1. Wykład 1

1.1. NWD, NWW i algorytm Euklidesa.

Twierdzenie 1.1 (o dzieleniu z resztą)**.** *Niech $a, b \in \mathbb{Z}$, $b \neq 0$. Wówczas istnieje dokładnie jedna para liczb całkowitych $q, r \in \mathbb{Z}$ taka, że*

$$a = qb + r \text{ oraz } 0 \leq r < |b|.$$

Dowód. Pokażemy najpierw istnienie stosownej pary. Załóżmy, że $b > 0$ i zdefiniujmy

$$q = \left[\tfrac{a}{b}\right] \text{ [1] oraz } r = a - bq.$$

Wówczas $q \leq \frac{a}{b} < q + 1$, a zatem $bq \leq a < bq + b$, skąd $0 \leq r = a - bq < b = |b|$. W przypadku, gdy $b < 0$, definiujemy

$$q = -\left[\frac{a}{|b|}\right] \text{ oraz } r = a - bq$$

i dalej rozumujemy analogicznie.

Pozostaje wykazać jednoznaczność wyboru powyższej pary. Załóżmy, że $a = bq_1 + r_1 = bq_2 + r_2$, gdzie $0 \leq r_1, r_2 < |b|$. Wówczas $r_2 - r_1 = b(q_1 - q_2)$. Jeśli $r_2 - r_1 \neq 0$, to wówczas $|b| \leq |r_2 - r_1| \leq \max\{r_1, r_2\} < |b|$. Zatem $r_2 - r_1 = 0$ i w konsekwencji $q_1 - q_2 = 0$. □

Definicja 1.2. *Niech $a, b \in \mathbb{Z}$, $b \neq 0$, niech $q, r \in \mathbb{Z}$ będą jednoznacznie wyznaczonymi liczbami całkowitymi takimi, że $a = qb + r$ i $0 \leq r < |b|$. Liczbę q nazywamy* **niepełnym ilorazem** *z dzielenia a przez b, zaś liczbę r* **resztą** *z dzielenia a przez b.*

Przykłady:

(1) Niech $a = 26$, $b = 11$. Bez trudu sprawdzamy, że wówczas $q = 2$ oraz $r = 4$.
(2) Niech $a = -26$, $b = 11$. Wówczas $q = -3$, a $r = 7$; w szczególności nie możemy powiedzieć, że resztą z dzielenia -26 przez 11 jest -4, gdyż wprawdzie $-26 = -2 \cdot 11 - 4$, ale $-4 < 0$.

Definicja 1.3. *Niech $a, b \in \mathbb{Z}$. Mówimy, że b* **dzieli** *a (lub że a* **jest podzielna przez** *b), jeśli dla pewnej liczby całkowitej $q \in \mathbb{Z}$ zachodzi $a = bq$, co oznaczamy $b|a$. W przeciwnym razie piszemy $b \nmid a$. Liczbę q nazywamy* **ilorazem** *z dzielenia a przez b.*

Przykłady:

(3) Jest jasne, że $2|4$, $3|18$, $-8|16$ i $157|0$.
(4) Bezpośrednio z definicji podzielności wynika też, że $0|a$ wtedy i tylko wtedy, gdy $a = 0$. Widzimy wszakże, że iloraz z dzielenia 0 przez 0 nie jest jednoznacznie określony.

Twierdzenie 1.4. *Niech $a, b, c \in \mathbb{Z}$. Wówczas:*

(1) $a|a$;
(2) $a|b \wedge b|c \Rightarrow a|c$;
(3) $a|b \wedge b|a \Rightarrow a = b \vee a = -b$;
(4) $a|0$;
(5) $1|a$;
(6) $a|b \Rightarrow a|bc$;
(7) $a|b \wedge a|c \Rightarrow a|b + c$.

[1] Przypomnijmy, że dla liczby rzeczywistej $x \in R$ symbolem $[x]$ oznaczamy największą liczbę całkowitą nie większą od x

Dowód. Udowodnimy dla przykładu część (3) twierdzenia. Jeżeli $a = 0$, to $a|b$ wtedy i tylko wtedy, gdy $b = 0$, a więc $a = b$. Podobnie, gdy $b = 0$, to $a = b = 0$, załóżmy więc, że $a, b \neq 0$. Niech $b = q_1 a$ i $a = q_2 b$, dla pewnych $q_1, q_2 \in \mathbb{Z}$. W szczególności $q_1, q_2 \neq 0$. Wówczas $b = q_1 q_2 b$, a więc $q_1 q_2 = 1$, skąd $q_1 = q_2 = 1$ lub $q_1 = q_2 = -1$. □

Definicja 1.5. *Niech $a_1, \ldots, a_k \in \mathbb{Z}$, $k \geq 2$. Liczbę $d \in \mathbb{N}$ taką, że*

(1) $d|a_1, \ldots, d|a_k$,
(2) $e|a_1, \ldots, e|a_k \Rightarrow e|d$,

nazywamy **największym wspólnym dzielnikiem** *liczb $a_1, \ldots, a_k$ i oznaczamy $NWD(a_1, \ldots, a_k)$. Liczbę $m \in \mathbb{N}$ taką, że*

(1) $a_1|m, \ldots, a_k|m$,
(2) $a_1|n, \ldots, a_k|n \Rightarrow m|n$,

nazywamy **najmniejszą wspólną wielokrotnością** *liczb $a_1, \ldots, a_k$ i oznaczamy $NWW(a_1, \ldots, a_k)$.*

Przykład:

(5) Sprawdzamy, że $NWD(24, 36) = 12$. Zauważmy, że, na przykład, $6|24$ i $6|36$, ale oczywiście $6 \neq NWD(24, 36)$. Ponadto $NWW(24, 26) = 72$. Podobnie zauważmy, że $24|144$ i $36|144$, ale $144 \neq NWW(24, 36)$.

Twierdzenie 1.6. *Niech $a, b \in \mathbb{N}$. Wówczas $NWD(a, b) \cdot NWW(a, b) = a \cdot b$.*

Dowód. Rozważmy $\frac{ab}{NWD(a,b)}$. Ponieważ $a, b, NWD(a, b) \in \mathbb{N}$, widzimy, że $\frac{ab}{NWD(a,b)} \geq 0$. Ponadto $\frac{ab}{NWD(a,b)} \in \mathbb{Z}$. Niech $NWD(a, b)q_1 = a$, dla pewnej liczby $q_1 \in \mathbb{N}$. Wówczas $\frac{ab}{NWD(a,b)} = \frac{NWD(a,b)q_1 b}{NWD(a,b)} = q_1 b$, a więc $b|\frac{ab}{NWD(a,b)}$. Analogicznie $a|\frac{ab}{NWD(a,b)}$. Wobec tego $NWW(a, b)|\frac{ab}{NWD(a,b)}$, czyli $NWW(a, b)NWD(a, b)|ab$.

Rozważmy $\frac{ab}{NWW(a,b)}$. Zauważmy, że $\frac{ab}{NWW(a,b)} \in \mathbb{N}$. Niech $NWW(a, b) = s_1 a$, dla pewnej liczby $s_1 \in \mathbb{N}$. Wówczas $\frac{ab}{NWW(a,b)} = \frac{ab}{s_1 a} = \frac{b}{s_1}$. Wobec tego $\frac{ab}{NWW(a,b)}|b$. Analogicznie $\frac{ab}{NWW(a,b)}|a$. Wobec tego $\frac{ab}{NWW(a,b)}|NWD(a, b)$, czyli $ab|NWW(a, b)NWD(a, b)$. □

Przykład:

(6) Odwołując się do poprzedniego przykładu sprawdzamy, że $NWD(24, 36)NWW(24, 36) = 12 \cdot 72 = 864 = 24 \cdot 36$.

Twierdzenie 1.7 (algorytm Euklidesa)**.** *Niech $a, b \in \mathbb{Z}$ i niech*

$$\begin{aligned}
a &= q_1 b + r_1, \ \textit{dla } 0 < r_1 < |b|, q_1, r_1 \in \mathbb{Z}, \\
b &= q_2 r_1 + r_2, \ \textit{dla } 0 < r_2 < r_1, q_2, r_2 \in \mathbb{Z}, \\
r_1 &= q_3 r_2 + r_3, \ \textit{dla } 0 < r_3 < r_2, q_3, r_3 \in \mathbb{Z}, \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, \ \textit{dla } 0 < r_n < r_{n-1}, q_n, r_n \in \mathbb{Z}, \\
r_{n-1} &= q_{n+1} r_n, \ \textit{dla } q_{n+1} \in \mathbb{Z}.
\end{aligned}$$

Wówczas $r_n = NWD(a, b)$.

Dowód. Algorytm zawsze się zatrzymuje, bo jest tylko skończenie wiele liczb naturalnych w przedziale $[0, |b|]$. Niech $d = NWD(a, b)$. Sprawdzamy, że kolejno

$$r_n|r_{n-1}, r_n|r_{n-2}, \ldots, r_n|r_1, r_n|b, r_n|a,$$

a więc w szczególności $r_n|d$. Podobnie, $d|a$ i $d|b$, a więc kolejno

$$d|r_1, d|r_2, \ldots, d|r_{n-1}, d|r_n.$$

Ponieważ zarówno d jak i r_n są liczbami dodatnimi, oraz równocześnie $d|r_n$ i $r_n|d$, więc $d = r_n$. □

Przykłady:

(7) Zastosujemy algorytm Euklidesa, aby obliczyć $NWD(66, 48)$. Wykonując kolejne kroki algorytmu otrzymujemy:

$$\begin{aligned} 66 &= 1 \cdot 48 + 18 \\ 48 &= 2 \cdot 18 + 12 \\ 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6, \end{aligned}$$

a więc $NWD(66, 48) = 6$.

(8) Główna zaleta w stosowaniu algorytmu Euklidesa w porównaniu ze znanym ze szkoły średniej "algorytmem" polegającym na wypisaniu wszystkich dzielników liczb, dla których chcemy znaleźć największy wspólny dzielnik, polega na tym, że nie potrzebujemy rozkładać liczb na czynniki pierwsze. W istocie, nie musimy nawet wiedzieć, czy są to liczby pierwsze, czy złożone. Jako przykład rozważmy tak zwane **liczby Fermata**. W liście do Frénicle de Bessy z 1640 roku Fermat wyraził przypuszczenie, że wszystkie liczby postaci $F_n = 2^{2^n} + 1$ są pierwsze. Jest tak w istocie dla małych n:

$$\begin{aligned} F_0 &= 2^{2^0} + 1 = 3, \\ F_1 &= 2^{2^1} + 1 = 5, \\ F_2 &= 2^{2^2} + 1 = 17, \\ F_3 &= 2^{2^3} + 1 = 257, \\ F_4 &= 2^{2^4} + 1 = 65537, \end{aligned}$$

ale już Euler w 1733 roku udowodnił, że liczba F_5 jest złożona i pokazał, że 641 jest jej dzielnikiem pierwszym:

$$F_5 = 2^{2^5} + 1 = 429467297 = 641 \cdot 6700417.$$

W 1909 roku Klein pokazał, że F_7 nie jest pierwsza, ale dopiero w 1970 roku Morrison i Brillhart znaleźli jej dzielnik pierwszy. Podobnie, Selfridge i Hurwitz udowodnili, że F_{14} nie jest liczbą pierwszą, ale do dziś nie są znane żadne dzielniki pierwsze liczby F_{14}. Pierwsze dwa przykłady liczb Fermata, dla których nie tylko nie znamy dzielników pierwszych, ale o których nie wiemy nawet, czy są pierwsze, czy złożone, to F_{22} i F_{24}. Stosując algorytm Euklidesa możemy jednak łatwo i szybko sprawdzić, że ich największym wspólnym dzielnikiem jest 1. Istotnie:

$$\begin{aligned} 2^{2^{24}} + 1 &= (2^{2^{22}})^4 + 1 = [(2^{2^{22}} + 1) - 1]^4 + 1 = \\ &= (2^{2^{22}} + 1)^4 - 4(2^{2^{22}} + 1)^3 + 6(2^{2^{22}} + 1)^2 - 4(2^{2^{22}} + 1) + 1 + 1 = \\ &= [(2^{2^{22}} + 1)^3 - 4(2^{2^{22}} + 1)^2 + 6(2^{2^{22}} + 1) - 4](2^{2^{22}} + 1) + 2, \\ 2^{2^{22}} + 1 &= 2^{2^{22}-1}2 + 1, \\ 2 &= 2 \cdot 1, \end{aligned}$$

a zatem $NWD(F_{22}, F_{24}) = 1$.

(9) Dane wygenerowane przez algorytm Euklidesa pozwalają wyznaczyć liczby całkowite x i y takie, że

$$66x + 48y = NWD(66, 48).$$

Istotnie, zaczynając od przedostatniego kroku i kolejno podstawiając otrzymujemy:

$$\begin{aligned} 6 &= 18 - 12 \\ &= 18 - (48 - 2 \cdot 18) = 3 \cdot 18 - 48 \\ &= 3(66 - 48) - 48 = 3 \cdot 66 - 4 \cdot 48, \end{aligned}$$

a więc $x = 3$ i $y = -4$.

Uwaga 1.8. *Niech $a, b, c \in \mathbb{Z}$. Algorytm Euklidesa dostarcza metody rozwiązywania równań*

$$ax + by = c$$

w liczbach całkowitych.

Twierdzenie 1.9. *Niech $a, b, c \in \mathbb{Z}$. Równanie*

$$ax + by = c$$

ma rozwiązanie w liczbach całkowitych wtedy i tylko wtedy, gdy $d = NWD(a, b)|c$.

Dowód. ($\Rightarrow$) : Załóżmy, że $ax_0 + by_0 = c$, dla pewnych liczb $x_0, y_0 \in \mathbb{Z}$. Wówczas, skoro $d|a$ i $d|b$, więc $d|ax_0$ i $d|by_0$, a zatem również $d|ax_0 + by_0 = c$.

($\Leftarrow$) : Załóżmy, że $d|c$ i niech $q \in \mathbb{Z}$ będzie taką liczbą, że $dq = c$. Stosując algorytm Euklidesa znajdujemy liczby całkowite $x_1, y_1 \in \mathbb{Z}$ takie, że $ax_1 + by_1 = d$. Wówczas $aqx_1 + bqy_1 = c$. □

Przykład:

(10) Rozwiążemy równanie $66x + 48y = 18$. Na podstawie poprzedniego przykładu wiemy już, że $66 \cdot 3 + 48 \cdot (-3) = 6$, a więc $66 \cdot 9 + 48 \cdot (-12) = 18$.

Twierdzenie 1.10. *Niech $a, b, c \in \mathbb{Z}$ i niech $d = NWD(a, b)|c$. Niech $x_0, y_0 \in \mathbb{Z}$ będą rozwiązaniami równania $ax + by = c$. Wówczas wszystkie całkowite rozwiązania tego równania dane są przez*

$$x = x_0 + \frac{bt}{d} \text{ oraz } y = y_0 - \frac{at}{d}, t \in \mathbb{Z}.$$

Dowód. Sprawdzamy, że

$$a\left(x_0 + \frac{bt}{d}\right) + b\left(y_0 - \frac{at}{d}\right) = ax_0 + by_0 = c.$$

Dalej, niech $x, y \in \mathbb{Z}$ będzie rozwiązaniem równania $ax + by = c$. Wtedy $ax + by = c = ax_0 + by_0$. Stąd $a(x - x_0) = b(y_0 - y)$. Jeżeli $a = a_1 d$ i $b = b_1 d$, dla pewnych $a_1, b_1 \in \mathbb{Z}$, to wówczas też $a_1(x - x_0) = b_1(y_0 - y)$. Ponieważ $NWD(a_1, b_1) = 1$, więc $b_1|x - x_0$. Niech $x - x_0 = b_1 t$, dla pewnego $t \in \mathbb{Z}$. Stąd $x = x_0 + b_1 t = x_0 + \frac{bt}{d}$. Ponadto $a_1 b_1 t = b_1(y_0 - y)$, skąd $y = y_0 - \frac{at}{d}$. □

Przykład:

(11) Wszystkie rozwiązania równania

$$66x + 48y = 18$$

wyrażą się wzorami

$$x = 9 + 8t, y = -12 - 11t, t \in \mathbb{Z}.$$

1.2. **Grupy, pierścienie i ciała.**

Definicja 1.11. *Niech A będzie niepustym zbiorem.* **Działaniem wewnętrznym** *(lub, krótko,* **działaniem***) w zbiorze A nazywamy funkcję $* : A \times A \to A$. Niech ponadto B będzie niepustym zbiorem.* **Działaniem zewnętrznym** *w zbiorze A nazywamy funkcję $* : B \times A \to A$.*

Uwaga 1.12. *To, że w zbiorze A określono działanie wewnętrzne $*$ w szczególności oznacza, że:*

(1) $\forall x, y \in A[*(x, y)$ *istnieje*$]$,
(2) $\forall x, y \in A[*(x, y) \in A]$.

Zamiast $*(x, y)$ będziemy na ogół pisać $x * y$.

Podobnie, jeśli $B \neq \emptyset$, to to, że w zbiorze A określono działanie zewnętrzne $\diamond$ w szczególności oznacza, że:

(1) $\forall a \in B \forall x \in A[\diamond(a, x)$ *istnieje*$]$,
(2) $\forall a \in B \forall x \in A[\diamond(a, x) \in A]$.

Zamiast $\diamond(a, x)$ będziemy na ogół pisać $a \diamond x$.

Na tym wykładzie będziemy zajmować się prawie wyłącznie działaniami wewnętrznymi.

Przykłady:

(1) Dodawanie liczb naturalnych jest działaniem w zbiorze $\mathbb{N}$.
(2) Mnożenie liczb naturalnych jest działaniem w zbiorze $\mathbb{N}$.
(3) Odejmowanie i dzielenie nie są działaniami w zbiorze $\mathbb{N}$: $3 - 5 \notin \mathbb{N}$ oraz $1 \div 2 \notin N$. Z drugiej strony, odejmowanie jest działaniem w $\mathbb{Z}$, a dzielenie jest działaniem w $\mathbb{Q} \setminus \{0\}$.
(4) Mnożenie wektorów na płaszczyźnie przez skalary rzeczywiste jest przykładem działania zewnętrznego.

Definicja 1.13. *Niech A będzie niepustym zbiorem, $a * i \circ$ działaniami w A.*

(1) *Mówimy, że $*$ jest* **łączne,** *jeżeli*
$$\forall x, y, z \in A[x * (y * z) = (x * y) * z].$$
(2) *Mówimy, że $*$ jest* **przemienne,** *jeżeli*
$$\forall x, y \in A[x * y = y * x].$$
(3) *Mówimy, że $*$ ma* **element neutralny** *e, jeżeli*
$$\forall x \in A[x * e = e * x = x].$$
(4) *Mówimy, że y jest* **elementem odwrotnym** *do x, jeżeli*
$$x * y = y * x = e.$$
(5) *Mówimy, że $\circ$* **jest rozdzielne względem** *$*$, jeżeli*
$$\forall x, y, z \in A[x \circ (y * z) = x \circ y * x \circ z].$$

Przykłady:

(5) Dodawanie i mnożenie liczb naturalnych są łączne i przemienne. 0 jest elementem neutralnym dodawania, a 1 jest elementem neutralnym mnożenia. Ponadto mnożenie jest rozdzielne względem dodawania. 1 nie ma elementu odwrotnego względem dodawania, a 2 nie ma elementu odwrotnego względem mnożenia.
(6) Rozważmy dodawanie i mnożenie liczb całkowitych. Każda liczba całkowita ma element odwrotny względem dodawania, ale 2 nie ma elementu odwrotnego względem mnożenia.

(7) Rozważmy dodawanie i mnożenie liczb wymiernych. Każda liczba wymierna ma element odwrotny względem dodawania i każda niezerowa liczba wymierna ma element odwrotny względem mnożenia.

Definicja 1.14. (1) **Algebrą** *nazywamy system* $(A, *_1, \ldots, *_n, B_1, \ldots, B_m, \diamond_1, \ldots, \diamond_m)$*, gdzie* A *jest niepustym zbiorem,* $*_1, \ldots, *_n$ *działaniami wewnętrznymi w zbiorze* A*, a* $\diamond_1, \ldots, \diamond_m$ *działaniami zewnętrznymi w zbiorze* A *(wraz z odpowiadającymi im zbiorami* $B_1, \ldots, B_m$*).*

(2) **Grupą** *nazywamy algebrę* $(G, *)$*, gdzie* $*$ *jest łaczne, ma element neutralny i każdy element w zbiorze* G *ma element odwrotny. Jeżeli ponadto* $*$ *jest przemienne, to grupę* $(G, *)$ *nazywamy* **przemienną** *(lub* **abelową***).*

(3) **Pierścieniem** *nazywamy algebrę* $(R, +, \cdot)$*, gdzie* $(R, +)$ *jest grupą abelową,* $a \cdot$ *jest łączne i rozdzielne względem* $+$*. Jeżeli* $\cdot$ *jest przemienne, to* $(R, +, \cdot)$ *nazywamy* **pierścieniem przemiennym.** *Jeżeli* $\cdot$ *ma element neutralny* 1*, to* $(R, +, \cdot)$ *nazywamy* **pierścieniem z jedynką.** *W tym wykładzie ograniczymy się do pierścieni przemiennych z jedynką, które będziemy krótko nazywać pierścieniami.*

(4) **Ciałem** *nazywamy pierścień przemienny z jedynką* $(F, +, \cdot)$*, w którym* $0 \neq 1$*, przy czym* 0 *oznacza element neutralny* $+$*, a* 1 *to element neutralny* $\cdot$ *i taki, że każdy* $\neq 0$ *element ma element odwrotny względem* $\cdot$*.*

Przykłady:

(8) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ są przykładami grup przemiennych. $(\mathbb{N}, +)$ nie jest grupą. Podobnie $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, gdzie $A^* = A \setminus \{0\}$, są grupami przemiennymi. $(\mathbb{N}^*, \cdot)$ i $(\mathbb{Z}^*, \cdot)$ nie są grupami.

(9) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ są przykładami pierścieni.

(10) $(\mathbb{Q}+, \cdot)$, $(\mathbb{R}, +, \cdot)$ są przykładami ciał. $(\mathbb{Z}, +, \cdot)$ nie jest ciałem.

Definicja 1.15. *Niech* $n \in \mathbb{N}$ *i oznaczmy przez* $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$*. W zbiorze* $\mathbb{Z}_n$ *definiujemy* **dodawanie modulo** n**:**

$$x \oplus_n y = \text{ reszta z dzielenia } x + y \text{ przez } n$$

oraz **mnożenie modulo** n**:**

$$x \otimes_n y = \text{ reszta z dzielenia } x \cdot y \text{ przez } n.$$

Przykłady:

(11) Sprawdzamy, że $2 \oplus_5 2 = 4$, $2 \oplus_5 4 = 1$, $2 \oplus_5 3 = 0$, $3 \oplus_6 5 = 2$ i $98 \oplus_{100} 2 = 0$.

(12) Podobnie, $2 \otimes_5 2 = 4$, $2 \otimes_5 4 = 3$, $2 \otimes_5 3 = 1$, $3 \otimes_6 2 = 0$ i $98 \otimes_{100} 2 = 96$.

Twierdzenie 1.16. *Niech* $n \in \mathbb{N}$*.*

(1) $(\mathbb{Z}_n, \oplus_n)$ *jest grupą przemienną.*

(2) $(\mathbb{Z}_n^*, \otimes_n)$ *jest grupą przemienną, o ile* n *jest liczbą pierwszą.*

(3) $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ *jest pierścieniem.*

(4) $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ *jest ciałem, o ile* n *jest liczbą pierwszą.*

Dowód. Sprawdzenie wszystkich aksjomatów jest dość czasochłonne, ale proste. Ograniczymy się do pokazania, że jeśli n jest liczbą pierwszą, to każdy element $x \in \mathbb{Z}_n^*$ ma element odwrotny względem $\otimes_n$.

Ustalmy $x \in \mathbb{Z}_n^*$. Chcemy pokazać, że istnieje $y \in \mathbb{Z}_n^*$ taki, że $x \otimes_n y = 1$, to znaczy

$$xy = 1 + qn,$$

dla pewnej liczby całkowitej $q \in \mathbb{Z}$. Jest to równoważne pokazaniu, że równanie

$$xy - qn = 1$$

ma rozwiązanie w liczbach całkowitych. Ponieważ n jest liczbą pierwszą, a zatem $NWD(x,n) = 1$, równanie to istotnie ma rozwiązanie wobec Twierdzenia 1.9. □

W dowolnej grupie $(G, *)$ wprowadzamy oznaczenie

$$\prod_{i=1}^{n} x_i = x_1 * \ldots * x_n.$$

W szczególności $\prod_{i=1}^{n} x = x^n$. Tradycyjnie używamy w teorii grup dwóch równoległych terminologii: addytywnej i multyplikatywnej, według następującego schematu:

Definicja	Notacja addytywna	Notacja multyplikatywna
działanie	$+$ dodawanie suma	$\cdot$ mnożenie iloczyn
element neutralny	0 zero	1 jedynka
potęga	nx wielokrotność	x^n potęga
element odwrotny	$-x$ element przeciwny	x^{-1} element odwrotny

Twierdzenie 1.17. *Niech $(G, *)$ będzie grupą. Wówczas:*

(1) *element neutralny e jest wyznaczony jednoznacznie;*
(2) $\prod_{i=1}^{m} x_i * \prod_{j=1}^{n} x_j = \prod_{j=1}^{m+n} x_j$, *dla* $x_1, \ldots, x_{m+n} \in G$;
(3) $x^{m+n} = x^m x^n$, *dla* $x \in G$;
(4) $(x^m)^n = x^{mn}$, *dla* $x \in G$;
(5) *element odwrotny jest wyznaczony jednoznacznie;*
(6) $(x_1^{n_1} * \ldots * x_k^{n_k})^{-1} = x_k^{-n_k} * \ldots * x_1^{-n_1}$, *dla* $x_1, \ldots, x_k \in G$;
(7) $(x^{-1})^{-1} = x$, *dla* $x \in G$;
(8) $(x^{-1} * y * x)^n = x^{-1} * y^n * x$, *dla* $x, y \in G$;
(9) *jeżeli* $x * y = x * z$, *to* $y = z$.

Dowód. Udowodnimy dla przykładu część (1): jeśli e i e' są dwoma elementami neutralnymi, to wówczas

$$e = e * e' = e'.$$

□

W dowolnym pierścieniu $(R, +, \cdot)$ wprowadzamy oznaczenia:

$$\begin{aligned}
xy + z &= (x \cdot y) + z, \\
\sum_{i=1}^{n} x_i &= x_1 + \ldots + x_n, \sum_{i=1}^{0} x_i = 0, \\
\prod_{i=1}^{n} x_i &= x_1 \cdot \ldots \cdot x_n, \prod_{i=1}^{0} x_i = 1, \\
nx &= \sum_{i=1}^{n} x, x^n = \prod_{i=1}^{n} x.
\end{aligned}$$

Twierdzenie 1.18. *Niech $(R, +, \cdot)$ będzie pierścieniem, niech $x, y, z \in R$, $n, m \in \mathbb{N}$. Wówczas:*

(1) $-(-x) = x$;
(2) $-(x + y) = -x - y$;
(3) $n(mx) = nmx$;
(4) $nx + mx = (n + m)x$;
(5) $0x = x0 = 0$;
(6) $(-1)x = -x$;
(7) $(-x)y = -(xy) = x(-y)$;
(8) $(-x)(-y) = xy$;
(9) $x(y - z) = xy - xz$;
(10) $(x - y)z = xz - yz$;
(11) *jeżeli* $x + y = x + z$, *to wówczas* $y = z$;
(12) $x^n x^m = x^{n+m}$;
(13) $(x^n)^m = x^{nm}$;
(14) $(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

Dowód. Udowodnimy dla przykładu część (5):

$$0x + 0x = (0 + 0)x = 0x$$

a zatem $0x = 0$. □