6. Algebrou za astronomické jaro

Gaussovské obory

1. *Ještě na téma jednoznačných rozkladů:* Vysvětlete následující „rozpor“:
   (a) V oboru $\mathbb{Z}[i\sqrt{3}]$ platí $(-2)2 = (i\sqrt{3}+1)(i\sqrt{3}-1)$, a proto se nejedná o obor s jednoznačným rozkladem (tj. Gaussův obor).
   (b) V oboru $\mathbb{Z}[\sqrt{2}]$ platí $\sqrt{2}\sqrt{2} = (-4+3\sqrt{2})(4+3\sqrt{2})$, a přesto se jedná o obor s jednoznačným rozkladem. [$(\pm 4+3\sqrt{2}) = \sqrt{2}(3\pm 2\sqrt{2})$, přičemž $3\pm 2\sqrt{2}$ jsou zde invertibilní (mají normu 1), tudíž $\pm 4+3\sqrt{2} \parallel \pm\sqrt{2}$]

2. Najděte ireducibilní rozklady následujících polynomů v oborech $\mathbb{Q}[x,y]$, $\mathbb{R}[x,y]$ a $\mathbb{C}[x,y]$:
   (a) x^2-y+2 [ireducibilní ve všech oborech, protože je primitivní a lineární v y]
   (b) x^2-2y^2 [$(x-\sqrt{2}y)(x+\sqrt{2}y)$ v $\mathbb{R}[x,y]$ a $\mathbb{C}[x,y]$, ireducibilní v $\mathbb{Q}[x,y]$.]
   (c) $x^2+xy+y-1$ [$(x+1)(x+y-1)$ ve všech oborech]
   (d) $2y^3+y^2x+yx^2+x^2+7y^2+7y-x+2$ [$(y+1)(x^2+x(y-1)+(2y^2+5y+2))$]

3. Spočítejte v $\mathbb{Z}[x,y]$ NSD následujících dvou (dechberoucím způsobem přenádherných) polynomů:
$$f = 2xy+2x^2y+8xy^2+15x^2y^2+7x^3y^2+8x^2y^3+13x^3y^3+5x^4y^3$$
$$g = 6y+6xy+24y^2+39xy^2+15x^2y^2.$$
[$y(x+1)(2+(5x+8)y)$]

Čínská věta 9.1. (o zbytcích pro polynomy)

4. Najděte v $\mathbb{Z}_2[x]$ modulo dané polynomy zbytky co nejnižších stupňů:
   (a) $x^9 \pmod{x^2+x+1}$ [1]
   (b) $x^{13} \pmod{x^4+x+1}$. [x^3+x^2+1]

5. Napište úplnou množinu zbytků $\pmod{x^2+x+1}$ v $\mathbb{Z}_3[x]$. Bude se lišit pokud, budeme uvažovat zbytky $\pmod{2x^2+1}$? [$0,1,2,x,x-1,x-2,2x,2x-1,2x-2$; ne, ovšem neznamená to, že počítání $\pmod{x^2+x+1}$ je to samé jako $\pmod{2x^2+1}$!]

6. Vyřešte kongruence:
   (a) $(x^3+x+1)f(x) \equiv 1 \pmod{x^4+x+1}$ v $\mathbb{Z}_2[x]$ [$(x^2+1)+q(x)(x^4+x+1)$ pro libovolné $q(x)\in\mathbb{Z}_2[x]$]
   (b) $(2x+1)f(x) \equiv x^3 \pmod{x^2+1}$ v $\mathbb{Z}_3[x]$. [$x+2+q(x)(x^2+1)$ pro libovolné $q(x)\in\mathbb{Z}_3[x]$]

7. Najděte polynom $f\in\mathbb{Z}_5[x]$ co nejmenšího stupně splňující
$$\begin{cases} f \equiv x+1 \pmod{x^2+1} \\ f \equiv x \pmod{x^3+1}. \end{cases}$$
[$3x^4+3x^3+4x+3$]

8. Najděte všechny polynomy $f\in\mathbb{Q}[x]$ stupně <3 splňující
$$\begin{cases} f \equiv x+1 \pmod{x^2+1} \\ f(0)=3. \end{cases}$$
[$3+2x^2-x^3 \pmod{x^3+x} = 3+x+2x^2$]

Další příklady

9. Najděte všechny polynomy $f \in \mathbb{Q}[x]$ stupně menšího než 3 splňující $f(0) = 1, f(1) = 0, f(2) = 2$ pomocí

   (a) pomocí Čínské věty o zbytcích

   (b) jako Lagrangeův interpolační polynom (*Důsledek 9.2 ve skriptech*). $[\frac{1}{2}(3x^2 - 5x + 2)]$

10. Buď p prvočíslo. S pomocí ČVZ pro polynomy ukažte, že polynom $\prod_{a \in \mathbb{Z}_p}(x - a) \in \mathbb{Z}_p[x]$ je roven polynomu $x^p - x$. [Oba polynomy mají za za kořen každé $a \in \mathbb{Z}_p$ tedy i jejich rozdíl má tuto vlastnost. Ten má ale stupeň $< n$, takový však dle ČVZ existuje jen jeden, čirou náhodou je to 0.]

11. Buď p prvočíslo a buďte $f(x), g(x) \in \mathbb{Z}_p[x]$ polynomy. Ukažte, že příslušná polynomiální zobrazení na $\mathbb{Z}_p$ jsou identická právě tehdy, když $f(x) \equiv g(x) \pmod{x^p - x}$.

12. Vymyslete analogii Lagrangeova vzorce na interpolaci polynomů více proměnných a dokažte, že každé zobrazení $\varphi : \mathbf{T}^n \to \mathbf{T}$, pro libovolné $n \in \mathbb{N}$ a konečné těleso $\mathbf{T}$, lze napsat jako polynomiální zobrazení.

13.* Najděte všechna řešení $u, v \in \mathbb{Z}$ rovnice $u^2 + 2209 = v^3$. *(Nápověda:* $2209 = 47^2$*, postup je podobný jako na str. 37 ve skriptech.)* $[u = \pm 52,\ v = 17]$