Věta 15 (Eisensteinovo lemma)**.** *Nechť* $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_+x + a_0 \in \mathbb{Z}[x]$*. Pokud existuje prvočíslo* p *takové, že* $p|a_0, \dots p|a_{n-1}$*,* $p \nmid a_n$*,* $p^2 \nmid a_0$*, potom je polynom* f *ireducibilní nad* $\mathbb{Z}$*.*

Nyní nás bude zajímat, jak určit kořeny polynomů:

Věta 16. *Nechť* $f \in \mathbb{Z}[x]$*,* $f = a_nx^n + \cdots + a_1x + a_0$*. Pokud je racionální číslo* $\frac{p}{q}$ *kořenem polynomu* f*, potom* $p|a_0, q|a_n$*.*

Příklad 73. Uveďte příklad

1. Konečného okruhu, který nebude oborem integrity.
2. Nekonečného okruhu, který nebude oborem integrity.
3. Konečného oboru integrity, který nebude tělesem.
4. Nekonečného oboru integrity, který nebude tělesem.
5. Konečeného tělesa.
6. Nekonečného tělesa.

Příklad 74. Rozhodněte, zda množina R s operacemi $\oplus$, $\odot$ tvoří okruh, komutativní okruh, obor integrity či těleso.

1. $R = \mathbb{Z}$, $a \oplus b = a + b + 3$, $a \odot b = -3$
2. $R = \mathbb{Z}$, $a \oplus b = a + b - 3$, $a \odot b = a \cdot b - 1$
3. $R = \mathbb{Z}$, $a \oplus b = a + b - 1$, $a \odot b = a + b - a \cdot b$
4. $R = \mathbb{Q}$, $a \oplus b = a + b$, $a \odot b = b$
5. $R = \mathbb{Q}$, $a \oplus b = a + b + 1$, $a \odot b = a + b + a \cdot b$
6. $R = \mathbb{Q}$, $a \oplus b = a + b - 1$, $a \odot b = a + b + a \cdot b$

Výsledek.

1. je okruh
2. není okruh
3. je obor integrity
4. není okruh
5. je těleso
6. není okruh

Příklad 75. Dokažte, že podmnožina komplexních čísel $\mathbb{Z}[i] = \{a+bi|a,b \in \mathbb{Z}\}$ tvoří obor integrity. Jedná se o těleso?

Výsledek. Ne

Příklad 76. Na množině $R = \mathbb{Q} \times \mathbb{Q}$ definujeme operace $\oplus$ a $\odot$ vztahem $(a,b) \oplus (c,d) = (a+c, b+d)$, $(a,b) \odot (c,d) = (ac+2bd, ad+bc)$. Dokažte, že $(R, \oplus, \odot)$ tvoří těleso.

Příklad 77. Na množině $R = \mathbb{R} \times \mathbb{R}$ definujeme operace $\oplus$ a $\odot$ vztahem $(a,b) \oplus (c,d) = (a+c, b+d)$, $(a,b) \odot (c,d) = (ac+2bd, ad+bc)$. Dokažte, že $(R, \oplus, \odot)$ netvoří obor integrity.

Příklad 78. Nechť X je neprázdná množina. Rozhodněte, zda $(\mathcal{P}(X), \div, \cap)$ tvoří okruh, obor integrity, těleso, přičemž $A \div B = (A \setminus B) \cup (B \setminus A)$.

Příklad 79. Označme symbolem $\mathbb{R}^{\mathbb{R}}$ množinu všech reálných funkcí. Definujme $(f \oplus g)(x) = f(x) + g(x)$, $(f \odot g)(x) = f(x) \cdot g(x)$. Rozhodněte, zda $(\mathbb{R}^{\mathbb{R}}, \oplus, \odot)$ tvoří okruh, obor integrity, těleso.

Příklad 80. Označme $R = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}|a,b,c,d \in \mathbb{Q}\}$. Rozhodněte, zda $(R, +, \cdot)$ tvoří okruh, obor integrity, těleso.

Příklad 81. Uveďte příklad

1. Polynomu 2011-tého stupně s celočíselnými koeficienty, který je nad $\mathbb{Z}$ ireducibilní.
2. Polynomu s celočíselnými koeficienty, který je nad $\mathbb{Z}$ ireducibilní, přesto má celočíselný kořen.
3. Polynomu s celočíselnými koeficienty, který je nad $\mathbb{Z}$ ireducibilní, nemá celočíselný kořen, ale má kořen racionální.
4. Polynomu s celočíselnými koeficienty, který je ireducibilní nad $\mathbb{Z}$, přesto nesplňuje podmínky Eisensteinova lemmatu.
5. Polynomu pátého stupně s celočíselnými koeficienty, který není nad $\mathbb{Z}$ ireducibilní, přesto nemá celočíselný kořen.
6. Polynomu třetího stupně, který je nad $\mathbb{Z}_5$ ireducibilní.
7. Polynomu pátého stupně, který není nad $\mathbb{Z}_5$ ireducibilní, přesto nemá kořen.
8. Nenulového polynomu, který má více kořenů, než je jeho stupeň.

Příklad 82. Určete všechny kořeny polynomu

1. $x^8 + 3x^4 + 1 \in \mathbb{Z}_5[x]$.
2. $x^5 + 3x^3 + x - 3 \in \mathbb{Z}_5[x]$.

Příklad 83. Určete součet, rozdíl, součin a podíl polynomů $f, g \in \mathbb{Z}_5[x]$, $f(x) = 3x^3 + 2x^2 + 4x + 1$, $g(x) = x^2 + 2x + 2$.

Příklad 84. Určete, kolik je polynomů $f(x) \in \mathbb{Z}_5[x]$ takových, že $f(3) = 2$.

Výsledek. 100

Příklad 85. Uveďte příklad normovaného polynomu třetího stupně s koeficienty ze $\mathbb{Z}_3$, jehož jediné kořeny budou 1 a -1, oba jednonásobné.

Příklad 86. Uveďte příklad 2010 polynomů 2011-tého stupně s racionálními koeficienty, jejichž jediné racionální kořeny budou dvojnásobný kořen 1, trojnásobný kořen $-\frac{1}{3}$ a pětinásobný kořen 0.

Příklad 87. Určete všechna $a \in \mathbb{Z}_5$ tak, aby byl polynom $x^3 + 3x^2 + 4x + a$ ireducibilní nad $\mathbb{Z}_5$.

Příklad 88. Určete všechna $a \in \mathbb{Z}_5$ tak, aby byl polynom $x^5 + 4x^4 + 4x^3 + 4x^2 + ax + 4$ ireducibilní nad $\mathbb{Z}_5$.

Příklad 89. Určete všechny polynomy $f \in \mathbb{Z}_2[x]$, které jsou nad $\mathbb{Z}_2$ ireducibilní a jsou

1. druhého stupně.
2. třetího stupně.
3. čtvrtého stupně.
4. pátého stupně.

Příklad 90. Dokažte, že jsou dané polynomy ireducibilní nad $\mathbb{Z}$:

1. $3x^5 + 2x^4 + 6x^3 - 14x^2 + 8x - 10$
2. $x^7 + 35x^5 - 70x^3 + 140x - 175$

3. $x^2 + 5x - 8$
4. $x^3 + x^2 + x - 1$
5. $x^4 + 8x^3 + 24x^2 - 18x - 1$ *Nápověda: Uvažujte Taylorův rozvoj se středem v 1.*

Příklad 91. Určete všechny racionální kořeny polynomu $f \in \mathbb{Z}[x]$:

1. $f(x) = 6x^5 - 11x^4 - 19x^3 + 18x^2 + 28x + 8$
2. $f(x) = 5x^6 + 11x^5 - 28x^4 - 26x^3 + 61x^2 - 17x - 6$
3. $f(x) = 4x^5 - 8x^4 - 27x^3 + 29x^2 + 44x + 12$
4. $f(x) = 4x^5 - 24x^4 + 37x^3 + 9x^2 - 32x - 12$
5. $f(x) = 2x^6 - 7x^5 - 6x^4 + 26x^3 + 14x^2 - 27x - 18$

Řešení.

1. $f(x) = (x + 1)(2x + 1)(3x + 2)(x - 2)(x - 2)$
2. $f(x) = (x + 3)(5x + 1)(x + 2)(x - 1)(x - 1)(x - 1)$
3. $f(x) = (x + 2)(2x + 1)(2x + 1)(x - 3)(x - 2)$
4. $f(x) = (x - 2)(2x + 1)(2x + 1)(x - 3)(x - 2)$
5. $f(x) = (x + 1)(x + 1)(x + 1)(x - 3)(x - 2)(2x - 3)$

Příklad 92. Metodou neurčitých koeficientů rozložte polynom $x^4 - 3x^3 + 5x^2 - 4x + 2$ na ireducibilní faktory nad $\mathbb{Z}$.

Výsledek. $f(x) = (x^2 - x + 1)(x^2 - 2x + 2)$

Příklad 93. Uveďte příklad kubického polynomu f s celočíselnými koeficienty, který má jedničku za kořen a platí, že $f(2) = f(3) = f(4)$.