Cvičení 1. 3. 2012

Čínská zbytková věta nám popisuje „hodné“ faktorokruhy: Pokud R je okruh a $I_1, \dots, I_k$ (oboustranné) ideály takové, že $I_i + I_j = R$ kdykoli $i \neq j$, tak

$$R/\bigcap_{j=1}^{k} I_j \simeq \prod_{j=1}^{k} R/I_j$$

Pokud R je komutativní okruh a polynom p má v R invertibilní vedoucí člen (například $p(x) = x^n + p_{n-1}x^{n-1} + \dots$), tak můžeme v R dělit pomocí p se zbytkem. Počítání v okruhu $R[x]/pR[x]$ pak funguje podobně jako počítání v $\mathbb{Z}_n$: Stačí provést násobení nebo sčítání v $R[x]$ a spočítat zbytek po dělení p.

Pokud T je těleso, tak $T[x]$ je obor integrity hlavních ideálů a navíc v něm lze každý polynom napsat jednoznačně (až na násobení nenulovými prvky T) jako součin prvočinitelů. Na $T[x]$ můžeme také zavést pojmem největšího společného dělitele (Na rozdíl od $\mathbb{Z}$ budeme mít NSD jednoznačného až na násobení nenulovým skalárem.)

Příklad 1. Spočtěte:

1. $(x+1)^2$ modulo x^2
2. $10x^3 + 3x^2 + x + 2$ modulo $x + 1$
3. $(x^2+1)(x^2+3x)$ modulo $x^3 + 1$

Příklad 2. Rozložte v $\mathbb{R}[x]$ na součin prvočinitelů:

1. $x^2 - 3x + 2$
2. $x^3 + x$
3. $x^4 - 2x^2 + 1$

Příklad 3. Spočtěte NSD polynomů v $\mathbb{R}[x]$:

1. $p = x^3 + 2x + 1$, $q = x^2 + 3$
2. $p = x^2 - 1$, $q = x - 1$
3. $p = 4x^4 + 6x^3 + x^2 + 1$, $q = x^2 + 4x + 3$

Příklad 4. Dokažte, že polynomy $p, q \in \mathbb{R}[x]$ jsou nesoudělné, právě když $p\mathbb{R}[x] + q\mathbb{R}[x] = \mathbb{R}[x]$.

Příklad 5 (Interpolace)**.** Dokažte pomocí ČZV, že pro každou n-tici $(a_1, b_1), \ldots, (a_n, b_n)$ reálných čísel (a_i jsou po dvou různá) existuje právě jeden polynom $p \in \mathbb{R}[x]$ stupně nejvýše $n-1$, že $p(a_i) = b_i$.

Příklad 6 (Sdílení tajemství)**.** K otevření sejfu je potřeba tajné přirozené číslo s. Máme k dispozici obří prvočíslo q (tak obří, že $q > s$). Náhodně (rovnoměrně, nezávisle) vybereme m čísel $p_1, \ldots, p_m$ z tělesa $\mathbb{Z}_q$ a vyrobíme polynom $p(x) = p_m x^m + p_{m-1} x^{m-1} + \cdots + p_1 x + s$.

Máme n bankéřů, říkejme jim $1, \ldots, n$. Bankéři číslo i sdělíme hodnotu $f(i)$, číslo q a stupeň polynomu f. Dokažte, že:

1. Skupina libovolných $m+1$ bankéřů se dokáže dohodnout a sejf otevřít.
2. Libovolná skupina o m a méně bankéřích nemá lepší šanci sejf otevřít, než kdyby číslo s tipovali z množiny $\{1, \ldots, q-1\}$.

Příklad 7. Pomocí ČZV dokažte, že pokud reálná čísla α, β jsou různá, $m, n \in \mathbb{N}$ a $p \in \mathbb{R}[x]$ je stupně nejvýše $m+n-1$, tak:

1. Polynomy $(x-\alpha)^n$ a $(x-\beta)^m$ jsou nesoudělné.
2. Polynom p lze jednoznačně napsat ve tvaru $(x-\alpha)^n s + (x-\beta)^m t$ pro nějaké $t, s \in \mathbb{R}[x]$.
3. Výraz $\frac{p}{(x-\alpha)^n (x-\beta)^m}$ má jednoznačný rozklad na parciální zlomky.