4 Počítání modulo polynom

„Co se vyplatilo jendou, vyplatí se i podruhé.“

V této kapitole zavedeme polynomy nad $\mathbb{Z}_p$ a ukážeme, že množina všech polynomů nad $\mathbb{Z}_p$ tvoří komutativní okruh s jednotkou. Je-li p prvočíslo, tak lze v tomto okruhu dělit se zbytkem každým nenulovým polynomem. Díky tomu můžeme, podobně jako v okruhu celých čísel, vytvořit faktorové okruhy modulo polynom. Počítáme-li modulo ireducibilní polynom, získáme komutativní těleso.

Polynomy nad $\mathbb{Z}_p$

4.1 Definice *Polynom $a(x)$ nad $\mathbb{Z}_p$* je výraz tvaru $a_k\,x^k + \ldots + a_1\,x + a_0$, kde koeficienty a_i jsou ze $\mathbb{Z}_p$. Symbol x nazýváme *proměnná*. Největší k takové, že $a_k \neq 0$, se nazývá *stupeň polynomu*, značí se $\mathrm{st}(a(x))$. Pro nulový polynom klademe $\mathrm{st}(0) = -1$. Množinu všech polynomů nad $\mathbb{Z}_p$ v proměnné x značíme $\mathbb{Z}_p[x]$.

4.2 Definice *Rovnost polynomů nad $\mathbb{Z}_p$* nastane, pokud oba polynomy mají stejný stupeň a stejné koeficienty u stejných mocnin.

Poznámka: Různé polynomy nad $\mathbb{Z}_p$ mohou určovat stejné funkce ze $\mathbb{Z}_p$ do $\mathbb{Z}_p$. Funkce jsou stejné tehdy, mají-li stejný definiční obor a dávají-li stejné výsledky v každém prvku definičního oboru. Je tedy p^p funkcí ze $\mathbb{Z}_p$ do $\mathbb{Z}_p$, zatímco polynomů nad $\mathbb{Z}_p$ je spočetně mnoho. Např. polynomy $x+1$ a x^2+1 určují stejné funkce ze $\mathbb{Z}_2$ do $\mathbb{Z}_2$.

4.3 Na množině polynomů nad $\mathbb{Z}_p$ jsou definovány *operace sčítání* a *násobení* analogicky jako pro reálné polynomy, pouze s koeficienty počítáme v $\mathbb{Z}_p$.

Pro stupně výsledných polynomů platí:

- $\mathrm{st}(a(x) + b(x)) \leq \max(\mathrm{st}(a(x)), \mathrm{st}(b(x)))$
- $\mathrm{st}(a(x) \cdot b(x)) = \mathrm{st}(a(x)) + \mathrm{st}(b(x))$, jsou-li oba polynomy nenulové, jinak by byl $\mathrm{st}(a(x) \cdot b(x)) = -1$.

Poznámka: Pro polynomy nad $\mathbb{Z}_n$, kde $n \neq p$, neplatí tento vztah pro stupeň součinu, protože okruh $\mathbb{Z}_n$ obsahuje dělitele nuly (tj. nenulové prvky, jejichž součin je nula). Např. v $\mathbb{Z}_6[x]$ je $\mathrm{st}(2x \cdot 3x) = \mathrm{st}(0) = -1$.

4.4 Tvrzení *Trojice $(\mathbb{Z}_p[x], +, \cdot)$ tvoří komutativní okruh s jednotkou. Invertibilními jsou v něm pouze nenulové konstanty.*

4.5 Věta o dělení se zbytkem *Pro libovolné polynomy $a(x), b(x) \in \mathbb{Z}_p[x]$, kde $b(x) \neq 0$, existují jednoznačně určené polynomy $r(x), z(x) \in \mathbb{Z}_p[x]$ tak, že*

$$a(x) = r(x)\,b(x) + z(x) \quad \text{a} \quad \mathrm{st}(z(x)) < \mathrm{st}(b(x)).$$

Důkaz Polynomy $r(x)$ a $z(x)$ najdeme stejným algoritmem pro dělení polynomů jako u reálných polynomů, pouze místo „dělení vedoucím koeficientem“ používáme „násobení k němu inverzním prvkem“.
Pro $\mathrm{st}(a(x)) < \mathrm{st}(b(x))$ je $r(x) = 0$ a $z(x) = a(x)$. V opačném případě spočteme první člen částečného podílu takto:

$$(a_k\,x^k + \ldots + a_1\,x + a_0) : (b_m\,x^m + \ldots + b_1\,x + b_0) = (a_k\,b_m^{-1}\,x^{k-m} + \ldots \quad)$$

Po zpětném vynásobení polynomu $b(x)$ prvním členem podílu a po odečnení tohoto součinu od polynomu $a(x)$ se sníží stupeň dělence. Postup opakujeme, dokud není stupeň dělence menší než $\mathrm{st}(b(x))$. ⊠

Poznámka: V algoritmu dělení polynomů je důležité, že jakýkoliv nenulový vedoucí koeficient polynomu $b(x)$ má v tělese $\mathbb{Z}_p$ inverzní prvek. To v okruhu $\mathbb{Z}_n$ neplatí, tudíž algoritmus dělení nebude pro polynomy, jejichž vedoucí koeficient nemá inverzní prvek, fungovat. Skutečně, v $\mathbb{Z}_n[x]$, kde n není prvočíslo, nelze dělit těmi polynomy, které mají neinvertibilní vedoucí koeficient. Tudíž pro polynomy nad $\mathbb{Z}_n$ nelze vystavět následující teorii opřenou o dělení se zbytkem. Naopak algoritmus dělení polynomů funguje pro polynomy nad libovolným tělesem T, pro ně se dá následující teorie zcela analogicky použít.

První sada důsledků:

4.6 Definice Polynom $a(x)$ *dělí* polynom $b(x)$ v $\mathbb{Z}_p[x]$, jestliže $b(x) = r(x)\,a(x)$ pro nějaký polynom $r(x) \in \mathbb{Z}_p[x]$. Značíme $a(x) \,|\, b(x)$.

Přitom nenulová konstanta c ze $\mathbb{Z}_p$ dělí každý polynom $b(x)$, neboť $b(x) = c \cdot (c^{-1}b(x))$. Relace dělitelnosti není uspořádáním na množině $\mathbb{Z}_p[x]$. Polynomy, které se liší o konstantní násobek, se dělí navzájem, tj. $a(x) \,|\, b(x)$ a $b(x) \,|\, a(x)$. Říkáme, že jsou to *asocionané polynomy*, a značíme $a(x) \,||\, b(x)$.

4.7 Definice Prvek $c \in \mathbb{Z}_p$ je *kořen* polynomu $q(x) \in \mathbb{Z}_p[x]$, jestliže platí $q(c) = 0$.

4.8 Tvrzení *Prvek $c \in \mathbb{Z}_p$ je kořenem polynomu $q(x) \in \mathbb{Z}_p[x]$ právě, když polynom $(x - c)$ dělí polynom $q(x)$.*

4.9 Tvrzení *Polynom $q(x) \in \mathbb{Z}_p[x]$ stupně $k \geq 0$ má v tělese $\mathbb{Z}_p$ nejvýše k kořenů.*

Důkaz indukcí podle k. Polynom stupně nula je nenulová konstanta, nemá tedy žádný kořen. Předpokládejme, že každý polynom stupně k má nejvýše k kořenů, a zvolme libovolně polynom $q(x)$ stupně $k + 1$. Pokud $q(x)$ nemá žádný kořen, tak počet kořenů je menší než $k + 1$. Pokud má $q(x)$ kořen c, tak $q(x) = (x - c)\,r(x)$, kde $\mathrm{st}(r(x)) = k$, tudíž dle předpokladu má polynom $r(x)$ nejvýše k kořenů. Přitom pro libovolný kořen b polynomu $q(x)$ platí $0 = q(b) = (b - c)\,r(b)$ v tělese $\mathbb{Z}_p$. Protože těleso nemá dělitele nuly, je buď $b = c$ nebo $r(b) = 0$, tj. b je kořen polynomu $r(x)$. Počet kořenů polynomu $q(x)$ je tudíž nejvýše $k + 1$. ⊠

Poznámka: Stejně by se dokázalo, že polynom nad libovolným tělesem má nejvýše tolik kořenů, kolik je jeho stupeň. Důkaz však selže pro polynomy nad okruhem, ve kterém jsou dělitelé nuly. Tam je skutečně možné, že polynom stupně k má více než k kořenů a že se dá rozložit různými způsoby na polynomy nižších stupňů. Např. v $\mathbb{Z}_8[x]$ platí $x^2 - 1 = (x - 1)(x + 1) = (x - 3)(x + 3)$. Polynom $x^2 - 1$ má celkem čtyři kořeny v okruhu $\mathbb{Z}_8$ a jsou to prvky $1, -1 = 7, 3, -3 = 5$.

4.10 Definice Polynom $q(x)$ stupně $k \geq 1$ se nazývá *ireducibilní* polynom nad $\mathbb{Z}_p$, jestliže se $q(x)$ nedá napsat jako součin dvou polynomů nad $\mathbb{Z}_p$ stupně menšího než k.

Každý polynom lze rozložit na $q(x) = c \cdot (c^{-1}q(x))$ pro $0 \neq c \in \mathbb{Z}_p$, stejně jako lze každé celé číslo rozložit na $n = 1 \cdot n$. Ireducibilní polynomy $q(x)$ má pouze tyto rozklady, aneb $q(x)$ je dělitelný pouze konstantami a polynomy asociovanými s $q(x)$.

4.11 Testování ireducibility polynomu $q(x)$: Polynom $q(x)$ je ireducibilní nad $\mathbb{Z}_p$, pokud není dělitelný žádným ireducibilním polynomem nad $\mathbb{Z}_p$ stupně nejvýše $\frac{\mathrm{st}(q(x))}{2}$.

Místo dělení polynomu $q(x)$ lineárními polynomy $(x - c)$ můžeme zkoušet, zda c není kořenem polynomu $q(x)$.

4.12 Tvrzení *Polynom $q(x)$ stupně $\mathrm{st}(q) \leq 3$ je ireducibilní nad $\mathbb{Z}_p$ právě, když $q(x)$ nemá kořen v $\mathbb{Z}_p$.*

4.13 Příklad Polynom x^2+1 je ireducibilní nad $\mathbb{Z}_3$, neboť nemá kořen v $\mathbb{Z}_3$. Tentýž polynom je ale rozložitelný nad $\mathbb{Z}_2$, neboť má kořen $c = 1$ v $\mathbb{Z}_2$, $x^2 + 1 = (x + 1)^2$ je jeho rozklad na ireducibilní polynomy v $\mathbb{Z}_2[x]$.
Polynom $x^4 + x^2 + 1$ sice nemá kořen v $\mathbb{Z}_2$, ale není ireducibilní, neboť $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ v $\mathbb{Z}_2[x]$.

4.14 Věta *Nad $\mathbb{Z}_p$ existují ireducibilní polynomy libovolného stupně $k \geq 1$.*

Uvědomme si, že situace s ireducibilními polynomy je nad $\mathbb{Z}_p$ naprosto jiná než u reálných polynomů. Mezi reálnými polynomy jsou kromě lineárních polynomů ireducibilní už jen kvadratické polynomy s komplexně sdruženými kořeny a všechny reálné polynomy stupně $k \geq 3$ jsou rozložitelné.

4.15 Tvrzení *Každý polynom $m(x)$ nad $\mathbb{Z}_p$ lze jednoznačně (až na pořadí) rozložit v $\mathbb{Z}_p[x]$ na součin konstanty a monických ireducibilních polynomů, tj. $m(x) = c \cdot q_1(x) \cdot \ldots \cdot q_n(x)$, kde $c \in \mathbb{Z}_p$ a všechny q_i jsou monické polynomy ireducibilní nad $\mathbb{Z}_p$ (monické polynomy mají vedoucí koeficient roven 1).*

Poznámka: Jednoznačnost rozkladů platí pro polynomy na libovolným tělesem, nemusí však platit pro polynomy nad okruhem, jak bylo ukázáno výše.

Druhá sada důsledků:

4.16 Definice *Největší společný dělitel* dvou polynomů $a(x), b(x) \in \mathbb{Z}_p[x]$ je takový polynom $d(x) \in \mathbb{Z}_p[x]$, že $d(x)$ dělí oba polynomy $a(x)$ i $b(x)$, že $d(x)$ je dělitelný všemi společnými děliteli obou polynomů a konečně že $d(x)$ je monický polynom (má vedoucí koeficient roven 1). Značíme $d(x) = \gcd(a(x), b(x))$.

Bez požadavku, aby největší společný dělitel byl monický, bychom měli celou třídu navzájem asociovaných největších společných dělitelů polynomů $a(x)$ a $b(x)$. Připusťme i tento pohled na věc.

4.17 Definice Polynomy jsou *nesoudělné*, pokud jejich největší společný dělitel je 1 (nebo nenulová konstanta, nebudeme-li požadovat monický největší společný dělitel).

4.18 Pro hledání největšího společného dělitele polynomů můžeme použít **Eukleidovův algoritmus**, protože se opírá pouze o dělení se zbytkem a v okruhu polynomů nad $\mathbb{Z}_p$ dělit se zbytkem umíme. Tudíž funguje i rozšířený Eukleidův algoritmus, který dokazuje Bezoutovu větu.

4.19 Věta (Bezoutova) *Největší společný dělitel $a(x), b(x) \in \mathbb{Z}_p[x]$ je jejich polynomiální kombinací,*

$$\gcd(a(x), b(x)) \;=\; k(x)a(x) \;+\; l(x)b(x) \quad \text{pro} \quad k(x), l(x) \in \mathbb{Z}_p[x].$$

4.20 Polynomiální rovnice $a(x)r(x) + b(x)s(x) = c(x)$, kde $a(x), b(x), c(x) \in \mathbb{Z}_p[x]$, má řešení v $\mathbb{Z}_p[x]$ právě, když $\gcd(a(x), b(x)) \mid c(x)$ v $\mathbb{Z}_p[x]$. Pokud nějaké řešení existuje, pak je jich nekonečně mnoho a jsou tvaru

$$(r(x), s(x)) = (r_p(x), s_p(x)) + k(x)(r_0(x), s_0(x)) \quad \text{pro} \quad k(x) \in \mathbb{Z}_p[x],$$

kde $(r_p(x), s_p(x))$ je partikulární řešení a najdeme ho pomocí rozšířeného Eukleidova algoritmu a kde $(r_0(x), s_0(x))$ je nesoudělné řešení homogenní rovnice, tedy $(r_0(x), s_0(x)) = (\frac{b(x)}{d(x)}, -\frac{a(x)}{d(x)})$ pro $d(x) = \gcd(a(x), b(x))$.

Třetí sada důsledků:

Konstrukce faktorových okruhů modulo polynom

4.21 Definice Polynomy $a(x), b(x) \in \mathbb{Z}_p[x]$ jsou *kongruentní modulo polynom* $m(x)$, jestliže $m(x) \mid (b(x) - a(x))$ v $\mathbb{Z}_p[x]$. Značíme $a(x) \equiv b(x) \pmod{m(x)}$.

4.22 Tvrzení *$a(x) \equiv b(x) \pmod{m(x)}$ právě, když mají $a(x)$ a $b(x)$ stejný zbytek po dělení polynomem $m(x)$.*

4.23 Tvrzení *Relace kongruence modulo polynom $m(x)$ je relace ekvivalence (tj. reflexivní, symetrická a tranzitivní relace) na množině všech polynomů nad $\mathbb{Z}_p$, která je zachována při sčítání a násobení:*
Pokud $a(x) \equiv b(x) \pmod{m(x)}$ a $c(x) \equiv d(x) \pmod{m(x)}$,
pak $a(x) + c(x) \equiv b(x) + d(x) \pmod{m(x)}$, a $a(x) \cdot c(x) \equiv b(x) \cdot d(x) \pmod{m(x)}$.

4.24 Relace kongruence modulo polynom $m(x)$ tudíž rozbije množinu polynomů nad $\mathbb{Z}_p$ na třídy navzájem ekvivalentních polynomů, tj. třídy $[a(x)]_{m(x)} = \{a(x) + k(x)m(x) \mid k(x) \in \mathbb{Z}_p[x]\}$. Polynomy v jedné třídě mají stejný zbytek po dělení polynomem $m(x)$, můžeme jej tedy zvolit za representanta této třídy. Třídy nazýváme zbytkové třídy modulo polynom $m(x)$. Množinu všech zbytkových tříd modulo $m(x)$ značíme $\mathbb{Z}_p[x]/m(x)$.
Má-li polynom $m(x)$ stupeň k, pak zbytkem po dělení $m(x)$ může být jakýkoliv polynom nad $\mathbb{Z}_p$ stupně menšího než k, je tedy celkem p^k různých zbytkových tříd.

$$\mathbb{Z}_p[x]/m(x) = \{[a(x)]_{m(x)}, a(x) \in \mathbb{Z}_p[x],\ \mathrm{st}(a(x)) < \mathrm{st}(m(x))\}$$

Na množině $\mathbb{Z}_n$ můžeme korektně definovat operace sčítání a násobení přes representanty:

$$[a(x)]_{m(x)} \oplus [b(x)]_{m(x)} = [a(x) + b(x)]_{m(x)}, \quad [a(x)]_{m(x)} \odot [b(x)]_{m(x)} = [a(x) \cdot b(x)]_{m(x)}$$

Díky definici přes representanty zdědí operace $\oplus$ a $\odot$ vlastnosti, které měly operace sčítání a násobení na polynomech nad $\mathbb{Z}_p$.

4.25 Tvrzení *Trojice* $(\mathbb{Z}_p[x]/m(x), \oplus, \odot)$ *tvoří komutativní okruh s jednotkou, tzv. faktorový okruh modulo polynom* $m(x)$.

V dalším textu zjednodušíme značení: pro prvky faktorových okruhů budeme používat jinou proměnnou než x, místo $[a(x)]_{m(x)}$ budeme psát většinou $a(z)$, násobení a sčítání budeme značit obyčejně $\cdot$ a $+$.

$$(\,\mathbb{Z}_p[x]/m(x) = \{a_{k-1}\,z^{k-1} + \ldots + a_1\,z + a_0,\; a_i \in \mathbb{Z}_p\}, +, \cdot\,)$$

Všimněme si, že sčítání je normálním sčítáním polynomů nad $\mathbb{Z}_p$, při sčítání se totiž nezvýší stupeň a počítání modulo $m(x)$ se neprojeví. Výsledkem násobení je zbytek po dělení součinu polynomů nad $\mathbb{Z}_p$ polynomem $m(x)$.

4.26 Lineární rovnice $a(z)r(z) = b(z)$ ve faktorovém okruhu $\mathbb{Z}_p[x]/m(x)$ řešíme převedením na polynomiální rovnici $a(x)r(x) + m(x)s(x) = b(x)$ v $\mathbb{Z}_p[x]$.
Víme tedy, že řešení existuje právě, když $\gcd(a(x), m(x)) \mid b(x)$. Pak všechna řešení mají tvar

$$r(z) = r_p(z) + k(z)r_0(z), \quad \text{kde} \quad r_0(z) = \frac{m(z)}{d(z)} \quad \text{pro} \quad d(x) = \gcd(a(x), m(x)).$$

Různá řešení v okruhu $\mathbb{Z}_p[x]/m(x)$ budou vznikat pro různé polynomy $k(x) \in \mathbb{Z}_p[x]$ stupně menšího než je $\mathrm{st}(d(x))$.

4.27 Tvrzení *Prvek* $a(z)$ *je invertibilní v okruhu* $\mathbb{Z}_p[x]/m(x)$ *právě, když je polynom* $a(x)$ *nesoudělný s polynomem* $m(x)$ *v* $\mathbb{Z}_p[x]$.

Důkaz Inverzní prvek k $a(z)$ řeší rovnici $a(z)r(z) = 1$. Řešení rovnice existuje jen, když $\gcd(a(x), m(x)) \mid 1$, tedy $a(x)$ je nesoudělný s $m(x)$. ⊠

4.28 Věta *Faktorový okruh* $\mathbb{Z}_p[x]/q(x)$ *je tělesem právě tehdy, když* $q(x)$ *je ireducibilní polynom nad* $\mathbb{Z}_p$.

Důkaz Ireducibilní polynom nemůže být soudělný se žádným polynomem nižšího stupně kromě 0, takže všechny nenulové prvky faktorového okruhu mají inverzní prvek. ⊠

4.29 Definice Nechť $q(x)$ je ireducibilní polynom nad $\mathbb{Z}_p$ stupně k. Těleso $\mathbb{Z}_p[x]/q(x)$ se nazývá *Galoisovo těleso* o p^k prvcích a značí se $GF(p^k)$.

4.30 Pro Galoisova tělesa lze dokázat:

- Pro libovolné prvočíslo p a přirozené číslo k existuje Galoisovo těleso o p^k prvcích (aneb existují ireducibilní polynomy nad $\mathbb{Z}_p$ libovolného stupně k).
- Každá dvě Galoisova tělesa o p^k prvcích jsou izomorfní (aneb na volbě ireducibilního polynomu nezáleží).
- Jiná konečná tělesa než tělesa Galoisova neexistují.

4.31 Příklady

- Okruh $A = \mathbb{Z}_2[x]/(x^2+1) = \{0, 1, z, z+1\}$ není těleso, protože polynom $x^2+1 = (x+1)^2$ není ireducibilní nad $\mathbb{Z}_2$. Konkrétně prvek $z+1$ nemá inverzní prvek.
- Okruh $B = \mathbb{Z}_2[x]/(x^2+x+1) = \{0, 1, z, z+1\}$ je těleso, neboť polynom x^2+x+1 je ireducibilní nad $\mathbb{Z}_2$.

Všimněme si, že okruhy A a B mají stejné prvky a stejné sčítání, liší se pouze násobením. Oba okruhy také obsahují prvky 0 a 1 (resp. [0], [1]) a s nimi se počítá stejně jako v $\mathbb{Z}_2$. Okruh B je navíc tělesem, říkáme, že B je *rozšíření tělesa*, či *nadtěleso* tělesa $\mathbb{Z}_2$.

4.32 Jiný pohled na násobení ve faktorovém okruhu $\mathbb{Z}_\mathbf{p}[\mathbf{x}]/\mathbf{m}(\mathbf{x})$

Nechť $m(x) = a_k x^k + \ldots + a_1 x + a_0$ je polynom je stupně k. V okruhu $\mathbb{Z}_p[x]/m(x)$ platí vztah

$$m(z) = a_k z^k + \ldots + a_1 z + a_0 = 0,$$

protože vydělíme-li polynom $m(x)$ sebou samým, dostaneme zbytek 0. Z této rovnosti můžeme vyjádřit

$$z^k = a_k^{-1}(-a_{k-1} z^{k-1} - \ldots - a_1 z - a_0).$$

Přitom okruh $\mathbb{Z}_p[x]/m(x)$ obsahuje polynomy stupně nejvýše $(k-1)$. Při vynásobení dvou prvků vznikne polynom stupně nejvýše $(2k-2)$. Potřebujeme tedy pravidla pro přepsání mocnin z^k, z^{k+1} až z^{2k-2}, celkem $(k-1)$ přepisovacích pravidel. Přepisovací pravidlo pro z^k jsme již odvodili ze vztahu $m(z) = 0$. Ostatní přepisovací pravidla získáme z tohoto pravidla postupným násobením proměnnou z a dosazováním předchozích pravidel.

Přepisovací pravidla lze použít i k řešení lineárních rovnic $a(z)r(z) = b(z)$ ve faktorovém okruhu $\mathbb{Z}_p[x]/m(x)$. Místo Eukleidova algoritmu budeme muset vyřešit soustavu k lineárních rovnic nad $\mathbb{Z}_p$ pro k neznámých koeficienktů polynomu $r(z)$.

4.33 Příklady

- Okruh $A = \mathbb{Z}_2[x]/(x^2+1) = \{0, 1, z, z+1\}$ má přepisovací pravidlo pro násobení $z^2 = -1$. Bývá zvykem značit $z = i$. Vytvořili jsme komplexní čísla nad $\mathbb{Z}_2$.
- Těleso $B = \mathbb{Z}_2[x]/(x^2+x+1) = \{0, 1, z, z+1\}$ má přepisovací pravidlo pro násobení $z^2 = z + 1$.
- Těleso $T = \mathbb{Z}_2[x]/(x^3+x+1) = \{a\alpha^2 + b\alpha + c,\, a, b, c \in \mathbb{Z}_2\}$ má dvě přepisovací pravidla pro násobení, $\alpha^3 = \alpha + 1$ a $\alpha^4 = \alpha^2 + \alpha$.

4.34 O okruzích $\mathbb{Z}_p[x]/(x^2+1)$ mluvíme též jako o komplexních číslech nad $\mathbb{Z}_p$ a značíme je $\mathbb{Z}_p[i]$. Tedy $\mathbb{Z}_p[i] = \{ai + b,\, a, b \in \mathbb{Z}_p,\, i^2 = -1\}$. Stejným způsobem vznikla i komplexní čísla nad $\mathbb{R}$, $\mathbb{C} = \mathbb{R}[x]/x^2 + 1$. Komplexní čísla nad $\mathbb{Z}_p$ však netvoří vždy těleso, neboť polynom $x^2 + 1$ nemusí být ireducibilní nad $\mathbb{Z}_p$. Např. $\mathbb{Z}_3[i]$ je těleso, ale $\mathbb{Z}_2[i]$ není těleso (viz příklad 4.13).