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

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

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 $E(x)$ 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.

Przypuśćmy, że tak nie jest, a więc że przy pewnych całkowitych $x=x_0$ i $y=y_0$ liczba $k=ax_0+by_0$ nie dzieli się bez reszty przez d. Oznaczając przez q iloraz, a przez r resztę, będziemy mieli

$$k=qd+r, \tag{3}$$

przy czym oczywiście r musi być jedną z liczb $1, 2, 3, 4, \ldots, d-1$. Ze wzorów (2) i (3) wnosimy, że r jest liczbą naturalną, mniejszą od d i taką, iż

$$r=k-qd=ax_0+by_0-q(a\xi+b\eta)$$

czyli

$$r=ax+by,$$

gdzie $x=x_0-q\xi$ i $y=y_0-q\eta$ są liczbami całkowitymi. Byłaby więc liczba r liczbą zbioru D mniejszą od d, co przeczy założeniu, że d jest właśnie najmniejszą liczbą zbioru D. Wyrażenie $ax+by$ jest zatem przy wszelkich całkowitych x i y podzielne przez d.

Stąd wnosimy w szczególności, że liczby

$$a=a\cdot 1+b\cdot 0 \quad \text{i} \quad b=a\cdot 0+b\cdot 1$$

są podzielne przez d, czyli że $d|a$ i $d|b$. Liczba d jest więc wspólnym dzielnikiem dla a i b.

Okażemy, że d jest największym wspólnym dzielnikiem liczb a i b. Rzeczywiście, załóżmy, że δ oznacza wspólny dzielnik liczb a i b, Skoro zachodzą, jak zakładamy, wzory

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

to można wyznaczyć takie liczby całkowite t i u, iż $a=t\delta$ i $b=u\delta$, skąd

$$d=a\xi+b\eta=(at+bu)\delta, \quad \text{czyli} \quad \delta|d.$$

Dzielnik d jest więc podzielny (bez reszty) przez każdy inny wspólny dzielnik liczb a i b. Stąd (i z uwagi, że $d>0$) już łatwy wniosek, że liczby a i b nie mają wspólnego dzielnika, który byłby większy od d. Jest więc $d=(a,b)$. Wstawiając tę wartość zamiast d do równości (2), otrzymujemy (1), c. b. d. d.

Zauważmy, że dowiedliśmy zarazem, iż największy wspólny dzielnik dwu liczb jest podzielny bez reszty przez każdy inny wspólny dzielnik tych liczb, czego już na innej drodze dowiedliśmy w Rozdziale I (twierdzenie 3, § 5, str. 4).

§ 2. Warunek na to, by dwie liczby były względnie pierwsze. Załóżmy, że liczby a i b są względnie pierwsze.

W myśl twierdzenia 1 istnieją takie liczby całkowite ξ i η, że

$$a\xi+b\eta=1.$$

Załóżmy teraz, że dla danych liczb całkowitych a i b istnieją takie liczby całkowite x i y, które spełniają równanie:

$$ax+by=1.$$

Lewa strona tego równania jest oczywiście podzielna przez każdy wspólny dzielnik liczb a i b. Ponieważ zaś prawa strona jest jednością, więc widzimy natychmiast, że $(a,b)=1$. Mamy zatem

Twierdzenie 2. *Na to, aby liczby całkowite a i b były względnie pierwsze, potrzeba i wystarcza, żeby istniały liczby całkowite x i y, spełniające równanie*

$$ax+by=1.$$

Stąd np. w szczególności liczby n i $n+1$ są zawsze względnie pierwsze, gdyż

$$(n+1)\cdot 1+n\ (-1)=1.$$

§ 3. Wyznaczanie największego wspólnego dzielnika za pomocą algorytmu Euklidesa. Dowiedliśmy w § 1 (tw. 1), że jeżeli jedna przynajmniej z liczb całkowitych a i b nie jest zerem, to istnieją liczby całkowite ξ i η spełniające równanie (1).

Zapytamy obecnie, w jaki sposób można przy danych a i b rzeczywiście wyznaczyć takie liczby całkowite ξ i η. Zauważymy, że chociaż wiemy o istnieniu liczb całkowitych ξ i η, spełniających to równanie, to stąd nie wynika jeszcze, że istnieje sposób pozwalający liczby te w każdym poszczególnym przypadku wyznaczyć. Rzeczywiście, przeglądając dowód z § 1, widzimy, że nie zawiera on żadnej wskazówki co do tego, jak można by liczby ξ i η otrzymać. Uogólniając tę uwagę, możemy stwierdzić, że wiedzieć, iż jakaś liczba istnieje, nie znaczy jeszcze potrafić ją obliczyć. Można wiedzieć (to znaczy dowieść), że liczba spełniająca jakieś warunki istnieje, ale nie mieć możności jej obliczenia. Takich przykładów jest mnóstwo w Teorii liczb[1]). W danym razie można jednak podać całkiem ogólny sposób wyznaczania szukanych liczb ξ i η za pomocą

[1]) Por. np. Rozdział I, § 8, str. 19.

skończonej liczby działań arytmetycznych. Podamy zarazem sposób wyznaczania największego wspólnego dzielnika dwu liczb.

Niech a i b będą liczbami naturalnymi, q ich ilorazem a r resztą z dzielenia a przez b. Mamy więc:

$$a = qb + r.$$

Z równości tej wynika natychmiast, że każdy wspólny dzielnik liczb a i b jest zarazem dzielnikiem liczby r, każdy zaś wspólny dzielnik liczb b i r jest dzielnikiem liczby a. Możemy więc powiedzieć, że liczby a i b z jednej strony, a liczby b i r z drugiej mają te same wspólne dzielniki. Wynika stąd od razu, że

$$(a, b) = (b, r).$$

Przyjmijmy dla ujednostajnienia oznaczeń:

$$a = n_0, \qquad b = n_1, \qquad r = n_2.$$

Będziemy mogli napisać:

$$(n_0, n_1) = (n_1\, n_2).$$

Gdyby było $n_2 = 0$, to mielibyśmy oczywiście $(n_0, n_1) = n_1$, gdyż wtedy liczba n_0 byłaby podzielna przez n_1. Jeżeli zaś $n_2 \neq 0$, to możemy dzielić n_1 przez n_2.

Oznaczmy przez n_3 resztę z tego dzielenia. Będziemy mogli znowu napisać:

$$(n_1, n_2) = (n_2, n_3).$$

Rozumując dalej w ten sposób, otrzymamy ciąg równości:

$$\begin{aligned} (n_0, n_1) &= (n_1, n_2), \\ (n_1, n_2) &= (n_2, n_3), \\ (n_2, n_3) &= (n_3, n_4), \\ &\cdots\cdots \\ (n_{k-2}, n_{k-1}) &= (n_{k-1}, n_k), \\ (n_{k-1}, n_k) &= (n_k, n_{k+1}). \end{aligned} \tag{4}$$

Ponieważ n_{i+1} oznacza tu ogólnie resztę z dzielenia liczby n_{i-1} przez n_i, więc $n_{i+1} < n_i$. Zatem

$$n_1 > n_2 > n_3 > \ldots \geqslant 0.$$

Lecz ciąg liczb całkowitych n_i, stale malejących i nieujemnych, nie może być nieskończony (gdyż różnych liczb całkowitych nieujemnych mniejszych od n_1 jest tylko n_1). W ciągu

równości (3) będzie zatem istniała ostatnia; niech to będzie równość k-ta

$$(n_{k-1}, n_k) = (n_k, n_{k+1}).$$

Gdyby było $n_{k+1} \neq 0$, to moglibyśmy w dalszym ciągu dzielić n_k przez n_{k+1} i wypisać następnie $(k+1)$-ą równość

$$(n_k, n_{k+1}) = (n_{k+1}, n_{k+2}),$$

co przeczy założeniu, że mamy tylko k równości w ciągu (3).

Jest więc $n_{k+1} = 0$ czyli $(n_{k-1}, n_k) = n_k$. Równości (1) dają kolejno:

$$(n_0\, n_1) = (n_1, n_2) = (n_2, n_3) = \ldots = (n_{k-1}, n_k) = n_k,$$

skąd

$$(n_0, n_1) = n_k.$$

Otrzymaliśmy następującą **regułę** wyznaczania największego wspólnego dzielnika liczb naturalnych:

Aby znaleźć największy wspólny dzielnik liczb n_0 i n_1, dzielimy n_0 przez n_1 i wyznaczamy resztę tego dzielenia n_2. Następnie dzielimy n_1 przez n_2 i wyznaczamy nową resztę n_3. Dalej dzielimy n_2 przez n_3 i t. d., postępując w ten sposób, aż dojdziemy do reszty 0. Przedostatnia reszta jest największym wspólnym dzielnikiem liczb n_0 i n_1.

Prawidło to znane jest pod nazwą *metody kolejnych dzieleń* albo *algorytmu Euklidesa*, lub wreszcie *algorytmu ułamka ciągłego*. Tę ostatnią nazwę usprawiedliwimy w § 4 (str. 34).

S. Lubelski poświęcił algorytmowi Euklidesa dłuższą monografię *Algorytm Euklidesa* (Wiadomości Matematyczne 42 (1936), str. 5-67). We wstępie do niej czytamy:

„Z pojęciem a. E. (algorytmu Euklidesa) spotyka się uczeń szkoły średniej już w arytmetyce. Następnie zapoznaje się on z tym pojęciem przy teorii wielomianów oraz w szerszym zakresie przy geometrii. Należy jednak wątpić, czy na ogół uczeń, student, a nawet nauczyciel, dostatecznie zdają sobie sprawę z doniosłości a. E. Dzięki a. E. zetknęli się starożytni z pojęciem odcinków niewspółmiernych i tym samym z liczbami niewymiernymi, wobec których naukowy świat starożytny stanął bezradny. A. E. przyczynił się w dużym stopniu do badań arytmetycznych nad liczbami zespolonymi, dając możność głębszego wejrzenia w zagadnienie, tyczące się liczb algebraicznych. W a. E. tkwi geneza ułamków łańcuchowych i teorii aproksymacji".

Największy wspólny dzielnik trzech lub więcej liczb można też wyznaczyć za pomocą kolejnych dzieleń, jak następuje [1]).

[1]) Ob. J. Fitz-Patrick, *Exercices d'Arithmétique*, wyd. 3-e, Paryż 1914, str. 49, ćwiczenie 328.

Niech np. c będzie najmniejszą z trzech liczb a, b, c. Dzielimy a i b przez c; odpowiednimi resztami niech będą r i ϱ. Z liczbami c, r i ϱ postępujemy jak z liczbami a, b i c i t. d., aż jedna z reszt będzie zerem. Wówczas największy wspólny dzielnik liczb a, b i c jest równy największemu wspólnemu dzielnikowi dwu pozostałych reszt.

Twierdzenie 3. *Największy wspólny dzielnik dwu liczb naturalnych n_0 i n_1 można wyznaczyć za pomocą algorytmu Euklidesa, przy czym liczba potrzebnych dzieleń kolejnych jest mniejsza od 5-krotnej liczby cyfr, jakie ma w układzie dziesiętnym większa z liczb n_0 i n_1.*

Dowód. Niech $n_0 > n_1$ i niech

$$
\begin{aligned}
n_0 &= q_1 n_1 + n_2,\\
n_1 &= q_2 n_2 + n_3,\\
&\cdots\cdots\cdots\\
n_{k-3} &= q_{k-2} n_{k-2} + n_{k-1},\\
n_{k-2} &= q_{k-1} n_{k-1} + n_k,\\
n_{k-1} &= q_k n_k
\end{aligned}
\tag{5}
$$

będzie ciągiem wszystkich k kolejnych dzieleń, dokonanych przy wyznaczaniu największego wspólnego dzielnika n_k liczb naturalnych n_0 i n_1.

Okażemy przede wszystkim, że dla $i = 0, 1, 2, \ldots, k$ zachodzi nierówność

$$n_{k-i} \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^i. \tag{6}$$

Zauważymy w tym celu, że nierówność ta zachodzi dla $i = 0$ oraz $i = 1$, gdyż $n_k \geqslant 1 = \left(\frac{1+\sqrt{5}}{2}\right)^0$, a także $n_{k-1} > n_k$, skąd

$$n_{k-1} \geqslant n_k + 1 \geqslant 2 > \frac{1+\sqrt{5}}{2}.$$

Niech dalej j oznacza liczbę naturalną mniejszą od k. Załóżmy, że nierówność (6) zachodzi dla $i = j-1$ oraz $i = j$; udowodnimy, że wówczas (6) zachodzi dla $i = j+1$.

Mamy $n_{k-j-1} = q_{k-j} n_{k-j} + n_{k-j+1}$; lecz $q_{k-j} \geqslant 1$, jest więc

$$n_{k-i-1} \geqslant n_{k-j} + n_{k-j+1}. \tag{7}$$

Z założenia wynika, że

$$n_{k-j} \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^j \quad \text{i} \quad n_{k-j+1} \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^{j-1}$$

skąd $n_{k-j} + n_{k-j+1} \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^{j-1}\left(\frac{1+\sqrt{5}}{2}+1\right) = \left(\frac{1+\sqrt{5}}{2}\right)^{j+1}$, gdyż $\frac{1+\sqrt{5}}{2}+1 = \left(\frac{1+\sqrt{5}}{2}\right)^2$. Wobec (7) mamy więc

$$n_{k-j-1} \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^{j+1},$$

czyli nierówność (6) jest prawdziwa dla $i = j+1$. Stąd przez indukcję wnosimy, że nierówność (6) zachodzi dla $i = 0, 1, 2, \ldots, k$.

Dla $i = k$ otrzymujemy z (6)

$$n_0 \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^k,$$

skąd $\log_{10} n_0 \geqslant k \cdot \log_{10}\left(\frac{1+\sqrt{5}}{2}\right)$. Lecz — jak łatwo sprawdzić — $\log_{10}\frac{1+\sqrt{5}}{2} > \frac{1}{5}$, skąd $\log_{10} n_0 > k/5$ czyli $k < 5\log_{10} n_0$.

Jeżeli liczba n, napisana w układzie dziesiętnym, ma z_n cyfr, to — jak wiadomo — zawsze $\log_{10} n < z_n$. Otrzymana na k nierówność daje zatem $k < 5z_{n_0}$, c. b. d. o.

Tak np. przy wyznaczaniu za pomocą kolejnych dzieleń największego wspólnego dzielnika dwu liczb sześciocyfrowych liczba potrzebnych dzieleń będzie zawsze mniejsza od 30.

§ 4. Rozwijanie liczby na ułamek łańcuchowy. Wyznaczymy teraz niewiadome w równaniu $(a, b) = ax + by$. Oznaczmy przez $q_1, q_2, \ldots$ kolejne ilorazy w dzieleniach n_0 przez n_1, n_1 przez n_2 i t. d. Będziemy mogli napisać ciąg równości (5) albo też:

$$\frac{n_0}{n_1} = q_1 + \cfrac{1}{\cfrac{n_1}{n_2}},$$

$$\frac{n_1}{n_2} = q_2 + \cfrac{1}{\cfrac{n_2}{n_3}},$$

$$\cdots\cdots$$

$$\frac{n_{k-2}}{n_{k-1}} = q_{k-1} + \frac{1}{\frac{n_{k-1}}{n_k}},$$

$$\frac{n_{k-1}}{n_k} = q_k,$$

skąd znajdujemy natychmiast:

$$\frac{n_0}{n_1} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \ldots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}}.$$

Algorytm Euklidesa jest więc również metodą rozwijania liczb wymiernych na ułamki ciągłe.

PRZYKŁAD. Rozwiniemy na ułamek ciągły liczbę 314159/100000. Kolejne dzielenia dają:

$$\begin{aligned}
314159 &= 3 \cdot 100000 + 14159\\
100000 &= 7 \cdot 14159 + 887\\
14159 &= 15 \cdot 887 + 854\\
878 &= 1 \cdot 854 + 33\\
854 &= 25 \cdot 33 + 29\\
33 &= 1 \cdot 29 + 4\\
29 &= 7 \cdot 4 + 1\\
4 &= 4 \cdot 1.
\end{aligned}$$

Jest więc

$$3{,}14159 = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{25 + \cfrac{1}{1 + \cfrac{1}{7 + \cfrac{1}{4}}}}}}}.$$

Powróćmy teraz do równości (4). Przedostatnia z nich daje:

$$n_k = n_{k-2} - q_{k-1} n_{k-1}$$

Rugując stąd n_{k-1} na mocy równości $n_{k-3} = q_{k-2} n_{k-2} + n_{k-1}$, otrzymamy:

$$n_k = n_{k-2} - q_{k-1}(n_{k-3} - q_{k-2} n_{k-2}) = -q_{k-1} n_{k-3} + (1 + q_{k-1} q_{k-2}) n_{k-2}.$$

Rugując stąd znowu n_{k-2} na podstawie równości dla n_{k-4} i postępując w ten sposób wciąż dalej, dojdziemy wreszcie — jak łatwo widzieć — do równości

$$n_k = n_0 \xi + n_1 \eta,$$

gdzie ξ i η są pewnymi liczbami całkowitymi.

Algorytm Euklidesa pozwala więc nie tylko wyznaczać (a, b), ale też rozwiązać w liczbach całkowitych ξ i η równanie

$$(a, b) = a\xi + b\eta.$$

Zakładaliśmy dotychczas, że a i b są liczbami naturalnymi. Nie uszczupla to ogólności naszych rozważań, gdyż zmiana znaku nie wpływa na podzielność danej liczby całkowitej przez inną, a więc też nie zmienia największego wspólnego dzielnika dwu liczb. Co się zaś tyczy rozwiązania równania (1), to zmieniając znak przy jednej lub obu liczbach a i b, wystarczyłoby zarazem zmienić znak przy jednej lub obu liczbach ξ i η. Gdyby jedna z liczb a i b, np. a, była zerem, to — jak łatwo widzieć — (a, b) równałoby się bezwzględnej wartości liczby b, równanie zaś miałoby wtedy jedną tylko niewiadomą (i znaleźlibyśmy $\eta = \pm 1$). Gdyby wreszcie obie liczby a i b były zerami, to każda liczba całkowita byłaby ich wspólnym dzielnikiem i przeto wśród wspólnych dzielników liczb a i b nie byłoby największego.

§ 5. Równania nieoznaczone 1-go stopnia o 2 niewiadomych. Otrzymane wyniki zastosujemy obecnie do teorii równania nieoznaczonego 1-go stopnia.

Niech będą dane liczby całkowite a, b i m, różne od zera. Równanie

$$ax + by = m \tag{8}$$

nazywamy *równaniem nieoznaczonym* 1-go stopnia względem (niewiadomych) x i y. Zapytamy, kiedy równanie (8) jest rozwiązalne w liczbach całkowitych i jak znaleźć ewentualnie wszystkie jego rozwiązania. Niech

$$(a, b) = d.$$

Załóżmy, że istnieją liczby całkowite x i y, spełniające równanie (8). Liczba $ax + by$ musi — jak wiemy z Rozdziału I, § 2 — być podzielna przez d; będzie więc też $d|m$, w myśl (8). A więc: warunkiem koniecznym dla rozwiązalności równania (8) w liczbach całkowitych jest, aby liczba m była podzielna przez największy wspólny dzielnik liczb a i b.

Załóżmy teraz, że warunek ten jest spełniony. Niech

(9) $$a = a'd, \qquad b = b'd \quad \text{i} \quad m = m'd.$$

Liczby a' i b' są względnie pierwsze. Można więc wyznaczyć (np. za pomocą algorytmu Euklidesa) takie liczby całkowite ξ i η, iż

(10) $$a'\xi + b'\eta = 1.$$

Niech:

(11) $$x_0 = m'\xi, \qquad y_0 = m'\eta.$$

Wobec (9), (10) i (11) będziemy mieli:

$$ax_0 + by_0 = a'dm'\xi + b'dm'\eta = (a'\xi + b'\eta)m = m$$

czyli

(12) $$ax_0 + by_0 = m.$$

A zatem warunek

$$(a, b) \mid m,$$

jest zarazem wystarczający dla rozwiązalności równania (8) w liczbach całkowitych.

Załóżmy teraz, że liczby całkowite x i y spełniają równanie (8). Wobec (12) będziemy mogli napisać:

$$ax + by = ax_0 + by_0,$$

skąd $a(x - x_0) = b(y_0 - y)$ oraz wobec (9)

(13) $$a'(x - x_0) = b'(y_0 - y).$$

Wobec $(a', b') = 1$ i $b' \mid a'(x - x_0)$ i w myśl twierdzenia 5 z Rozdziału I (§ 7, str. 6) znajdujemy $b' \mid x - x_0$ czyli $x - x_0 = b't$, gdzie t jest liczbą całkowitą. Wzór (13) daje wobec tego

$$a'b't = b'(y_0 - y),$$

skąd (z uwagi, że $b' \neq 0$, gdyż $b'd = b \neq 0$) dostajemy $a't = y_0 - y$.

Równości $x - x_0 = b't$ i $y_0 - y = a't$ dają:

(14) $$x = x_0 + b't, \qquad y = y_0 - a't.$$

Jeżeli więc x, y jest rozwiązaniem równania (5) w liczbach całkowitych, to przy pewnym całkowitym t muszą zachodzić wzory (14).

Załóżmy teraz, że we wzorach (14) przyjęliśmy jakąkolwiek wartość całkowitą na t i wyznaczyliśmy liczby x i y. Będziemy mieli wobec (14) z uwagi, że w myśl (6) jest $ab' = a'b$,

$$ax + by = a(x_0 + b't) = b(y_0 - a't) = ax_0 + by_0,$$

zatem wobec (12)

$$ax + by = m.$$

A więc:

Na to, żeby liczby całkowite x, y spełniały równanie (5), potrzeba i wystarcza, iżby zachodziły wzory (14) przy pewnym całkowitym t.

Wzory (14) przy $t = 0, \pm 1, \pm 2, \ldots$ przedstawiają zatem najogólniejsze rozwiązanie (w liczbach całkowitych) równania nieoznaczonego (5). O ile więc równanie to jest rozwiązalne w liczbach całkowitych, to ma nieskończenie wiele rozwiązań.

ĆWICZENIA. 1. Przedstawić największy wspólny dzielnik liczb $a = 314$ i $b = 100$ w postaci $ax + by$, gdzie x i y są liczbami całkowitymi.

Rozwiązanie. Za pomocą kolejnych dzieleń otrzymujemy

$$314 = 3 \cdot 100 + 14, \qquad 100 = 7 \cdot 14 + 2, \qquad 14 = 7 \cdot 2;$$

jest więc $(314, 100) = 2$.

Druga z ostatnich równości daje $2 = 100 - 7 \cdot 14$, a że na mocy pierwszej jest $14 = 314 - 3 \cdot 100$, więc $2 = 100 - 7 \cdot (314 - 3 \cdot 100) = 22 \cdot 100 - 7 \cdot 314$. Zatem $(314, 100) = 22 \cdot 100 - 7 \cdot 314$.

2. Rozwiązać równanie $314x + 100y = 18$ w liczbach całkowitych x i y.

Rozwiązanie. Jest $(314, 100) = 2$ (p. ćwiczenie 1) i $7 \cdot 314 + 22 \cdot 100 = 2$; wobec $18 : 2 = 9$, dane równanie jest więc rozwiązalne. Biorąc $x_0 = -7 \cdot 9 = -63$, $y_0 = 100 \cdot 9 = 900$, będziemy mieli $314x_0 + 100y_0 = 18$. Rozwiązaniem ogólnym będzie więc

$$x = x_0 + 50t, \qquad y = y_0 - 157t.$$

§ 6. Równania nieoznaczone 1-go stopnia o n niewiadomych. Niech teraz będzie danych n liczb całkowitych

(15) $$a_1, a_2, \ldots, a_n,$$

z których jedna przynajmniej nie jest zerem.

Oznaczmy przez d najmniejszą liczbę naturalną postaci

(16) $$a_1x_1 + a_2x_2 + \ldots + a_nx_n,$$

gdzie $x_1, x_2, \ldots, x_n$ są liczbami całkowitymi. Zupełnie tak samo jak w § 1 udowodnimy, że taka liczba d istnieje i że jest dzielnikiem każdej liczby postaci (16). Stąd w szczególności wynika, że d jest dzielnikiem każdej z liczb (15). Z drugiej strony, skoro d daje się przedstawić w formie (16), to musi być podzielne przez każdy wspólny dzielnik liczb (15). Dochodzimy więc do wniosku, że d jest największym wspólnym dzielnikiem liczb (15).

Dowiedliśmy więc, że największy wspólny dzielnik liczb (15) daje się przedstawić w postaci (16) (przy pewnych całkowitych wartościach zmiennych $x_1, x_2, \ldots, x_n$).

Stąd w szczególności wynika (podobnie jak w § 2), że na to, aby liczby (15) nie miały wspólnego dzielnika większego od jedności, potrzeba i wystarcza, by równanie

$$a_1 x_1 + a_2 x_1 + \ldots + a_n x_n = 1$$

było rozwiązalne w liczbach całkowitych $x_2, x_2, \ldots, x_n$.

Opierając się na otrzymanych wnioskach, można udowodnić z łatwością (podobnie jak w § 5), że na to, aby równanie nieoznaczone

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = m \tag{17}$$

było rozwiązalne w liczbach całkowitych $x_1, x_2, \ldots, x_n$, potrzeba i wystarcza, by liczba m była podzielna przez największy wspólny dzielnik liczb $a_1, a_2, \ldots, a_n$.

Pokażemy teraz, w jaki sposób można wyznaczyć jedno rozwiązanie całkowite równania (17) w razie jego rozwiązalności. Sprowadzimy mianowicie wyznaczanie rozwiązania równania o $n > 2$ niewiadomych do wyznaczania rozwiązania równania o mniejszej liczbie niewiadomych, jak następuje.

Niech $(a_1, a_2, \ldots, a_{n-1}) = \delta$ i niech $\xi_1, \xi_2, \ldots, \xi_{n-1}$ będą liczbami całkowitymi, spełniającymi równanie o $n-1$ niewiadomych

$$a_1 \xi_1 + a_2 \xi_2 + \ldots + a_{n-1} \xi_{n-1} = \delta; \tag{18}$$

liczby takie — jak wiemy — istnieją. Niech dalej u i v będą liczbami całkowitymi, spełniającymi równanie o dwu niewiadomych

$$\delta u + a_n v = m. \tag{19}$$

Równanie to jest rozwiązalne. Istotnie, (δ, a_n) jako wspólny dzielnik liczb δ i a_n jest zarazem wspólnym dzielnikiem liczb $a_1, a_2, \ldots, a_n$; zatem $(\delta, a_n) | (a_1, a_2, \ldots, a_n)$, a ponieważ $(a_1, a_2, \ldots, a_n) | m$ (skoro, jak zakładamy, równanie (17) jest rozwiązalne), więc mamy stąd $(\delta, a_n) | m$, co dowodzi rozwiązalności równania (19) w liczbach u i v całkowitych.

Przyjmując zatem:

$$x_1 = \xi_1 u, \qquad x_2 = \xi_2 u, \qquad \ldots, \qquad x_{n-1} = \xi_{n-1} u, \qquad x_n = v,$$

wnosimy, wobec (18) i (19), że liczby całkowite $x_1, x_2, \ldots, x_n$ spełniają równanie (17).

§ 7. Wyznaczanie największego wspólnego dzielnika i najmniejszej wspólnej wielokrotności n liczb. Pokażemy obecnie, w jaki sposób *wyznaczanie największego wspólnego dzielnika n liczb można sprowadzić do kolejnego wyznaczania największego wspólnego dzielnika dwu liczb.*

Oznaczmy ogólnie dla $k = 2, 3, \ldots, n$ (gdzie $n > 2$) przez d_k największy wspólny dzielnik liczb $a_1, a_2, \ldots, a_k$ i niech

$$d = (d_{n-1}, a_n). \tag{20}$$

Wyznaczona w ten sposób liczba d jest oczywiście dzielnikiem liczby d_{n-1}, tym bardziej zatem dzielnikiem każdej z liczb $a_1, a_2, \ldots, a_{n-1}$, gdyż $d_{n-1} = (a_1, a_2, \ldots, a_{n-1})$.

Ponieważ zaś wobec (20) d jest też dzielnikiem liczby a_n, więc d jest wspólnym dzielnikiem liczb $a_1, a_2, \ldots, a_{n-1}, a_n$, skąd $d \leqslant d_n$ (gdyż d_n jest największym wspólnym dzielnikiem tych liczb).

Z drugiej strony, liczba d_n, jako wspólny dzielnik liczb $a_1, a_2, \ldots, a_{n-2}, a_{n-1}$, jest (w myśl twierdzenia 3 z Rozdziału I, § 5) dzielnikiem ich największego wspólnego dzielnika d_{n-1}, a że oczywiście $d_n | a_n$, więc d_n jest wspólnym dzielnikiem liczb d_{n-1} i a_n; zatem w myśl (20) $d_n \leqslant d$.

Otrzymane nierówności $d \leqslant d_n$ i $d_n \leqslant d$ dają $d = d_n$ czyli wobec (20)

$$d_n = (d_{n-1}, a_n).$$

Dla wyznaczenia liczby d_n wystarcza więc wyznaczyć kolejno:

$$d_2 = (a_1, a_2), \quad d_3 = (d_2, a_3), \quad d_4 = (d_3, a_4), \quad \ldots, \quad d_n = (d_{n-1}, a_n).$$

Całkiem podobnie moglibyśmy wyznaczanie najmniejszej wspólnej wielokrotności n liczb $a_1, a_2, \ldots, a_n$ sprowadzić do kolejnego wyznaczania najmniejszej wspólnej wielokrotności dwu liczb (a więc, w rezultacie, do wyznaczania największego wspólnego dzielnika dwu liczb w myśl twierdzenia 4 z Rozdziału I, § 6), jak to czytelnik sam zechce bliżej zbadać.

Między najmniejszą wspólną wielokrotnością a największym wspólnym dzielnikiem n liczb nie zachodzi jednak zależność tak prosta jak dla dwu liczb. Mamy np.

$$a_1 a_2 a_3 = [a_1, a_2, a_3] \cdot (a_2 a_3, a_1 a_3, a_1 a_2) = (a_1, a_2, a_3) \cdot [a_2 a_3, a_1 a_3, a_1 a_2].$$

Udowodnimy ogólnie, że

$$[a_1, a_2, \ldots, a_m] \cdot \left(\frac{a_1 a_2 \ldots a_m}{a_1}, \frac{a_1 a_2 \ldots a_m}{a_2}, \ldots, \frac{a_1 a_2 \ldots a_m}{a_m}\right) = a_1 \ldots a_m.$$

$$(a_1, a_2, \ldots, a_m) \cdot \left[\frac{a_1 a_2 \ldots a_m}{a_1}, \frac{a_1 a_2 \ldots a_m}{a_2}, \ldots, \frac{a_1 a_2 \ldots a_m}{a_m}\right] = a_1 \ldots a_m.$$

Dowód. Niech p będzie liczbą pierwszą; wykładnikami, z jakimi p wchodzi do rozwinięcia liczb $a_1, a_2, \ldots, a_m$, niech będą odpowiednio liczby $\alpha_1, \alpha_2, \ldots, \alpha_m$. Do rozwinięcia $[a_1, a_2, \ldots, a_m]$ liczba p wchodzi oczywiście z wykładnikiem $\max(\alpha_1, \alpha_2, \ldots, \alpha_m)$, do rozwinięcia $(a_1, a_2, \ldots, a_m)$ — z wykładnikiem $\min(\alpha_1, \alpha_2, \ldots, \alpha_m)$, do rozwinięcia $\left(\frac{a_1 a_2 \ldots a_m}{a_1}, \frac{a_1 a_2 \ldots a_m}{a_2}, \ldots, \frac{a_1 a_2 \ldots a_m}{a_m}\right)$ — z wykładnikiem $\min(\sigma-\alpha_1, \sigma-\alpha_2, \ldots, \sigma-\alpha_m)$. gdzie $\sigma=\alpha_1+\alpha_2+\ldots+\alpha_m$; wreszcie do rozwinięcia $\left[\frac{a_1 a_2 \ldots a_m}{a_1}, \frac{a_1 a_2 \ldots a_m}{a_2}, \ldots, \frac{a_1 a_2 \ldots a_m}{a_m}\right]$ liczba p wchodzi z wykładnikiem $\max(\sigma-\alpha_1, \sigma-\alpha_2, \ldots, \sigma-\alpha_m)$ i do rozwinięcia $a_1 a_2 \ldots a_m$ — z wykładnikiem σ. Lecz jak łatwo widzieć:

$$\max(\alpha_1, \alpha_2, \ldots, \alpha_m)+\min(\sigma-\alpha_1, \sigma-\alpha_2, \ldots, \sigma-\alpha_m)=\sigma,$$

$$\min(\alpha_1, \alpha_2, \ldots, \alpha_m)+\max(\sigma-\alpha_1, \sigma-\alpha_2, \ldots, \sigma-\alpha_m)=\sigma,$$

skąd prawdziwość wzorów (21).

Inny dowód. Niech $N=[a_1, a_2, \ldots, a_n]$ i $P=a_1 a_2 \ldots a_n$. Największy wspólny dzielnik liczb

$$\frac{NP}{a_1}, \quad \frac{NP}{a_2}, \quad \ldots, \quad \frac{NP}{a_m}$$

jest oczywiście równy N-krotnemu największemu wspólnemu dzielnikowi liczb

$$\frac{P}{a_1}, \quad \frac{P}{a_2}, \quad \ldots, \quad \frac{P}{a_m},$$

jakoteż P-krotnemu największemu wspólnemu dzielnikowi liczb

$$\frac{N}{a_1}, \quad \frac{N}{a_2}, \quad \ldots, \quad \frac{N}{a_m};$$

lecz ten ostatni jest równy 1, gdyby bowiem był równy $d>1$, to — jak łatwo widzieć — liczba $N:d$ byłaby wspólną wielokrotnością liczb $a_1, a_2, \ldots, a_m$ wbrew określeniu liczby N, która jest większa niż $N:d$. Jest więc $N\cdot\left(\frac{P}{a_1}, \frac{P}{a_2}, \ldots, \frac{P}{a_m}\right)=P$, c. b. d. o.

ROZDZIAŁ III

ZASADNICZE WŁASNOŚCI KONGRUENCJI KONGRUENCJE 1-go STOPNIA O MODULE PIERWSZYM

§ 1. Kongruencje i ich ważniejsze własności. O dwu danych liczbach całkowitych a i b mówimy, że *przystają do siebie według modułu* m, jeżeli różnica tych liczb jest podzielna przez m. Wyrażamy to na piśmie w ten sposób:

$$a \equiv b \pmod{m}$$

i wzór ten nazywamy *kongruencją* [1]).

Jasne jest, że dwie liczby przystające do siebie według danego modułu naturalnego m dają przy dzieleniu przez ten moduł jednakowe reszty i na odwrót.

Kongruencje mają wiele własności przypominających analogiczne własności *równości* (co też usprawiedliwia używanie symbolu $\equiv$ przypominającego znak równości). Ważniejszymi z nich są:

I. Prawo tożsamości, które polega na tym, że każda liczba przystaje sama do siebie według każdego modułu:

$$a \equiv a \pmod{m}$$

przy wszelkim całkowitym a i naturalnym m. Dla dowodu wystarczy zauważyć, że liczba $a-a=0$ jest podzielna przez każde naturalne m.

II. Prawo symetrii, polegające na tym, że kongruencja

$$a \equiv b \pmod{m}$$

równoważna jest zawsze kongruencji

$$b \equiv a \pmod{m}.$$

Dla dowodu wystarczy zauważyć, że liczby $a-b$ i $b-a$ są zawsze jednocześnie podzielne lub jednocześnie niepodzielne przez m.

---

[1]) Znakowanie to wprowadził Karol Fryderyk Gauss.