Příklad 1. *Rozložte polynom x^4+1 nad*

- $\mathbb{Z}_3$,
- $\mathbb{C}$,
- $\mathbb{R}$.

Řešení.

- $(x^2+x+2)(x^2+2x+2)$
- Kořeny jsou všechny čtvrté odmocniny z -1, ty leží v komplexní rovině na jednotkové kružnici a mají argumenty postupně $\pi/4$, $\pi/4+\pi/2$, $\pi/4+\pi$ a $\pi/4+3\pi/2$, jsou to tedy čísla $\pm\sqrt{2}/2 \pm i\sqrt{2}/2$. Rozklad tedy je
$$(x-\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2})(x-\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2})(x+\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2})(x-\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}).$$
- Vynásobením kořenových činitelů komplexně sdružených kořenů v rozkladu nad $\mathbb{C}$ dostáváme rozklad nad $\mathbb{R}$:
$$(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1).$$

□

Příklad 2. *Máme množinu čtyř slov, která chceme přenášet binárním kódem, který by uměl opravovat jednoduché chyby. Jakou nejmenší délku kódového slova můžeme použít, požadujeme-li, aby všechna kódová slova měla stejnou délku? Proč?*

Řešení. Označme hledanou délku jako n. Minimální Hammingova vzdálenost dvou kódových slov musí být alespoň tři. To znamená, že když pokud ve dvou kódových slovech změním jeden bit, nemohu dostat stejná slova. Množina slov, které dostanu z jednoho kódového slova změnou nejvýše jednoho bitu čítá (včetně původního slova) $n+1$ slov. Pro různá kódová slova musím dostat různé množiny. Celkem tedy takto dostáváme $4(n+1)$ různých slov délky n. Slov délky n je ovšem 2^n, požadujeme tedy $4(n+1)\leq 2^n$. Tato nerovnost je splněna až pro $n\leq 5$. Kódová slova musí tedy mít délku minimálně 5. Hledaná kódová slova délky 5 s minimální Hammingovou vzdáleností 3 jsou například: 00111, 01001, 10100, 11010. □

Příklad 3. *Náhodně rozřízneme úsečku délky l na dvě části. Určete distribuční funkci a hustotu pravděpodobnosti rozdělení obsahu obdélníka, jehož délky stran jsou rovny délkám takto vzniklých úseček.*

Řešení. Spočítejme hledanou distr. funkci. Označme ještě X náhodnou veličinu s rovnoměrným rozložením na intervalu $\langle 0,l\rangle$ udávající délku jedné ze stran (délka druhé je pak $l-X$). Obsah obdélníka S, tedy součin $x(l-x)$ pro $x\in\langle 0,l\rangle$ může zřejmě nabývat hodnot $\langle 0,l^2/4\rangle$. Volíme-li $d\in\langle 0,l^2/4\rangle$, můžeme psát

$$F(d)=P[S\leq d]=P[X(l-X)\leq d]$$

Hledáme tedy ty hodnoty x, pro které je $x(l-x)\leq d$. Řešíme kvadr. nerovnici, kořeny odpovídající kvadratické rovnice jsou $\frac{l-\sqrt{l^2-4d}}{2}$ a $\frac{l+\sqrt{l^2-4c}}{2}$, hodnoty x uvnitř tohoto intervalu nerovnici nesplňují, hodnoty vně potom ano. Je tedy

$$P[X(l-X)\leq d]=P[X\in\langle 0,l\rangle\setminus(\frac{l-\sqrt{l^2-4d}}{2},\frac{l+\sqrt{l^2-4d}}{2})]=\frac{l-\sqrt{l^2-4d}}{l}=1-\frac{\sqrt{l^2-4d}}{l}$$

Celkem

$$F(x)=\begin{cases}0 & \text{pro} \quad x\leq 0\\ 1-\frac{\sqrt{l^2-4x}}{l} & \text{pro} \quad 0\leq x\leq\frac{l^2}{4}\\ 1 & \text{pro} \quad x>\frac{l^2}{4}\end{cases}$$

Hustotu pravděpodobnosti pak dostaneme derivací:

$$x(x)=\begin{cases}0 & \text{pro} \quad x\leq 0\\ \frac{2}{l\sqrt{l^2-4x}} & \text{pro} \quad 0\leq x\leq\frac{l^2}{4}\\ 0 & \text{pro} \quad x>\frac{l^2}{4}\end{cases}$$

□

Příklad 4.

1. *Dokažte, že pro libovolné prvočíslo $p\in\mathbb{N}$ platí: $p|(p-1)^{p^2-1}$ (nápověda:jak zní Eulerova věta pro p, tj. Malá Fermatova věta?)*

2. *Udejte příklad komutativního okruhu, který není oborem integrity. Zdůvodněte proč.*

3. *Určete konstantu a tak aby funkce*

$$f(x) = \begin{cases} 0 & \textit{pro} \quad x \leq 1 \\ a\ln(x) & \textit{pro} \quad 1 < x < 2 \\ 0 & \textit{pro} \quad 2 \leq x \end{cases}$$

   zadávala hustotu pravděpodobnosti nějaké náhodné veličiny.

Řešení.

1. Tvrzení neplatí (stačí dosadit $p = 2$). Mělo být $p|(p-1)^{p^2-1} - 1$.
2. Např $(\mathbb{Z}_4, +, \cdot)$, kde $[2] \cdot [2] = [4] = [0]$, dvojka je tedy netriviálním dělitelem nuly.
3. Podmínka na to, aby zadaná funkce zadávala hustotu pravděpodobnosti je

$$\int_{-\infty}^{\infty} f(x) = 1$$

   Bude potřeba spočítat $\int \ln(x)\,\mathrm{d}x$:

$$\int \ln(x)\,\mathrm{d}x = x\ln(x) - \int 1\,\mathrm{d}x = x\ln(x) - x = x(\ln(x) - 1).$$

   Celkem

$$\int_{-\infty}^{\infty} f(x) = \int_1^2 a\ln(x) = a[x(\ln(x)-1)]_1^2 = a(2\ln(2) - 1),$$

   tedy $a = \frac{1}{2\ln(2)-1}$.

□