ROZDZIAŁ I

PODZIELNOŚĆ LICZB I ROZKŁAD NA CZYNNIKI PIERWSZE

§ 1. Podzielność jednej liczby przez drugą. Teoria liczb zajmuje się badaniem własności liczb całkowitych. Dopóki nie uogólnimy pojęcia liczby całkowitej, będziemy przez *liczby całkowite* rozumieli liczby

$$0, +1, -1, +2, -2, \ldots$$

W szczególności, liczby całkowite dodatnie, t. j. liczby ciągu

$$1, 2, 3, 4, 5, 6, \ldots$$

nazywać będziemy *liczbami naturalnymi*.

O dwu liczbach całkowitych a i b mówimy, że a jest *podzielne* (bez reszty) przez b — albo że a jest *wielokrotnością* liczby b, albo że b jest *dzielnikiem* liczby a — jeżeli istnieje taka liczba całkowita k, iż

$$a = kb.$$

Wyrażamy to na piśmie symbolem

$$b \mid a$$

(czytaj: b *jest dzielnikiem* a).

Twierdzenie 1. *Wzory*

$$a \mid b \quad i \quad b \mid c$$

pociągają za sobą zawsze wzór

$$a \mid c.$$

Dowód. W myśl założeń twierdzenia oraz w myśl definicji symbolu $x \mid y$, istnieją takie liczby całkowite k i l, iż

$$b = ka \quad \text{i} \quad c = lb,$$

skąd

$$c = lka,$$

a ponieważ iloczyn lk jest znowu liczbą całkowitą, więc ostatnia równość dowodzi, że $a \mid c$, c. b. d. o.

Dowiedzione twierdzenie możemy też wypowiedzieć w postaci:
Dzielnik dzielnika danej liczby jest znowu dzielnikiem tej liczby.

Moglibyśmy też powiedzieć, że stosunek $x|y$ jest *przechodni.*

Wniosek. *Jeżeli* $a|b$, *to przy wszelkim całkowitym* k *mamy* $a|kb$.

Z definicji dzielnika wynika bowiem, że przy wszelkich całkowitych b i k mamy $b|kb$, skąd wobec $a|b$ oraz w myśl twierdzenia 1 znajdujemy $a|kb$, c. b. d. o.

§ 2. Wspólne dzielniki dwu liczb. Jeżeli a, b i d są liczbami całkowitymi, takimi iż

$$d|a \quad \text{i} \quad d|b,$$

to d nazywamy *wspólnym dzielnikiem* liczb a i b.

Podobnie określamy wspólny dzielnik więcej niż dwu liczb całkowitych. Łatwo widzieć, że *wspólny dzielnik dwu liczb jest dzielnikiem ich sumy, jako też ich różnicy* (szczegółowy dowód pozostawiamy czytelnikowi). Stąd oraz z wniosku z twierdzenia 1 wynika natychmiast, że *jeżeli*

$$d|a \quad i \quad d|b,$$

to przy wszelkich całkowitych x *i* y *mamy*

$$d|(ax+by).$$

Łatwo też widzieć, że wspólny dzielnik dwu i więcej liczb jest dzielnikiem ich sumy algebraicznej.

§ 3. Największy wspólny dzielnik. Liczby względnie pierwsze. Największy ze wspólnych dzielników liczb $a, b, ..., l$ nazywamy *największym wspólnym dzielnikiem* tych liczb i oznaczamy przez $(a,b,...,l)$. Jasne jest, że jeżeli jedna przynajmniej z danych liczb $a,b,...,l$ nie jest zerem, to symbol $(a,b,...,l)$ ma oznaczoną wartość, przy czym

$$(a,b,...,l) \geqslant 1,$$

gdyż liczba 1 jest w każdym razie jednym ze wspólnych dzielników liczb $a,b,...,l$.

Dwie liczby a,b, dla których $(a,b)=1$, nazywamy *względnie pierwszymi.*

Łatwo widzieć, że *jeżeli liczby* a *i* b *podzielimy przez ich największy wspólny dzielnik* d, *to otrzymamy liczby względnie pierwsze.*

Istotnie, niech $a=da_1$ i $b=db_1$; liczby a_1 i b_1 są więc całkowite. Gdyby liczby a_1 i b_1 nie były względnie pierwsze, to ich największy wspólny dzielnik δ byłby większy od 1 i mielibyśmy $a_1=\delta a_2$ i $b_1=\delta b_2$ przy a_2 i b_2 całkowitych, skąd $a=d\delta a_2$ i $b=d\delta b_2$; to dowodzi, że liczba $d\delta$, która wobec $\delta>1$ jest większa od d, jest wspólnym dzielnikiem liczb a i b, co niemożliwe, skoro d jest największym wspólnym dzielnikiem tych liczb.

Łatwo dalej widzieć, że *jeżeli* $(a,b)=1$ *i* $\delta|a$, *to* $(\delta,b)=1$. Istotnie, gdyby było $(\delta,b)=d>1$, to mielibyśmy $d|\delta$, skąd wobec $\delta|a$ i twierdzenia 1 byłoby $d|a$, a z drugiej strony $d|b$. Liczba $d>1$ byłaby więc wspólnym dzielnikiem liczb a i b wbrew założeniu, że $(a,b)=1$.

Można dowieść, że dla liczb naturalnych k i m: jeżeli $k<17$, to w ciągu m, $m+1$, $m+2$, ..., $m+k-1$ istnieje co najmniej jedna liczba, która jest pierwsza względem każdej z pozostałych liczb tego ciągu. Nie jest to jednak prawdą dla $k=17$, $m=2184$, ani dla żadnej liczby $k>17$ (przy odpowiednich m).

Łatwo jest sprawdzić, że jeżeli a i b są dwiema różnymi liczbami z ciągu 17 kolejnych liczb 2184, 2185, ..., 2200, to $2\leqslant(a,b)\leqslant 13$. Po odrzuceniu bowiem liczb podzielnych przez 2, 3, 5 i 7 pozostaną 2 liczby podzielne przez 11 (mianowicie 2189 i 2200) oraz 2 liczby podzielne przez 13 (mianowicie 2184 i 2197).

Trudniej znacznie byłoby dowieść tego twierdzenia dla $k\leqslant 16$ (por. § 7, ćwiczenia 2 i 4), jako też twierdzenia, że dla każdej liczby naturalnej $k\geqslant 17$ istnieją liczby naturalne m, dla których żadna z liczb ciągu m, $m+1,...,m+k-1$ nie jest pierwszą względem każdej z pozostałych [1]).

§ 4. Najmniejsza wspólna wielokrotność. Liczbę całkowitą W, która jest podzielna przez każdą z liczb naturalnych $a,b,...,l$, nazywamy *wspólną wielokrotnością* tych liczb. Najmniejszą liczbę naturalną N, która jest wspólną wielokrotnością liczb naturalnych $a,b,...,l$, nazywamy *najmniejszą wspólną wielokrotnością* tych liczb i oznaczamy przez $[a,b,...,l]$. Liczba taka istnieje zawsze, gdyż istnieją liczby naturalne, podzielne przez każdą z liczb $a,b,...,l$ (np. ich iloczyn), w każdym zaś zbiorze (różnych) liczb naturalnych istnieje jedna najmniejsza.

Twierdzenie 2. *Każda wspólna wielokrotność liczb naturalnych* $a,b,...,l$ *jest podzielna przez najmniejszą wspólną wielokrotność tych liczb.*

[1]) Ob. S. S. Pillaï, Proceedings of the Indian Academy of Sciences, Section A, 11 (1940), str. 6-12, oraz L. Brauer, Bulletin of the American Mathematical Society 47 (1941), str. 328-331.

Dowód. Przypuśćmy, wbrew twierdzeniu, że wspólna wielokrotność W liczb naturalnych $a, b, ..., l$ nie jest podzielna przez najmniejszą wspólną wielokrotność N tych liczb. Oznaczając przez q iloraz całkowity z dzielenia W przez N, a przez r resztę z tego dzielenia, będziemy więc mieli

$$W = qN + r,$$

gdzie r jest liczbą naturalną mniejszą od N. Stąd $r = W - qN$, co dowodzi (ob. § 2), że liczba r jest podzielna przez każdą z liczb $a, b, ..., l$ (gdyż liczby W i N są przez te liczby podzielne). Liczba naturalna r byłaby więc wspólną wielokrotnością liczb $a, b, ..., l$, mniejszą od N, wbrew określeniu liczby N.

Tym samym twierdzenie 2 jest dowiedzione.

§ 5. Własność największego wspólnego dzielnika. Udowodnimy

Twierdzenie 3. *Największy wspólny dzielnik liczb całkowitych jest podzielny przez każdy inny wspólny dzielnik tych liczb.*

Dowód [1]). Niech $a, b, ..., l$ będą danymi liczbami całkowitymi, $d, d' d'', ...$ — ich wspólnymi dzielnikami i d — największym z nich. Oznaczmy przez n najmniejszą wspólną wielokrotność dzielników $d, d', d'', ...$ W myśl twierdzenia 2 każda z liczb $a, b, ..., l$, jako wspólna wielokrotność liczb $d, d', d'', ...$, jest podzielna przez n. Wynika stąd, że n jest wspólnym dzielnikiem liczb $a, b, ..., l$, zatem $n \leqslant d$, gdyż d jest największym wspólnym dzielnikiem tych liczb. Lecz z drugiej strony musi być $n \geqslant d$, gdyż n jest wielokrotnością liczb $d, d', ...$ Zatem $n = d$; dowodzi to, że d jest podzielne przez każdą z liczb $d, d', d'', ...$, c. b. d. o.

§ 6. Zależność między największym wspólnym dzielnikiem a najmniejszą wspólną wielokrotnością dwu liczb. Zachodzi następujące

Twierdzenie 4. *Iloczyn dwu liczb naturalnych jest równy iloczynowi ich największego wspólnego dzielnika przez ich najmniejszą wspólną wielokrotność.*

Dowód. Niech N oznacza najmniejszą wspólną wielokrotność liczb naturalnych a i b. Ponieważ iloczyn ab jest oczywiście wspólną wielokrotnością liczb a i b, więc w myśl twierdzenia 2

[1]) według Stieltjesa.

ab jest podzielne przez N i przeto możemy napisać

$$ab = dN, \tag{1}$$

gdzie d jest liczbą naturalną, Z drugiej strony, skoro N jest wielokrotnością liczb a i b, to mamy

$$N = ka \quad \text{i} \quad N = lb, \tag{2}$$

gdzie k i l są liczbami naturalnymi. Wobec (1) i (2) znajdujemy

$$ab = dka \quad \text{i} \quad ab = dlb,$$

zatem

$$b = dk \quad \text{i} \quad a = dl,$$

co dowodzi, że d jest wspólnym dzielnikiem liczb a i b.

Niech teraz δ oznacza jakikolwiek wspólny dzielnik liczb a i b. Mamy więc

$$a = \delta a_1 \quad \text{i} \quad b = \delta b_1, \tag{3}$$

gdzie a_1 i b_1 są liczbami naturalnymi. Wobec (3) znajdujemy

$$\delta a_1 b_1 = a b_1 \quad \text{i} \quad \delta a_1 b_1 = a_1 b,$$

co dowodzi, że liczba $\delta a_1 b_1$ jest wspólną wielokrotnością liczb a i b, a przeto w myśl twierdzenia 2 musi być podzielna przez N:

$$\delta a_1 b_1 = Nt, \tag{4}$$

gdzie t jest liczbą całkowitą. Lecz na mocy (1) i (3) jest

$$dN = ab = \delta^2 a_1 b_1,$$

skąd wobec (4) jest $dN = \delta Nt$, a stąd $d = \delta t$, czyli $\delta | d$.

Liczba d jest więc wspólnym dzielnikiem liczb a i b, podzielnym przez każdy inny wspólny dzielnik δ tych liczb, co dowodzi, że d jest największym wspólnym dzielnikiem liczb a i b. Ze wzoru (1) wynika więc prawdziwość twierdzenia.

W szczególności, jeżeli $(a, b) = 1$, to $d = (a, b) = 1$ i wzór (1) daje $ab = N$. Mamy więc

Wniosek. *Najmniejszą wspólną wielokrotnością dwu liczb naturalnych względnie pierwszych jest ich iloczyn.*

§ 7. Zasadnicze twierdzenie arytmetyki. Niech teraz a i b będą dwiema liczbami naturalnymi względnie pierwszymi, a c taką liczbą naturalną, iż $b | ac$. Liczba ac jest więc podzielna przez a i przez b, zatem też, w myśl twierdzenia 2, przez najmniejszą wspólną wielokrotność tych liczb, która wobec $(a, b) = 1$ oraz w myśl wniosku z twierdzenia 4, jest ich iloczynem ab. Mamy więc $ac = tab$, gdzie t jest liczbą całkowitą, skąd $c = tb$ czyli $b | c$.

Udowodniliśmy w ten sposób

Twierdzenie 5. *Liczba dzieląca iloczyn dwu liczb i pierwsza względem jednego z czynników jest dzielnikiem drugiego czynnika.*

Twierdzenie to, zwane niekiedy *zasadniczym twierdzeniem arytmetyki*, udowodniliśmy dla liczb naturalnych, łatwo jednak widzieć, że jest ono prawdziwe dla wszelkich liczb całkowitych, gdyż zmiana znaku nie wpływa na podzielność jednej liczby przez drugą.

ĆWICZENIE. Dowieść następującego uogólnienia twierdzenia 5: *Jeżeli* (dla liczb całkowitych a, b i c) *mamy* $c \mid ab$, *to* $c \mid b(a,c)$ [1]).

Twierdzenie 6. *Jeżeli liczby a, b i c są całkowite oraz*

$$(a,c)=1 \qquad i \qquad (b,c)=1,$$

to mamy też

$$(ab,c)=1.$$

Dowód. Niech $(ab,c)=d$; wobec $d \mid c$ i $(a,c)=1$ będziemy mieli (ob. § 3) $(d,a)=1$, skąd wobec $d \mid ab$ oraz w myśl twierdzenia 5 znajdujemy $d \mid b$, a stąd wobec $d \mid c$ i $(b,c)=1$ otrzymujemy $d=1$ czyli $(ab,c)=1$, c. b. d. o.

Twierdzenie 6 uogólnia się z łatwością na dowolną liczbę czynników. Jeżeli np. mamy liczby całkowite a_1, a_2, a_3, a_4 i c, takie iż

$$(a_1,c)=1, \qquad (a_2,c)=1, \qquad (a_3,c)=1, \qquad (a_4,c)=1,$$

to możemy, wobec dwu pierwszych równości i w myśl dowiedzionego twierdzenia 6, napisać $(a_1a_2,c)=1$, co wobec $(a_3,c)=1$ daje, znów w myśl twierdzenia 6, $(a_1a_2a_3,c)=1$, skąd znowu wobec $(a_4,c)=1$ znajdujemy w tenże sposób

$$(a_1a_2a_3a_4,c)=1,$$

Zatem *liczba, pierwsza względem każdego z czynników, jest pierwszą względem ich iloczynu.*

Twierdzenie 7. *Jeżeli liczba naturalna jest m-tą potęgą liczby wymiernej, to jest też m-tą potęgą liczby naturalnej* (dla naturalnych m).

Dowód. Załóżmy, że liczba naturalna n jest m-tą potęgą liczby wymiernej p/q. Możemy tu oczywiście założyć, że q jest liczbą naturalną i że liczby p i q są względnie pierwsze. Skoro $n=(p/q)^m$, to $nq^m=p^m$, skąd $q \mid p^m$; wobec twierdzenia 5 i uwagi, że $(p,q)=1$, jest to możliwe tylko w razie $q=1$, skąd $n=p^m$, c. b. d. o.

[1]) B. A. Niewęgłowski, Wiadomości Matematyczne 6 (1906), str. 252.

Z twierdzenia 7 wynika natychmiast

Wniosek. *Pierwiastek m-tego stopnia z liczby naturalnej, która nie jest m-tą potęgą liczby naturalnej, jest liczbą niewymierną.*

W szczególności wynika stąd, że liczby:

$$\sqrt{2},\ \sqrt{3},\ \sqrt{5},\ \sqrt{6},\ \sqrt{7},\ \sqrt{8},\ \sqrt{10},\ \sqrt[3]{2},\ \sqrt[3]{3},\ \sqrt[3]{4}$$

są niewymierne.

Od stuleci nie jest rozstrzygnięte pytanie, czy poza parą liczb 8 i 9 istnieją dwie kolejne liczby naturalne, będące potęgami innych liczb naturalnych o wykładnikach większych od jedności.

ĆWICZENIA. 1. Dowieść, że jeżeli liczby x i y są całkowite i $z=x+y$, to każda z liczb x, y i z jest dzielnikiem liczby $z^3-x^3-y^3$.

2. Dowieść, że jeżeli m jest liczbą naturalną, to wśród liczb

$$m, \quad m+1, \quad m+2, \quad m+3$$

istnieje co najmniej jedna, która jest pierwszą względem każdej z trzech pozostałych.

Dowód. Łatwo widzieć, że jeżeli liczba m jest nieparzysta, to

$$(m+2,\ m(m+1)(m+3))=1,$$

jeżeli zaś liczba m jest parzysta, to

$$(m+1,\ m(m+2)(m+3))=1.$$

3. Kiedy spośród trzech kolejnych liczb naturalnych każde dwie są względnie pierwsze?

Odpowiedź. Gdy najmniejsza z nich jest nieparzysta.

4. Dowieść, że wśród dziesięciu jakichkolwiek kolejnych liczb naturalnych

(*) $$m, \quad m+1, \quad \ldots, \quad m+9$$

istnieje co najmniej jedna taka, która jest pierwsza względem wszystkich pozostałych.

Dowód. Wśród dziesięciu kolejnych liczb naturalnych mamy 5 nieparzystych, wśród pięciu zaś kolejnych liczb nieparzystych mamy — jak łatwo widzieć — co najmniej trzy niepodzielne przez 3. Lecz wśród nieparzystych, gdzie różnica między największą a najmniejszą jest mniejsza od 10, istnieje co najwyżej jedna podzielna przez 5 i co najwyżej jedna podzielna przez 7. Wnosimy stąd, że wśród dziesięciu kolejnych liczb naturalnych istnieje co najmniej jedna taka, która jest niepodzielna przez 2, 3, 5 i 7. Taka liczba a jest — jak łatwo widzieć — pierwsza względem każdej innej b spośród liczb (*), gdyż w razie $(a,b)\neq 1$ liczby a i b posiadałyby wspólny dzielnik pierwszy p. Musiałoby tu być $p>7$, zatem $p\geqslant 11$, gdyż liczba a jest niepodzielna przez 2, 3, 5 i 7. Lecz dwie różne z liczb ciągu (*) nie mogą być jednocześnie podzielne przez żadną liczbę większą lub równą 10. Jest więc $(a,b)=1$, c, b. d. o.

5. Dowieść, że (przy całkowitych x i y) jeśli liczba $11x+2y$ jest podzielna przez 19, to i liczba $18x+5y$ jest podzielna przez 19. (J. Fitz-Patrick).

Dowód wynika natychmiast z tożsamości

$$7(11x+2y)+(18x+5y)=19(5x+y).$$

6. Dowieść, że każda liczba całkowita różna od 0 może być przedstawiona w postaci $(3x-1)(2y-1)$, gdzie x i y są liczbami całkowitymi, i podobnie w postaci $(3x+1)(2y+1)$.

7. Dowieść, że dla naturalnego n iloczyn $n(n+1)(n+2)$ jest wtedy i tylko wtedy podzielny przez 4, gdy n nie jest postaci $4k+1$, gdzie $k=0,1,2,\ldots$

8. Dowieść, że dla naturalnych n liczba $n(n+1)(n+2)(n+3)$ jest podzielna przez 8, lecz nie zawsze jest podzielna przez 16.

9. Dowieść, że dla naturalnych n iloczyn n kolejnych liczb naturalnych $k(k+1)\ldots(k+n-1)$ jest podzielny przez $n!$

Dowód wynika ze wzoru

$$\frac{k(k+1)\ldots(k+n-1)}{n!}=\binom{k+n-1}{n}.$$

§ 8. Liczby pierwsze i ich ważniejsze własności. Liczby złożone i ich rozkład na czynniki pierwsze. Liczbę całkowitą p, większą od jedności, nazywamy *liczbą pierwszą*, jeżeli p posiada tylko dwa dzielniki naturalne (mianowicie 1 i p).

Twierdzenie 8. *Każda liczba całkowita większa od jedności posiada przynajmniej jeden dzielnik, będący liczbą pierwszą.*

Dowód. Niech dana będzie liczba całkowita $n>1$. Liczba n posiada dzielniki większe od jedności, gdyż samo n jest jednym z nich. Oznaczmy przez d *najmniejszy* ze wszystkich większych od jedności dzielników liczby n. Udowodnimy, że d jest liczbą pierwszą. Przypuśćmy bowiem, że d nie jest liczbą pierwszą; w myśl definicji liczb pierwszych, istniałaby liczba δ większa od jedności, lecz mniejsza od d, będąca dzielnikiem dla d, a tym bardziej dla n, co znów przeczy założeniu, że d oznacza najmniejszy ze wszystkich większych od jedności dzielników liczby n. Twierdzenie zostało tym samym udowodnione.

Wniosek. *Każda liczba całkowita $n>1$, która nie jest liczbą pierwszą, daje się przedstawić jako iloczyn samych tylko czynników pierwszych i to tylko w jeden sposób.*

Dowód. Niech n będzie liczbą całkowitą, większą od jedności i nie będącą liczbą pierwszą. Liczba n ma więc w myśl twierdzenia 8 dzielnik pierwszy p.

Dzielnik ten spełnia nierówność $1<p<n$, tak iż można napisać

$$n=pn',$$

gdzie n' jest liczbą całkowitą. Ponieważ $n'=n/p$, znajdziemy wobec nierówności dla p:

$$1<n'<n.$$

Jeżeli n' jest liczbą pierwszą, to wzór $n=pn'$ przedstawia już rozkład liczby n na iloczyn samych czynników pierwszych; w przeciwnym razie możemy dla liczby n' powtórzyć rozumowanie, któreśmy zastosowali do liczby n, wyznaczając dzielnik pierwszy p' liczby n' i pisząc

$$n=p'n''.$$

gdzie $1<n''<n'$.

Jeżeli n'' nie jest liczbą pierwszą, to powyższe rozumowanie możemy znów powtórzyć i t. d.

Ciąg równości:

$$n=pn', \qquad n'=p'n'', \qquad n''=p''n''', \qquad \ldots$$

nie może być nieskończony, gdyż liczby n', n'', n''', ... (jako wyrazy ciągu malejącego) są różnymi liczbami naturalnymi, zawartymi między 1 a n. W ciągu tych równości istnieje zatem ostatnia. Niech nią będzie równość r-ta:

$$n^{(r-1)}=p^{(r-1)}n^{(r)}.$$

Gdyby liczba $n^{(r)}$ nie była pierwszą, to powtarzając dla $n^{(r)}$ powyższe rozumowanie, moglibyśmy napisać jeszcze równość $(r+1)$-szą, co przeczyłoby założeniu, że r-ta jest ostatnią. Liczba $n^{(r)}$ jest więc liczbą pierwszą; oznaczmy ją przez $p^{(r)}$. Otrzymaliśmy ciąg równości:

$$n=pn', \quad n'=p'n'', \quad n''=p''n''', \quad \ldots, \quad n^{(r-1)}=p^{(r-1)}p^{(r)},$$

skąd natychmiast

$$n=pp'p''\ldots p^{(r-1)}p^{(r)}, \tag{5}$$

gdzie strona prawa jest iloczynem samych tylko czynników pierwszych. Wniosek został więc udowodniony.

Ponieważ te liczby całkowite, które nie są same pierwszymi, rozwijają się na iloczyn liczb pierwszych, nazywamy je *złożonymi*.

Liczby 1 nie zaliczamy ani do liczb pierwszych, ani do liczb złożonych.

Zbierając we wzorze (5) równe czynniki, możemy ten wzór przedstawić jeszcze w postaci

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \tag{6}$$

gdzie $p_1, p_2, \dots, p_k$ są to same różne liczby pierwsze, każdy zaś z wykładników $\alpha_1, \alpha_2, \dots, \alpha_k$ jest liczbą naturalną. Tym samym udowodniliśmy pierwszą część twierdzenia 8 (istnienie rozkładu na czynniki pierwsze).

Uwaga. Liczby pierwsze mogą być też objęte wzorem (6), mianowicie dla $k=1$ i $\alpha_1=1$. Wzór (6), przy odpowiednim naturalnym k oraz naturalnych α, może więc przedstawiać każdą liczbę całkowitą $n>1$.

Wzór (6) nazywamy *rozwinięciem liczby n na czynniki pierwsze.*

Udowodnimy obecnie drugą część twierdzenia, mianowicie, że *każda liczba całkowita $n>1$ daje jeden tylko rozkład na czynniki pierwsze* (jeżeli nie zwracać uwagi na porządek czynników).

Dowód oprzemy na następującym lemacie:

Lemat. *Jeżeli a jest liczbą całkowitą, p zaś liczbą pierwszą, to albo a jest podzielne przez p, albo a i p są względnie pierwsze.*

Istotnie, jeżeli p jest liczbą pierwszą, to posiada tylko dwa dzielniki naturalne: 1 i p, może więc być tylko $(a,p)=1$ lub $(a,p)=p$. W pierwszym wypadku liczby a i p są względnie pierwsze, w drugim mamy oczywiście $p|a$.

Jako natychmiastowy wniosek z lematu dostajemy:

Jeżeli p i q są liczbami pierwszymi, to albo $(p,q)=1$, albo $p=q$.

Załóżmy teraz, że

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k} \quad \text{i} \quad n = q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}$$

przedstawiają dwa rozwinięcia liczby n na czynniki pierwsze.

Gdyby żadna z liczb pierwszych $q_1, q_2, \dots, q_l$ nie była równa liczbie p_1, to każda z tych liczb byłaby pierwszą względem p_1. Liczba n byłaby więc iloczynem samych liczb pierwszych względem p_1, a więc na mocy twierdzenia 6 sama byłaby liczbą pierwszą względem p_1, co przeczy pierwszemu z wypisanych dla n rozwinięć. Wśród liczb q znajduje się więc liczba p_1. To samo możemy oczywiście powiedzieć o każdej z pozostałych liczb $p_2, p_3, \dots, p_k$. Zupełnie tak samo możemy dowieść, że każda z liczb $q_1, q_2, \dots, q_l$ jest równa jednej z liczb $p_1, p_2, \dots, p_k$.

Mamy więc dwa zbiory samych różnych liczb:

$$p_1, p_2, \dots, p_k \quad \text{i} \quad q_1, q_2, \dots, q_l$$

takie, że każda liczba pierwszego zbioru znajduje się w drugim zbiorze i na odwrót. Jasnym jest, że zbiory takie mogą się różnić co najwyżej porządkiem swych elementów. Zakładając, że zbiory zostały jednakowo uporządkowane (np. według wielkości swych elementów), będziemy mieli:

$$p_1 = q_1, \quad p_2 = q_2, \quad \dots, \quad p_k = q_l,$$

przy czym oczywiście $k=l$.

Wreszcie udowodnimy, że

$$\alpha_1 = \beta_1 \quad \alpha_2 = \beta_2, \quad \dots, \quad \alpha_k = \beta_l.$$

Przypuśćmy np., że $\alpha_1 < \beta_1$: będzie więc $\beta_1 = \alpha_1 + \delta_1$, gdzie δ_1 jest liczbą naturalną. Z równości

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

po podzieleniu obu stron przez $p_1^{\alpha_1}$, otrzymujemy:

$$p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k} = p_1^{\delta_1} p_2^{\beta_2} \dots p_k^{\beta_k}.$$

Prawa strona, jako zawierająca czynnik $p_1^{\delta_1}$, musi być podzielna przez liczbę pierwszą p_1, gdy tymczasem lewa strona jest iloczynem samych liczb pierwszych różnych od p_1, a więc liczbą pierwszą względem p_1. Ta sprzeczność dowodzi, że nie może być $\alpha_1 < \beta_1$. Zupełnie tak samo dowiedlibyśmy, że nie może być $\beta_1 < \alpha_1$. Musi więc być $\alpha_1 = \beta_1$. Podobnie $\alpha_2 = \beta_2$ i t. d.

Dowiedliśmy zatem, że każda liczba całkowita większa od jedności, daje jeden i tylko jeden rozkład na czynniki pierwsze (jeżeli nie uważamy za różne rozwinięć, które się różnią jedynie porządkiem czynników).

Gdy mamy rozwinięcia liczb a i b na czynniki pierwsze:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \qquad b = q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l},$$

to największy ich wspólny dzielnik, jak również najmniejsza ich wspólna wielokrotność, mogą być — jak łatwo widzieć — znalezione w następujący sposób.

Aby otrzymać (a, b), wypisujemy wszystkie te czynniki pierwsze, które występują w obu rozwinięciach, każdy w najniższej potędze, w jakiej występuje.

Aby otrzymać $[a, b]$, wypisujemy wszystkie czynniki pierwsze obu rozwinięć, każdy w najwyższej potędze w jakiej występuje [1]). Podobnie postępujemy dla więcej niż dwu liczb.

ĆWICZENIA. 1. Dowieść, że dla wszelkich całkowitych $a_1, a_2, ..., a_n$ mamy

$$\left.\begin{array}{l}(a_1 a_2 \dots a_n \pm 1, a_i) = 1\\ ([a_1, a_2, ..., a_n] \pm 1, a_i) = 1\end{array}\right\} \quad \text{dla } i = 1, 2, ..., n.$$

Dla każdego ciągu skończonego liczb całkowitych potrafimy więc za pomocą elementarnych działań arytmetycznych znaleźć liczbę pierwszą względem każdego z wyrazów tego ciągu.

2. Dowieść, że dla wszelkich liczb naturalnych a, b, c mamy

$$[(a, b), c] = ([a, c], [b, c]) \quad \text{i} \quad ([a, b], c) = [(a, c), (b, c)].$$

Wzory te dowodzą, że wyznaczanie największego wspólnego dzielnika i najmniejszej wspólnej wielokrotności są dwoma działaniami na liczbach naturalnych, z których każde jest rozdzielne względem drugiego.

3. Dowieść, że jeżeli liczby a i b są nieparzyste i względnie pierwsze, a m jest liczbą naturalną, to

$$((a+b)^m, (a-b)^m) = 2^m, \qquad (a^m + b^m, a^m - b^m) = 2.$$

4. Dowieść, że w każdym ciągu skończonym kolejnych liczb naturalnych

$$(*) \qquad n, \quad n+1, \quad \dots, \quad n+k$$

istnieje liczba, która jest podzielna przez pewną taką potęgę liczby 2, przez którą nie jest podzielna żadna inna liczba tego ciągu.

Dowód. Niech 2^α oznacza najwyższą potęgę liczby 2, która jest dzielnikiem co najmniej jednej z liczb (*), np. liczby $n+q$. Musi więc być $n+q = 2^\alpha(2t-1)$, gdzie t jest całkowite. Gdyby istniała jeszcze liczba $n+r$ ciągu (*) podzielna przez 2^α, to musiałoby być $n+r = 2^\alpha(2s-1)$ i w razie, gdyby było np. $n+q < n+r$, mielibyśmy $2t-1 < 2s-1$, skąd $2t-1 < 2t < 2s-1$, oraz $n+q < 2^{\alpha+1}t < n+r$. Liczba $2^{\alpha+1}t$ należałaby więc do ciągu (*) i byłaby podzielna przez $2^{\alpha+1}$, wbrew określeniu liczby α. W ciągu (*) istnieje więc tylko jedna liczba podzielna przez 2^α.

5. Opierając sie na ćwiczeniu 4, dowieść, że dla naturalnych n i k liczba $S = \frac{1}{n} + \frac{1}{n+1} + \dots + \frac{1}{n+k}$ nie może być całkowita.

Dowód wynika stąd, że jeżeli $n+q$ jest liczbą ciągu (*) podzielną przez 2^α i taką, że żadna inna liczba tego ciągu nie jest podzielna przez 2^α, to po sprowadzeniu sumy S do najmniejszego wspólnego mianownika, licznik nie będzie podzielny przez 2^α.

6. Dowieść, że każdą potęgę liczby naturalnej o wykładniku naturalnym $n > 1$ można w jeden i tylko jeden sposób przedstawić jako sumę tylu kolejnych liczb nieparzystych, ile wynosi podstawa tej potęgi.

[1]) Twierdzenie, że $(a, b)[a, b] = ab$, wynika wówczas z łatwością z uwagi, że dla wszelkich całkowitych α i β mamy $\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$.

Dowód. Niech będą dane liczby naturalne a i $n > 1$. Chcemy, aby było $a^n = (2x+1) + (2x+3) + \dots + (2x+2a-1)$. Ponieważ $1+3+5+\dots+(2a-1) = a^2$, więc $a^n = 2ax + a^2$, co daje $x = \frac{a^{n-1} - a}{2}$. Skoro $n > 1$, więc a^{n-1} jest parzyste lub nieparzyste jednocześnie z a, zatem x jest liczbą całkowitą i, jak łatwo widzieć, $x \geqslant 0$. Stąd łatwy wniosek, że istnieje żądany rozkład i to tylko jeden.

7. Dowieść, że każda liczba naturalna n daje się w jeden i tylko jeden sposób przedstawić w postaci b^k, gdzie b i k są liczbami naturalnymi, przy czym b nie jest potęgą żadnej liczby naturalnej o wykładniku większym od 1.

Uwaga. Można okazać, że k jest największą liczbą naturalną, dla której liczba $\sqrt[k]{n}$ jest naturalna. Jeżeli $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ jest rozkładem liczby n na czynniki pierwsze, to $k = (\alpha_1, \alpha_2, ..., \alpha_s)$.

Na to więc żeby liczba naturalna $n > 1$ nie była potęgą żadnej liczby naturalnej o wykładniku większym od 1, potrzeba i wystarcza, by $(\alpha_1, \alpha_2, ..., \alpha_s) = 1$. Niech Z będzie zbiorem wszystkich takich właśnie liczb naturalnych. Jak łatwo widzieć — jeżeli dla każdej liczby zbioru Z wypiszemy kolejno wszystkie jej potęgi naturalne, to otrzymamy wszystkie liczby naturalne większe od 1, każdą raz tylko. Daje nam to podwójny ciąg nieskończony:

$$\begin{array}{l}2, \ 2^2, \ 2^3, \ 2^4, \dots\\ 3, \ 3^2, \ 3^3, \ 3^4, \dots\\ 5, \ 5^2, \ 5^3, \ 5^4, \dots\\ 6, \ 6^2, \ 6^3, \ 6^4, \dots\\ 7, \ 7^2, \ 7^3, \ 7^4, \dots\\ 10, \ 10^2, \ 10^3 \ 10^4, \dots\\ \dots\dots\dots\\ \dots\dots\dots\\ \dots\dots\dots\end{array}$$

W każdym z otrzymanych w ten sposób wierszy występuje jedna tylko liczba ze zbioru Z, mianowicie pierwsza w wierszu. Na każdą liczbę zbioru Z przypada zatem nieskończenie wiele liczb nie należących do Z. Zdawałoby się więc, że liczby zbioru Z są wśród liczb naturalnych rzadkie. Okażemy jednak, że jest wręcz przeciwnie [1]), że rzadkimi są liczby naturalne nie należące do Z. Zbiór ich oznaczymy przez T.

O zbiorze X liczb naturalnych mówimy, że jest w zbiorze wszystkich liczb naturalnych *rzadki*, jeżeli oznaczając dla każdej liczby naturalnej n przez X_n liczbę wszystkich niewiększych od n liczb zbioru X, mamy $\lim_{n=\infty} \frac{X_n}{n} = 0$.

Jeżeli jest $b^k \leqslant n$, gdzie b i k są liczbami naturalnymi większymi od 1, to $b \leqslant \sqrt{n}$ oraz $k \leqslant \lg n / \lg 2$. Liczb takich jest więc nie więcej niż $\frac{\sqrt{n} \lg n}{\lg 2}$, a że — jak wiadomo z Analizy — jest $\lim_{n=\infty} \frac{\lg n}{\sqrt{n}} = 0$, więc łatwy stąd wniosek, że

[1]) Paradoks ten podał E. Borel.

$\lim_{n=\infty}\frac{T_n}{n}=0$, gdyż $T_n\leqslant 1+\frac{\sqrt{n}\lg n}{2}$. Zbiór T jest więc rzadki w zbiorze wszystkich liczb naturalnych, c. b. d. o.

8. Dowieść, że jeżeli a i b są różnymi liczbami naturalnymi, nie będącymi potęgami innych liczb naturalnych o wykładniku większym od 1, to przy żadnych naturalnych k i l nie może być $a^k=b^l$.

9. Dowieść, że kwadrat każdej liczby pierwszej $p>3$ jest postaci $24k+1$, gdzie k jest liczbą naturalną.

§ 9. Dowód, że liczb pierwszych jest nieskończenie wiele. Zapytamy obecnie, ile jest liczb pierwszych. Już Euklides dowiódł, że liczb pierwszych jest nieskończenie wiele. Udowodnimy następujące

Twierdzenie 9. *Jeżeli n jest liczbą naturalną i $n>2$, to między n a $n!$ znajduje się co najmniej jedna liczba pierwsza* [1]).

Dowód. Ponieważ $n>2$, więc liczba całkowita

$$N=n!-1$$

jest oczywiście większa od 1, musi więc posiadać dzielnik pierwszy p. Nie może być $p\leqslant n$, gdyż przez żadną liczbę naturalną, większą od jedności i nie większą od n, liczba N oczywiście nie jest podzielna. Jest więc $p>n$, a z drugiej strony oczywiście $p\leqslant N$, gdyż p jest dzielnikiem liczby N. Liczba pierwsza p spełnia więc nierówność

$$n<p<n!$$

Można udowodnić, że dla $n>3$ już między n a $2n-2$ zawiera się co najmniej jedna liczba pierwsza. Jest to t. zw. *postulat Bertranda*, udowodniony przez Czebyszewa w roku 1850. Dowód tego twierdzenia jest już jednak bardzo trudny, chociaż nie należy jeszcze do najtrudniejszych w Teorii liczb.

Breusch udowodnił następujące dwa uogólnienia postulatu Bertranda [2]):

1) Jeżeli $x\geqslant 48$, to między x a $^9/_8x$ leży co najmniej jedna liczba pierwsza.

2) Jeżeli $x\geqslant 7$, to między x a $2x$ leży co najmniej jedna liczba pierwsza każdej z postaci $3k+1$, $3k+2$, $4k+1$, $4k+3$.

[1]) $n!$ oznacza iloczyn $1\cdot 2\cdot 3\cdot\ldots\cdot n$.

[2]) R. Breusch, Mathematische Zeitschrift 34 (1932), str. 505-526.

Nie wiadomo natomiast, czy dla każdej liczby naturalnej n istnieje taka liczba pierwsza p, dla której $n^2<p<(n+1)^2$.

Dowiedliśmy wyżej (tw. 8), że jeżeli n jest liczbą złożoną, to najmniejszy dzielnik tej liczby większy od jedności jest liczbą pierwszą. Okażemy obecnie, że ten dzielnik p spełnia nierówność

$$p\leqslant\sqrt{n}.$$

Istotnie, niech $n=pm$, gdzie oczywiście $1<m<n$.

Gdyby było $p>\sqrt{n}$, to wobec $m=\frac{n}{p}$ mielibyśmy $m<\frac{n}{\sqrt{n}}$ czyli $m<\sqrt{n}<p$, skąd $m<p$, wbrew założeniu, że p jest najmniejszym z większych od jedności dzielników liczby n.

Jako natychmiastowy wniosek stąd otrzymujemy

Twierdzenie 10. *Jeżeli liczba całkowita $n>1$ nie jest podzielna przez żadną z liczb pierwszych nie większych od $\sqrt{n}$, to sama jest liczbą pierwszą.*

Więc np., żeby się przekonać, że 641 jest liczbą pierwszą, wystarczy sprawdzić, że liczba 641 nie jest podzielna przez żadną z liczb pierwszych $p\leqslant\sqrt{641}$, t. j. przez żadną z liczb:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23.$$

Z twierdzenia 10 wynika natychmiast, że dla otrzymania wszystkich liczb pierwszych ciągu $2, 3, \ldots, n$ wystarczy usunąć z tego ciągu wszystkie wielokrotności liczb pierwszych niewiększych od $\sqrt{n}$.

Łatwy sposób otrzymywania kolejnych liczb pierwszych podał matematyk grecki Eratosthenes. Bardzo przystępnie opisuje ten sposób Ruziewicz [1]):

„Wypisujemy kolejne liczby naturalne, począwszy od liczby 2. Zaliczając 2 do zbioru liczb pierwszych, wykreślamy z pozostałego zbioru (a więc rozpoczynając liczenie od 3) co drugą liczbę, a więc każdą liczbę większą od 2 i podzielną przez 2. Pierwsza liczba, która nie została wykreślona, a więc w tym wypadku 3, nie jest podzielna przez 2, nie jest zatem podzielna przez żadną liczbę pierwszą mniejszą od niej, a że musi być przez jakąś liczbę pierwszą podzielna, więc sama jest pierwszą. Dołączając

[1]) S. Ruziewicz, *Z zagadnień matematyki, III. Co wiemy, a czego nie wiemy o liczbach całkowitych?* Kosmos B 53 (1928), str. 234-235.

znów 3 do zbioru liczb pierwszych, wykreślamy dalej, rozpoczynając od 4, co trzecią liczbę, a więc wszystkie liczby podzielne przez 3, z wyjątkiem samej liczby 3 (przy liczeniu liczby wykreślone w poprzednim stadium liczymy tak, jakby nie były wykreślone, a więc np. rozpoczynamy liczenie co trzeciej liczby od 4, chociaż 4 zostało już poprzednio wykreślone). Pierwsza liczba, która pozostała niewykreślona ani w pierwszym, ani w drugim stadium (jest nią liczba 5), musi być liczbą pierwszą. Jakkolwiek twierdzenie, że 5 jest liczbą pierwszą, wynika z tabliczki mnożenia i najprostszych twierdzeń o liczbach całkowitych, przeprowadzamy tu rozumowanie, jakie przeprowadza się przy postępowaniu Eratosthenesa, gdyż w tym stadium zrozumiemy już, dlaczego postępowanie to doprowadza nas do samych liczb pierwszych. Otóż obecnie nie ma już w naszej tablicy żadnej liczby podzielnej przez 2, ani żadnej liczby podzielnej przez 3, z wyjątkiem liczb pierwszych 2 i 3. Jakąż własność musi mieć pierwsza z kolei po 3 niewykreślona liczba? Nie jest ona podzielna przez żadną liczbę pierwszą od niej mniejszą (a więc ani przez 2, ani przez 3), ponieważ wszystkie liczby złożone, podzielne przez jedną z takich liczb, wykreśliliśmy z tablicy. Ponieważ zaś musi liczba ta, jako większa od 1, być przez jakąś liczbę pierwszą podzielna, więc musi sama być liczbą pierwszą. 5 jest zatem liczbą pierwszą. Począwszy teraz od 6, wykreślamy co piątą liczbę (nie uwzględniając przy tym liczeniu, że niektóre liczby zostały wykreślone w poprzednich stadiach), a więc wykreślamy wszystkie liczby podzielne przez 5. Teraz więc żadna liczba nie wykreślona w jednym z dotychczasowych stadiów, oprócz 2, 3, 5, nie jest podzielna ani przez 2, ani przez 3, ani przez 5. Pierwsza z kolei napotkana nie wykreślona liczba, tj. 7, musi więc być (o czym przekonywamy się, rozumując jak o liczbie 5) liczbą pierwszą. Dalej rozpoczynając liczenie od 8, wykreślamy co siódmą liczbę z kolei i tak postępujemy dalej.

Otrzymujemy w ten sposób tablicę, w której pozostały, jako nie wykreślone, same liczby pierwsze.

Tablica otrzymana sposobem Eratosthenesa nosi nazwę *sita Eratosthenesa*. Oczywiście metoda otrzymywania liczb pierwszych przy pomocy sita Eratosthenesa nie daje nam dowodu na to, że liczb tych jest nieskończenie wiele, nie wiemy bowiem *a priori*, czy po jakimś stadium wykreślania nie okaże się, że wszystkie liczby, począwszy od jakiejś, zostały już wykreślone

Widzimy, jak niezmiernie prosty, a nawet mechaniczny, jest sposób uzyskiwania kolejnych liczb pierwszych przy pomocy sita. Wydawałoby się zatem, że rozkład liczb, jakie otrzymujemy po „przesianiu", czyli rozkład liczb pierwszych, jest niezmiernie prosty, że np. łatwo przewidzieć, ile wynosi tysięczna z kolei liczba pierwsza, i że istnieją jakieś proste wzory, pozwalające nam to obliczyć. Okazuje się jednak, że tak nie jest. Rozkład liczb pierwszych jest bardzo skomplikowany, liczby te są rozrzucone bardzo nieregularnie. Wzoru, pozwalającego nam obliczyć liczbę pierwszą, znajdującą się na oznaczonym z kolei miejscu (np. tysięczną, milionową i t. p.), nie posiadamy".

Dla otrzymania wszystkich liczb pierwszych nieparzystych nie większych od n^2 (gdzie n jest daną liczbą naturalną większą od jedności) można też postępować jak następuje. Tworzymy ciągi:

$$
\begin{array}{llllllll}
9, & 15, & 21, & 27, & 33, & 39, & \ldots \\
25, & 35, & 45, & 55, & 65, & 75, & \ldots \\
49, & 63, & 77, & 91, & 105, & 119, & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
q^2, & q^2+2q, & q^2+4q, & q^2+6q, & q^2+8q, & q^2+10q, & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots
\end{array}
$$

i wypisujemy je dopóty, dopóki otrzymujemy liczby mniejsze niż n^2. Liczby nieparzyste, nie zawarte w tych ciągach, są szukanymi liczbami pierwszymi.

Dowód opiera się na tym, że wszystkie liczby postaci $q^2+2kq=q(q+2k)$, gdzie $q\geqslant 3$ i $k\geqslant 0$, są złożone, oraz że jeżeli m jest liczbą złożoną nieparzystą, a q jej najmniejszym dzielnikiem pierwszym (oczywiście nieparzystym), to $m=qr$, przy czym r, jako liczba nieparzysta niemniejsza od q, jest postaci $q+2k$, gdzie k jest liczbą całkowitą nieujemną.

Sito to nie różni się istotnie od erastothenesowego, lecz ma postać nieco krótszą, gdyż nie potrzebujemy wypisywać liczb parzystych[1]).

Czytelnik zechce zastosować tę metodę dla $n=10$ i porównać ją z sitem Eratosthenesa.

[1]) J. Fitz-Patrick, *Exercices d'Arithmétique*, Wyd. 3-e, Paryż 1914, str. 50 i 338, zadanie 332.

Oznaczmy n-tą z kolei liczbę pierwszą przez p_n, przez $\pi(x)$ zaś — liczbę liczb pierwszych niewiększych od x. Mamy więc:

$$p_1=2,\quad p_2=3,\quad p_3=5,\quad p_4=7,\quad p_5=11,\quad p_{10}=29,$$
$$\pi(1)=0,\quad \pi(2)=1,\quad \pi(3)=2,\quad \pi(4)=2,\quad \pi(5)=3,\quad \pi(10)=4,$$
$$\pi(20)=7,\quad \pi(50)=10,\quad \pi(100)=25.$$

Można dalej obliczyć, że np.

$$\pi(1000)=168,\quad \pi(10\,000)=1229,\quad \pi(10^8)=5\,761\,455.$$

Udowodnimy w Rozdziale VII, § 2, że stosunek $\pi(n):n$ zmierza do 0, stosunek zaś $p_n:n$ wzrasta nieograniczenie wraz z n.

Jak łatwo widzieć, mamy $\pi(p_n)=n$ dla $n=1,2,3,\ldots$ Z postulatu Bertranda wynika, że $p_{n+1}<2p_n$.

Zeitz[1]) dowiódł, że jeżeli p_n jest n-tą z kolei liczbą pierwszą, to $p_{n+1}<\sqrt{p_1p_2\ldots p_n}$, jeżeli zaś $n\geqslant r(2^r+1)$ przy naturalnym r, to $p_{n+1}<\sqrt[r]{p_1p_2\ldots p_n}$.

Ciekawą zależność między funkcjami p_n a $\pi(n)$ zmiennej naturalnej n znalazł współczesny matematyk norweski Viggo Brun, który udowodnił, że jeżeli przy danym naturalnym n będziemy wyznaczali kolejne liczby

$$n-\pi(n)=n_1,\quad n-\pi(n+n_1)=n_2,\quad n-\pi(n+n_1+n_2)=n_3\quad \text{i t. d.},$$

to przy pewnym naturalnym k będziemy mieli

$$n-\pi(n+n_1+n_2+\ldots+n_k)=0$$

i wówczas będzie

$$p_n=n+n_1+n_2\ldots+n_k\ ^2).$$

Więc np. dla $n=6$ znajdujemy kolejno:

$$6-\pi(6)=3,\quad 6-\pi(6+3)=2,\quad 6-\pi(6+3+2)=1,$$
$$6-\pi(6+3+2+1)=1,\quad 6+\pi(6+3+2+1+1)=0,$$

skąd

$$p_6=6+3+2+1+1=13.$$

Czytelnik znajdzie podobnie

$$p_5=5+2+1+1+1+1=11.$$

[1]) H. Zeitz, Sitzungsberichte der Berliner Mathematischen Gesellschaft 31 (1932), str. 4-8.

[2]) Dla dowodu ob. mój *Wstęp do Teorji liczb*, Książnica-Atlas 1933, str. 19.

Mając daną liczbę naturalną n, możemy więc zawsze za pomocą skończonej (zależnej od n) liczby dzieleń przekonać się, czy liczba n jest, czy nie jest pierwszą. Teoretycznie, zagadnienie, czy dana liczba naturalna n jest, czy nie jest pierwszą, jest więc zawsze rozstrzygalne. Inaczej jest w praktyce dla wielkich n, gdyż liczba potrzebnych dzieleń może być zbyt duża, aby je można było wykonać. Np. do dziś nie wiemy, czy liczba $2^{101}-1$ (która ma 31 cyfr) jest, czy nie jest pierwszą. Nie potrafimy dotąd wypisać w układzie dziesiętnym żadnej liczby pierwszej o 40 lub więcej cyfrach, chociaż potrafimy dla każdego danego naturalnego n określić efektywnie liczbę pierwszą większą od n (np. jako najmniejszy większy od jedności dzielnik liczby $n!+1$).

Lehmer ogłosił tablicę liczb pierwszych aż do 10 milionów[1]). W tablicy tej wskazany jest najmniejszy dzielnik pierwszy każdej liczby niewiększej od 10 170 000 niepodzielnej przez 2, 3, 5 lub 7.

Poletti podaje[2]), że J. P. Kulik obliczył tablicę liczb pierwszych do stu milionów i rękopis jego znajduje się w Akademii Wiedeńskiej.

Gdy Euler dowiódł, że liczba $2^{31}-1$ jest pierwsza; była to największa ze znanych wówczas liczb pierwszych. Dopiero w drugiej połowie XIX-go wieku rekord ten został pobity przez innych matematyków.

Największą ze znanych obecnie liczb pierwszych jest — jak podał E. Fauquembergue w 1917 roku — liczba

$$2^{127}-1=170\,141\,183\,460\,469\,231\,731\,687\,303\,715\,884\,105\,727,$$

która ma 39 cyfr.

Oczywiście, potrafimy jednoznacznie określić liczbę pierwszą większą od powyższej, np. jako najmniejszą liczbę pierwszą p spośród liczb większych od $2^{127}-1$, ale tej liczby p nie potrafimy wypisać za pomocą cyfr układu dziesiętnego (potrafimy atoli na mocy postulatu Bertranda wywnioskować, że ta liczba p będzie również miała 39 cyfr, gdyż będzie mniejszą niż $2(2^{127}-1)$).

[1]) D. N. Lehmer, *Factor table for the first ten millions*, Washington Carnegie Institution 1909.

[2]) L. Poletti, *Tavole di numeri primi etc.*, Manuali Hoepli, Milano 1920, str. XII. Ob. też A. Ferrier, *Les nombres premiers*, Paryż, 1947, str. 19.

Zauważymy jeszcze, że o liczbie $2^{257}-1$, mającej 78 cyfr, którą potrafimy wypisać, wiadomo, iż jest złożona, natomiast nie znaleziono dotąd dla niej żadnego dzielnika pierwszego [1]). Nie znamy też rozkładu na czynniki pierwsze liczby $2^{256}+1$, chociaż wiemy, że jest złożona [2]).

Łatwo jest dać przykład liczby naturalnej, którą potrafimy wypisać w układzie dziesiętnym i o której potrafimy z łatwością dowieść, że jest złożona, ale nie potrafimy, przy dzisiejszym stanie nauki, wypisać w układzie dziesiętnym żadnego jej dzielnika pierwszego. Taką jest np. liczba $(2^{101}-1)^2$, mająca 61 cyfr.

Rozkładem wielkich liczb na czynniki pierwsze zajmował się w osobnej książce Kraïtchik [3]). W niej jest poświęcony cały rozdział [4]) dowodowi, że liczba $\frac{10^{23}-1}{9}$ jest pierwsza. Kraïtchik ogłosił też [5]) listę 94 liczb pierwszych większych od 10^{12}. Tablicę rozkładu na czynniki pierwsze wszystkich liczb niewiększych niż 256000 ogłosił Kaván [6]).

Nie znamy wzoru, który by dawał nieskończenie wiele liczb pierwszych.

Fermat sądził, że wzorem takim jest $2^{2^n}+1$ [7]), co jednak okazało się błędne, gdyż — jak wykazał Euler w 1732 roku — jest $641 \mid 2^{2^5}+1$, F. Landry zaś w 1880 roku podał, że $274177 \mid 2^{2^6}+1$. O liczbie $2^{2^{10}}+1$ nie wiemy, czy jest pierwsza, czy nie; natomiast wiemy, że $319489 \mid 2^{2^{11}}+1$ i $114689 \mid 2^{2^{12}}+1$. Dowiedziono, że liczba $2^{2^{38}}+1$ (mająca kilkadziesiąt miliardów cyfr) jest podzielna przez $2^{41}\cdot 3+1$ i że liczby $2^{2^n}+1$ są złożone dla $n=6, 7, 8, 9, 11, 12, 18, 23, 36, 38$ i 73.

---

[1]) Por. I. Arnold, *Teoria czisieł* (po rosyjsku), Moskwa 1939, str. 93.

[2]) Ob. M. Kraïtchik, *Recherches sur la Théorie des nombres*, Tom I, Paryż 1922, str. 133.

[3]) M. Kraïtchik, *Recherches sur la Théorie des Nombres*, Tom II *(Factorisation)*, Paryż 1929.

[4]) M. Kraïtchik, tamże, str. 38-53.

[5]) M. Kraïtchik, Mathematica 7 (1933), str. 93.

[6]) G. Kaván, *Factor tables giving the complete decomposition into prime factors of all numbers up to 256000*, Londyn 1937 (513 stronic).

[7]) W liście do Pascala z 29. VIII. 1654 pisał P. Fermat o tym swoim przypuszczeniu: „C'est une vérité de laquelle je vous réponds. La démonstration en est très malaisée, et je vous avoue que je n'ai pu encore la trouver pleinement; je ne vous la proposerais pas pour la chercher, si j'en étais venu à bout".

Nie wiadomo dotąd, czy istnieje choć jedna liczba pierwsza postaci 2^n+1 dla naturalnych $n>16$. Nie wiadomo również, czy liczby

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

są wszystkie pierwsze, ani czy liczba

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

jest pierwsza, a nawet czy istnieje nieskończenie wiele liczb pierwszych postaci n^2+1 lub 2^n-1.

Istnieją natomiast wzory, dające dużo liczb pierwszych. Np. wzór Eulera x^2+x+41 daje same liczby pierwsze dla $x=0, 1, 2, \ldots, 39$, jako też dla $x=-1, -2, -3, \ldots, -40$. Wzór $2x^2+29$ daje same liczby pierwsze dla $x=0, 1, \ldots, 28$.

Można jednak dowieść, że żaden wielomian $f(x)$ o współczynnikach całkowitych nie może dawać samych tylko liczb pierwszych dla wartości naturalnych zmiennej x. Gdyby bowiem było $f(n)=p$, gdzie p jest liczbą pierwszą, to — jak łatwo widzieć — musiałoby być $p \mid f(n+kp)$ dla $k=1, 2, \ldots$, a że dla dostatecznie wielkich k mamy $f(n+kp)>p$, więc liczba $f(n+pk)$ jest złożona.

Istnieje tylko jedna para kolejnych liczb naturalnych, które obie są pierwsze: są to mianowicie liczby 2 i 3. Istnieje natomiast więcej par liczb pierwszych, stanowiących dwie kolejne liczby nieparzyste, np.:

5 i 7, 11 i 13, 17 i 19, 29 i 31, 41 i 43, 59 i 61, 2081 i 2083, 2087 i 2089, 30011 i 30013, 30137 i 30139, 10^9+7 i 10^9+9.

Liczby takie nazywają się *bliźniaczymi*.

Nie wiadomo dotąd, czy istnieje nieskończenie wiele par liczb bliźniaczych. Brun dowiódł, że jeżeli kolejnych par liczb bliźniaczych (a_k, b_k), gdzie $k=1, 2, \ldots$, jest nieskończenie wiele, to szereg nieskończony

$$\frac{1}{a_1}+\frac{1}{b_1}+\frac{1}{a_2}+\frac{1}{b_2}+\frac{1}{a_3}+\frac{1}{b_3}+\ldots$$

czyli

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{3}+\frac{1}{5}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\ldots$$

jest zbieżny.

Dowód tego twierdzenia, choć względnie elementarny (bez użycia Rachunku całkowego i Teorii funkcji zmiennej zespolonej), jest dosyć skomplikowany [1]).

W zestawieniu z twierdzeniem o rozbieżności szeregu $\sum 1/p$, rozciągniętego na wszystkie liczby pierwsze [2]), twierdzenie Bruna dowodzi, że pary liczb bliźniaczych występują wśród liczb pierwszych rzadko.

Nie ma trzech kolejnych liczb pierwszych nieparzystych. Istnieją natomiast czwórki liczb pierwszych w jednej i tej samej dziesiątce, np.

$$11,\quad 13,\quad 17,\quad 19,$$
$$101,\quad 103,\quad 107,\quad 109.$$

Największą znaną taką czwórką jest

$$10013950+x,\quad \text{gdzie } x=1,3,7,9.$$

Z drugiej strony łatwo dowieść — co pozostawiamy czytelnikowi — że wśród każdych dziesięciu kolejnych liczb naturalnych większych od 2 jest co najmniej sześć złożonych. L. Aubry dowiódł, że wśród każdych trzydziestu kolejnych liczb nieparzystych jest co najmniej piętnaście liczb złożonych.

Łatwo też wskazać 100 kolejnych liczb naturalnych, z których żadna nie jest pierwsza, np. liczby

$$101!+k,\quad \text{gdzie } k=2,3,\ldots,101.$$

Można atoli obliczyć, że już między liczbami 1671800 a 1671900 nie ma żadnej liczby pierwszej.

Nie wiemy, czy dla każdej liczby parzystej istnieje choćby jedna para liczb pierwszych, których różnicą byłaby ta liczba.

Nie wiemy też, czy istnieje liczba parzysta, która daje się przedstawić na nieskończenie wiele sposobów jako różnica dwu liczb pierwszych.

Inne nie rozstrzygnięte dotąd zagadnienie, tyczące się liczb pierwszych, stanowi t. zw. *hipoteza Goldbacha* (z 1742 roku): mianowicie, że każda liczba parzysta większa od 2 jest sumą dwu liczb pierwszych.

[1]) Dowód ten podaje E. Landau w swej książce *Vorlesungen über Zahlentheorie*, tom I *(Aus der elementaren und additiven Zahlentheorie)*, Lipsk 1927, str. 71-78.

[2]) Ob. Rozdział VII, § 1, str. 159.

Gdyby przypuszczenie to było prawdziwe, to wynikałoby stąd natychmiast, że każda liczba naturalna większa od 5 jest sumą trzech liczb pierwszych. Tego dotąd nie dowiedziono, natomiast L. Schnirelman udowodnił (w 1930 roku), że istnieje taka stała liczba naturalna s, że każda liczba naturalna jest sumą co najwyżej s liczb pierwszych, a Heilbronn, Landau i Scherk dowiedli, że każda dostatecznie wielka liczba naturalna jest sumą 71 lub mniej liczb pierwszych [1]). Wreszcie I. Winogradow dowiódł w 1937 roku, że każda dostatecznie wielka liczba parzysta jest sumą czterech lub mniej liczb pierwszych. Tchudakoff [2]) nazywa *twierdzeniem Goldbacha-Winogradowa* twierdzenie, w myśl którego istnieje taka liczba n_0, że każda liczba nieparzysta $n \geqslant n_0$ jest sumą trzech nieparzystych liczb pierwszych. Co zaś do przypuszczenia Goldbacha, to zostało ono sprawdzone dla wszystkich liczb parzystych mniejszych od 60000 [3]).

Zauważymy jeszcze, że — jak sprawdził Euler — każda liczba naturalna n, gdzie $1<n<2500$, jest postaci $n=p+2m^2$, gdzie p jest liczbą pierwszą, a m — całkowitą, ale okazało się, że nie jest to prawdą dla $n=5777$ i $n=5993$ [4]).

ĆWICZENIA. 1. Dowieść, że każdy z siedmiu wyrazów postępu $150k+7$ dla $k=0,1,\ldots,6$ jest liczbą pierwszą.

2. Dowieść, że wielomian x^4+4 daje dla całkowitych x tylko jedną liczbę pierwszą (liczbę 5).

Dowód wynika z tożsamości $x^4+4=(x^2+2x-2)(x^2-2x+2)$.

3. Dowieść, że przy każdym naturalnym n liczba $2^{4n+2}+1$ jest złożoną.

Dowód wynika z tożsamości

$$2^{4n+2}+1=(2^{2n+1}+2^{n+1}+1)(2^{2n+1}-2^{n+1}+1).$$

4. Wskazać n kolejnych liczb naturalnych, z których żadna nie jest pierwszą.

Odpowiedź: liczby postaci $(n+1)!+k$ dla $k=2,3,\ldots,n+1$.

5. Znaleźć najmniejszą liczbę złożoną postaci 3^n+2, gdzie n jest liczbą naturalną.

Odpowiedź: $3^4+2=245$.

[1]) H. Heibronn, E. Landau i P. Scherk, Časopis pro pěstováni Matematiky a Fysiky 65 (1940), str. 117-140.

[2]) N. Tchudakoff, Annals of Mathematics 48 (1947), str. 545.

[3]) Ob. A. A. Fraenkel, Scripta Mathematica 9 (1943), str. 81, odnośnik [13].

[4]) Ob. tamże, str. 81-82.

6. Dowieść, że iloczyn każdych czterech kolejnych liczb naturalnych, zwiększony o 1, jest kwadratem liczby naturalnej.

Dowód: $(n-1)n(n+1)(n+2)+1=(n^2+n-1)^2$.

7. Dowieść przy pomocy postulatu Bertranda, że 5 jest jedyną liczbą naturalną, która jest sumą wszystkich liczb pierwszych od niej mniejszych [1]).

Dowód. Przypuśćmy, że istnieją liczby naturalne większe od 5, będące sumami wszystkich liczb pierwszych od nich mniejszych; niech m będzie najmniejszą z nich. Niech $p_1<p_2<\ldots<p_n$ będą wszystkimi liczbami pierwszymi mniejszymi od m. Jest więc $p_1+p_2+\ldots+p_n=m$ i $m\leqslant p_{n+1}$, a zatem $p_1+p_2+\ldots+p_n\leqslant p_{n+1}$. Z postulatu Bertranda wynika, że $p_{n+1}\leqslant 2p_n$. Jest więc $p_1+p_2+\ldots+p_n\leqslant 2p_n$, skąd $p_1+p_2+\ldots+p_{n-1}\leqslant p_n$. Liczba p_n, która jest mniejsza od m, jest więc sumą wszystkich liczb pierwszych od niej mniejszych. Wobec określenia liczby m dowodzi to, że nie może być $p_n>5$. Jest więc $p_n\leqslant 5$, skąd wynika, że $m=p_1+p_2+\ldots+p_n$ jest jedną z liczb 2, $2+3$ i $2+3+5$. Lecz $m>5$, zatem $m=2+3+5=10$, co niemożliwe, gdyż liczba 10 jest mniejsza niż suma wszystkich liczb pierwszych od niej mniejszych. Niema więc liczb naturalnych $n>5$ będących sumą wszystkich liczb pierwszych od nich mniejszych. Z liczb zaś naturalnych $n\leqslant 5$ — jak łatwo sprawdzić — tylko liczba 5 ma tę własność.

8. Dowieść przy pomocy postulatu Bertranda, że dla żadnej liczby naturalnej $n>1$ liczba $n!$ nie jest potęgą liczby naturalnej o wykładniku większym od jedności.

Dowód. Niech n będzie liczbą naturalną większą od 1. Ponieważ 2!, 3!, 4! i 5! nie są potęgami liczb naturalnych o wykładnikach większych od 1, więc możemy dalej założyć, że $n>5$. Niech a oznacza największą liczbę całkowitą nie przekraczającą $\frac{n}{2}+1$. Wobec $n>5$, mamy $n\geqslant 6$ i $a\geqslant 4$; w myśl postulatu Bertranda istnieje więc taka liczba pierwsza p, że $a<p<2a-2$; a stąd wobec $\frac{n}{2}<a\leqslant\frac{n}{2}+1$ znajdujemy $p<2\left(\frac{n}{2}+1\right)-2=n$ i $2p>2a>n$. Liczba $n!$ jest więc podzielna przez p, lecz nie jest podzielna przez p^2, a przeto nie może być potęgą liczby naturalnej o wykładniku większym niż 1.

9. Znaleźć wszystkie liczby naturalne n, dla których wszystkie współczynniki newtonowskie $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}$ są nieparzyste [2]).

Odpowiedź: $n=2^s-1$, gdzie s jest liczbą naturalną.

Istotnie, przypuśćmy, że n jest taką liczbą naturalną, dla której liczby $\binom{n}{k}$ (dla $k=1,2,\ldots,n$) są wszystkie nieparzyste. Ponieważ $\binom{n}{1}=n$, więc liczba n jest

[1]) Por. J. Arnold, *Teoria czisieł* (po rosyjsku), Moskwa 1939, str. 259, ćwiczenie 111.

[2]) Por. I. M. Winogradow, *Osnowy tieorii czisieł* (po rosyjsku), Moskwa-Leningrad 1940, str. 22, zadanie 9.

nieparzystą, zatem liczba $n+1$ parzystą, a przeto istnieją takie liczby naturalne s i q, że $n=2^s(2q-1)-1$. W razie, gdyby było $q>1$, byłoby $2^s<n$, zatem $\binom{n}{2^s}=\binom{n}{2^s-1}\frac{n-2^s+1}{2^s}=\binom{n}{2^s-1}2(q-1)$ i, wobec całkowitości liczby $\binom{n}{2^s-1}$, liczba $\binom{n}{2^s}$ byłaby parzystą wbrew założeniu. Jest więc $q=1$, zatem $n=2^s-1$.

Z drugiej strony, jeżeli $n=2^s-1$ i $k=2^p-1(2q-1)\leqslant n$, to $p-1<s$ oraz $n-k+1=2^s-2^{p-1}(2q-1)=2^{p-1}[2^{s-p+1}-(2q-1)]$, co dowodzi, że liczby $n-k+1$ i k są podzielne przez tę samą potęgę liczby 2. Wynika stąd, że $\binom{n}{k}=\prod_{j=1}^{n}\frac{n-j+1}{j}$ jest liczbą nieparzystą dla $k=1,2,\ldots,n$.

10. Dowieść, że w granicach tablic liczb pierwszych, t. j. dla $n\leqslant 10^7$, liczby naturalne n nie mogą mieć więcej niż 8 różnych dzielników pierwszych.

Dowód. Jeżeli liczba n ma k różnych dzielników pierwszych, to jej rozwinięcie na czynniki pierwsze jest $n=q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_k^{\alpha_k}$, przy czym

$$q_1\geqslant 2,\quad q_2\geqslant 3,\quad \ldots,\quad q_k\geqslant p_k,$$

gdzie p_k jest k-tą z kolei liczbą pierwszą. Jest więc $n\geqslant p_1\cdot p_2\cdot\ldots\cdot p_k$, co dla $k=9$ daje $n\geqslant 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23=223092870$. Jeżeli więc $n\leqslant 2\cdot 10^8$, to $k\leqslant 8$.

Uwaga. Najmniejszą liczbą naturalną mającą 8 różnych dzielników pierwszych jest, jak łatwo widzieć, liczba

$$2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19=9699690.$$

11. Czy liczba $10^{100}+1$ jest pierwszą?

Odpowiedź: nie, gdyż jest podzielna przez 10^1+1.

12. Dowieść, że dla każdej liczby naturalnej n istnieje taka liczba pierwsza $p>n$, że liczba $p+2$ jest złożona.

Dowód. Niech n będzie daną liczbą naturalną. Istnieje liczba pierwsza $q>3$, taka że $n<q$. Niech

$$p=\begin{cases} q, & \text{jeżeli liczba } q+2 \text{ jest złożona,}\\ q+2, & \text{jeżeli liczba ta jest pierwsza.}\end{cases}$$

W pierwszym przypadku liczba $p+2$ jest więc złożona na mocy określenia, a w drugim — jako podzielna przez 3, ponieważ z trzech kolejnych liczb nieparzystych zawsze, jak wiadomo, jedna jest podzielna przez 3, a liczby q i $q+2$, jako pierwsze i większe od 3, nie są przez 3 podzielne.

13. Dowieść, że dla każdej liczby naturalnej n istnieje taka liczba pierwsza $p>n$, że liczba $p-2$ jest złożona.

Dowód. Istnieje liczba pierwsza $q>n+6$. Jeżeli liczba $q-2$ jest złożona, wystarczy przyjąć $p=q$, w przeciwnym zaś razie wystarczy przyjąć $p=q-2$, gdyż wówczas liczba $p-2$ jest złożona jako podzielna przez 3, a większa niż 3.

Uwaga. Znacznie trudniej jest dowieść, że dla każdej liczby naturalnej n istnieje taka liczba pierwsza $p>n$, iż zarówno liczba $p-2$ jak i liczba $p+2$ jest złożona. Takimi są — jak łatwo widzieć — wszystkie liczby pierwsze postępu arytmetycznego $15k+8$ ($k=0,1,2,\ldots$), ale dowód, że w tym postępie jest nieskończenie wiele liczb pierwszych, jest niełatwy.

14. Dowieść, że na to, by liczba nieparzysta $n>9$ była pierwsza, potrzeba i wystarcza, żeby żadna z liczb

$$n, \quad n+1^2, \quad n+2^2, \quad \ldots, \quad n+\left[\mathrm{E}\left(\frac{n-9}{6}\right)\right]^2 \text{ [1]}$$

nie była kwadratem.

Dowód. Jeżeli dla $0 \leqslant k \leqslant \frac{n-9}{6}$ mamy $n+k^2=l^2$, to $n=(l-k)(l+k)$, przy czym $l-k>1$, gdyż w razie $l-k=1$ byłoby $l=k+1$ i $n=l+k=2k+1$, wbrew temu, że $n-9 \geqslant 6k$. Warunek jest więc konieczny.

Z drugiej strony, jeżeli $n=ab$, gdzie $a \geqslant b>1$, to z uwagi na nieparzystość liczby n mamy $b \geqslant 3$, zatem $a=\frac{n}{b} \leqslant \frac{n}{3}$ i $\frac{a-b}{2} \leqslant \frac{1}{2}\left(\frac{n}{3}-3\right)=\frac{n-9}{6}$. Zarazem $n+\left(\frac{a-b}{2}\right)^2=\left(\frac{a+b}{2}\right)^2$. Warunek jest więc dostateczny.

15. Zastosować wynik ćwiczenia 12 do dowodu, że liczba 9991 jest złożona.

Dowód. Znajdujemy $9991+3^2=100^2$, skąd $9991=97 \cdot 103$. Badanie tej liczby zwykłą metodą byłoby znacznie dłuższe.

16. Dowieść, że dla naturalnych n jest $\frac{\pi(n)}{n} \leqslant \frac{2}{3}$, oraz znaleźć wszystkie liczby naturalne n, dla których $\frac{\pi(n)}{n}=\frac{2}{3}$.

Odpowiedź. Jest jedna tylko taka liczba: $n=3$.

17. Dowieść, że wśród dwunastu kolejnych liczb naturalnych większych od liczby 3 jest zawsze co najmniej 8 złożonych.

18. Znaleźć wszystkie liczby naturalne n, dla których jest $\frac{\pi(n)}{n} \geqslant \frac{1}{2}$.

Odpowiedź. Takie są przede wszystkim liczby naturalne n dla $2 \leqslant n \leqslant 8$, a dla $n \geqslant 9$ liczbami ciągu $1, 2, \ldots, n$, które nie są pierwsze, są w każdym razie liczby parzyste większe od 2 oraz liczby 1 i 9, co razem daje więcej niż $\frac{n}{2}$ liczb. Warunkowi zadania czynią więc zadość jedynie liczby $2, 3, \ldots, 8$.

---

[1] Ob. definicję symbolu $\mathrm{E}(x)$ na str. 49.

ROZDZIAŁ II

RÓWNANIA NIEOZNACZONE PIERWSZEGO STOPNIA

§ 1. Forma liniowa dla największego wspólnego dzielnika.

Twierdzenie 1. *Dla każdych dwu liczb całkowitych a i b, z których przynajmniej jedna jest różna od 0, istnieją takie liczby całkowite ξ i η, iż*

$$(a, b)=a\xi+b\eta. \tag{1}$$

Dowód. Weźmy pod uwagę pewien zbiór liczb naturalnych D, który określimy w następujący sposób: liczbę naturalną n zaliczamy do zbioru D wtedy i tylko wtedy, gdy istnieją takie liczby całkowite x i y, że

$$n=ax+by.$$

Wyrażamy to krócej, mówiąc, że zbiór D jest zbiorem wszystkich liczb naturalnych *postaci* (lub *formy*) $ax+by$.

Zbiór D w każdym razie nie jest pusty (to znaczy, że zawiera co najmniej jedną liczbę), gdyż jeżeli np. $a \neq 0$, to jedna z liczb

$$a=a \cdot 1+b \cdot 0, \qquad -a=a \cdot (-1)+b \cdot 0$$

(ta mianowicie, która jest dodatnia) musi należeć do D w myśl określenia tego zbioru. Oznaczmy przez d najmniejszą liczbę naturalną, należącą do zbioru D. Będziemy więc mieli przy pewnych całkowitych ξ i η równość

$$d=a\xi+b\eta, \tag{2}$$

a przy tym dla każdej liczby naturalnej n, która jest postaci $ax+by$, zachodzić będzie nierówność

$$n \geqslant d.$$

Okażemy, że wyrażenie $ax+by$ przy wszelkich całkowitych x i y jest podzielne bez reszty przez d.