Algebra liniowa I. Lista 2

Pierścieniem (przemiennym z jednością) nazywamy zbiór z działaniami mnożenia i dodawania, które spełniają wszystkie postulaty zawarte w definicji ciała, za wyjątkiem istnienia elementu odwrotnego.

W szczególności, każde ciało jest pierścieniem. Przykładami pierścieni są $\mathbb{Z}$ oraz wszystkie $\mathbb{Z}_n$, $n > 1$.

Element x pierścienia P nazywamy *odwracalnym*, jeśli ma element odwrotny. W przeciwnym razie nazywamy go nieodwracalnym. Element x jest *dzielnikiem zera*, jeśli istnieje niezerowy element $y \in P$, że $x \cdot y = 0$.

Zadanie 1. Niech P – pierścień przemienny z jednością 1.

(1) Wykazać, że $0 \cdot x = x \cdot 0 = 0$, dla każdego $x \in P$.

(2) Element $x \in P$ jest odwracalny wtedy i tylko wtedy, gdy przekształcenie $M_x \colon P \to P$ dane wzorem $M_x(z) = x \cdot z$ przekształca P na P.

(3) Element $x \in P$ jest dzielnikiem zera wtedy i tylko wtedy, gdy M_x nie jest *różnowartościowe*.

(4) Jeśli P ma skończenie wiele elementów, to element $x \in P$ jest dzielnikiem zera wtedy i tylko wtedy, gdy x nie jest odwracalny.

Zadanie 2. Jeśli n, k to liczby całkowite nieujemne, to symbolem $\binom{n}{k}$ oznaczamy liczbę k-elementowych podzbiorów zbioru n-elementowego. Oczywiście, $\binom{n}{0} = 1 = \binom{n}{n}$. Jeśli $k > n$, to $\binom{n}{k} = 0$. Wykazać, że jeśli $k \geqslant 1$, to zachodzi związek

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

Dla liczby naturalnej m, niech $m! = 1 \cdot 2 \cdot \ldots \cdot m$, o ile $m \geqslant 1$, oraz $m! = 1$, o ile $m = 0$. Wykazać, że jeśli $n \geqslant k \geqslant 0$, to

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

Zadanie 3. Dla dowolnych liczb x, y i $n \in \mathbb{N}$ zachodzi *wzór dwumianowy*, zwany też wzorem Newtona.

$$(x+y)^n = \binom{n}{0}x^n y^0 + \binom{n}{1}x^{n-1}y^1 + ... + \binom{n}{k}x^{n-k}y^k + ... + \binom{n}{n}x^0 y^n.$$

Zadanie 4. Jeżeli p jest liczbą pierwszą, $k \in \{1, ..., p-1\}$, to p dzieli $\binom{p}{k}$.

Zadanie 5. Wykazać, że jeśli $x \equiv x' \pmod{n}$ oraz $y \equiv y' \pmod{n}$, to

$$x + y \equiv x' + y' \pmod{n} \quad \text{oraz} \quad x \cdot y \equiv x' \cdot y' \pmod{n}.$$

Zadanie 6. Niech $n > 1$ – liczba naturalna złożona. Element $x \in \mathbb{Z}_n$ jest odwracalny wtedy i tylko wtedy, gdy n i x nie mają wspólnych dzielników większych niż 1 (są względnie pierwsze).

Zadanie 7. Wyznaczyć element odwrotny do $x \in \mathbb{Z}_n$, o ile istnieje, w następujących przypadkach: (1) $n = 11$, $x = 5$; (2) $n = 14$, $x = 9$; (3) $n = 81$, $x = 77$; (4) $n = 8$, $x = 6$.

Zadanie 8. Wykazać

Małe twierdzenie Fermata *Dla każdej liczby pierwszej p i każdej całkowitej x*

$$x^p \equiv x \pmod{p}.$$

(Jeśli nie potrafisz, zajrzyj na koniec listy.)

Zadanie 9. Obliczyć w $\mathbb{Z}_n$: (1) $2011^{\odot 2012}$, $n = 2012$; (2) $345 \odot 316$, $n = 1021$; (3) $(102 \oplus 103) \odot 100$, $n = 113$; (4) $(10 \odot 5 \odot 9)^{\odot 10}$, $n = 11$.

Zadanie 10. Obliczyć resztę z dzielenia: (1) $(105489)^{10}$ przez 11; (2) 17^{1320} przez 1321.

Zadanie 11. Wykazać następujące nierówności:

a) $\sqrt{ab} \leqslant \dfrac{a+b}{2}$, dla dowolnych liczb nieujemnych a, b;

b) $\sqrt[n]{a_1 a_2 \cdots a_n} \leqslant \dfrac{a_1 + a_2 + \cdots + a_n}{n}$, dla dowolnych liczb nieujemnych $a_1, \ldots, a_n$ (nierówność między średnimi geometryczną i arytmetyczną);

c) $x_1y_1 + x_2y_2 + \cdots + x_ny_n \leqslant \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2} \cdot \sqrt{y_1^2 + y_2^2 + \cdots + x_n^2}$, dla dowolnych liczb $x_1, y_1, \ldots, x_n, y_n$ (nierówność Schwarza);

d) $\sqrt[n]{(a_1 + b_1)(a_2 + b_2) \cdots (a_n + b_n)} \geqslant \sqrt[n]{a_1 a_2 \cdots a_n} + \sqrt[n]{b_1 b_2 \cdots b_n}$, dla dowolnych liczb nieujemnych $a_1, b_1, \ldots, a_n, b_n$.

Zadanie 12. Wyznacz wzór na sumę:

(1) $1 + 2^2 + 3^2 + \cdots + k^2 + \cdots + n^2$

(2) $1 + \cos(x) + \cos(2x) + \cos(3x) + \cdots + \cos(kx) + \cdots + \cos(nx), \quad x \in \mathbb{R}$;

(3) $0 + \sin(x) + \sin(2x) + \sin(3x) + \cdots + \sin(kx) + \cdots + \sin(nx), \quad x \in \mathbb{R}$.

(**Wskazówka.** Stosując liczby zespolone, wzorów (2) i (3) możemy poszukiwać równocześnie.)

Zadanie 13. Wykazać, że dla dowolnych liczb zespolonych z, w mamy: (1) $\overline{zw} = \bar{z}\bar{w}$; (2) $|z|^2 = z\bar{z}$; (3) jeśli $z = a + b\,\mathrm{i}$, gdzie $a, b \in \mathbb{R}$, to$|z|^2 = a^2 + b^2$.

Zadanie 14. Wykazać, dla dowolnej pary liczb zespolonych w i z zachodzi wzór równoległoboku: $|w + z|^2 + |w - z|^2 = 2(|w|^2 + |z|^2)$.

Zadanie 15. Wykazać, że jeśli każda z liczb naturalnych m i n jest sumą dwu kwadratów liczb całkowitych, to ich iloczyn $m \cdot n$ też ma tę własność.

Zadania rozrywkowe z broszurki Władimira Igorewicza Arnolda:
Zadania dla dzieci od 5 do 15 lat. CD

1. Ślimak przemieszcza się w górę słupa 3cm w ciągu dnia. Potem nocą, kiedy śpi, zsuwa się o 2cm. Którego dnia dostanie się na szczyt 10-metrowego słupa.

2. Czy liczba 140359156002848 dzieli się przez 4206377084?

3. Gąsienica chce przejść z jednego rogu pokoju (przy podłodze) do rogu przeciwległego (przy suficie). Pokój ma kształt sześcianu. Znaleźć najkrótszą drogę jej wędrówki.

4. Obliczyć sumę

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{99 \cdot 100}.$$

(z błędem mniejszym niż 1% właściwej odpowiedzi).

Dowód małego twierdzenia Fermata. Wystarczy założyć, że x jest liczbą naturalną. Gdyby x była niedodatnia, to dodalibyśmy na tyle dużą krotność lp liczby p, że $x + lp > 0$. Na mocy $(**)$

$$x^p \equiv (x + lp)^p \equiv x + lp \equiv x \pmod{p}.$$

$$\uparrow$$

pod warunkiem, że wiemy już, że twierdzenie jest prawdziwe dla liczb naturalnych

Jeżeli x jest teraz naturalna, to

$$\begin{aligned} x^p &= ((x-1)+1)^p \\ &\overset{(\diamond)}{=} (x-1)^p + \left(\binom{p}{1}(x-1)^{p-1} + ... + \binom{p}{p-1}(x-1)\right) + 1 \\ &\equiv (x-1)^p + 1 \pmod{p}, \end{aligned}$$

bo część objęta dużymi nawiasami jest krotnością p. Biorąc rozkład $x - 1 = (x - 2) + 1$ i powtarzając rozumowanie, dostaniemy

$$(x-1)^p + 1 \equiv (x-2)^p + 2 \pmod{p}.$$

Z tych samych powodów

$$(x-2)^p + 2 = (x-3)^p + 3 \pmod{p}$$

itd., aż dojdziemy do równości

$$1^p + (x-1) \equiv x \pmod{p}.$$

Porównując skrajne wyrażenia w wytworzonym ciągu równości, dostaniemy tezę. □

Wniosek 1 (małe twierdzenie Fermata – II postać) *Dla każdej liczby całkowitej x , niepodzielnej przez p*

$$x^{p-1} \equiv 1 \pmod{p}.$$

Dowód. Z lematu 3, $x^p - x = x(x^{p-1} - 1)$ dzieli się przez p. Ale p nie dzieli x, więc stąd, że p jest liczbą pierwszą wynika, iż p dzieli $x^{p-1} - 1$. □

Niech $x^{\odot k} = \underbrace{x \odot ... \odot x}_{k-\text{krotnie}}$. Z dowiedzionej już łączności wynika że wyrażenie po prawej stronie ma sens. Zastosujmy wniosek 4. Wtedy

$$x \odot x^{\odot(p-2)} = x^{\odot(p-1)} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Ponieważ $x \odot x^{\odot(p-2)}$ i 1 różnią się o krotność p i leżą w $\mathbb{Z}_p$, więc

$$x \odot x^{\odot(p-2)} = 1.$$

W rezultacie $x^{\odot(p-2)}$ jest szukanym elementem odwrotnym u. □