$$n=d^2+2y^2+3z^2+6t^2,$$

c. b. d. o.

124. Oznaczmy przez G twierdzenie Gaussa, że każda liczba naturalna postaci $4k+1$ jest sumą trzech kwadratów, a przez L — twierdzenie E. Lionneta, że każda liczba nieparzysta jest sumą czterech kwadratów liczb naturalnych, z których dwie są kolejne. Dowieść równoważności twierdzeń G i L.

Dowód. Załóżmy twierdzenie G i niech $l=2k+1$ będzie daną liczbą nieparzystą. Na mocy G jest $4k+1=x^2+y^2+z^2$, gdzie x, y i z są liczbami całkowitymi, z których — jak łatwo widzieć — jedna musi być nieparzysta, a dwie parzyste. Zatem

(i) $$4k+1=4q^2+4r^2+(2s+1)^2,$$

gdzie q, r i s są całkowite. Stąd

(ii) $$2k+1=(q+r)^2+(q-r)^2+s^2+(s+1)^2,$$

co dowodzi prawdziwości twierdzenia L. Tak więc z G wynika L.

Na odwrót, załóżmy twierdzenie L i niech k będzie liczbą całkowitą nieujemną. Na mocy L jest

(iii) $$2k+1=x^2+y^2+s^2+(s+1)^2,$$

gdzie x, y, s i $s+1$ są liczbami całkowitymi. Stąd

$$x^2+y^2=2k-2s^2-2s,$$

wobec czego liczba x^2+y^2 jest parzysta, a więc również liczby $x+y$ i $x-y$ są parzyste.

Niech $x+y=2q$ i $x-y=2r$, gdzie q i r są całkowite. Stąd $x=q+r$ i $y=q-r$, skąd na mocy (iii) wynika wzór (ii), który pociąga za sobą (i), co dowodzi prawdziwości twierdzenia G. Tak więc z L wynika G.

125. Dowieść, że liczba naturalna, której cyframi (w układzie dziesiętnym) są same jedynki, może (lecz nie musi) być pierwsza tylko wtedy, jeżeli liczba jej cyfr jest pierwsza.

Uwaga. Nie wiemy, czy wśród takich liczb jest nieskończenie wiele pierwszych, a także czy jest wśród nich nieskończenie wiele złożonych.

Dowód. Niech n będzie liczbą naturalną o m cyfrach (w układzie dziesiętnym), które wszystkie są jedynkami. Jeżeli m jest liczbą złożoną, $m=rs$, gdzie $r>1$ i $s>1$, to

$$n=(10^m-1)/9=[(10^r)^s-1]/9,$$

skąd wynika z łatwością, że liczba naturalna $(10^r-1)/9$ jest dzielnikiem liczby n większym od 1, a mniejszym od n; dowodzi to, że liczba n jest złożona.

Liczba 11 jest pierwsza; liczby $111=3\cdot 37$, $11111=41\cdot 271$, $1111111=239\cdot 4649$ są złożone.

126. Niech $f(x)$ oznacza sumę cyfr liczby naturalnej x (w układzie dziesiętnym). Dowieść, że ciąg nieskończony

$$x,\ f(x),\ ff(x),\ fff(x),\ \ldots$$

ma zawsze, poczynając od pewnego miejsca, wszystkie wyrazy równe (mianowicie równe jednej z liczb $1, 2, \ldots, 9$).

127. Niech $g(x)$ oznacza sumę kwadratów cyfr liczby naturalnej x (w układzie dziesiętnym). Dowieść, że ciąg nieskończony

$$x,\ g(x),\ gg(x),\ ggg(x),\ \ldots$$

jest zawsze okresowy, o okresie (który może być mieszany) złożonym bądź z liczby 1, bądź z ośmiu wyrazów

$$4,\ 16,\ 37,\ 58,\ 89,\ 145,\ 42,\ 20,$$

bądź z ich cyklicznych przestawień, i że każdy z tych 9 przypadków zachodzi dla nieskończenie wielu liczb naturalnych x [1]).

[1]) Por. A. Porges, American Mathematical Monthly, tom 52 (1945), str. 379-382.

128. Dowieść, że jeżeli a jest liczbą nieparzystą, to $2^{n+2} \mid a^{2^n}-1$ dla $n=1,2,\ldots$ (lecz niekoniecznie dla $n=0$).

129. Dowieść, że dla $n=0,1,2,\ldots$ liczba $\frac{11^{3^n}+1}{3^{n+1}}$ jest naturalna złożona.

Dowód polega na wykazaniu, że liczba ta jest podzielna przez 3 dla n naturalnych.

130. Dowieść, że $11 \mid 20^{45}-1$.

Dowód. $2^5=32\equiv-1 \pmod{11}$, skąd

$$2^{45}\equiv(-1)^9\equiv 1 \pmod{11},$$

a że $10\equiv-1 \pmod{11}$, więc $10^{45}\equiv-1 \pmod{11}$. Zatem

$$20^{45}=2^{45}\cdot 10^{45}\equiv(-1)(-1)\equiv 1 \pmod{11},$$

skąd $11 \mid 20^{45}-1$, c. b. d. o.

131. Dowieść, że $43 \mid 2^{77}+1$.

Dowód. $2^7=128\equiv-1 \pmod{43}$, skąd $2^{77}\equiv(-1)^{11}\equiv-1 \pmod{43}$.

132. Ile cyfr po przecinku ma ułamek dziesiętny skończony dla liczby 2^{-n}, a ile dla liczby 5^{-n} (gdzie n jest liczbą naturalną)?

Odpowiedź: n w obu przypadkach.

133. Którą cyfrą po przecinku jest pierwsza różna od zera cyfra rozwinięcia dziesiętnego liczb:

$$2^{-10},\quad 2^{-100},\quad 2^{-1000},\quad 5^{-10},\quad 5^{-100},\quad 5^{-1000}?$$

Odpowiedź. Jak łatwo obliczyć, pierwsza różna od zera cyfra rozwinięcia dziesiętnego liczby 2^{-n} (gdzie n jest liczbą naturalną) występuje na miejscu $E(n\log_{10}2)+1$ po przecinku, a rozwinięcia dziesiętnego liczby 5^{-n} — na miejscu $E(n\log_{10}5)+1$ po przecinku.

Ponieważ $\log_{10}2=0{,}30103$ i $\log_{10}5=1-\log_{10}2$, więc dla liczb danych w ćwiczeniu będą to miejsca:

4, 31, 302, 7, 70, 699.

134. Dowieść, że jeżeli p jest liczbą pierwszą, to istnieje nieskończenie wiele liczb pierwszych postaci $2pk+1$, gdzie k jest liczbą całkowitą [1]).

[1]) Por. J. Winogradow, *Osnowy teorii czisel*, wyd. 5-e, Moskwa-Leningrad 1949, str. 106 (1c) i str. 159.

Dowód. Wobec twierdzenia 9 z Rozdziału IV (str. 76), wystarczy założyć, że p jest liczbą pierwszą nieparzystą.

Niech q będzie liczbą pierwszą nieparzystą i niech a będzie taką liczbą całkowitą, dla której

$$(*)\qquad a^p\equiv 1 \pmod{q}.$$

Jak wiemy ze str. 173, wykładnik δ, do którego należy liczba a według modułu q, musi być dzielnikiem liczby p, a ponieważ p jest liczbą pierwszą, więc albo $\delta=1$, albo $\delta=p$; zarazem $\delta \mid q-1$ na mocy wniosku ze str. 183.

Jeżeli $\delta=1$, to

$$(**)\qquad a\equiv 1 \pmod{q},$$

a jeżeli $\delta=p$, to $p \mid q-1$, skąd wnosimy wobec nieparzystości liczb pierwszych p i q, że $2p \mid q-1$, a zatem że $q=2pk+1$, gdzie k jest liczbą całkowitą.

Niech w szczególności $a=2$ i niech q będzie dzielnikiem pierwszym liczby 2^p-1. Oczywiście nie może tu zachodzić kongruencja (**), a przeto — jak dowiedliśmy przed chwilą — musi być $q=2pk+1$. Dzielniki pierwsze liczby 2^p-1 są więc liczbami postaci $2pk+1$. Jest to twierdzenie 5 z Rozdziału V (§ 3, str. 119).

Istnieją zatem liczby pierwsze postaci $2pk+1$. By dowieść, że jest ich nieskończenie wiele, niech $p_1, p_2, \ldots, p_n$ będą pierwszymi tej postaci i niech $a=2p_1p_2\ldots p_n$. Zatem $a\equiv 2 \pmod{p}$. Oznaczając przez q dzielnik pierwszy liczby nieparzystej

$$s=a^{p-1}+a^{p-2}+\ldots+a+1,$$

okażemy, że

$$(***)\qquad a\not\equiv 1 \pmod{q}.$$

Istotnie w przeciwnym razie byłoby $s\equiv p \pmod{q}$, a ponieważ $s\equiv 0 \pmod{q}$ na mocy założenia, że $q \mid s$, więc $p\equiv 0 \pmod{q}$. Z uwagi na to, że liczby p i q są pierwsze, wynika stąd, że $p=q$, i przypuszczenie, że wzór (***) nie zachodzi, dałoby $a\equiv 1 \pmod{p}$ wbrew temu, że $a\equiv 2 \pmod{p}$. Tym samym wzór (***) jest dowiedziony.

Z drugiej strony, wobec $q \mid s$ oraz oczywistej równości $a^p-1=(a-1)s$ zachodzi kongruencja (*), z której wynika — jak widzieliśmy — że q jest liczbą postaci $2pk+1$.

Otóż jest ono liczbą różną od $p_1, p_2, \ldots, p_n$, gdyż wobec (*) liczba $2p_1p_2\ldots p_n = a$ nie jest podzielna przez q. Liczb pierwszych postaci $2pk+1$ jest więc nieskończenie wiele.

Jako natychmiastowy wniosek stąd otrzymujemy:

Każdy z postępów arytmetycznych

$$6k+1, \quad 10k+1, \quad 14k+1, \quad 22k+1, \quad 26k+1,$$

tym bardziej więc *każdy z postępów arytmetycznych*

$$3k+1, \quad 5k+1, \quad 7k+1, \quad 11k+1, \quad 13k+1$$

zawiera nieskończenie wiele liczb pierwszych.

135. Dowieść, że jeżeli liczba a należy według modułu m do wykładnika $\delta_1\delta_2$, to liczba a^{δ_1} należy według modułu m do wykładnika δ_2 [2]).

136. Dowieść, że jeżeli $(\delta_1, \delta_2) = 1$ i liczba a_1 należy według modułu m do wykładnika δ_1, a liczba a_2 do wykładnika δ_2, to liczba a_1a_2 należy do wykładnika $\delta_1\delta_2$.

---

[2]) Ob. tamże, str. 93.