6 Počítání modulo polynom

1. V $\mathbb{Z}_2[x]$ najděte největší společný dělitel $d(x)$ polynomů $p(x) = x^7+x^6+x^5+x^4+x$ a $q(x) = x^3+1$.
2. Řešte rovnici $(x+1)r(x) = x+2$ v okruhu $A = \mathbb{Z}_3[x]/q(x)$, kde $q(x) = x^2+2x+2$. Tvoří tento okruh těleso? Kolik prvků má okruh A?
3. Rozhodněte, zda je okruh $B = \mathbb{Z}_3[x]/q(x)$, kde $q(x) = x^3+1$, těleso. Najděte inverzní prvek k prvku x^2+1 a vypište všechny prvky, které nemají v okruhu B inverzní prvek.

(6.1) dělení polynomů v $\mathbb{Z}_n$

(6.2) 1) zjistím, zda má polynom inverzi - hledám v $\mathbb{Z}_3/q(x)$
- $c_1 \in D(q(x), a)$
- $c_1 \in D = 1 \rightarrow$ existuje inverze
- inverzi zjistím rozšířeným Euklidem

2) vypočtu hodnotu polynomu $r(x)$
- upravím pomocí inverzu tak, abych měla tvar $r(x) = \dots$
- vypočtu

3) je okruh těleso?
(V) okruh polynomů nad $\mathbb{Z}_p[x]/q(x)$ je těleso, jestliže $q(x)$ je ireducibilní v $\mathbb{Z}_p[x]$
$\mathbb{Z}_p[x]$ je těleso, pokud p je prvočíslo.
- do $q(x)$ postupně dosadím prvky $\mathbb{Z}_p$ a vypočtu, pokud $\neq 0$, pak $q(x)$ nemá reálné kořeny $\rightarrow$ je ireducibilní $\rightarrow$ $q(x)$ je rovněž těleso

4) počet prvků v okruhu
$|A| = p^k = 3^{(2)} \rightarrow$ stupeň polynomu $q(x)$
$\rightarrow \mathbb{Z}_3$

5) prvky v okruhu A

$A = \{ax + b, \quad a, b \in \mathbb{Z}_p\}$

6) ověřím, zda rovnice leží v okruhu
- ~~ta~~ - která část není prvkem, ta se udělá mod $q(x)$

(6.3)

1) předpoklad - $\mathbb{Z}_p$ je těleso

2) zjistím, zda je $q(x)$ těleso
- viz (6.2)

3) hledám inverzní prvek
- $GCD(q(x), a)$
- $GCD = 1 \rightarrow$ inverze existuje

4) vypočtu inverzi - zde složité
vyjádřím „1" $\Rightarrow$ vypočtu z „2" která je o krok předtím

5) prvky, které nemají inverzi
= prvky, které ~~- jsou soudělné~~ přes inverzi
~~- jsou soudělné~~

$B = \{ax + b; \quad a, b \in \mathbb{Z}_p\}$
- jsou soudělné přes inverzní prvek
- soudělné přes výsledek
  $q(x) : (\text{prvek} \cdot \text{inverze})$
- ~~prvky~~ určit nejvyšší stupeň (dle inverze)

$h(x)\ (\text{inverze}) = a\ (\text{inverze})\quad a \in \mathbb{Z}_p$

$h(x)\ (\ \ ) = bx + c\ (\ \ )\quad b, c \in \mathbb{Z}_p$