1. Określenie pierścienia

Definicja 1. Niech P będzie zbiorem, w którym określone są działania $+$, $\cdot$ (dodawanie i mnożenie). Mówimy, że struktura $(P, +, \cdot)$ jest *pierścieniem*, jeżeli spełnione są następujące aksjomaty:

P1. $\forall x, y, z \in P \;\; (x + y) + z = x + (y + z)$;
P2. $\exists 0 \in P \;\; \forall x \in P \;\; 0 + x = x + 0 = x$;
P3. $\forall x \in P \;\; \exists - x \in P \;\; x + (-x) = (-x) + x = 0$;
P4. $\forall x, y \in P \;\; x + y = y + x$;
P5. $\forall x, y, z \in P \;\; (xy)z = x(yz)$;
P6. $\forall x, y, z \in P \;\; x(y + z) = xy + xz, \;\; (y + z)x = yx + zx$.

Pierścień, w którym dodatkowo spełniony jest:

P7. $\forall x, y \in P \;\; xy = yx$,

nazywamy *pierścieniem przemiennym.*

Jeśli ponadto:
P8. $\exists 1 \in P \;\; \forall x \in P \;\; x \cdot 1 = 1 \cdot x = x$,
to nazywamy go pierścieniem z jedynką.
W dalszym ciągu (poza przykładami) rozpatrujemy tylko pierścienie przemienne z jedynką.

Przykłady.

1. Zbiór liczb całkowitych ze zwykłymi działaniami dodawania i mnożenia $(\mathbb{Z}, +, \cdot)$ i elementami wyróżnionymi 0 i 1 jest pierścieniem przemiennym z jedynką.

2. $(\mathbb{Z}_n, +_n, \cdot_n)$ — zbiór reszt z dzielenia przez n z działaniami dodawania i mnożenia modulo n i elementami wyróżnionymi 0 i 1 jest także pierścieniem przemiennym z jedynką.

3. $(M_n(\mathbb{R}), +, \cdot)$ — pierścień macierzy kwadratowych stopnia n o elementach rzeczywistych z działaniami dodawania i mnożenia macierzy jest pierścieniem nieprzemiennym (ale z jedynką); zerem jest macierz zerowa, jedynką macierz jednostkowa I_n.

4. Zbiór funkcji ciągłych (rzeczywistych lub zespolonych) $C(a, b)$ ze zwykłymi działaniami dodawania i mnożenia funkcji jest pierścieniem przemiennym z jedynką, którą jest funkcja stała 1 (elementem zerowym jest funkcja stała 0).

5. $(L_1(\mathbb{R}), +, *)$ — zbiór funkcji całkowalnych na $\mathbb{R}$ ze zwykłym dodawaniem i mnożeniem splotowym:

$$(f * g)(x) = \int_{-\infty}^{\infty} f(t)g(x - t)\, dt$$

jest pierścieniem przemiennym (bez jedynki).

Lemat 1. *W dowolnym pierścieniu P: $0 \cdot b = b \cdot 0 = 0$ dla dowolnego $b \in P$.*

D o w ó d. $0 \cdot b = (0 + 0) \cdot b = 0 \cdot b + 0 \cdot b$, a stąd $0 \cdot b = 0$. □

Lemat 2. *W dowolnym pierścieniu P: $(-a) \cdot (-b) = a \cdot b$ dla dowolnych $a, b \in P$.*

D o w ó d. Ponieważ $a + (-a) = 0$, więc $0 = 0 \cdot (-b) = [a + (-a)](-b) = a(-b) + (-a)(-b)$. Ale także $a(-b) + ab = a[(-b) + b] = a \cdot 0 = 0$, więc $ab = (-a)(-b)$. □

Definicja 2. Niech P będzie pierścieniem przemiennym z jedynką. Element $a \in P$, $a \neq 0$ nazywamy *dzielnikiem zera*, jeśli istnieje $b \in P$, $b \neq 0$ takie, że $ab = ba = 0$.

Przykłady.

1. W pierścieniu $\mathbb{Z}_6$ jest $2 \cdot 3 = 0$. Zatem elementy 2 i 3 są dzielnikami zera.

2. Niech $f \in C(0, 1)$ będzie funkcją równą zero na przedziale $< a, b > \subset (0, 1)$, zaś g — dowolną niezerową funkcją równą 0 *poza* przedziałem $< a, b >$. Wtedy $f \cdot g = 0$, a więc takie funkcje są dzielnikami zera w pierścieniu $C(0, 1)$..

Definicja 3. Pierścień przemienny z jedynką bez dzielników zera nazywamy *dziedziną całkowitości*.

Lemat 3. *Następujące warunki są równoważne:*
1. *P jest dziedziną całkowitości.*
2. *W P obowiązuje* prawo skracania*:*

$$ab = ac\ ,\ a \neq 0 \implies b = c.$$

D o w ó d. $(1) \Rightarrow (2) : ab = ac \Leftrightarrow ab - ac = 0 \Leftrightarrow a(b-c) = 0 \Rightarrow (a = 0 \vee b - c = 0) \Rightarrow b = c$.
$(2) \Rightarrow (1)$: niech $ab = 0$ i np. $a \neq 0$. Wtedy $ab = a \cdot 0$, więc $b = 0$. □

Przykłady.

1. $\mathbb{Z}$ jest dziedziną całkowitości.

2. $\mathbb{Z}_m$ jest dziedziną całkowitości $\Leftrightarrow$ m jest liczbą pierwszą.
D o w ó d. . Różny od 0 element r pierścienia $\mathbb{Z}_m$ jest dzielnikiem zera wtedy i tylko wtedy, gdy istnieją liczby s i t $(0 < t < s \leqslant m-1)$ takie, że $rs = mt$. Jest to możliwe wtedy i tylko wtedy, gdy liczby r i m mają wspólny podzielnik większy od 1. Zatem dzielnikami zera w $\mathbb{Z}_m$ są wszystkie liczby różne od 0, mające z m wspólny podzielnik większy od 1. Stąd jeśli m jest liczbą pierwszą, to dzielników zera nie ma.

Znane Czytelnikowi pojęcie ciała pojawia się teraz jako szczególny przypadek pierścienia.

Definicja 4. *Ciało* jest to pierścień przemienny z jedynką, $1 \neq 0$, w którym elementy niezerowe tworzą grupę ze względu na mnożenie.

Przykłady. Zbiory $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ze zwykłymi działaniami, zbiór $\mathbb{Z}_p$ dla liczb pierwszych p (z działaniami modulo p) tworzą ciała.
Każde ciało jest dziedziną całkowitości, ale nie na odwrót. Przykładem dziedziny całkowitości nie będącej ciałem jest *pierścień Gaussa*:

$$\mathbb{Z}[i] = \{a + bi :\ a, b \in \mathbb{Z}\}.$$

Aby to wykazać przypuśćmy, że element $a+bi \in \mathbb{Z}[i]$ ma odwrotność, tj. istnieje taki element $c+di \in \mathbb{Z}[i]$, że $(a+bi)(c+di) = 1$. Wtedy także $|(a+bi)(c+di)|^2 = 1$, czyli

$$1 = |(a+bi)|^2 \cdot |(c+di)|^2 = (a^2+b^2)(c^2+d^2)$$

Liczby a, b, c, d są całkowite, więc musi być $a^2 + b^2 = 1$, $c^2 + d^2 = 1$. Stąd $a = \pm 1, b = 0$, lub $a = 0, b = \pm 1$. Zatem w $\mathbb{Z}[i]$ odwrotności mają tylko $1, -1, i, -i$.
Dzieleniem przez a nazywamy mnożenie przez element odwrotny do a; *ilorazem* $\frac{a}{b}$ nazywamy taki element x, że $bx = a$.

Lemat 4. *W dowolnym ciele wykonalne jest dzielenie (oprócz dzielenia przez 0) i jest ono jednoznaczne.*

2. Ideały pierścieni

Definicja 5. Podgrupę I grupy addytywnej pierścienia P, spełniającą warunek:

$$\text{jeżeli } a \in I \text{ i } b \in P, \text{ to } ab \in I,$$

nazywamy *ideałem* pierścienia P.

Oznaczamy: $I \lhd P$. Zatem definicja ideału zawiera dwa warunki:
I1. $\forall a, b \in I \Rightarrow a - b \in I$
I2. $\forall a \in I, b \in P \Rightarrow ab \in I$

Przykłady.

1. W pierścieniu $\mathbb{Z}$ zbiór liczb podzielnych przez n (dla dowolnego n) tworzy ideał.

2. W $C(a,b)$ ideałem jest zbiór:

$$I_{(c,d)} = \{f \in C(a,b) \mid f|_{(c,d)} = 0\} \ , \ \ a \leqslant c \leqslant d \leqslant b.$$

Jeżeli $I \lhd P$, to I jest dzielnikiem normalnym grupy $(P,+)$. Można więc utworzyć grupę ilorazową P/I. Jej elementami są warstwy względem podgrupy I. Warstwę zawierającą element a będziemy oznaczali $a+I$. W tej grupie określimy mnożenie wzorem:

$$(a+I)(b+I) = ab+I.$$

Wykażemy, że powyższy wzór poprawnie określa mnożenie. Mamy więc wykazać, że jeżeli $a+I = a'+I$, $b+I = b'+I$, to $ab+I = a'b'+I$. Z założenia $a-a' \in I$, $b-b' \in I$. Z określenia ideału $b(a-a') \in I$, $a'(b-b') \in I$. Po dodaniu mamy $ab-a'b' \in I$, czyli $ab+I = a'b'+I$.

3. Homomorfizmy pierścieni

Odwzorowanie pierścieni zachowujące działania nazywamy homomorfizmem.

Definicja 6. Odwzorowanie $f : P \longrightarrow R$ pierścienia P w pierścień R nazywamy *homomorfizmem*, jeśli dla dowolnych $x, y \in P$:

$$f(x+y) = f(x) + f(y) \ , \ f(xy) = f(x)f(y).$$

Pojęcia takie jak mono-, epi-, izo-, endo- czy automorfizm określamy podobnie jak dla grup. Jeżeli uwzględnić w P i R tylko dodawanie, to każdy homomorfizm f pierścienia P w pierścień R jest równocześnie homomorfizmem grupy abelowej P w grupę abelową R. Wnioskujemy stąd, że dla dowolnych $x, y \in P$ zachodzą równości:

$$f(0) = 0 \ , \ f(-x) = -f(x) \ , \ f(x-y) = f(x) - f(y).$$

Przykłady.

1. Przyporządkowanie każdej liczbie całkowitej reszty z dzielenia jej przez ustaloną liczbę całkowitą m określa epimorfizm $\mathbb{Z} \longrightarrow \mathbb{Z}_m$.

2. Odwzorowanie lim pierścienia c ciągów zbieżnych w pierścień $\mathbb{R}$ przyporządkowujące ciągowi jego granicę jest epimorfizmem.

Jądrem homomorfizmu f (oznaczenie $\ker f$) nazywamy zbiór

$$\ker f = \{x \in P \mid f(x) = 0\}$$

wszystkich elementów pierścienia P przechodzących poprzez odwzorowanie f w zero pierścienia R.

Lemat 5. *Jądro homomorfizmu $f : P \longrightarrow R$ jest ideałem pierścienia P.*

D o w ó d. Niech $x, y \in \ker f$. Wtedy $f(x-y) = f(x) - f(y) = 0 - 0 = 0$, więc $x-y \in \ker f$. Jeżeli $x \in \ker f$, $y \in P$, to $f(xy) = f(x)f(y) = 0 \cdot f(y) = 0$, zatem $xy \in \ker f$. □

Przykład. Jądrem pierwszego z powyższych homomorfizmów jest zbiór liczb całkowitych podzielnych przez m, jądrem drugiego — zbiór ciągów zbieżnych do zera.

Obraz homomorfizmu $f : P \longrightarrow R$, tj. zbiór wszystkich elementów pierścienia R, które są obrazami choć jednego elementu pierścienia P, oznaczać będziemy $\operatorname{im} f$.
Następujące twierdzenie podamy bez dowodu.

Twierdzenie 1. (podstawowe o homomorfizmie) *. Niech P i R będą pierścieniami, $f : P \longrightarrow R$ homomorfizmem. Wtedy* $\operatorname{im} f \cong P/\ker f$*. Odwrotnie, jeśli I jest dowolnym ideałem P, to istnieje epimorfizm (mianowicie homomorfizm naturalny $\pi : P \longrightarrow P/I$), którego jądrem jest I.*

4. Pierścienie ilorazowe

Własności ideałów w istotny sposób wpływają na własności odpowiednich pierścieni ilorazowych.

Definicja 7. Ideał I pierścienia P nazywamy *maksymalnym,* jeśli $I \neq P$ i każdy ideał J pierścienia P zawierający I jest równy I lub P.

Przykład. Rozpatrzmy *ewaluację*, tj. homomorfizm $\delta_c : C(a,b) \longrightarrow \mathbb{R}$ określony wzorem $\delta_c(f) = f(c)$. Jądro J tego homomorfizmu jest ideałem maksymalnym, bo każdy ideał zawierający wszystkie funkcje przyjmujące w c wartość 0 i chociaż jedną funkcję, której wartość w c jest różna od 0, jest równy $C(a,b)$. (Dowód. Przypuśćmy, że J zawiera funkcję g, $g(c) \neq 0$ i niech $f \in C(a,b)$. Oznaczmy $\alpha = \frac{f(c)}{g(c)}$. Wtedy $f = (f - \alpha g) + \alpha g$ oraz $f - \alpha g \in J$. Zatem $f \in J$.)

Okazuje się, że dzieląc przez ideał maksymalny otrzymujemy ciało. Do dowodu potrzebny będzie następujący lemat.

Lemat 6. *Pierścień jest ciałem wtedy i tylko wtedy, gdy zawiera dokładnie dwa ideały.*

D o w ó d. ($\Rightarrow$) Jeżeli P jest ciałem, to $\{0\} \neq P$. Niech I będzie ideałem niezerowym ciała P; niech $0 \neq a \in I$. Element a ma więc odwrotność, tzn. istnieje taki element $b \in P$, że $ba = 1$. Wtedy dla dowolnego $c \in P$: $c = c \cdot 1 = cba \in I$, bo $a \in I$. Zatem $I = P$. ($\Leftarrow$) Każdy pierścień ma ideały $\{0\}$ i P. Z założenia wynika, że $\{0\} \neq P$. Niech $0 \neq a \in P$. Zbiór $I = \{ab | b \in P\}$ jest ideałem w P, niezerowym,bo $a \in P$. Zatem $I = P$. Stąd wynika, że $1 \in I$, a dalej, że istnieje $b \in P$ takie, że $ab = 1$. Zatem a jest elementem odwracalnym. Wobec tego P jest ciałem. □

Twierdzenie 2. *Jeżeli $I \lhd P$, to pierścień P/I jest ciałem wtedy i tylko wtedy, gdy I jest ideałem maksymalnym.*

D o w ó d. (Pierścień P/I jest ciałem) $\Leftrightarrow$ (P/I ma dokładnie dwa ideały) $\Leftrightarrow$ (istnieją dokładnie dwa ideały pierścienia P zawierające I) $\Leftrightarrow$ (I jest ideałem maksymalnym). □

W dowodzie wykorzystaliśmy fakt, że odwzorowanie kanoniczne $\pi : P \longrightarrow P/I$ określa wzajemnie jednoznaczną odpowiedniość między ideałami pierścienia P/I a tymi ideałami pierścienia P, które zawierają I.
Rozważymy teraz inną klasę ideałów.

Definicja 8. Ideał I pierścienia P nazywamy *pierwszym*, jeżeli $I \neq P$ oraz

$$ab \in I \Rightarrow a \in I \text{ lub } b \in I \text{ dla } a, b \in P.$$

Inaczej mówiąc, I jest ideałem pierwszym, gdy $I \neq P$ oraz

$$(a \notin I) \wedge (b \notin I) \Rightarrow ab \notin I \text{ dla } a, b \in P. \tag{1}$$

Twierdzenie 3. *Niech $I \lhd P$. Pierścień P/I jest dziedziną całkowitości wtedy i tylko wtedy, gdy I jest ideałem pierwszym.*

D o w ó d. Warunek (1) jest równoważny warunkowi:

$$(a + I \neq I) \wedge (b + I \neq I) \Rightarrow ab + I \neq I \text{ dla } a, b \in P, \tag{2}$$

czyli warunkowi:

$$[a] \neq 0 \wedge [b] \neq 0 \Rightarrow [a][b] \neq 0 \text{ dla } [a], [b] \in P/I, \tag{3}$$

(gdzie $[a], [b]$ oznaczają warstwy elemetów a, b), a więc jest równoważny temu, że pierścień P/I nie ma dzielników zera. □

Wniosek 1. *Każdy ideał maksymalny jest pierwszy.*

D o w ó d. I jest maksymalny $\Leftrightarrow$ P/I jest ciałem $\Rightarrow$ P/I jest dziedziną całkowitości $\Leftrightarrow$ I jest pierwszy. □

Bezpośrednio z określenia ideału wynika, że jeżeli $\{I_\alpha\}_{\alpha\in A}$ jest niepustą rodziną ideałów pierścienia P, to również $I = \bigcap_{\alpha\in A} I_\alpha$ jest ideałem pierścienia P.
Jeżeli B jest pewnym podzbiorem zawartym w P, to niech $\{I_\alpha\}_{\alpha\in A}$ będzie rodziną wszystkich ideałów pierścienia P zawierających B. Wtedy $I = \bigcap_{\alpha\in A} I_\alpha$ jest najmniejszym ideałem pierścienia P zawierającym zbiór B. Ideał I nazywamy *ideałem generowanym przez zbiór* B i oznaczamy (B). Zbiór B nazywamy *zbiorem generatorów ideału* I. Ideał generowany przez zbiór $\{a_1, a_2, \ldots, a_n\}$ oznaczamy prościej $(a_1, a_2, \ldots, a_n)$. Ideał nazywamy *głównym*, jeżeli jest generowany przez zbiór jednoelementowy, a *skończenie generowanym,* jeżeli ma skończony zbiór generatorów. Pierścień całkowity, którego każdy ideał jest główny, nazywamy *pierścieniem ideałów głównych.*

Lemat 7. *Jeżeli B jest podzbiorem pierścienia P, to (B) jest zbiorem elementów postaci $a_1b_1 + a_2b_2 + \cdots + a_rb_r$, gdzie $a_1, a_2, \ldots, a_r \in P$, $b_1, b_2, \ldots b_r \in B$, $r = 1, 2, \ldots$*

Wniosek 2. *Ideał główny (a) generowany przez element $a \in P$ jest zbiorem elementów postaci ab, gdzie $b \in P$.*

Twierdzenie 4. *Każdy ideał pierścienia liczb całkowitych $\mathbb{Z}$ jest główny.*

D o w ó d. $\{0\}$ jest ideałem głównym. Niech $I \lhd \mathbb{Z}$, $I \neq \{0\}$. Niech $a \neq 0$ będzie tą liczbą całkowitą należącą do I, która ma najmniejszy moduł. Dla dowolnego $b \in I$ istnieją takie $q, r \in \mathbb{Z}$, $0 \leqslant r < |a|$, że $b = aq + r$. Ponieważ $a, b \in I$ oraz $r = b - aq$, więc $r \in I$. Ale $|r| < |a|$, więc $r = 0$. Zatem $b = aq$, czyli $b \in (a)$. Wynika stąd, że $I \subset (a)$. Inkluzja odwrotna jest oczywista. □

W pierścieniu $\mathbb{Z}$ szczególną rolę odgrywają liczby pierwsze.

Definicja 9. Element nieodwracalny $p \in P \setminus \{0\}$ o tej własności, że

$$p|ab \;\Rightarrow\; (p|a \text{ lub } p|b) \text{ dla dowolnych } a, b \in P,$$

nazywamy *pierwszym.*

Pojęcie to jest ważne w rozpatrywaniu problemów podzielności i rozkładu elementów na czynniki.

Definicja 10. Każde przedstawienie dowolnego niezerowego elementu a pierścienia P w postaci iloczynu dowolnej liczby czynników

$$a = a_1a_2 \ldots a_k \quad (k \geqslant 2) \tag{4}$$

nazywamy *rozkładem elementu a na czynniki.* Rozkład (4) nazywamy *rozkładem właściwym*, jeżeli $k \geqslant 2$ i żaden z czynników $a_1, a_2, \ldots, a_k$ nie jest odwracalny. Element a nazywamy *nierozkładalnym*, jeżeli nie istnieje dla a żaden właściwy rozkład na czynniki; w przeciwnym razie mówimy, że a jest *elementem rozkładalnym.*

Nietrudno wykazać, że każdy element pierwszy jest elementem nierozkładalnym. Jednak nie każdy element nierozkładalny jest pierwszy .
Podamy jeszcze (bez dowodu) dwie własności pierścienia ideałów głównych.

Twierdzenie 5. *Niech P będzie pierścieniem ideałów głównych, $a \neq 0$, $a \in P$. Ideał (a) jest maksymalny wtedy i tylko wtedy, gdy a jest elementem pierwszym w P.*

Twierdzenie 6. *Jeżeli P jest pierścieniem ideałów głównych i $a \neq 0$, $a \in P$, to pierścień klas reszt $P/(a)$ jest ciałem wtedy i tylko wtedy, gdy a jest elementem pierwszym w P.*

5. Kongruencje

Definicja 11. Dwie liczby całkowite a i b nazywamy *kongruentnymi (przystającymi)* według modułu m (lub *modulo* m), jeżeli różnią się o całkowitą wielokrotność liczby m. Piszemy wtedy $a \equiv b \mod m$. Zatem

$$a \equiv b \mod m \iff m|(a-b).$$

Łatwo wykazać, że dwie liczby całkowite a i b są przystające modulo m wtedy i tylko wtedy, gdy podzielone przez $|m|$ dają te same reszty.
Niech

$$ax \equiv b \mod m$$

będzie kongruencją liniową z niewiadomą x. Rozwiązanie istnieje wtedy i tylko wtedy, gdy równanie

$$ax + ny = b$$

ma rozwiązanie w liczbach całkowitych x, y.

Twierdzenie 7. *Równanie $ax + ny = b$ ma rozwiązania $x, y \in \mathbb{Z}$ wtedy i tylko wtedy, gdy* $\text{nwd}(a, n)|b$

Relacja przystawania modulo n jest relacją równoważności w $\mathbb{Z}$. Zatem dzieli ona zbiór $\mathbb{Z}$ na klasy równoważności. Np. dla relacji przystawania modulo 3 mamy następujące klasy:

$$[0] = \{\ldots, -3, 0, 3, 6, 9, \ldots\},$$

$$[1] = \{\ldots, -2, 1, 4, 7, 10, \ldots\},$$

$$[2] = \{\ldots, -1, 2, 5, 8, 11, \ldots\},$$

Zbiór klas relacji przystawania modulo n oznaczamy $\mathbb{Z}_n$. Np. $\mathbb{Z}_3 = \{[0], [1], [2]\}$. Aby uprościć pisownię można klasy reprezentować liczbami, np. klasę [2] liczbą 2. Uzyskujemy wtedy poniższą interpretację.
Niech n będzie liczbą naturalną. Rozpatrzmy zbiór $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ możliwych reszt z dzielenia przez n. W zbiorze tym wprowadzimy działania *dodawania i mnożenia modulo p*. Określone są one następująco:

$$a + b = \text{ reszta z dzielenia zwykłej sumy przez } n,$$

$$a \cdot b = \text{ reszta z dzielenia zwykłego iloczynu przez } n.$$

Piszemy $a + b = c \mod p$. Na przykład:

$$2 + 2 = 1 \mod 3,\ 2 \cdot 2 = 1 \mod 3,\ 3 + 4 = 2 \mod 5,\ 3 \cdot 2 = 1 \mod 5.$$

Zbiory $\mathbb{Z}_n$ są skończone, więc można sporządzić dla nich kompletne tabelki działań. Przykładowo dla $\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

oraz dla $\mathbb{Z}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

.

Można sprawdzić, że działania modulo n spełniają aksjomaty definicji pierścienia. W szczególności istnieją elementy przeciwne, np. $-2 = 1 \mod 3$.
Z powyższych tabel widzimy też, że istnieją elementy odwrotne, np. $2^{-1} = 2 \mod 3$.
Aby działania mod p spełniały aksjomaty definicji ciała, konieczne (i wystarczające) jest, by p było liczbą pierwszą.
Np. patrząc na tabelki dla $\mathbb{Z}_4 = \{0, 1, 2, 3\}$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

.

widzimy, że $\mathbb{Z}_4$ nie jest ciałem, bo nie istnieje 2^{-1}.

Zadania.
1. Wykazać, że jeśli p jest liczbą pierwszą i $k = 1, 2, \ldots, n-1$, to p dzieli $\binom{p}{k}$.
2. Wykazać, że dla $x, y \in \mathbb{Z}_p$, gdzie p jest liczbą pierwszą, mamy wzór $(x+y)^p = x^p + y^p$.
3. Udowodnić przez indukcję, że jeśli p jest liczbą pierwszą i $n \in \mathbb{N}$, to

$$(x+y)^{p^n} = x^{p^n} + y^{p^n}$$

6. Chińskie twierdzenie o resztach

Twierdzenie 8. (chińskie o resztach) *Niech $m = m_1 m_2 \cdots m_r$, gdzie $\operatorname{nwd}(m_i, m_j) = 1$, gdy $i \neq j$. Wówczas układ kongruencji (gdzie $a_1, a_2, \ldots, a_k$ są dowolnymi liczbami całkowitymi):*

$$x \equiv a_1 \mod m_1, \quad x \equiv a_2 \mod m_2, \quad \ldots \quad x \equiv a_r \mod m_r$$

spełnia dokładnie jedna liczba $1 \leqslant x \leqslant m$. Ponadto, jeśli b jest rozwiązaniem, to zbiór wszystkich rozwiązań pokrywa się ze zbiorem tych x, dla których $x \equiv b \mod m$.

Przykład. Rozwiązać układ kongruencji:

$$x \equiv 3 \mod 13,$$
$$x \equiv 4 \mod 37.$$

Rozwiązanie. Rozwiązaniami pierwszej kongruencji są liczby $x = 3 + 13t$, $t \in \mathbb{Z}$. Podstawiając do drugiej kongruencji uzyskamy $3 + 13t \equiv 4 \mod 37$, czyli $13t \equiv 1 \mod 37$. Aby rozwiązać tę kongruencję posłużymy się algorytmem Euklidesa. Mamy kolejno: $37 = 2 \cdot 13 = 11$, $13 = 1 \cdot 11 + 2$, $11 = 5 \cdot 2 + 1$, a więc

$$1 = 11 - 5 \cdot 2 = 11 - 5 \cdot (13 - 11) = 6 \cdot 11 - 5 \cdot 13 = 6 \cdot (37 - 2 \cdot 13) - 5 \cdot 13 = 6 \cdot 37 - 17 \cdot 13,$$

zatem $-17 \cdot 13 \equiv 1 \mod 37$, więc $t \equiv -17 \equiv 20 \mod 37$. Stąd

$$x = 3 + 13(20 + 37u) = 263 + 481u, \quad u \in \mathbb{Z}.$$

U w a g a. Algorytm Euklidesa służył tu do wyznaczenia odwrotności w ciele $\mathbb{Z}_{37}$; uzyskaliśmy $13^{-1} = 20$.
Dowód chińskiego twierdzenia o resztach.

Skonstruujemy rozwiązanie. Niech $M_k = \frac{m}{m_k}$. Wtedy $\text{nwd}(M_k, m_k) = 1$, więc z algorytmu Euklidesa istnieją liczby całkowite x_k, y_k takie, że $M_k x_k + m_k y_k = 1$. Stąd wynika, że $M_k x_k \equiv 1 \mod m_k$. Zatem liczba x zdefiniowana jako

$$x = \sum_{k=1}^{r} a_k x_k M_k,$$

ma własność

$$x \equiv a_k x_k M_k \equiv a_k \mod m_k,$$

a więc jest szukanym rozwiązaniem.
Przykład. Rozwiążemy jeszcze raz układ

$$\begin{aligned} x &\equiv 3 \mod 13, \\ x &\equiv 4 \mod 37. \end{aligned}$$

Mamy: $m = 13 \cdot 37 = 481$, $M_1 = 37$, $M_2 = 13$. Ponieważ (jak już wiemy) $6 \cdot 37 - 17 \cdot 13 = 1$, więc $x_1 = 6, x_2 = -17$. Stąd

$$x = 3 \cdot 6 \cdot 37 = 4 \cdot (-17) \cdot 13 = -218 \equiv 263 \mod 481.$$

Z twierdzenia o resztach wynika, że jeśli $m = m_1 m_2 \dots m_r$ jest iloczynem liczb parami względnie pierwszych, to każda liczba naturalna x mniejsza od m jest jednoznacznie określona przez reszty z dzielenia przez $m_1, m_2, \dots m_r$. Mówimy że ciąg $a_1, a_2, \dots a_r$ tych reszt jest *reprezentacją przez reszty* lub *reprezentacją modularną* liczby x.
Przykład. Wyznaczyć najmniejszą liczbę naturalną x, która daje reszty $3, 2, 1$ przy dzieleniu przez $5, 7, 9$ odpowiednio.
Rozwiązanie. Liczba x spełnia układ

$$\begin{aligned} x &\equiv 3 \mod 5, \\ x &\equiv 2 \mod 7, \\ x &\equiv 1 \mod 9 \end{aligned}$$

Z pierwszej kongruencji $x = 3 + 5t$. Zatem z drugiej: $3 + 5t \equiv 2 \mod 7$, czyli $5t \equiv -1 \mod 7$. Ale w $\mathbb{Z}_7$ jest $5^{-1} = 3$, więc $t \equiv -3 \mod 7$. Dalej, $x = 3 + 5(-3 + 7u) = -12 + 35u$, i z trzeciej kongruencji $-12 + 35u \equiv 1 \mod 9$, czyli $-3 - u \equiv 1 \mod 9$. A więc $u = 4 + 9v$, zatem

$$x = -12 + 35(-4 - 9v) = -12 - 140 - 315v = -152 - 315v = 163 - 315(v + 1),$$

gdzie v jest dowolną liczbą całkowitą. Szukaną liczbą jest zatem 163.
Bardziej formalnie, reprezentacja przez reszty jest izomorfizmem pierścieni:

$$f : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}.$$

W rozpatrywanym przykładzie mieliśmy izomorfizm

$$f : \mathbb{Z}_{315} \to \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_9.$$

Takie izomorfizmy umożliwiają projektowanie szybkich sumatorów liczb. Normalnie dodawanie wymaga obliczania kolejnych cyfr i przenoszenia na następne miejsce. Posługując się reprezentacją przez reszty możemy dodawać je wszystkie jednocześnie.