Teorie nejen čísel 3 – Polynomy

Milý příteli,
vítej u závěrečného dílu letošního seriálu. Minule jsme si ukázali sílu jednotek pomocí Pellovy rovnice, jejíž řešení se dají všechna vyrobit z jednoho fundamentálního, i na konečných tělesech, jejichž (nenulové) prvky se dají všechny vyrobit z jednoho primitivního.

V tomto díle se zaměříme na to, jak si upéct okruhy *polynomů* a jak potom budou chutnat v závislosti na tom, z jakého těsta je pečeme. Při jejich zkoumání se vrátíme ke kořenům.[1] Proto oprášíme znalosti z prvního dílu, především to, že když už „funguje“ dělení s nějakým malým zbytkem, tak už „fungují“ i obdoby prvočísel a jednoznačný rozklad na ně. Na závěr potom změníme žánr a jako detektivové se naučíme skládat velkou modulární skládačku ze spousty menších kousků.

Jak seriál číst

Tak jako v předchozích dílech na Tebe i nyní čeká množství cvičení a úloh na procvičení. Na konci seriálu nalezneš návody ke cvičením i k úlohám a také řešení cvičení. Tak jako dříve přisuzujeme některým cvičení mírně odlišný význam: vykřičníky označují obzvláště důležitá cvičení, která mnohdy využíváme v některých pozdějších důkazech, zatímco cvičení s hvězdičkou se zabývají nějakou zajímavostí nebo náročnější myšlenkou, která není k dalšímu chápání seriálu nutná.

Okruhy polynomů

Doposud jsme v seriálu vyráběli nové, větší okruhy z těch menších tak, že jsme k nim přidali nový prvek. Ten jsme vždy zvolili tak, aby splňoval nějakou rovnost: když například k celým číslům přidáváme imaginární jednotku i, máme $i^2 = -1$, takže jakýkoliv výraz s vysokými mocninami i dovedeme zjednodušit, a k zapsání libovolného prvku $\mathbb{Z}[i]$ nám tak stačí tvar $a + bi$, kde $a, b \in \mathbb{Z}$. Podobně když jsme v minulém díle vyráběli osmiprvkové těleso, přidali jsme k $\mathbb{Z}_2$ prvek α splňující $\alpha^3 = \alpha + 1$, což nám dovolilo vystačit pro zapsání prvků $\mathbb{Z}_2[\alpha]$ s tvarem $a\alpha^2 + b\alpha + c$, kde $a, b, c \in \mathbb{Z}_2$. Tentokráte to zkusíme jinak: budeme přidávat prvek x, po kterém nebudeme požadovat vůbec nic. Dostaneme tak okruhy, jejichž prvky jsou nějaké výrazy s neznámou.

Úmluva. Není-li řečeno jinak, bude v tomto dílu R vždy značit nějaký (libovolný) komutativní okruh.

Definice. *Polynomem*[2] *nad* R rozumíme výraz tvaru

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

kde n je nezáporné celé číslo a *koeficienty* $a_0, a_1, \ldots, a_n$ jsou prvky R. Koeficientu a_0 říkáme *absolutní člen* a polynom, který má všechny koeficienty kromě a_0 nulové, nazveme *konstantní*.

[1] A to ve více než jednom významu ...

[2] Nebo též česky *mnohočlenem*.

Polynomy sčítáme tak, že sečteme koeficienty u jednotlivých mocnin, kupříkladu

$$(ax^2 + bx + c) + (dx + e) = ax^2 + (b + d)x + (c + e).$$

Při násobení zase roznásobíme všechny členy, součiny mocnin x znásobíme jako $x^k \cdot x^\ell = x^{k+\ell}$ a výsledky posčítáme, například

$$\begin{aligned}(ax^2 + bx + c) \cdot (dx + e) &= adx^3 + aex^2 + bdx^2 + bex + cdx + ce = \\ &= (ad)x^3 + (ae + bd)x^2 + (be + cd)x + ce.\end{aligned}$$

Polynomy nad R tvoří okruh, který značíme $R[x]$.

Poznámka. Symbol x v zápisu polynomů představuje nějakou úplně obecnou proměnnou, která nemá žádnou konkrétní hodnotu. Okruh $R[x]$ tedy vzniká tím, že k R přidáme prvek x, kterému ale nepřiřkneme vůbec žádné specifické vlastnosti. Později uvidíme, že nám toto umožňuje za x dosadit libovolnou hodnotu. V tomto dílu seriálu pro nás však samotné x bude vždy značit proměnnou v zápisu polynomu a pro konkrétní hodnoty vždy použijeme jiné písmenko.

V zapisování polynomů si budeme dovolovat některá zjednodušení: členy s nulovým koeficientem budeme vynechávat, namísto $(-a)x$ budeme psát $-ax$ a s koeficienty 1 se nebudeme obtěžovat (tedy místo $1x$ napíšeme jen x).

Poznámka. Každý prvek $a \in R$ se vyskytuje i v $R[x]$ jako konstantní polynom a, takže můžeme uvažovat, že R je podmnožinou množiny $R[x]$, resp. dokonce i podokruhem okruhu $R[x]$.

Cvičení 1. Okruh $R[x]$ je triviální, právě pokud je triviální R. Připomeňme, že okruhu říkáme *triviální*, pokud má jen jeden prvek.

Polynomy jsou *konečné* výrazy tvořené násobením a sčítáním proměnné x a nějakých konstant z okruhu R. Nekonečné výrazy jako například

$$1 + x + x^2 + x^3 + x^4 + x^5 + \cdots,$$

kde máme nenulový koeficient u nekonečně mnoha mocnin x^k, za polynomy nepovažujeme. U každého polynomu tak máme nějaký největší exponent mocniny, která má ještě nenulový koeficient.

Definice. Mějme nenulový polynom $f \in R[x]$ zapsaný ve tvaru $f = a_n x^n + \cdots + a_1 x + a_0$, kde n je nezáporné celé číslo. *Stupněm* polynomu f rozumíme největší k takové, že $a_k \neq 0$. Stupeň f značíme $\deg f$ a pro $f = 0$ dodefinováváme $\deg 0 = -\infty$.

Poznámka. Konstantní jsou ty polynomy, které mají stupeň 0 nebo $-\infty$. Polynomům stupňů 1, 2 a 3 říkáme po řadě *lineární*, *kvadratické* a *kubické*.

Stupeň je tedy exponent nejvyšší mocniny x, která „je“ v daném polynomu. Proč stupeň nulového polynomu definujeme jako mínus nekonečno? Když se domluvíme, že

$$-\infty + n = -\infty \qquad \text{a} \qquad -\infty + (-\infty) = -\infty,$$

pak platí následující:

Tvrzení. *Nechť je R obor integrity. Potom pro $f, g \in R[x]$ platí* $\deg(fg) = \deg f + \deg g$.

Důkaz. Nejprve předpokládejme, že f, g jsou oba nenulové. Nechť je $f = a_n x^n + \cdots + a_0$ a $g = b_m x^m + \cdots + b_0$, kde $a_n, b_m \neq 0$. Potom když roznásobíme

$$(a_n x^n + \cdots + a_0) \cdot (b_m x^m + \cdots + b_0),$$

pak dostaneme hromadu členů, v nichž nejvyšší zastoupená mocnina x bude x^{n+m}. Ta však vznikne pouze z $a_n x^n \cdot b_m x^m$ a z žádného jiného součinu. Koeficient při x^{n+m} tak ve výsledném polynomu bude $a_n b_m$, což z předpokladu $a_n, b_m \neq 0$ znamená, že tento koeficient je nenulový, jelikož pracujeme v oboru integrity. Žádné vyšší mocniny x v součinu nevzniknou, takže už $\deg(fg) = n + m = \deg f + \deg g$.

Zbývá vyřešit případy, kdy je alespoň jeden z f, g nulový. Potom je ale i $fg = 0$, takže $\deg(fg) = -\infty$. I jeden z f, g je ale nulový, takže $\deg f + \deg g$ je součet $-\infty$ a buďto celého čísla, nebo dalšího $-\infty$. V obou případech je tento součet $-\infty$, takže dokazované tvrzení platí. □

Příklad. Předpoklad, že R je obor integrity, nemůžeme v předchozím tvrzení vypustit. Když např. v $\mathbb{Z}_4[x]$ vezmeme $f = g = 2x + 1$, pak $\deg f = \deg g = 1$, ale $fg = 4x^2 + 4x + 1 = 1$, takže $\deg(fg) = 0$.

Cvičení(!) 2. Pro polynomy f, g platí $\deg(f + g) \leq \max\{\deg f, \deg g\}$, a pokud navíc $\deg f \neq \deg g$, pak už určitě nastává rovnost.

S pomocí stupně si zvládneme rozmyslet některé základní vlastnosti okruhů polynomů – kdy se jedná o obory integrity a posléze jak mohou vypadat jednotky.

Tvrzení. *Je-li R oborem integrity, pak jím je i $R[x]$.*

Důkaz. Mějme $f, g \in R[x]$ splňující $fg = 0$. Stupeň pravé strany je $-\infty$. Pokud f ani g nejsou nulové polynomy, pak jsou jejich stupně alespoň 0, čímž dostaneme

$$-\infty = \deg 0 = \deg(fg) = \deg f + \deg g \geq 0 + 0 = 0,$$

což je spor. □

Jak je to v okruzích polynomů s dělitelností? Z obecné definice dělitelnosti platí $f \mid g$, když existuje polynom h takový, že $fh = g$. Pokud pracujeme nad oborem integrity, tak rovnou víme, že bychom takové h měli hledat se stupněm $\deg g - \deg f$. Přímo z obecné definice bychom mohli rovnou také modulit, ale podrobněji se na modulení polynomů a některá jeho specifika podíváme o něco později.

Cvičení(!) 3. Nechť je R obor integrity. Pokud jsou $f, g \in R[x]$ nenulové polynomy, pak $f \mid g$ implikuje $\deg f \leq \deg g$.

Cvičení(!) 4. Mějme $a \in R$ a polynom $f \in R[x]$. Pak $a \mid f$, právě když a dělí (v okruhu R) všechny koeficienty f.

Cvičení 5. Rozhodni, zda platí následující dělitelnosti nad uvedenými okruhy:

(i) $x^2 + x + 1 \mid x^4 + x^2 + 1$ nad $\mathbb{Q}$,
(ii) $x + 1 \mid x^2 - \sqrt{2}$ nad $\mathbb{R}$,
(iii) $2x + 2 \mid x^2 - 1$ nad $\mathbb{Z}$,
(iv) $x^2 + 1 \mid x^5 + x^4 + x^3 + x^2 + x + 1$ nad $\mathbb{Z}_2$.

S pomocí stupně se také můžeme podívat na to, jaké existují v $R[x]$ jednotky, tedy polynomy, které dělí 1.

Tvrzení. *Pro obor integrity R jsou jednotkami v $R[x]$ pouze jednotky z R.*

Důkaz. Pokud je R triviální, pak je i $R[x]$ triviální a tvrzení platí (v obou je jednotkou jejich jediný prvek). Nadále předpokládejme, že R není triviální – potom ani $R[x]$ není triviální.

Pokud je u jednotkou v R, znamená to, že $uv = 1$ pro nějaké $v \in R$. Pak jsou ale u, v také prvky $R[x]$, takže u je jednotkou i v $R[x]$.

Dále řešme $uv = 1$ pro $u, v \in R[x]$. Pokud je jedno z u, v nula, pak dostaneme $0 = 1$ a rovnost neplatí ($R[x]$ není triviální). Dále když jedno z u, v nebude konstantní, pak

$$0 = \deg 1 = \deg(uv) = \deg u + \deg v \geq 1 + 0,$$

což je spor. Řečeno slovy: součin nenulových polynomů může být konstantní, jen když jsou oba činitelé rovněž konstantní. Takže řešení $uv = 1$ můžeme dostat jen tehdy, když jsou u i v konstantní, tedy když se jedná o jednotky z R. □

Příklad. Bez předpokladu, že R je obor integrity, by předchozí tvrzení neplatilo. Např. v $\mathbb{Z}_4[x]$ je $2x+1$ jednotkou, protože platí $(2x+1)(-2x+1) = -4x^2+1 = 1$.

V seriálu se polynomy nad okruhy, které nejsou obory integrity, příliš zabývat nebudeme, takže tvrzení plynoucí z této vlastnosti můžeme považovat za celkem základní poučky: násobení sčítá stupně a přidání x k oboru integrity R nám nerozbije krácení v rovnicích ani nepřidá žádné nové jednotky.

Dosazování a kořeny

Dosud jsme s polynomy jenom počítali jako v jakémkoliv jiném okruhu. Nyní si představíme nástroj, který už je specifickou vlastností polynomů – lze do nich dosazovat.

Definice. Máme-li v $R[x]$ polynom $f = c_n x^n + \cdots + c_1 x + c_0$, můžeme do něj *dosadit* nějaký jiný polynom $g \in R[x]$ tím, že „místo x napíšeme g“, tedy

$$f(g) = c_n g^n + \cdots + c_1 g + c_0.$$

Poznámka. Když se omezíme na dosazování pouze prvků $a \in R$, pak nám polynom dává zobrazení z R do R. Potom říkáme, že *f nabývá v bodě a hodnoty $f(a)$*. Samotný polynom však odlišujme od zobrazení, které takto definuje. Např. nad $\mathbb{Z}_2$ určují polynomy x^2 a x totožná zobrazení, jelikož

$$0^2 \equiv 0 \pmod 2 \qquad \text{i} \qquad 1^2 \equiv 1 \pmod 2.$$

Přesto se však jedná o odlišné polynomy a v $\mathbb{Z}_2[x]$ platí $x^2 \neq x$.

Příklad. Pro libovolný polynom f získáme dosazením nuly jeho absolutní člen. Naproti tomu $f(1)$ bude součet všech koeficientů.

Příklad. Když do polynomu f dosadíme polynom x, pak jsme jenom „místo x napsali x“, takže se nic nezmění. Zápisy f a $f(x)$ pro nás tedy představují stejný polynom. Pro některé konkrétní polynomy se nemusí nic změnit i pro jiná dosazení – kupříkladu $f = x^4 + x^2 + 1$ splňuje $f(-x) = f$.

Cvičení 6. Nechť je R obor integrity. Potom pro nekonstantní polynomy $f, g \in R[x]$ platí

$$\deg(f(g)) = \deg f \cdot \deg g.$$

Když už umíme do polynomů dosazovat, pojďme se podívat na nějaké hezké vlastnosti, které se k dosazování vážou.

Lemma. (rozdíl argumentů dělí rozdíl hodnot) *Pro polynom $f \in R[x]$ a libovolná $a, b \in R[x]$ platí $a - b \mid f(a) - f(b)$.*

Důkaz. Nechť $f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$, pak můžeme vyjádřit

$$\begin{aligned} f(a) - f(b) &= \left(c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a + c_0\right) - \left(c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0\right) = \\ &= c_n \left(a^n - b^n\right) + c_{n-1} \left(a^{n-1} - b^{n-1}\right) + \cdots + c_1 (a - b) + c_0 (1 - 1). \end{aligned}$$

Když si nyní vezmeme člen $c_k(a^k - b^k)$, pak můžeme nahlédnout, že je opravdu dělitelný $a - b$, jelikož platí

$$a^k - b^k = (a - b)\left(a^{k-1} + a^{k-2} b + \cdots + a b^{k-2} + b^{k-1}\right).$$

Tato rovnost platí, protože když na pravé straně roznásobíme závorky, všechny smíšené členy tvaru $a^{k-j}b^j$ se navzájem vyruší a zbude jen $a^k - b^k$. Tím jsme hotovi, jelikož každý člen ve vyjádření $f(a) - f(b)$ je dělitelný $a - b$, pročež je tím dělitelný i celý součet. □

Jak za chvíli uvidíme, toto lemma se může hodit při řešení některých olympiádních úloh. V úlohách se nejčastěji hodí dosazovat za a, b konstanty (typicky celá čísla, pracujeme-li nad $\mathbb{Z}$). Všimni si ale, že lemma platí i tehdy, když jsou a, b nekonstantní polynomy – na použitých dělitelnostech se totiž nic nezmění. Z tohoto důvodu se lemma může hodit i tehdy, když chceme nahlédnout nějakou dělitelnost v okruhu polynomů.

Úloha 1. Nechť je $f \in \mathbb{Z}[x]$. Dokaž, že pokud pro nějaké celé číslo a platí[3] $f(f(\dots f(a)\dots)) = a$, kde f je použito k-krát za sebou, pak už dokonce $f(f(a)) = a$.

Definice. *Kořenem* polynomu $f \in R[x]$ rozumíme takový prvek $t \in R$, který splňuje $f(t) = 0$.

Příklad. Polynom $x^2 - 5x + 6$ má nad okruhem $\mathbb{Z}$ kořeny 2 a 3. Polynom $x^2 + 1$ nemá nad $\mathbb{R}$ žádný kořen, ale nad $\mathbb{C}$ už má dvojici kořenů i a $-i$. Polynom $x^3 - 2x$ nad $\mathbb{Z}_5$ má jen jeden kořen 0. Pro konstantní polynom 0 nad okruhem R je kořenem libovolný prvek R.

Poznámka. I když máme polynom f nad R, občas se může vyplatit podívat se na něj nad nějakým širším okruhem $S \supset R$ a hledat kořeny tam. Např. v předchozím příkladě je polynom $x^2 + 1$ celočíselný, ale kořeny má až teprve v komplexních číslech.

Cvičení(!) 7. Když $f \mid g$, pak je každý kořen f také kořenem g.

Cvičení 8. Dokaž, že libovolný kořen polynomu dělí jeho absolutní člen.

Cvičení 9. Mějme polynom $f \in \mathbb{Z}[x]$, který ve třech různých bodech $a, b, c \in \mathbb{Z}$ nabývá hodnoty 1 nebo -1. Ukaž, že potom nemůže mít celočíselný kořen.

Předchozí cvičení naznačují, že kořeny mohou být užitečné pro používání dosazovacího lemmatu a dovedou nám něco říci o příslušném polynomu. Je snadné odvodit, že jediným kořenem lineárního polynomu $ax + b$ je v tělese (třeba reálných číslech) číslo $t = \frac{-b}{a}$. Obdobně je známý vzoreček pro kořeny kvadratického polynomu, které mohou existovat nanejvýš dva. Jak je to ale obecně?

V minulém díle jsme už kořeny potkali při zkoumání těles – okruhů, v nichž je každý nenulový prvek jednotkou, jako jsou například racionální čísla $\mathbb{Q}$ nebo konečná tělesa $\mathbb{Z}_p$ pro prvočísla p. Nastínili jsme, že počet kořenů polynomu tvaru $x^n - 1$ je nad tělesem nanejvýš n, to jest stupeň daného polynomu. Nyní už se toho nebudeme bát, protože o polynomech víme více, a dokážeme si to obecněji.

Věta. *Pokud je R obor integrity, pak má nenulový polynom $f \in R[x]$ nejvýše $\deg f$ různých kořenů v R.*

Důkaz. Budeme postupovat indukcí podle stupně f. Máme nenulový polynom, takže $\deg f \geq 0$. Pokud $\deg f = 0$, pak je f nenulový konstantní, takže $f = c \neq 0$, kde $c \in R$. To ale znamená $f(t) = c \neq 0$ pro každé $t \in R$, takže f nemá žádný kořen. Skutečně tedy má nanejvýš $0 = \deg f$ kořenů.

Nyní postupujme indukcí. Pokud f nemá žádné kořeny, jsme hotovi. Pokud má nějaký kořen t, použijeme lemma. Za a vezmeme lineární polynom x a za b vezmeme kořen t. Pak vidíme, že

$$x - t \mid f(x) - f(t) = f - 0 = f.$$

Z definice dělitelnosti to znamená $f = (x - t) \cdot g$ pro nějaký polynom $g \in R[x]$. Předpokládáme, že R je obor integrity, tudíž platí

$$\deg f = \deg(x - t) + \deg g = 1 + \deg g$$

[3] Abychom dostali $f(a)$, dosadíme do polynomu a. Abychom dostali $f(f(a))$, dosadíme do něj $f(a)$. Takto můžeme pokračovat dále a dostávat „více f kolem a“.

neboli $\deg g = n-1$. Nyní z indukčního předpokladu víme, že g má nanejvýš $n-1$ kořenů a $x-t$ má navíc nanejvýš jeden nový[4] kořen t. Jelikož je R oborem integrity, musí kořen f být kořenem $x-t$ nebo kořenem g, takže f má celkově nanejvýš n kořenů. □

Příklad. (varovný) Bez předpokladu, že R je obor integrity, věta nemusí platit. Například nad okruhem $\mathbb{Z}_8$ má polynom x^2-1 hned čtyři různé kořeny 1, 3, 5 a 7.

Tvrzení, které jsme používali v minulém díle, totiž že $x^n = 1$ má nad tělesem T nanejvýš n řešení, je jen speciální případ právě dokázané věty, jelikož každé těleso už je i obor integrity. Z věty také snadno plynou dva užitečné důsledky (v obou stále předpokládáme, že R je obor integrity).

Důsledek. *Má-li polynom $f \in R[x]$ stupně nejvýše n alespoň $n+1$ různých kořenů, pak už $f = 0$.*

Důkaz. Kdyby $f \neq 0$, pak má z věty nanejvýš n různých kořenů. □

Důsledek. *Pokud se dva polynomy $f, g \in R[x]$ stupně nanejvýš n shodují v alespoň $n+1$ různých bodech, pak jsou už nutně totožné.*

Důkaz. Body, v nichž se f a g shodují, jsou kořeny polynomu $f-g$, který tak má alespoň $n+1$ kořenů. Taktéž má ale stupeň nanejvýš n, z čehož plyne $f-g=0$ neboli $f=g$. □

Omezení na počet kořenů, resp. na to, v kolika bodech se mohou dva polynomy shodovat, se často hodí i v úlohách – můžeme si hned nějakou zkusit.

Příklad. Jsou dána tři různá reálná čísla a, b, c. Zjednoduš polynom

$$f = \frac{(x-a)(x-b)}{(c-a)(c-b)} + \frac{(x-b)(x-c)}{(a-b)(a-c)} + \frac{(x-c)(x-a)}{(b-c)(b-a)}.$$

Řešení. Není třeba cokoliv roznásobovat. Když dosadíme a, dostaneme v prostředním zlomku $\frac{(a-b)(a-c)}{(a-b)(a-c)} = 1$, zatímco ve zbylých dvou bude některá závorka v čitateli 0. Máme tedy $f(a) = 1$ a obdobně $f(b) = f(c) = 1$. Polynom f a konstantní polynom 1 mají oba stupeň nanejvýš 2 a shodují se ve třech různých bodech, takže dostáváme rovnost polynomů $f = 1$.

Cvičení 10. Nenulový polynom $f \in \mathbb{R}[x]$ stupně n s navzájem různými reálnými kořeny $t_1, \ldots, t_n$ nazveme *vteřinový*, pokud $f(t_i+1) = 1$ pro každé $i = 1, 2, \ldots, n$. Najdi všechny vteřinové polynomy.

Úloha 2. Polynomy $f, g, h \in \mathbb{Q}[x]$ splňují $x^2+x+1 \mid f$ a $f(x) = g(x^3) + x \cdot h(x^3)$. Dokaž, že $x-1$ dělí g i h.

Úloha 3. Mějme polynom $f \in \mathbb{Z}[x]$ stupně $n > 1$ a označme $g(x) = f(f(\ldots(x)\ldots))$, kde f je aplikováno k-krát. Dokaž, že existuje nanejvýš n celočíselných řešení t rovnice $g(t) = t$.

Podíváme-li se znovu na důkaz věty o počtu kořenů, mohli bychom postup přeformulovat takto: z polynomu f stupně n postupně vytýkáme lineární dvojčleny $x-t$, až nakonec dostaneme vyjádření $f = (x-t_1)\cdots(x-t_r)\cdot g$, kde g je nějaký polynom bez kořenů. Pokud zrovna budeme mít štěstí a z f půjde vytknout n takových dvojčlenů, pak bude g jenom nějaká konstanta a obdržíme tvar $f = c(x-t_1)\cdots(x-t_n)$. Speciálně tak platí:

Pozorování. Má-li polynom f nad oborem integrity R stupeň n a také n *navzájem různých* kořenů $t_1, \ldots, t_n$, potom už $f = c_n(x-t_1)\cdots(x-t_n)$, kde c_n je koeficient u x^n.

Úloha 4. Nechť je $f \in \mathbb{R}[x]$ polynom stupně 2020 takový, že $f(k) = \frac{1}{k}$ pro $k \in \{1, \ldots, 2021\}$. Najdi hodnotu $f(2022)$.

Máme-li takové součinové vyjádření polynomu, je namístě položit si otázku: jak souvisí kořeny $t_1, \ldots, t_n$ (ty nemusí být nutně navzájem různé) s koeficienty f? Drobný příklad vztahu koeficientů a kořenů jsme už viděli v jednom ze cvičení (kořeny dělí absolutní člen), nyní si tento vztah poněkud upřesníme. Pro jednoduchost budeme uvažovat $c = 1$.

[4] Pokud je t i kořenem g, tak se nejedná o nový kořen a f jich má stejně mnoho jako g.

Tvrzení. (Viètovy[5] vztahy) *Mějme polynom $f = x^n + c_{n-1}x^{n-1} + \cdots c_1 x + c_0 \in R[x]$ vyjádřený ve tvaru $f = (x - t_1)\cdots(x - t_n)$ pro nějaké kořeny $t_1, \ldots, t_n \in R$. Potom roznásobením dostáváme vztahy*

$$\begin{aligned} c_0 &= (-1)^n \cdot t_1 \cdots t_n, \\ c_1 &= (-1)^{n-1} \cdot (t_1 \cdots t_{n-1} + \cdots + t_2 \cdots t_n), \\ &\vdots \\ c_{n-1} &= -(t_1 + \cdots + t_n). \end{aligned}$$

Slovy: c_{n-k} se rovná $(-1)^k$ krát součet všech součinů (neuspořádaných) k-tic z čísel $t_1, \ldots, t_n$.

Důkaz. Prostě roznásobíme – vyrobíme spoustu členů, z nichž každý vznikne tak, že si v každé ze závorek $(x - t_i)$ vybereme buďto x, nebo $-t_i$. Mocninu x^{n-k} potom budou obsahovat přesně ty členy, kde jsme si v $n - k$ závorkách vybrali x a v k závorkách $-t_i$. Když tyto členy pak posčítáme, dostaneme v koeficientu c_{n-k} přesně součty všech k-tic kořenů t_i přenásobené $(-1)^k$. □

Pracujeme-li nad tělesem, můžeme se snadno vyrovnat i s tím, když u x^n máme nějaký koeficient $c_n \neq 0$. Prostě můžeme celý polynom vydělit konstantou c_n a z hlediska kořenů se nic nezmění. Ve Viètových vztazích bychom potom prostě místo c_k psali $\frac{c_k}{c_n}$.

V případě kvadratického polynomu odpovídají Viètovy vztahy metodě řešení kvadratické rovnice pomocí rozkladu na součin dvou závorek namísto počítání diskriminantu.

Příklad. Mějme reálná čísla a, b, c, d, pro která platí

$$a + b = c + d \qquad \text{a} \qquad ab = cd.$$

Dokaž, že $\{a, b\} = \{c, d\}$, tedy že se tyto dvojice čísel mohou lišit jen pořadím.

Řešení. Uvažme Viètovy vztahy pro polynomy

$$f = (x - a)(x - b), \qquad g = (x - c)(x - d).$$

Víme, že pak platí, že lineární koeficienty jsou rovny $-(a + b)$ a $-(c + d)$ a absolutní členy jsou rovny ab a cd. Z toho už jasně vidíme, že jde o totožné kvadratické polynomy, tedy i jejich kořeny budou stejné.

Myšlenka tohoto příkladu se nám občas hodí i jinde než v algebře. Pokud například v geometrii najdeme dvě dvojice délek, které splňují uvedené rovnosti, pak také víme, že jsou (v nějakém pořadí) stejné. Také si můžeme všimnout, že polynomy nám dovedou pomoct i v situacích, které na první pohled žádný polynom neobnášejí.

Cvičení 11. Mějme pro dvě různá reálná čísla a, b rovnost $a^2 + 4a + 1 = b^2 + 4b + 1 = 0$. Urči hodnotu $\frac{a}{b} + \frac{b}{a}$.

Úloha 5. Nechť jsou a, b, c reálná čísla, taková že

$$a + b + c > 0, \qquad ab + bc + ca > 0, \qquad abc > 0.$$

Dokaž, že a, b, c jsou kladná.

Na závěr této kapitolky si ukážeme ještě jedno tvrzení, které může pomoci, když zkoumáme racionální kořeny celočíselných polynomů, tedy když se na $f \in \mathbb{Z}[x]$ podíváme nad $\mathbb{Q}$.

[5] François Viète (1540–1603), francouzský matematik, má se svým jménem spojen také vzorec pro π v podobě nekonečného součinu $\frac{2}{\pi} = \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2+\sqrt{2}}}{2} \cdot \frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2} \cdots$

Věta. (o racionálním kořenu) *Mějme polynom* $f(x) = c_n x^n + \cdots + c_0 \in \mathbb{Z}[x]$, *kde* $c_n \neq 0$, *a zkusme do něj dosazovat racionální čísla. Potom je-li zlomek v základním tvaru* $\frac{p}{q}$ *kořenem* f, *pak* $p \mid c_0$ *a* $q \mid c_n$.

Důkaz. Dosaďme $\frac{p}{q}$. Víme, že $c_n \left(\frac{p}{q}\right)^n + \cdots + c_0 = f\left(\frac{p}{q}\right) = 0$. Když tento vztah vynásobíme q^n, získáme

$$c_n p^n + c_{n-1} p^{n-1} q + \cdots + c_1 p q^{n-1} + c_0 q^n = 0.$$

Nyní zde vystupují jen celá čísla. To znamená, že všechny členy až na $c_n p^n$ jsou dělitelné q, tudíž i ono musí být. Předpokládáme, že $\frac{p}{q}$ je v základním tvaru, takže p, q jsou nesoudělná, pročež už z $q \mid c_n p^n$ plyne $q \mid c_n$. Analogicky jsou všechny členy krom $c_0 q^n$ dělitelné p, takže $p \mid c_0$. □

Věta o racionálním kořenu má spoustu fajn důsledků, které si můžeš zkusit nahlédnout.

Definice. Říkáme, že polynom $f = c_n x^n + \cdots + c_0$ je *monický*, pokud $c_n = 1$.

Cvičení(!) 12. Nahlédni, že je-li $f \in \mathbb{Z}[x]$ monický, pak už je každý racionální kořen polynomu f dokonce celé číslo.

Cvičení 13. Nechť je a racionální číslo takové, že $n = a^7 - 7a^5 + 5a^3 - 3a + 7$ je celé číslo. Potom musí a také být celým číslem.

Cvičení 14. Najdi všechny racionální kořeny polynomu $6x^3 - 11x^2 + 6x - 1$.

Úloha 6. Jsou dána celá čísla a, b, c taková, že

$$\frac{a}{b} + \frac{b}{c} + \frac{c}{a} \qquad \text{i} \qquad \frac{b}{a} + \frac{c}{b} + \frac{a}{c}$$

jsou také celá čísla. Dokaž, že $|a| = |b| = |c|$.

Ireducibilní polynomy

Podívejme se nyní, jaké prvky hrají v okruzích $R[x]$ roli prvočísel. V prvním díle jsme se ve vší obecnosti zabývali pojmy, které prvočísla zobecňují – ireducibilními prvky a prvočiniteli. Nyní se zaměříme na ireducibilní prvky v okruzích polynomů a ukážeme si některé jejich základní vlastnosti. Uvidíme, že obzvláště hezky vypadá situace v polynomech nad tělesy.

Definice. *Ireducibilním polynomem* nad R míníme polynom $f \in R[x]$, který je v tomto okruhu ireducibilním prvkem.

Jinými slovy: polynom je ireducibilní, pokud není nulou ani jednotkou a nedá se rozložit na součin dvou polynomů, které také nejsou jednotky.

Příklad. Dokažme, že polynom $f = x^2 - 2$ je nad $\mathbb{Q}$ ireducibilní. Pro spor nechť není, pak existují polynomy $g, h \in \mathbb{Q}[x]$, které nejsou jednotky a splňují $f = gh$. Určitě jsou nenulové, a jelikož je $\mathbb{Q}$ těleso, každý nenulový konstantní polynom je jednotka. Pak musí být $\deg g, \deg h \geq 1$, tedy vzhledem k $\deg f = 2$ dokonce $\deg g = \deg h = 1$. Když si nyní označíme koeficienty, máme $g = ax + b$, $h = cx + d$ a platí

$$x^2 - 2 = (ax + b)(cx + d) = acx^2 + (ad + bc)x + bd.$$

Porovnáním koeficientů tak $ac = 1$. BÚNO můžeme předpokládat $a = c = 1$, neboť jinak bychom namísto g, h prostě uvažovali $\frac{1}{a} \cdot g$, $\frac{1}{c} \cdot h$ a stále by platilo $\frac{g}{a} \cdot \frac{h}{c} = gh \cdot \frac{1}{ac} = f \cdot \frac{1}{1}$. Dále z koeficientů u x musí být $0 = d + b$, takže $b = -d$. Konečně z absolutních členů pak $-2 = bd = -d^2$. To však nemá řešení, protože $\sqrt{2}$ ani $-\sqrt{2}$ nejsou racionální čísla. Polynom f je tak opravdu ireducibilní.

V příkladu jsme postupovali přímo z definice. Místo toho jsme si mohli ušetřit práci tím, že bychom se zajímali o kořeny.

Cvičení(!) 15. Nechť je K těleso a polynom $f \in K[x]$ má stupeň nanejvýš 3. Potom pokud f není ireducibilní, pak má v K kořen.

Cvičení(!) 16. Nad tělesem je každý lineární polynom ireducibilní.

Příklad. (varovný) Máme-li několik v sobě obsažených okruhů, jako například $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, pak jsou v sobě obsaženy i odpovídající okruhy polynomů, tedy $\mathbb{Z}[x] \subset \mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x]$. To, zda je daný polynom ireducibilní, pak může záležet na tom, nad jakým okruhem se na něj díváme.

(i) Polynom $2x + 2$ se nad $\mathbb{Z}$ rozkládá na $2 \cdot (x + 1)$, takže není ireducibilní, protože 2 není nad $\mathbb{Z}$ jednotkou, avšak nad $\mathbb{Q}$ už ano, a $2x + 2$ tak ireducibilní je.

(ii) Polynom $x^2 - 2$ je ireducibilní nad $\mathbb{Q}$, jelikož nemá v $\mathbb{Q}$ kořen, ale nad $\mathbb{R}$ už se rozkládá na $(x + \sqrt{2})(x - \sqrt{2})$.

(iii) Polynom $x^2 + 1$ je ireducibilní nad $\mathbb{R}$, jelikož nemá v $\mathbb{R}$ kořen, ale v komplexních číslech se rozkládá na $(x + i)(x - i)$.

Hovoříme-li tedy o ireducibilitě, musíme specifikovat, nad jakým okruhem ji míníme.

Úloha 7. Jsou dána navzájem různá celá čísla $a_1, a_2, \ldots, a_n$ a polynom

$$f = (x - a_1)(x - a_2) \cdots (x - a_n) - 1.$$

Dokaž, že f je nad $\mathbb{Z}$ ireducibilní.

Úloha 8. Urči, pro která přirozená n lze zvolit n navzájem různých celých čísel $a_1, a_2, \ldots, a_n$ tak, aby polynom

$$f = (x - a_1)(x - a_2) \cdots (x - a_n) + 1$$

nebyl nad $\mathbb{Z}$ ireducibilní.

Obecně není jednoduché dokázat ireducibilitu nějakého daného polynomu. Pokud bychom např. spoléhali na řešení soustavy rovnic v koeficientech jako v příkladu s $x^2 - 2$ nad $\mathbb{Q}$, museli bychom pro polynomy vysokého stupně řešit obří soustavy nelineárních rovnic se spoustou proměnných. Toto by nemělo být příliš překvapivé – v celých číslech je taky výpočetně náročné rozhodnout, zda je nějaké dané číslo prvočíslem.

Nyní si ukážeme, že nad tělesy jsou ireducibilní polynomy automaticky prvočinitelé. Stejně jako dříve v seriálu to provedeme přes eukleidovskost. Připomeňme, že obor nazýváme *eukleidovský*, pokud v něm umíme dělit se zbytkem tak, aby zbytek byl v nějakém smyslu menší než dělitel. Formálněji požadujeme, aby existovala *eukleidovská funkce* d, která prvkům oboru přiřazuje nezáporná celá čísla tak, aby pro libovolná $a, b \in R$, $b \neq 0$, platilo

(i) $d(a) = 0$, právě když $a = 0$,

(ii) $d(a) \leq d(ab)$,

(iii) existují $q, r \in R$ taková, že $a = bq + r$ a zároveň $d(r) < d(b)$.

Z prvního dílu již víme, že eukleidovský obor je nutně i gaussovský, tedy že rozklad na ireducibilní prvky je v něm jednoznačný. Zde si rozmyslíme, že polynomy nad tělesem dovedeme dělit se zbytkem tak, aby zbytek měl menší stupeň než dělitel.

Tvrzení. *Pro libovolné těleso K je $K[x]$ eukleidovský obor.*

Důkaz. Jako eukleidovskou funkci použijeme stupeň, avšak abychom dostáli formální definici eukleidovské funkce, drobně si ho upravíme. Pro $f \in K[x]$ definujme

$$d(f) = \begin{cases} 1 + \deg f, & \text{pokud } f \neq 0, \\ 0, & \text{pokud } f = 0. \end{cases}$$

Ověřme, že toto vyhovuje jako eukleidovská funkce. Pro nenulový polynom f platí $\deg f \geq 0$, takže d nabývá nezáporných celočíselných hodnot a platí $d(f) = 0$, právě když $f = 0$. Dále pro $f, g \in K[x]$, kde $g \neq 0$, platí, že když $f = 0$, tak $d(f) = d(fg) = 0$, zatímco pro $f \neq 0$ máme

$$d(f) = 1 + \deg f \leq 1 + \deg f + \deg g = 1 + \deg(fg) = d(fg),$$

kde využíváme $\deg g \geq 0$. Dohromady tak vždy platí $d(f) \leq d(fg)$.

Tím jsou splněny podmínky (i), (ii) pro eukleidovskou funkci, zbývá tak dokázat, že pro $f, g \in K[x]$, kde $g \neq 0$, dovedeme zvolit polynomy $q, r \in K[x]$ tak, aby bylo $f = gq + r$ a zároveň $d(r) < d(g)$. Označme $n = \deg f$, $m = \deg g$. Budeme postupovat jako při dělení polynomů pod sebe: v jednom kroku vždy od f odečteme vhodný násobek g tak, abychom vyrušili nejvyšší mocninu x, která ještě zbývá, a postupně takto vyrušíme všechny mocniny s exponentem větším nebo rovným m. Pojďme si to rozmyslet podrobněji.

Pokud $n < m$, můžeme prostě zvolit $q = 0$, $r = f$. Nadále tedy předpokládejme $n \geq m$ a mějme

$$f = a_n x^n + \cdots + a_1 x + a_0, \qquad g = b_m x^m + \cdots + b_1 x + b_0.$$

Zvolíme q tak, abychom vyrušili členy $a_n x^n + \cdots + a_m x^m$ v polynomu f. Koeficienty q budeme volit postupně: stanovíme si pro polynom q stupeň $n - m$ a předpis

$$q = c_{n-m} x^{n-m} + \cdots + c_1 x + x_0,$$

kde $c_{n-m}, \ldots, c_1, c_0$ jsou zatím neurčené koeficienty. Postupně je určíme tak, aby $r = f - gq$ byl polynom stupně menšího než m. Využijeme přitom toho, že b_m je nenulový prvek tělesa K, takže už to je jednotka, tedy existuje $\frac{1}{b_m}$.

Nejprve zvolíme c_{n-m} tak, abychom vyrušil člen x^n – jednoduše položíme $c_{n-m} = \frac{a_n}{b_m}$. Tím zařídíme, že polynom

$$\begin{aligned} f - c_{n-m} x^{n-m} \cdot g &= \left(a_n x^n + a_{n-1} x^{n-1} + \cdots\right) - \left(\frac{a_n}{b_m} b_m x^n + \frac{a_n}{b_m} b_{m-1} x^{n-1} + \cdots\right) = \\ &= \left(a_n - \frac{a_n}{b_m} b_m\right) x^n + \left(a_{n-1} - \frac{a_n}{b_m} b_{m-1}\right) x^{n-1} + \cdots \end{aligned}$$

bude mít stupeň nanejvýš $n - 1$, jelikož koeficient u x^n vyjde $a_n - \frac{a_n}{b_m} b_m = a_n - a_n = 0$. Stejný postup ale můžeme opakovat: zvolíme c_{n-m-1} takovým způsobem, aby mezivýsledný polynom

$$f - (c_{n-m} x^{n-m} + c_{n-m-1} x^{n-m-1}) \cdot g$$

postrádal člen s x^{n-1}, tedy aby měl stupeň nanejvýš $n - 2$, atp. Tento proces se nám nemůže „rozbít“, dokud nám zbývají koeficienty ke stanovení, neboť vždy prostě zvolíme

$$c_{n-m-k} = \frac{1}{b_m} \cdot \big(\text{koeficient u } x^{n-k} \text{ v posledním mezivýsledku}\big).$$

V závěrečném kroku pomocí volby c_0 vyrušíme mocninu x^m, takže nakonec dostaneme, že $r = f - q \cdot g$ má stupeň menší než $m = \deg g$, tudíž $d(r) < d(g)$, jak jsme chtěli. □

Důsledek. *$K[x]$ je gaussovský obor, takže každý nenulový polynom nad K má jednoznačný*[6] *rozklad na součin ireducibilních polynomů. Dále pro libovolné nenulové polynomy $f, g \in K[x]$ existuje jejich největší společný dělitel h a také existují Bézoutovy koeficienty*[7] *$u, v \in K[x]$ splňující Bézoutovu identitu $uf + vg = h$.*

[6] Až na změny pořadí a přenásobení jednotkami.

[7] Tento pojem si nepleťme s koeficienty polynomu, což jsou prvky K – pracujeme s okruhem polynomů $K[x]$, takže Bézoutovy koeficienty jsou zde taktéž polynomy.

Příklad. Rozklady polynomů x^2-1 a x^3+x^2+x+1 na ireducibilní polynomy v $\mathbb{Q}[x]$ jsou

$$x^2-1=(x+1)(x-1), \qquad \text{a} \qquad x^3+x^2+x+1=(x+1)(x^2+1).$$

Jejich největší společný dělitel je tak $x+1$, což lze pomocí Bézoutových koeficientů $-\frac{x}{2}-\frac{1}{2}$ a $\frac{1}{2}$ vyjádřit jako $x+1=\left(-\frac{x}{2}-\frac{1}{2}\right)\cdot(x^2-1)+\frac{1}{2}\cdot(x^3+x^2+x+1)$.

Předpoklad, že K je těleso, nemůžeme z tvrzení o eukleidovskosti vypustit – bez něj by totiž b_m nemusela být jednotka, takže bychom neměli zaručeno, že vždy dovedeme vyrušit nejvyšší mocninu x v mezivýsledku.

Příklad. (varovný) $\mathbb{Z}[x]$ není eukleidovský obor. Kdyby byl, pak by v něm musela fungovat Bézoutova identita, tedy by existoval největší společný dělitel každých dvou $f,g\in\mathbb{Z}[x]$, který by navíc musel být vyjádřitelný jako $uf+vg$ pro nějaká $u,v\in\mathbb{Z}[x]$. Jako protipříklad zvolme $f=x$, $g=2$. Dělitelé 2 jsou jenom ±1 a ±2, přitom však $2\nmid x$. Společnými děliteli x a 2 jsou tak pouze ±1, takže 1 je jejich největší společný dělitel. Rovnice $ux+2v=1$ ale nemá řešení – každý polynom $ux+2v$ totiž má sudý absolutní koeficient, což 1 nesplňuje.

Ohledně společných dělitelů polynomů nám něco dovedou říct jejich kořeny. Ukažme si to nad $\mathbb{Q}$: pokud mají polynomy $f,g\in\mathbb{Q}[x]$ nějaký společný kořen $t\in\mathbb{Q}$, pak platí $x-t\mid f$ i $x-t\mid g$, takže $x-t$ je společný dělitel f a g. S pomocí eukleidovskosti si však dovedeme rozmyslet, že nám mohou pomoci i kořeny, které nejsou racionální.

Tvrzení. *Mějme polynomy $f,g\in\mathbb{Q}[x]$ takové, že nějaké $t\in\mathbb{C}$ je kořenem obou z nich. Potom jsou f, g v $\mathbb{Q}[x]$ soudělné*[8].

Důkaz. Pro spor nechť jsou f, g nesoudělné. Potom máme pro nějaká $u,v\in\mathbb{Q}[x]$ Bézoutovu identitu $uf+vg=1$. Dosazením t se však z této rovnosti stane

$$1=u(t)\cdot f(t)+v(t)\cdot g(t)=u(t)\cdot 0+v(t)\cdot 0=0,$$

což je spor. Určitě tedy musí f, g být soudělné. □

Důsledek. (kořeny chodí spolu) *Pokud je $f\in\mathbb{Q}[x]$ ireducibilní a sdílí nějaký komplexní kořen s $g\in\mathbb{Q}[x]$, pak už v okruhu $\mathbb{Q}[x]$ platí $f\mid g$. Speciálně je pak už každý (komplexní) kořen f taktéž kořenem g.*

Důkaz. Polynom f je ireducibilní, takže jeho děliteli jsou (až na přenásobení jednotkou) jen 1 a f. Z tvrzení nesmí být 1 největším společným dělitelem f a g, takže už jím musí být f, z čehož $f\mid g$. □

Gaussovo lemma

Podívejme se nyní blíže na okruh celočíselných polynomů $\mathbb{Z}[x]$. Ten sice není eukleidovský, ale ukážeme si, že je stále gaussovský. Uvidíme, že z hlediska rozkládání se na součin menších polynomů není příliš velký rozdíl v tom, jestli se na celočíselný polynom díváme v $\mathbb{Z}[x]$ nebo v $\mathbb{Q}[x]$. V $\mathbb{Q}[x]$ už máme jednoznačný rozklad na ireducibilní polynomy, který posléze přeneseme do $\mathbb{Z}[x]$. Abychom toho docílili, budeme se muset vypořádat s prvočíselnými konstantními polynomy, jelikož prvočíslo $p\in\mathbb{Z}$ je (konstantní) ireducibilní polynom v $\mathbb{Z}[x]$, ale v $\mathbb{Q}[x]$ se z něj stává jednotka.

Definice. Celočíselný polynom f nazýváme *primitivní*, pokud jej nedělí žádné přirozené číslo $d>1$.

Poznámka. Pokud $f=a_nx^n+\cdots+a_0\in\mathbb{Z}[x]$, pak je f primitivní právě tehdy, když jsou čísla $a_n,\ldots,a_1,a_0$ nesoudělná. Tím míníme, že celá $(n+1)$-tice nemá jiného společného dělitele než ±1, ačkoliv některé dvojice koeficientů spolu soudělné být mohou.

[8] Připomeňme, že prvky a, b okruhu R nazýváme *soudělné*, pokud mají společného dělitele, který není jednotka.

Příklad. Polynom $x^3 + 2x^2 + 3x + 4$ je primitivní, zatímco $2x^2 + 8x + 14$ není, jelikož všechny koeficienty jsou sudé. Polynom $6x^2+10x+15$ je zase primitivní – ačkoliv je každá dvojice koeficientů soudělná, všechny tři dohromady už jsou nesoudělné.

Když zkoumáme ireducibilitu polynomu, zajímá nás, jestli se dá rozložit na součin menších polynomů. V $\mathbb{Z}[x]$ však můžeme narazit na docela nezajímavé rozklady jako

$$2x + 2 = 2 \cdot (x + 1),$$

kde jenom vytkneme jedno celé číslo ze všech koeficientů. Následně takovýto polynom není ireducibilní v $\mathbb{Z}[x]$, ale v $\mathbb{Q}[x]$ najednou může být ireducibilní – vytknuté celé číslo 2 se v $\mathbb{Q}[x]$ stává jednotkou, takže rozklad jako $2 \cdot (x + 1)$ už není v rozporu s ireducibilitou. Primitivní polynomy jsou přesně ty, které tyto nezajímavé rozklady neumožňují.

Cvičení(!) 17. Když v $\mathbb{Z}[x]$ máme $f = gh$ a f je primitivní, pak jsou i oba polynomy g, h primitivní.

Cvičení(!) 18. Mějme polynom $f \in \mathbb{Q}[x]$. Pak existuje primitivní $g \in \mathbb{Z}[x]$ a racionální číslo k takové, že $f = k \cdot g$. Tento zápis je navíc jednoznačný až na přenásobení jednotkou.

Cvičení 19. Nekonstantní ireducibilní polynom nad $\mathbb{Z}$ musí být primitivní.

Nyní už si dovedeme rozmyslet *Gaussovo lemma* – několik tvrzení o vztahu rozkladů nad $\mathbb{Z}$ a $\mathbb{Q}$. První hovoří o prvočíslech, další o primitivních polynomech a poslední dává do souvislosti ireducibilitu nad $\mathbb{Z}$ a nad $\mathbb{Q}$. Ačkoliv to tak na první pohled nemusí vypadat, říkají jednotlivé verze vesměs totéž, jen každá v jiné formulaci, a proto se název *Gaussovo lemma* používá pro všechny tři.

Ačkoliv cílíme na souvislost $\mathbb{Z}[x]$ s $\mathbb{Q}[x]$, začneme souvislostí s okruhy $\mathbb{Z}_p[x]$.

Pozorování. (modulení konstantou) Mějme celočíselný polynom $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. Máme-li dáno celé číslo m, můžeme se na koeficienty podívat modulo m a získat tím polynom

$$\hat{f} = (a_n \bmod m)x^n + \cdots + (a_0 \bmod m) \in \mathbb{Z}_m[x].$$

Sčítání polynomů odpovídá sčítání jednotlivých dvojic koeficientů, zatímco při násobení polynomů budou koeficienty výsledku rovny nějakému součtu součinů původních koeficientů. Modulení však zachovává sčítání i násobení celých čísel, takže v důsledku se tyto operace zachovají i na polynomech neboli pro $f, g \in \mathbb{Z}[x]$ dostaneme

$$\widehat{(f + g)} = \hat{f} + \hat{g}, \qquad \widehat{(f \cdot g)} = \hat{f} \cdot \hat{g}.$$

Pozor, sčítání, resp. násobení $\hat{f}$ a $\hat{g}$ zde už myslíme v okruhu $\mathbb{Z}_m[x]$, protože v tomhle okruhu tyto polynomy bydlí. Také si všimněme, že modulením se může stupeň snížit (pokud se některé koeficienty vysokých mocnin x vynulují), ale nemůže se zvýšit, tedy $\deg \hat{f} \leq \deg f$.

Lemma. (Gaussovo – verze o prvočíslech) *Každé prvočíslo $p \in \mathbb{Z}$ je prvočinitelem v $\mathbb{Z}[x]$.*

Důkaz. Dokažme podle definice prvočinitele: mějme polynomy $f, g \in \mathbb{Z}[x]$ tak, že $p \mid fg$, a dokažme, že $p \mid f$ nebo $p \mid g$. Označme $h = fg$ a podívejme se podle předchozího pozorování na celou věc modulo p. Máme $p \mid h$, takže zmodulený polynom $\hat{h}$ bude prostě 0. Tím dostáváme rovnost $0 = \hat{h} = \hat{f} \cdot \hat{g}$ (v okruhu $\mathbb{Z}_p[x]$, nikoliv už v $\mathbb{Z}[x]$).

Z prvočíselnosti p je $\mathbb{Z}_p$ obor integrity, takže i $\mathbb{Z}_p[x]$ je obor integrity. Tím pádem z $0 = \hat{f} \cdot \hat{g}$ plyne, že jeden z $\hat{f}$, $\hat{g}$ musí být 0. BÚNO nechť $\hat{f} = 0$. To značí, že zmodulením f se všechny koeficienty f vynulovaly, takže se muselo jednat o samé násobky p neboli $p \mid f$, jak jsme chtěli. □

Lemma. (Gaussovo – verze o primitivnosti) *Nechť jsou $f, g \in \mathbb{Z}[x]$ primitivní polynomy. Potom je také $f \cdot g$ primitivní.*

Důkaz. Pro spor nechť fg není primitivní. Pak je fg násobkem nějakého přirozeného čísla $n > 1$. Potom můžeme vzít nějaké prvočíslo $p \mid n$ a stále budeme mít $p \mid fg$. Jenže podle verze o prvočíslech je p prvočinitel v $\mathbb{Z}[x]$, takže z $p \mid fg$ plyne $p \mid f$ nebo $p \mid g$, což je spor s primitivností těchto polynomů. □

Lemma. (Gaussovo – verze o ireducibilitě) *Nechť je $f \in \mathbb{Z}[x]$ primitivní. Potom je f ireducibilní v $\mathbb{Z}[x]$, právě pokud je ireducibilní v $\mathbb{Q}[x]$.*

Důkaz. Dokážeme ekvivalentně, že f *není* ireducibilní v $\mathbb{Z}[x]$, právě když *není* ireducibilní v $\mathbb{Q}[x]$. Nechť se nejprve rozkládá $f = gh$ pro polynomy $g, h \in \mathbb{Z}[x]$, které nejsou jednotky. Máme f primitivní, takže g ani h nemohou být konstantní – kdyby třeba g bylo konstantní, pak to nemůže být ± 1 (to jsou jednotky), takže by f mělo přirozeného dělitele většího než 1. Oba polynomy g, h jsou tedy nekonstantní, což znamená, že nejsou jednotkami v $\mathbb{Q}[x]$. Vzhledem k $\mathbb{Z}[x] \subset \mathbb{Q}[x]$ tak rozklad $f = gh$ dokládá, že ani v $\mathbb{Q}[x]$ není f ireducibilní.

Nyní dokažme opačnou implikaci. Nechť $f = gh$ pro nekonstantní polynomy $g, h \in \mathbb{Q}[x]$ a dokažme, že ani v $\mathbb{Z}[x]$ není f ireducibilní. Podle dřívějšího cvičení můžeme k polynomům g, h zvolit racionální čísla $\frac{a_1}{b_1}$, $\frac{a_2}{b_2}$ tak, že $g_1 = \frac{a_1}{b_1} \cdot g$ i $h_1 = \frac{a_2}{b_2} \cdot h$ jsou primitivní celočíselné polynomy. Pak máme

$$g_1 h_1 = \frac{a_1}{b_1} g \cdot \frac{a_2}{b_2} h = \frac{a_1 a_2}{b_1 b_2} \cdot gh = \frac{a_1 a_2}{b_1 b_2} \cdot f,$$
$$B g_1 h_1 = A f,$$

kde jsme označili $A = a_1 a_2$, $B = b_1 b_2$. Nyní máme rovnost v $\mathbb{Z}[x]$, kde jsou f, g_1 i h_1 primitivní polynomy, ale naproti tomu nám přibyly konstanty A, B. Těch se však dovedeme zbavit. Uvažujme prvočíslo $p \mid A$. To dělí pravou stranu rovnosti, takže dělí i levou. Podle verze o prvočíslech je p prvočinitel, takže dělí některý činitel na levé straně. Ale g_1, h_1 jsou primitivní, takže je p dělit nemůže. Platí proto $p \mid B$, takže toto prvočíslo můžeme z A a B zkrátit. Obdobně když prvočíslo $q \mid B$, pak i $q \mid Af$, ale nemůže být $q \mid f$, takže $q \mid A$.

Toto můžeme opakovat a postupně takto vykrátit všechna prvočísla z A, B. Celkově se tedy A a B liší jen o jednotku, tedy $A = \pm B$. Zůstane nám tak rovnost $f = \pm g_1 h_1$, v níž máme celočíselné polynomy. Z předpokladu jsou g_1 i h_1 nekonstantní, takže to určitě nejsou jednotky v $\mathbb{Z}[x]$, čímž je dokázáno, že f není ireducibilní v $\mathbb{Z}[x]$. □

Cvičení(!) 20. Mějme $f, g \in \mathbb{Z}[x]$ a nechť je f primitivní. Potom když $f \mid g$ v okruhu $\mathbb{Q}[x]$, pak $f \mid g$ i v $\mathbb{Z}[x]$.

Důsledek. *$\mathbb{Z}[x]$ je gaussovský obor.*

Důkaz. Vezměme polynom $f \in \mathbb{Z}[x]$, nalezněme jeho rozklad na ireducibilní polynomy a ukažme, že je tento rozklad jednoznačný (až na pořadí a přenásobení jednotkami). Vytkněme nejprve z f největší celé číslo t, které jej dělí, takže mějme $f = c \cdot g$ pro $c \in \mathbb{Z}$ a primitivní $g \in \mathbb{Z}[x]$. Tento rozklad na $c \cdot g$ je (až na přenásobení ± 1) jednoznačný, protože c je prostě největší společný dělitel koeficientů f. V celých číslech pak rozložíme c na součin prvočísel $p_1 \cdots p_k$, což je jednoznačné.

Zbývá se tedy postarat o primitivní polynom g. Na něj se můžeme dívat jako na prvek $\mathbb{Q}[x]$, což je eukleidovský, a tedy i gaussovský obor, takže máme jednoznačný rozklad

$$g = g_1 \cdots g_\ell$$

na ireducibilní polynomy $g_1, \ldots, g_\ell \in \mathbb{Q}[x]$. Každý racionální polynom g_i však můžeme zapsat jako $\frac{a_i}{b_i} \cdot f_i$, kde $\frac{a_i}{b_i}$ je nějaký zlomek a f_i je primitivní celočíselný polynom. Přitom se ale f_i liší od g_i jen přenásobením konstantou, což je v $\mathbb{Q}[x]$ jednotka, takže když je g_i ireducibilní nad $\mathbb{Q}$, je i f_i ireducibilní nad $\mathbb{Q}$. Spolu s primitivností to podle Gaussova lemmatu ve verzi o ireducibilitě znamená, že f_i je ireducibilní nad $\mathbb{Z}$. Tím máme rozklad

$$g = \frac{a_1 \cdots a_\ell}{b_1 \cdots b_\ell} \cdot f_1 \cdots f_\ell,$$
$$(b_1 \cdots b_\ell) \cdot g = (a_1 \cdots a_\ell) \cdot f_1 \cdots f_\ell.$$

Toto je rovnost v $\mathbb{Z}[x]$ a polynomy g i $f_1, \ldots, f_\ell$ jsou primitivní, takže stejně jako v důkazu verze o ireducibilitě už musí být $b_1 \cdots b_\ell = \pm a_1 \cdots a_\ell$. BÚNO je znaménko $\pm$ v této rovnosti $+$, takže máme rozklad $g = f_1 \cdots f_\ell$ na ireducibilní polynomy nad $\mathbb{Z}$.

Nahlédněme, že tento rozklad je jednoznačný. Mějme dva rozklady $g = f_1 \cdots f_\ell = h_1 \cdots h_m$ na ireducibilní (primitivní) celočíselné polynomy. Z primitivnosti jsou všechny zúčastněné polynomy ireducibilní i nad $\mathbb{Q}$, takže zde máme dva rozklady g na ireducibilní polynomy v $\mathbb{Q}[x]$. Zde je ale rozklad jednoznačný, takže $f_1 \cdots f_\ell$ a $h_1 \cdots h_m$ se musí lišit jen pořadím činitelů a přenásobením jednotkami nad $\mathbb{Q}$, tedy konstantami. Aby se však zachovala celočíselnost a primitivnost polynomů, musí se jednat jen o přenásobení plus nebo minus jedničkou. Jedná se tedy jen o změnu pořadí a přenásobení jednotkami nad $\mathbb{Z}$, což znamená, že rozklad g na ireducibilní polynomy nad $\mathbb{Z}$ je jednoznačný.

Tím je dohromady pro původní f jednoznačně určen rozklad $f = p_1 \cdots p_k \cdot f_1 \cdots f_\ell$. □

Poznámka. Z předchozího důkazu plyne, že ireducibilní prvky, resp. prvočinitelé v $\mathbb{Z}[x]$ jsou následujících dvou druhů:

(i) prvočísla $p \in \mathbb{Z}$,

(ii) primitivní polynomy $f \in \mathbb{Z}[x]$, které jsou ireducibilní nad $\mathbb{Q}$.

Příklad. Rozložme polynom $f = 12x^6 - 60x^4 - 12x^2 + 60$ nad $\mathbb{Z}$ na ireducibilní polynomy. Nejprve můžeme ze všech koeficientů vytknout $12 = 2 \cdot 2 \cdot 3$. Následně si všimneme, že 1 i -1 jsou kořeny, takže dovedeme vytknout $(x-1)(x+1)$. Po vytknutí zbude polynom $x^4 - 4x^2 - 5$. Zde můžeme buďto hned uhodnout rozklad, anebo si všimneme, že máme jen sudé mocniny x, takže rozložíme polynom s poloviční exponenty $x^2 - 4x - 5$ díky zjevnému kořenu -1 na $(x+1)(x-5)$, což zpětným přepsáním na dvojnásobné exponenty dá rozklad $x^4 - 4x^2 - 5 = (x^2+1)(x^2-5)$. Dostaneme tak rozklad

$$f = 2 \cdot 2 \cdot 3 \cdot (x-1) \cdot (x+1) \cdot (x^2+1) \cdot (x^2-5).$$

Poslední dva kvadratické polynomy nemají racionální kořeny, takže jsou ireducibilní nad $\mathbb{Q}$, a díky své primitivnosti jsou tak ireducibilní i nad $\mathbb{Z}$.

Závěrem povídání o Gaussově lemmatu uveďme bez důkazu, že Gaussovo lemma lze formulovat obecněji pro libovolný gaussovský obor R namísto $\mathbb{Z}$. Můžeš si zkusit rozmyslet, že když všude místo $\mathbb{Z}$ napíšeme gaussovský obor R (a „prvočinitel v R“ místo „prvočíslo“), všechny důkazy stále fungují. Z toho pak plyne následující:

Tvrzení. *Je-li R gaussovský obor, pak už je gaussovský i $R[x]$.*

Neformálně řečeno: když funguje rozklad na „prvočísla“ v R, pak už funguje i rozklad na ireducibilní polynomy v $R[x]$. V důkazu tohoto tvrzení bychom opět postupovali takřka stejně jako v $\mathbb{Z}$, jenom bychom si museli zadefinovat „zlomky“, v nichž jsou čitatel a jmenovatel prvky obecného oboru integrity R. Tím bychom dostali jeho *podílové těleso* K, díky němuž bychom si mohli jednoznačný rozklad na ireducibilní polynomy v $K[x]$ půjčit a poupravit do $R[x]$, což je přesně to, co jsme dělali s $R = \mathbb{Z}$ a $K = \mathbb{Q}$.

Eisensteinovo kritérium

Gaussovo lemma nám dává jednoduchý vztah mezi ireducibilitou nad $\mathbb{Q}$ a nad $\mathbb{Z}$, ale stále nemáme žádný snadný způsob, jak ireducibilní polynomy rozeznat. K tomuto účelu existuje mnoho kritérií, která jsou postačujícími (ale ne nutnými) podmínkami ireducibility. My si zde ukážeme jedno z nich.

Tvrzení. (Eisensteinovo kritérium) *Mějme primitivní polynom $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. Pokud nějaké prvočíslo p splňuje*

(i) $p \mid a_i$ *pro* $0 \le i \le n-1$, (ii) $p \nmid a_n$, (iii) $p^2 \nmid a_0$,

pak je f ireducibilní nad $\mathbb{Z}$.

Důkaz. Pro spor nechť lze rozložit $f = gh$ pro $g, h \in \mathbb{Z}[x]$, které nejsou jednotkami. Díky primitivnosti f nemohou g ani h být konstantní. Na situaci se podíváme modulo p a následně využijeme jednoznačného rozkladu na ireducibilní polynomy v $\mathbb{Z}_p[x]$. Tím zjistíme, že absolutní koeficienty polynomů g i h jsou násobky p, což dá spor s předpokladem (iii).

Zmodulený polynom $\hat{f} \in \mathbb{Z}_p[x]$ bude mít podle předpokladu (i) všechny koeficienty kromě a_n nulové, takže zbude $\hat{f} = a_n x^n$. Z předpokladu (ii) je a_n nenulové v $\mathbb{Z}_p$, takže $\deg \hat{f} = n$. Spolu se zmodulenými $\hat{g}, \hat{h} \in \mathbb{Z}_p[x]$ pak máme v okruhu $\mathbb{Z}_p[x]$ rovnost

$$a_n x^n = \hat{f} = \hat{g} \cdot \hat{h}.$$

Rozmysleme si, že $\hat{g}$ musí mít tvar $\hat{g} = bx^k$ pro $b \not\equiv 0$. Jelikož je $\mathbb{Z}_p$ těleso, funguje v $\mathbb{Z}_p[x]$ jednoznačný rozklad na ireducibilní polynomy. Ale lineární polynom x je určitě ireducibilní, takže máme rozklad

$$\hat{f} = a_n x^n = a_n \cdot \underbrace{x \cdots x}_{n\text{-krát}},$$

kde a_n je jednotka. Jinými slovy má $\hat{f}$ ve svém rozkladu jen jediný ireducibilní polynom x, ale zato jej má hned n-krát. Polynom $\hat{g}$ potom nemůže mít ve svém rozkladu jiné ireducibilní polynomy než x, takže $\hat{g} = bx^k$ pro nějaké k a $b \in \mathbb{Z}_p$. Nemůže přitom být $b = 0$, jelikož $\hat{f} \neq 0$. Z tohoto vyvodíme, že $\hat{g}$ má nulový absolutní člen, avšak k tomu si potřebujeme rozmyslet, jaký má stupeň.

Máme tedy $\hat{g} = bx^k$, obdobně pak i $\hat{h} = cx^\ell$ pro nenulové $c \in \mathbb{Z}_p$. Nahlédněme, že $k = \deg g$ a $\ell = \deg h$, tedy že se nám modulením nezmenšili stupně. Platí $k \leq \deg g$, $\ell \leq \deg h$ a zároveň

$$k + \ell = n = \deg f = \deg g + \deg h.$$

Kdyby $k < \deg g$ nebo $\ell < \deg h$, pak už by předchozí rovnost nemohla platit, takže určitě $k = \deg g$, $\ell = \deg h$. Víme, že g i h jsou nekonstantní, takže $k, \ell \geq 1$. Z toho plyne, že $\hat{g}$ i $\hat{h}$ mají nulové absolutní členy, takže absolutní člen $b_0 \in \mathbb{Z}$ polynomu g i absolutní člen $c_0 \in \mathbb{Z}$ polynomu h musely být násobky p. Z rozkladu $f = gh$ pak máme $a_0 = b_0 c_0$, což značí $p^2 \mid a_0$. To je spor s předpokladem (iii), žádný popsaný rozklad $f = gh$ tedy nemůže existovat, pročež je f ireducibilní. □

Cvičení 21. Pro prvočíslo p a přirozené n je polynom $x^n + p$ ireducibilní nad $\mathbb{Z}$.

Pozorování. (posunutí argumentu) Je-li $c \in \mathbb{Z}$, pak je f ireducibilní, právě když je ireducibilní $\tilde{f} = f(x + c)$. Když se rozkládá $f = gh$, pak i $\tilde{f} = g(x + c) \cdot h(x + c)$, a obdobně když $\tilde{f} = \tilde{g} \cdot \tilde{h}$, pak i $f = \tilde{f}(x - c) = \tilde{g}(x - c) \cdot \tilde{h}(x - c)$. Při zkoumáni ireducibility polynomu si tedy můžeme libovolně „posunout argument“ a nic se nezmění.

Příklad. Ukažme, že $f = x^4 + x^3 + x^2 + x + 1$ je ireducibilní nad $\mathbb{Z}$. Posunutím argumentu můžeme namísto f zkoumat

$$\begin{aligned} f(x+1) &= (x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1 = \\ &= \big(x^4 + 4x^3 + 6x^2 + 4x + 1\big) + \big(x^3 + 3x^2 + 3x + 1\big) + \big(x^2 + 2x + 1\big) + (x+1) + 1 = \\ &= x^4 + 5x^3 + 10x^2 + 10x + 5, \end{aligned}$$

což je ireducibilní polynom skrze Eisensteinovo kritérium s $p = 5$.

Úloha 9. Pro prvočíslo $p \in \mathbb{N}$ je polynom $f = x^{p-1} + x^{p-2} + \cdots + x + 1$ je ireducibilní nad $\mathbb{Z}$.

Když spojíme Eisensteinovo kritérium s Gaussovým lemmatem, dostaneme informaci o ireducibilitě nad $\mathbb{Q}$. V této verzi budeme moci vypustit předpoklad o primitivnosti: pokud f není primitivní, můžeme vytknout $f = d \cdot f_1$ pro nějaké primitivní f_1, a přenásobení konstantou d, což je nad $\mathbb{Q}$ jednotka, na ireducibilitě nic nezmění.

Drobnou úpravou důkazu lze také získat zobecnění Eisensteinova kritéria, které zaručuje vysoký stupeň nějakého činitele v rozkladu na ireducibilní polynomy.

Tvrzení. (Eisensteinovo kritérium nad $\mathbb{Q}$) *Mějme polynom $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ stupně n. Pokud nějaké prvočíslo p splňuje*

(i) $p \mid a_i$ *pro* $0 \le i \le n-1$, (ii) $p \nmid a_n$, (iii) $p^2 \nmid a_0$,

pak je f ireducibilní nad $\mathbb{Q}$.

Cvičení(*) 22. (rozšířený Eisenstein) Mějme polynom $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ stupně n. Pokud pro nějaké prvočíslo p a přirozené k platí

(i) $p \mid a_i$ pro $0 \le i \le k-1$, (ii) $p \nmid a_k$, (iii) $p^2 \nmid a_0$,

pak je f násobkem nějakého ireducibilního polynomu stupně alespoň k.

Úloha 10. Dokaž, že pro každé přirozené číslo n je polynom $x^{n+1} + 5x^n + 3$ ireducibilní nad $\mathbb{Z}$.

Modulení polynomů

K důkazům Gaussova lemmatu a Eisensteinova kritéria se nám hodilo zmodulit celočíselný polynom f nějakým prvočíslem p, čímž jsme dostali polynom $\hat{f} \in \mathbb{Z}_p[x]$. Co když nás ale zajímá modulení nějakým nekonstantním polynomem? Pro jednoduchost budeme jako modulo uvažovat jen *monické* polynomy, tedy takové, které mají u nejvyšší mocniny x koeficient 1.

Příklad. Zkusme se nad $\mathbb{Z}$ podívat na $f = x^3 + 2x^2 + x + 1$ modulo $x - 1$. Upravíme f postupným odečítáním násobků $x - 1$ tak, abychom dostali polynom s co nejmenším stupněm. Podobně jako v důkazu eukleidovskosti $K[x]$ postupně dostaneme

$$\begin{aligned} f - x^2 \cdot (x-1) &= \big(x^3 + 2x^2 + x + 1\big) - \big(x^3 - x^2\big) = 3x^2 + x + 1, \\ f - \big(x^2 + 3x\big)(x-1) &= \big(3x^2 + x + 1\big) - \big(3x^2 - 3x\big) = 4x + 1, \\ f - \big(x^2 + 3x + 4\big)(x-1) &= 4x + 1 - (4x - 4) = 5. \end{aligned}$$

Dohromady tak $f \equiv 5 \pmod{x-1}$. Samozřejmě bychom při počítání mod $x - 1$ mohli používat i $f \equiv 4x + 1$ nebo $f \equiv 5x$ nebo jakýkoliv jiný polynom tvaru $f + g \cdot (x-1)$ pro $g \in \mathbb{Z}[x]$, ale nahrazení f za konstantní polynom 5 pravděpodobně povede k nejsnazšímu počítání.

Všimněme si, že v předchozím příkladu máme $f \equiv 5 = f(1)$. To není náhodou: když se na okruh $R[x]$ podíváme modulo $x - a$ pro nějaké $a \in R$, znamená to, že jsme dosud naprosto neurčité proměnné x nařídili vlastnost $x - a \equiv 0$ neboli $x \equiv a$. To povede k $f(x) \equiv f(a)$ pro každé $f \in R[x]$. Formálněji:

Tvrzení. *Pro $f \in R[x]$ a $a \in R$ platí $f \equiv f(a) \pmod{x-a}$.*

Důkaz. Rozdíl argumentů dělí rozdíl hodnot, takže $x - a \mid f(x) - f(a)$, tedy $f(x) - f(a) \equiv 0 \pmod{x-a}$, což přesně chceme. □

Z tohoto plyne, že všechny zbytkové třídy polynomů mod $x - a$ (prvky okruhu $R[x]/(x-a)$) můžeme reprezentovat nějakým prvkem původního okruhu R. Pokud pracujeme nad oborem integrity, pak už je toto vyjádření dokonce jednoznačné – kdyby jeden polynom f byl kongruentní dvěma různým $b_1, b_2 \in R$, pak už by nenulová konstanta $b_1 - b_2$ byla násobkem lineárního polynomu $x - a$, což není možné. V jistém smyslu se tedy okruh $R[x]/(x-a)$ „chová úplně stejně“ jako R. Pro úplnost uveďme trochu formálněji, co přesně myslíme tím, že se okruhy chovají úplně stejně.

Definice. Řekněme, že okruhy R a S jsou *izomorfní*, pokud lze jejich prvky navzájem popárovat[9] zobrazením $\varphi\colon R \to S$ splňujícím

$$\varphi(a + b) = \varphi(a) + \varphi(b), \qquad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

[9]Požadujeme tedy *bijekci*: každému prvku R musí odpovídat právě jeden prvek S a naopak.

pro libovolná $a, b \in R$. Takové zobrazení φ pak nazýváme *izomorfismus* a skutečnost, že R a S jsou izomorfní, značíme $R \simeq S$.

Jinými slovy: okruhy jsou izomorfní, pokud se liší jenom nějakým přejmenováním svých prvků a jinak je jejich vnitřní struktura úplně stejná, tzn. toto přejmenování zachovává sčítání i násobení. Například pro $R[x]/(x-a) \simeq R$ je izomorfismem přiřazení $\varphi(f) = f(a)$. Snadno si pak lze rozmyslet, že dosazení jednoho pevně zvoleného prvku se chová hezky ke sčítání i násobení polynomů.

Izomorfní okruhy jsou z hlediska okruhových vlastností (cokoliv, co hovoří jen o pojmech odvozených ze sčítání a násobení) opravdu naprosto totožné. Slibujeme, že na pochopení seriálu bohatě stačí jen intuitivní představa, že izomorfní okruhy jsou stejné až na přejmenování prvků.

Ukázali jsme si, jak modulit lineárním polynomem. Co však polynomy vyšších stupňů? Ukážeme si, že modulení *ireducibilním* polynomem je jako přidání jeho kořenu.

Příklad. Podívejme se na $\mathbb{Z}[x]$ modulo x^2+1. To odpovídá tomu, že proměnné x přiřkneme vlastnost $x^2+1 \equiv 0$ neboli $x^2 \equiv -1$, což je stejný vztah, jaký splňuje komplexní číslo i, které je kořenem x^2+1. Libovolný polynom $f \in \mathbb{Z}[x]$ můžeme modulo x^2+1 zjednodušit tak, že každou mocninu x^k pro $k \geq 2$ přepíšeme na $x^k \equiv -x^{k-2}$. Dokud je exponent větší než 1, můžeme toto opakovat a postupně dostat

$$x^k \equiv -x^{k-2} \equiv x^{k-4} \equiv -x^{k-6} \equiv \cdots,$$

takže každou mocninu x^k nakonec upravíme na $\pm x$ nebo ± 1. Každý prvek $\mathbb{Z}[x]/(x^2+1)$ tak dovedeme zapsat jako $ax+b$, kde $a, b \in \mathbb{Z}$ a x je prvek splňující $x^2 \equiv -1$. Tento zápis je navíc jednoznačný, protože kdyby jeden polynom $f \in \mathbb{Z}[x]$ byl kongruentní dvěma různým a_1x+b_1, a_2x+b_2, pak už by kvadratický polynom x^2+1 dělil nenulový polynom $(a_1x+b_1)-(a_2x+b_2)$, který má stupeň nanejvýš 1.

To vše nápadně připomíná Gaussova celá čísla $\mathbb{Z}[i]$. Všechno, co jsme řekli o $\mathbb{Z}[x]/(x^2+1)$, zůstane v platnosti pro $\mathbb{Z}[i]$, pokud jen budeme místo x psát i: každý prvek $\mathbb{Z}[i]$ také dovedeme zapsat jako $ai+b$, kde $a, b \in \mathbb{Z}$ a rovněž i je prvek splňující $i^2 = -1$. Dostaneme tedy párování zbytkových tříd $ax+b \bmod x^2+1$ s čísly $ai+b$.

Tím jsme nahlédli $\mathbb{Z}[x]/(x^2+1) \simeq \mathbb{Z}[i]$. Všimněme si, že polynomu $f \equiv ax+b$ odpovídá číslo $ai+b$, což je přesně jeho hodnota $f(i)$ v komplexním bodě i.

Příklad. Nahlédněme, že $\mathbb{Z}[x]$ modulo x^3-2 se chová stejně jako okruh

$$\mathbb{Z}[\sqrt[3]{2}] = \left\{ a\left(\sqrt[3]{2}\right)^2 + b\sqrt[3]{2} + c : a, b, c \in \mathbb{Z} \right\}.$$

K tomu si rozmyslíme, že $f \equiv g \pmod{x^3-2}$, právě když $f(\sqrt[3]{2}) = g(\sqrt[3]{2})$. Izomorfismem následně bude párování, které zbytkové třídě $f \bmod x^3-2$ přiřadí číslo $f(\sqrt[3]{2})$. V jednom směru: pokud $f \equiv g$, pak máme $f = g + h \cdot (x^3-2)$ pro nějaký polynom h, takže

$$f(\sqrt[3]{2}) = g(\sqrt[3]{2}) + h(\sqrt[3]{2}) \cdot \left(\left(\sqrt[3]{2}\right)^3 - 2\right) = g(\sqrt[3]{2}) + h(\sqrt[3]{2}) \cdot 0 = g(\sqrt[3]{2}).$$

V druhém směru: když $f(\sqrt[3]{2}) = g(\sqrt[3]{2})$, pak už je $\sqrt[3]{2}$ kořenem polynomu $f-g \in \mathbb{Q}[x]$. Polynom x^3-2 je ireducibilní (třeba Eisensteinovým kritériem) nad $\mathbb{Z}$, a proto i nad $\mathbb{Q}$ a sdílí kořen $\sqrt[3]{2}$ s polynomem $f-g$. Podle důsledku „kořeny chodí spolu“ už tedy musí dělitelnost $x^3-2 \mid f-g$ platit v okruhu $\mathbb{Q}[x]$, a tedy Gaussovým lemmatem i v $\mathbb{Z}[x]$, což přesně znamená $f \equiv g \pmod{x^3-2}$.

Úloha 11. Najdi všechna celá čísla k, pro něž existují celá čísla a, b taková, že polynomy $f = x^5 - kx - 1$ a $g = x^2 - ax - b$ mají společný komplexní kořen.

Argumentace, kterou jsme v příkladu použili pro ireducibilní polynom x^3-2 a okruh $\mathbb{Z}[\sqrt[3]{2}]$, platí obecně, čímž dostáváme:

Tvrzení. *Nechť je* $f = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \in \mathbb{Z}[x]$ *monický ireducibilní polynom s kořenem* $\alpha \in \mathbb{C}$. *Potom*

$$\mathbb{Z}[x]/(f) \simeq \mathbb{Z}[\alpha] = \left\{b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 : b_{n-1}, \ldots, b_1, b_0 \in \mathbb{Z}\right\},$$

přičemž polynomu g *odpovídá jeho hodnota* $g(\alpha)$.

Ještě si ukažme využití modulení polynomů nad konečnými tělesy $\mathbb{Z}_p$. Pomocí něho totiž dovedeme snáze konstruovat konečná tělesa libovolné velikosti. Pokud budeme chtít konečné těleso s p^n prvky, kde p je prvočíslo, stačí najít ireducibilní polynom stupně n nad $\mathbb{Z}_p$.

Tvrzení. *Nechť je* $f \in \mathbb{Z}_p[x]$ *ireducibilní polynom* a $\deg f = n$. *Potom je* $\mathbb{Z}_p[x]/(f)$ *konečné těleso s* p^n *prvky.*

Důkaz. Nechť $f = c_nx^n + \cdots + c_0$. BÚNO můžeme uvažovat $c_n = 1$, protože bychom kdykoliv mohli f přenásobit konstantou c_n^{-1} a nic by se nezměnilo. Když nějaký polynom zmodulíme f, pak dovedeme všechny mocniny x^k přepsat na polynom menšího stupně pomocí vztahu

$$x^n \equiv -\left(c_{n-1}x^{n-1} + \cdots + c_0\right).$$

Všechny prvky $\mathbb{Z}_p[x]/(f)$ tak dovedeme reprezentovat jako $a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ pro nějaká $a_{n-1}, \ldots, a_0 \in \mathbb{Z}_p$. Naopak jsou všechny tyto polynom navzájem nekongruentní – libovolný jejich rozdíl má stupeň nanejvýš $n-1$, takže nemůže být násobkem f. Prvků $\mathbb{Z}_p[x]/(f)$ je tak přesně p^n, protože každý z n koeficientů volíme z p prvků tělesa $\mathbb{Z}_p$. Z toho speciálně plyne, že okruh $\mathbb{Z}_p[x]/(f)$ je konečný. Z eukleidovskosti $\mathbb{Z}_p[x]$ je ireducibilní f také prvočinitel, takže $\mathbb{Z}_p[x]/(f)$ je obor integrity. Konečný obor integrity je už nutně těleso, takže jsme skutečně sestrojili konečné těleso s p^n prvky. □

Cvičení 23. Sestroj těleso se 125 prvky.

Cvičení(*) 24. Nechť je R eukleidovský obor a $p \in R$ prvočinitel. Dokaž, že $R/(p)$ je těleso, a to i tehdy, když je $R/(p)$ nekonečná množina. To lze například využít, když v $\mathbb{Q}[x]$ modulíme libovolným ireducibilním polynomem.

Čínská zbytková věta

V druhém díle jsme podrobně zkoumali konečná tělesa, což byly typicky faktorokruhy, které jsme dostali modulením pomocí prvočinitele. Stejně tak polynomy jsme se dosud odvážili modulit jen těmi ireducibilními. Co když ale budeme chtít pracovat modulo nějaký složený prvek? Ukážeme si, jak takové faktorokruhy rozkládat na menší kousky.

Definice. Nechť jsou R, S dva komutativní okruhy. Jejich *direktním součinem* $R \times S$ míníme následovný okruh:

(i) Jeho nosnou množinou je množina uspořádaných dvojic (r, s) pro $r \in R$, $s \in S$.

(ii) Jeho operace jsou pro $(a, b), (c, d) \in R \times S$ definovány jako

$$(a, b) + (c, d) = (a + c, b + d), \qquad (a, b) \cdot (c, d) = (a \cdot c, b \cdot d),$$

přičemž v první složce provádíme sčítání a násobení v R, zatímco v druhé složce provádíme sčítání a násobení v S.

Analogicky definujeme direktní součin $R_1 \times \cdots \times R_n$ nějakých n okruhů.

Pozorování. Nulou je v $R \times S$ prvek $(0, 0)$, jedničkou zase $(1, 1)$. Mínusy se taktéž aplikují na každou složku zvlášť, tedy $-(a, b) = (-a, -b)$.

Cvičení(*) 25. Nechť je X nějaká množina. Vzpomeňme si na okruh $\mathcal{P}(X)$ definovaný na množině podmnožin X, kde jako součet podmnožin $A, B \subseteq X$ figuruje jejich symetrická diference $A \oplus B$ (množina těch prvků, které jsou v právě jedné z A, B) a jako jejich součin figuruje průnik $A \cap B$. Rozmysli si, že pro n-prvkovou množinu X je okruh $\mathcal{P}(X)$ izomorfní okruhu $\mathbb{Z}_2^n = \underbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n\text{-krát}}$.

Direktní součin je jenom formální popis toho, že si dva okruhy žijí každý po svém, ale zabalíme je do jedné krabičky a díváme se na ně zároveň. Hned si dokážeme Čínskou zbytkovou větu, jež říká, že za určitých podmínek lze $R/(k\ell)$ rozlomit na $R/(k)$ a $R/(\ell)$ neboli že R mod $k\ell$ se chová stejně jako R mod k a R mod ℓ zabalené dohromady.

Věta. (Čínská zbytková) *Nechť je R eukleidovský obor a $k, \ell \in R$ jsou nesoudělná. Potom pro libovolná $a, b \in R$ existuje $c \in R$, které zároveň splní obě kongruence*

$$c \equiv a \pmod{k}, \qquad c \equiv b \pmod{\ell}.$$

Všechna taková c jsou navíc navzájem kongruentní mod $k\ell$.

Důkaz. Využijeme toho, že v eukleidovském oboru platí Bézoutova identita. Největším společným dělitelem k a ℓ je podle předpokladu nesoudělnosti jednička. Existují tedy Bézoutovy koeficienty $u, v \in R$, které nám splní $uk + v\ell = 1$. Zmodulením této rovnosti mod k a mod ℓ dostáváme

$$v\ell \equiv 1 \pmod{k} \qquad \text{a zároveň} \qquad uk \equiv 1 \pmod{\ell}.$$

Potom můžeme jednoduše zvolit $c = b \cdot uk + a \cdot v\ell$, čímž bude zaručeno, že

$$c \equiv a \cdot v\ell \equiv a \cdot 1 \equiv a \pmod{k} \qquad \text{a zároveň} \qquad c \equiv b \cdot uk \equiv b \cdot 1 \equiv b \pmod{\ell}.$$

Zbývá si rozmyslet jednoznačnost c mod $k\ell$. Uvažujme dvě $c_1, c_2 \in R$, která splňují

$$c_1 \equiv c_2 \equiv a \pmod{k} \qquad \text{a zároveň} \qquad c_1 \equiv c_2 \equiv b \pmod{\ell}.$$

Potom máme $c_1 - c_2 \equiv a - a \equiv 0 \pmod{k}$, takže $k \mid c_1 - c_2$. Obdobně $\ell \mid c_1 - c_2$, z čehož dohromady nesoudělností k, ℓ plyne i $k\ell \mid c_1 - c_2$ neboli $c_1 \equiv c_2 \pmod{k\ell}$. □

Důsledek. *Při splnění podmínek věty je $R/(k\ell)$ izomorfní okruhu $R/(k) \times R/(\ell)$, přičemž izomorfismem je zde přiřazení $\varphi(a \bmod k\ell) = (a \bmod k,\ a \bmod \ell)$.*

Důkaz. Z věty víme, že φ je skutečně vzájemné párování prvků $R/(k\ell)$ a $R/(k) \times R/(\ell)$. Stačí si tedy rozmyslet, že φ zachovává operace. To je ale jasné, protože se v obou složkách jedná jen o modulení a modulení operace skutečně zachovává. □

Poznámka. Snadnou indukcí plyne, že věta platí i pro více (ale konečně mnoho) modul: jsou-li $k_1, \ldots, k_n \in R$ navzájem nesoudělné prvky, pak $R/(k_1 \cdots k_n) \simeq R/(k_1) \times \cdots \times R/(k_n)$.

Poznámka. Všimni si, že eukleidovskost v důkazu používáme jen na to, abychom mohli vzít Bézoutovu identitu $uk + v\ell = 1$. O něco obecněji bychom tedy Čínskou zbytkovou větu mohli formulovat pro prvky k, ℓ libovolného okruhu, pro které lze splnit $uk + v\ell = 1$. Třeba s okruhem $\mathbb{Z}[x]$ (ten není eukleidovský) tak stále můžeme dokázat např. $\mathbb{Z}[x]/(x^2+x) \simeq \mathbb{Z}[x]/(x) \times \mathbb{Z}[x]/(x+1)$, což je posléze izomorfní $\mathbb{Z} \times \mathbb{Z}$, jelikož $\mathbb{Z}[x]$ modulo monický lineární polynom se chová jako $\mathbb{Z}$.

Na praktické použití Čínské zbytkové věty v úlohách se hodí následující úhel pohledu: máme-li něco splnit modulo $k\ell$, pak se můžeme zcela odděleně starat o to, abychom to splnili mod k a mod ℓ. Stejně tak pokud je nějaká podmínka formulována modulo $k\ell$, jsou to jenom dvě nezávislé podmínky, jedna mod k, druhá mod ℓ.

Příklad. Dokaž, že pro libovolné přirozené n existují $a, b \in \mathbb{Z}$ splňující $4a^2 + 9b^2 \equiv 1 \pmod{n}$.

Řešení. Zapišme $n = 2^k \cdot \ell$, kde ℓ je liché číslo. Podle zbytkové věty nám stačí ukázat, že zadaná kongruence má řešení mod 2^k a mod ℓ. Modulo 2^k můžeme zvolit $a \equiv 0$, $b \equiv 3^{-1}$, čímž myslíme takový prvek, že $3^{-1} \cdot 3 \equiv 1$. Ten existuje, protože 3 a 2^k jsou nesoudělná čísla. Modulo ℓ zase zvolíme $b \equiv 0$ a $a \equiv 2^{-1}$, což můžeme, jelikož 2 a ℓ jsou nesoudělná. Poté už si jen ze zbytkové věty poručíme

$$a \equiv 0 \pmod{2^k}, \qquad b \equiv 3^{-1} \pmod{2^k},$$
$$a \equiv 2^{-1} \pmod{\ell}, \qquad b \equiv 0 \pmod{\ell}$$

a máme vyhráno.

Cvičení 26. Jsou dána dvě různá kladná prvočísla p, q. Dokaž, že $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Když už takto pomocí Čínské zbytkové věty lámeme úlohu mod n na menší kusy, často se vyplatí ji rozlámat, co nejvíc to jen jde. Pro n s prvočíselným rozkladem

$$n = p_1^{k_1} \cdots p_r^{k_r},$$

kde jednotlivá prvočísla $p_1, \ldots, p_r$ jsou navzájem různá, to znamená dívat se zvlášť na jednotlivé mocniny $p_i^{k_i}$.

Definice. *Prvočíselnou mocninou* rozumíme číslo tvaru p^k pro $k \in \mathbb{N}$ a prvočíslo $p \in \mathbb{N}$.

Cvičení(!) 27. Urči v závislosti na $n \in \mathbb{N}$, kolik z čísel $1, 2, \ldots, n$ je nesoudělných s n.

Úloha 12. Dokaž, že pro každé $n \in \mathbb{N}$ existuje n po sobě jdoucích přirozených čísel, z nichž žádné není prvočíselná mocnina.

Čínská zbytková věta dovede posloužit i tam, kde se o dvou nesoudělných modulech na první pohled nic neříká. Použijeme ji tak, že si prostě v navzájem nesoudělných modulech objednáme nějaké podmínky, které nám úlohu vyřeší, a Čínská zbytková věta nám bude černou skříňkou, která splnění těchto podmínek zařídí.

Příklad. Jsou dána přirozená čísla a, b taková, že pro libovolné $n \in \mathbb{N}$ platí $b^n + n \mid a^n + n$. Dokaž, že $a = b$.

Řešení. Zadání nám dává spoustu dělitelností a chce po nás dokázat rovnost. To obecně nemusí být vůbec snadné, ale zde budeme schopni ukázat, že každé prvočíslo p dělí rozdíl $a - b$. Každé nenulové celé číslo přitom má jenom konečně mnoho dělitelů, takže tohle už zaručí $a - b = 0$.

Nejprve si zadanou dělitelnost ekvivalentně upravme na $b^n + n \mid (a^n + n) - (b^n + n)$, tedy $b^n + n \mid a^n - b^n$. Nechť je dále dáno libovolné prvočíslo $p \in \mathbb{N}$. Rozmyslíme si, že dovedeme zvolit n tak, aby platilo $p \mid b^n + n$ a zároveň $a^n - b^n \equiv a - b \pmod{p}$. Zde přichází do hry zbytková věta. Když se na výrazy díváme mod p, pak se n, které přičítáme k b^n, chová jako zbytek mod p, zatímco všechna n v exponentech se chovají jako zbytky mod $p - 1$, protože z malé Fermatovy věty je $a \equiv a^p \equiv a^{2p-1} \equiv \cdots \pmod{p}$. Čísla p a $p - 1$ jsou zjevně nesoudělná (společný dělitel musí dělit i rozdíl), takže si zbytky v těchto modulech můžeme navolit zcela nezávisle. Objednejme si tedy $n \equiv 1 \pmod{p-1}$ a $n \equiv -b \pmod{p}$. Z první kongruence budeme mít mod p zaručeno $a^n \equiv a$, $b^n \equiv b$, takže zbude

$$b^n + n \equiv b + (-b) \equiv 0 \qquad \text{a zároveň} \qquad a^n - b^n \equiv a - b.$$

To bude znamenat $p \mid b^n + n \mid a^n - b^n$, tedy $0 \equiv a^n - b^n \equiv a - b \pmod{p}$, jak jsme chtěli, což zaručí $a - b = 0$.

Mohli jsme dosazovat přímo do $b^n + n \mid a^n + n$, avšak s $a^n - b^n$ na pravé straně je už před zformulováním důkazu jasné, že náš postup musí uspět: volbou $n \pmod{p-1}$ si dělence upravíme na $a - b \pmod{p}$ a volba $n \pmod{p}$ nám zbude na zařízení $p \mid b^n + n$.

Úloha 13. Uvažujme v rovině mřížové body $(a, b) \in \mathbb{Z}^2$ s celočíselnými souřadnicemi. Bod (a, b) je *viditelný*, pokud jsou a, b nesoudělná celá čísla. Dokaž, že pro libovolné $n \in \mathbb{N}$ existuje čtverec $n \times n$ mřížových bodů, z nichž žádný není viditelný.

Úloha 14. Dokaž, že existuje přirozené číslo n takové, že pro libovolné $a \in \mathbb{Z}$ nemá číslo $a^2 + a + n$ žádného (kladného) prvočíselného dělitele menšího než 2021.

Příklad. (Lagrangeova[10] interpolace) Představme si tuto situaci: jsme v tělese K a někdo nám prozradil hodnoty

$$b_0 = f(a_0), \qquad b_1 = f(a_1), \qquad \ldots, \qquad b_n = f(a_n)$$

[10] Joseph-Louis Lagrange (1736–1813), francouzský matematik italského původu, se podílel mj. i na vzniku a standardizaci metru a kilogramu.

pro nějaká navzájem různá $a_1, \ldots, a_n \in K$. Jak z nich odhalíme polynom $f \in K[x]$? Víme, že dosazení a_i je jako modulení polynomem $x - a_i$, takže se jedná o situaci z Čínské zbytkové věty: známe zbytky f modulo jednotlivá $x - a_i$, což jsou z různosti všech a_i nesoudělné polynomy. Z Čínské zbytkové věty je tak f jednoznačně určeno modulo $(x - a_0)(x - a_1) \cdots (x - a_n)$. To je polynom stupně $n+1$, takže všechny zbytkové třídy půjdou reprezentovat právě jedním polynomem stupně nejvýše n.

Pro tento polynom lze dokonce vymyslet explicitní, ač trochu komplikovaný předpis. Pro každé $k \in \{0, 1, \ldots, n\}$ si označme

$$f_k = \text{součin polynomů } \frac{x - a_j}{a_k - a_j} \text{ pro } 0 \leq j \leq n,\ j \neq k.$$

Tento předpis zařídí, že $f_k(a_k) = 1$, protože každý ze zlomků v součinu bude po dosazení $\frac{a_k - a_j}{a_k - a_j} = 1$. Naproti tomu dosazení a_j pro $j \neq k$ povede k tomu, že dostaneme v součinu člen $\frac{a_j - a_j}{a_k - a_j} = 0$, takže $f_k(a_j) = 0$. Nyní můžeme vzít

$$f = b_0 f_0 + b_1 f_1 + \cdots + b_n f_n,$$

což už skutečně zařídí $f(a_k) = b_k$ pro každé k, neboť $b_k f_k(a_k) = b_k$ a $b_j f_j(a_k) = 0$ pro $j \neq k$. Zároveň je každý f_k součinem n lineárních polynomů, takže $\deg f_k = n$, z čehož má i f stupeň nanejvýš n.

Příklad. Polynom $x^4 - 5x^2 + 6$ není nad $\mathbb{Q}$ ireducibilní, jelikož se rozkládá na $(x^2 - 2)(x^2 - 3)$. Oba polynomy $x^2 - 2$ a $x^2 - 3$ jsou ireducibilní, takže skloubením Čínské zbytkové věty s tvrzením o modulení ireducibilním polynomem dostaneme

$$\mathbb{Z}[x]/(x^4 - 5x^2 + 6) \simeq \mathbb{Z}[x]/(x^2 - 2) \times \mathbb{Z}[x]/(x^2 - 3) \simeq \mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[\sqrt{3}].$$

Libovolnému polynomu f v tomto přiřazení odpovídá dvojice hodnot $\big(f(\sqrt{2}), f(\sqrt{3})\big)$.

Cvičení(*) 28. Nechť je T konečné těleso. Nahlédni, že libovolné zobrazeni $F\colon T \to T$ se dá reprezentovat polynomem, tedy existuje $f \in T[x]$ splňující $F(a) = f(a)$ pro každé $a \in T$.

Závěr

Seriál doputoval do svého úplného závěru. Víme již, že jak pracovat s výrazy s proměnnou pomocí okruhů polynomů, dovedeme do nich dosazovat a také rozpoznávat jejich kořeny. Nezalekneme se ani ireducibilních polynomů a máme dobrou představu, co to znamená modulit polynomy. Konečně pomocí Čínské zbytkové věty dovedeme velké děsivé problémy lámat na menší a přátelštější.

Doufáme, že Tě naše kuchařské lekce bavily. Snad se nám podařilo Tě přesvědčit o tom, že důvěrně známá prostředí, pojmy a myšlenky jako celá čísla, prvočísla a jednoznačnost rozkladu na ně se dají zobecňovat a že tyto obecnější pohledy nám dovedou dát hlubší znalosti, které bychom bez nich jen těžko nahlíželi. Algebraický pohled na teorii čísel, se kterým jsme v průběhu seriálu k věcem přistupovali, skýtá nepřeberné množství krás a tajů – věz, že to, co jsme si stihli ukázat, je jen špičkou ledovce.

Nyní nám nezbývá než se rozloučit. Seriál pro Tebe psali Fíla a Matěj, ale jak to tak bývá, nápomocna nám byla mnohá další PraSátka. Zde bychom rádi poděkovali Hedvice, Danilovi, Kubovi, Pavlovi a Radkovi. Ze všeho nejvíce však děkujeme a gratulujeme Tobě, že ses dočetl(a) až na konec, a přejeme hodně štěstí při řešení úloh třetí seriálové série!

Návody ke cvičením

1. Když je R triviální, pak není moc možností, jak zvolit koeficienty polynomů v $R[x]$.

2. Kdy se mohou nejvyšší mocniny x vyrušit?

3. Použij tvrzení o stupni součinu.

4. Rozepiš podle definice dělitelnosti.

5. Pozor na to, nad jakým okruhem pracujeme. Pokud dělitelnost platí, je jasné, jaký stupeň by měl mít podíl.

6. Kde vznikne nejvyšší mocnina x?

7. Rozepiš z definice dělitelnosti.

8. Máš možnost dosadit dvě čísla. Jedno bude zřejmě kořen a jedno číslo, kterým dostaneme jen absolutní člen.

9. Pro spor předpokládej, že existuje kořen $t \in \mathbb{Z}$, a vhodně použij lemma.

10. Podívej se na kořeny a stupeň polynomu $f(x+1) - f(x) - 1$.

11. Vyjádři pomocí Viètových vztahů pro polynom $x^2 + 4x + 1$.

12. Použij větu o racionálním kořenu.

13. Věta o racionálním kořenu.

14. Věta o racionálním kořenu dává jen několik možných zlomků, které by mohly být kořenem.

15. V rozkladu f na součin menších polynomů musí jeden činitel být lineární.

16. Jaké stupně mohou mít dělitelé lineárního polynomu?

17. Co kdyby nebyly?

18. Násobením vyrob celá čísla a poté poděl největším společným dělitelem.

19. Celočíselný dělitel dává rozklad na nejednotky.

20. Vezmi $g = fh$ pro $h \in \mathbb{Q}[x]$ a pomocí Gaussova lemmatu dokaž $h \in \mathbb{Z}[x]$.

22. Vezmi rozklad f na ireducibilní polynomy, zmodul a využij jednoznačný rozklad v $\mathbb{Z}_p[x]$.

23. $125 = 5^3$, takže stačí najít ireducibilní polynom stupně 3 nad $\mathbb{Z}_5$.

24. Použij Bézoutovu identitu.

25. Zapiš do k-té složky, zdali podmnožina obsahuje k-tý prvek X.

26. Podívej se zvlášť mod p a mod q, dostaneš známou větu.

27. Nejprve vyřeš pro prvočíselné mocniny a poté vynásob.

28. Interpolace.

Návody k úlohám

1. Vytvoř posloupnost $a_{i+1} = f(a_i)$, kde $a_0 = a$. Víme, že po nějakém počtu kroků (nejvýše k) se zase dostaneme k a_0. Použij na rozdíly dvou následujících členů lemma a následně využij zacyklení.

2. Dosaď kořeny x^2+x+1. Potom buďto prostě dopočítej $g(1)$, $h(1)$, anebo si všimni, že polynom $h(1) \cdot x + g(1)$ má moc kořenů.

3. Pokud jsou a, b dvě řešené $g(t) = t$, použij na ně opakovaně lemma o rozdílu argumentů, dokud se situace nezacyklí. Následně nahlédni, že pokud je řešení $g(t) = t$ příliš mnoho, už musí být f lineární.

4. Uvaž polynom $g = x \cdot f - 1$. Zadání mu dává spoustu kořenů, zbývá určit koeficient c_n.

5. Viètovy vztahy s kubickým polynomem. Zkus pro spor uvažovat, že je nějaký kořen nekladný.

6. Využij polynom $\left(x - \frac{a}{b}\right)\left(x - \frac{b}{c}\right)\left(x - \frac{c}{a}\right)$.

7. Předpokládej $f = gh$, jaké potom mohou být hodnoty $g(a_i)$, $h(a_i)$? Dokaž $g + h = 0$ a všimni si, že polynom f umí nabývat kladných hodnot.

8. Předpokládej $f = gh$ a dokaž $g - h = 0$. Zamysli se, zda umí f nabývat záporných reálných hodnot.

9. Posuň argument, posčítej kombinační čísla a použij Eisensteina s prvočíslem p. Hodí se vědět, že $\binom{p}{k}$ je násobek p pro $0 < k < p$.

10. Aplikuj rozšířeného Eisensteina. Pak už stačí říct, že daný polynom nemá kořen.

11. Rozliš, zda je g ireducibilní. Pokud je, pak už $f \equiv 0 \pmod{g}$.

12. Nechť je a začátek hledaného úseku. Vyber si $2n$ prvočísel a požaduj $a \equiv -i \pmod{p_i q_i}$ pro $i = 0, 1, \ldots, n-1$.

13. Poruč si pro každý bod hledaného čtverce prvočíslo, kterým mají být souřadnice soudělné.

14. Polynom $x^2 + x$ nad $\mathbb{Z}_p$ neumí nabývat všech hodnot mod p. Podle toho navol $n \pmod{p}$.

Řesení cvičení

1. Podle předchozí poznámky $R \subseteq R[x]$, takže když má $R[x]$ jediný prvek, pak i R má jediný prvek. Naopak když je R triviální, jeho jediný prvek je 0. V polynomu $f \in R[x]$ musí všechny koeficienty být prvky R, takže jsou všechny 0, pročež je $f = 0$ jediným prvkem $R[x]$.

2. Nechť je $n = \max\{\deg f, \deg g\}$. V f ani g nejsou nenulové koeficienty u žádných mocnin x vyšších než x^n, takže žádné vyšší mocniny nemohou vzniknout ani v součtu, tedy $\deg(f+g) \leq n$. Pokud $\deg f \neq \deg g$, pak BÚNO $\deg f = n > \deg g$. Koeficient u x^n tak bude v g nula, takže odpovídající koeficient v $f + g$ bude stejný jako v f, kde je nenulový, takže už $\deg(f+g) = n$.

3. Z definice dělitelnosti máme $g = f \cdot h$ pro nějaké $h \in R[x]$. Kdyby $h = 0$, pak $g = f \cdot 0 = 0$, což je spor, takže $h \neq 0$. Potom ale $\deg h \geq 0$, takže $\deg g = \deg(fh) = \deg f + \deg h \geq \deg f$.

4. Nechť je $f = b_n x^n + \cdots + b_0$. Pokud máme $b_i = a \cdot c_i$ pro každé i, pak $f = a \cdot g$ pro $g = c_n x^n + \cdots + c_0$, takže $a \mid f$. Naopak když $a \mid f$, značí $f = ag$ pro nějaké $g \in R[x]$ a každý koeficient f je a-krát příslušný koeficient g.

5. (i) Platí $(x^2 + x + 1)(x^2 - x + 1) = x^4 + x^2 + 1$, takže uvedená dělitelnost vskutku platí.

(ii) Dělitelnost neplatí. Kdyby platila, tak by vzhledem k $(x+1)(x-1) = x^2 - 1$ muselo i $(x^2 - \sqrt{2}) - (x^2 - 1) = 1 - \sqrt{2}$ být násobkem $x+1$. Jenže $\deg(x+1) = 1 > 0 = \deg(1 - \sqrt{2})$, což by byl spor.

(iii) Nad $\mathbb{Q}$ bychom sice měli $(2x+2) \cdot \frac{1}{2}(x-1) = x^2 - 1$, jenže $\frac{1}{2}(x-1)$ není prvek $\mathbb{Z}[x]$. Kdyby opravdu $2x + 2 \mid x^2 - 1$, znamenalo by to i $2 \mid x^2 - 1$, jenže polynom 2 nedělí koeficienty 1 ani -1. Dělitelnost tedy neplatí.

(iv) Platí $(x^2 + 1)(x^3 + x^2) = x^5 + x^4 + x^3 + x^2$, takže kdyby zadaná dělitelnost platila, měli bychom i $x^2 + 1 \mid x + 1$, což díky stupňům nemůže platit ($\mathbb{Z}_2$ je obor integrity).

6. Nechť $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, kde $a_n \neq 0$, a $m = \deg g > 0$. Potom $f(g) = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_0$. Jsme v oboru integrity, takže $\deg(g^k) = \deg(g^k) = k \cdot \deg g = km$. Nenulovostí a_n tak má sčítanec $a_n g^n$ stupeň nm, zatímco každý nižší sčítanec $a_k g^k$ má menší stupeň $km < nm$, jelikož m je kladné. Mocnina x^{nm} ze sčítance $a_n g^n$ se tak nemůže vyrušit, čímž už $\deg(f(g)) = nm$, jak jsme chtěli.

7. Z definice dělitelnosti máme $g = f \cdot h$ pro nějaký polynom h. Je-li t kořen f, pak dosazením $g(t) = f(t) \cdot h(t) = 0 \cdot h(t) = 0$.

8. Dosadíme kořen t a 0. Podle lemmatu pak dostáváme $a = a - 0 \mid f(a) - f(0) = 0 - c_0 = c_0$, kde c_0 je absolutní člen f.

9. Z našeho lemmatu víme, že $a - t \mid f(a) - f(t) = f(a) = \pm 1$. Analogicky pro b a c dostáváme, že $a - t$, $b - t$ i $c - t$ dělí plus nebo mínus jedničku. To v celých číslech znamená, že jsou plus mínus

jedna, takže z Dirichletova principu jsou alespoň dvě totožná, což je ale spor s tím, že jsou a, b, c různá.

10. Označme $g = f(x+1) - f(x)$. Každé t_i je pak kořenem polynomu $g-1$. Nahlédněme, že g bude mít stupeň přesně $n-1$. Nechť $f = a_n x^n + \cdots + a_1 x + a_0$. Potom se mocnina x^n v $a_n(x+1)^n - a_n x^n$ vyruší, zatímco člen x^{n-1} vzniklý z $a_n(x+1)^n + a_{n-1}(x+1)^{n-1} - a_n x^n - a_{n-1}x^{n-1}$ bude podle binomické věty přesně $a_n \binom{n}{1} x^{n-1}$, takže bude nenulový. Polynom $g-1$ má stupeň nanejvýš $n-1$, ale n různých kořenů, takže už platí $g = 1$. To má mít stupeň $n-1$, takže určitě $n = 1$. Pak už snadno dořešíme, že vteřinové polynomy jsou přesně $f = x + c$ pro libovolné $c \in \mathbb{R}$.

11. Polynom $x^2 + 4x + 1$ má dva různé kořeny a, b, takže z Viètových vztahů víme, že $ab = 1$ a $a + b = -4$. Z toho upravíme $\frac{a}{b} + \frac{b}{a} = \frac{a^2+b^2}{ab} = \frac{(a+b)^2-2ab}{ab} = \frac{16-2}{1} = 14$. Obecné bychom v úlohách podobného rázu vyjádřili hledanou hodnotu pomocí symetrických výrazů ve Viètových vztazích.

12. Je-li $\frac{p}{q}$ racionální kořen v základním tvaru, pak $q \mid c_n = 1$, takže jde opravdu o celé číslo.

13. Pokud chceme, aby $a^7 - 7a^5 + 5a^3 - 3a + 7 = n$, pak má $a = \frac{p}{q}$ být kořenem $x^7 - 7x^5 + 5x^3 - 3x + 7 - n$. Z věty o racionálním kořenu máme $q \mid 1$, což znamená, že a je celé číslo.

14. Stačí vyzkoušet všechny $\frac{p}{q}$ pro $p \mid 1$, $q \mid 6$, tedy $\pm\frac{1}{6}$, $\pm\frac{1}{3}$, $\pm\frac{1}{2}$ a ± 1. Zjistíme, že kořeny jsou 1, $\frac{1}{2}$ a $\frac{1}{3}$.

15. Platí $f = gh$ pro nějaké $g, h \in K[x]$, které nejsou jednotky. Všechny nenulové konstantní polynomy jsou jednotky (K je těleso), takže $\deg g, \deg h \geq 1$. Ale také $\deg g + \deg h = \deg(gh) = \deg f \leq 3$, takže jedno z g, h je lineární. BÚNO $\deg g = 1$. Potom máme $g = ax + b$ pro nějaká $a, b \in K$. Tento lineární dvojčlen má kořen $-\frac{b}{a}$, takže toto je i kořenem f jakožto násobku g.

16. Uvažujme polynom f stupně 1 nad tělesem K a nechť $f = gh$ pro $g, h \in K[x]$. Tyto polynomy jsou určitě nenulové a součet jejich stupňů je 1, takže jeden je lineární a jeden konstantní. Ale nenulový konstantní polynom nad tělesem je jednotka, takže f nelze rozložit na součin dvou nejednotek.

17. Nechť pro spor g není primitivní. Potom nějaké $d \in \mathbb{Z}$, které není jednotkou, dělí g. Potom ale určitě i $d \mid gh = f$, což je spor s primitivností f.

18. Koeficienty f jsou zlomky, vezměme tedy nějaké přirozené číslo N, které je násobkem všech jmenovatelů těchto zlomků. Polynom $h = N \cdot f$ pak určitě bude ležet v $\mathbb{Z}[x]$. Koeficienty h jsou celá čísla, můžeme tedy vzít jejich největšího společného dělitele d. BÚNO je d kladné, potom je d to největší přirozené číslo, které splňuje $d \mid h$. Polynom $g = \frac{1}{d} \cdot h = \frac{N}{d} \cdot f$ potom nemůže být dělitelný žádným přirozeným číslem kromě 1, neboť $t \mid g$ znamená $td \mid h$. Máme tedy vyhráno a k polynomu g vezmeme racionální číslo $q = \frac{N}{d}$.

Zbývá jednoznačnost. Nechť $f = k_1 g_1 = k_2 g_2$, potom $g_2 = \frac{k_1}{k_2} g_1$. Zapišme zlomek v základním tvaru $\frac{p}{q} = \frac{k_1}{k_2}$. Jmenovatel q musí být společným jmenovatelem koeficientů g_1, což je primitivní polynom, takže $q = \pm 1$. Posléze $g_2 = \pm p g_1$, takže primitivností g_2 i $p = \pm 1$, z čehož $k_1 = \pm k_2$, $g_1 = \pm g_2$.

19. Budiž uvažovaný polynom f. Pokud $a \mid f$ pro nějaké $a \in \mathbb{Z}$, pak máme $f = ag$ a z nekonstantnosti f je i g nekonstantní, takže není jednotkou. Rozklad $f = ag$ tak dosvědčuje, že f není ireducibilní.

20. Mějme $g = fh$ pro nějaké $h \in \mathbb{Q}[x]$. Přepišme h na násobek primitivního celočíselného polynomu, tedy $h = \frac{a}{b} \cdot h_1$, kde $a, b \in \mathbb{Z}$ a $h_1 \in \mathbb{Z}[x]$ je primitivní. Potom $b \cdot g = a \cdot f h_1$. Každé prvočíslo $p \mid b$ nyní dělí pravou stranu, ale nemůže dělit f ani h_1 (primitivní polynomy), tedy $p \mid a$. Takto můžeme postupně krátit, až dostaneme $b \mid a$. To znamená $\frac{a}{b} \in \mathbb{Z}$, takže ve skutečnosti bylo $h = \frac{a}{b} h_1$ celočíselné, což značí $f \mid g$ nad $\mathbb{Z}$.

21. Díky koeficientu 1 u x^n je daný polynom primitivní a s prvočíslem p jsou splněny všechny tři podmínky Eisensteinova kritéria, takže máme vyhráno.

22. Nechť je $f = g_1 \cdot g_2 \cdots g_r$ rozklad f na ireducibilní polynomy. Zmodulme na obou stranách prvočíslem p. Nalevo dostaneme $\hat{f} = (a_n \bmod p)x^n + \cdots + (a_k \bmod p)x^k$, tedy $x^k \mid \hat{f}$. Polynom x je ireducibilní nad $\mathbb{Z}_p$, takže ve zmodulené rovnosti $\hat{f} = \hat{g}_1 \cdots \hat{g}_r$ se musí tyto násobky x nějak rozdělit mezi činitele na pravé straně. Kdyby však x dělilo některé dva, BÚNO $x \mid \hat{g}_1, \hat{g}_2$, pak mají g_1 i g_2 absolutní členy, které jsou násobky p. Absolutní člen f je součinem absolutních členů všech g_i, takže toto by znamenalo $p^2 \mid a_0$, což je spor. Určitě tak celé x^k dělí jedno jediné $\hat{g}_i$, BÚNO $x^k \mid \hat{g}_1$. Nemůže být $\hat{g}_1 = 0$, neboť pak by bylo $p \mid g_1 \mid f$, což vzhledem k $p \nmid a_k$ neplatí. Takže je $\hat{g}_1$ nenulový, a tudíž $k \leq \deg \hat{g}_1 \leq \deg g_1$, jak jsme chtěli.

23. Stačí najít vhodný polynom nad $\mathbb{Z}_5$. Aby byl polynom stupně ≤ 3 nad tělesem ireducibilní, stačí, aby v něm neměl kořen. To splňuje třeba $x^3 + x + 1$, takže $\mathbb{Z}_5[x]/(x^3 + x + 1)$ je 125prvkové těleso. (Stejně dobře lze použít i mnoho jiných polynomů.)

24. Stačí dokázat, že libovolný prvek $a \in R$, který není 0 mod p, má k sobě inverzní prvek $b \in R$ splňují $ab \equiv 1 \pmod{p}$. K tomu využijme toho, že a, p jsou nesoudělné prvky, takže existují Bézoutovy koeficienty u, v splňující rovnost $ua + vp = 1$. Pak stačí vzít $b = u$.

25. BÚNO nechť $X = \{1, 2, \ldots, n\}$. Předepišme izomorfismus $\varphi\colon \mathcal{P}(X) \to \mathbb{Z}_2^n$ tak, že pro $A \subseteq X$ bude $\varphi(A) = (a_1, \ldots, a_n)$, kde

$$a_k = \begin{cases} 1, & \text{pokud } k \in A, \\ 0, & \text{pokud } k \notin A. \end{cases}$$

Nyní uvažme dvě $A, B \subseteq X$ a odpovídající $\varphi(A) = (a_1, \ldots, a_n)$, $\varphi(B) = (b_1, \ldots, b_n)$. Prvek k leží v $A \oplus B$, právě když leží v právě jedné z A, B. To odpovídá tomu, že ve dvojici a_k, b_k je jedno 0 a druhé 1, což znamená $a_k + b_k \equiv 1 \pmod 2$. Podobně když $k \notin A \oplus B$, tak $a_k \equiv b_k$, tedy $a_k + b_k \equiv 0$. Z tohoto tedy vidíme, že $\varphi(A) + \varphi(B) = \varphi(A \oplus B)$.

Obdobně prvek k leží v $A \cap B$, právě když leží v obou. To odpovídá tomu, že $a_k \equiv b_k \equiv 1$. Potom $a_k \cdot b_k \equiv 1$, zatímco v ostatních případech (kdy je jedno z a_k, b_k nula) už nutně $a_k \cdot b_k \equiv 0$. Z toho vidíme, že $\varphi(A) \cdot \varphi(B) = \varphi(A \cap B)$.

26. Jakožto různá prvočísla jsou p, q nesoudělná, takže můžeme použít Čínskou zbytkovou větu. Stačí tedy dokázat zvlášť dvě odpovídající kongruence mod p a mod q. Modulo p máme dokázat $q^{p-1} \equiv 1 \pmod{p}$, což je ale jen malá Fermatova věta, protože z různosti $q \not\equiv 0 \pmod{p}$. Obdobně pro modulo q, takže máme hotovo.

27. Nejprve vyřešme případ, kdy je $n = p^k$ prvočíselná mocnina. Potom jsou s n soudělné právě násobky p, kterých je mezi $1, 2, \ldots, p^k$ přesně p^{k-1}. Nesoudělných čísel tedy zbude $p^k - p^{k-1} = p^{k-1}(p-1)$.

Nyní mějme n s prvočíselným rozkladem $n = p_1^{k_1} \cdots p_r^{k_r}$. Nějaké $a \in \{1, 2, \ldots, n\}$ je nesoudělné s n, právě když je nesoudělné s každou prvočíselnou mocninou $p_i^{k_i}$. Podle zbytkové věty tedy číslo a nesoudělné s n odpovídá nějakému a_1 nesoudělnému s $p_1^{k_1}$, nějakému a_2 nesoudělnému s $p_2^{k_2}$ atd., takže jejich počty se znásobí. Celkem tedy dostaneme $p_1^{k_1-1}(p_1 - 1) \cdots p_r^{k_r-1}(p_r - 1)$ čísel nesoudělných s n.

28. Použijeme Lagrangeovu interpolaci. Za body a_i vezmeme úplně všechny prvky T a jako hodnoty $f(a_i)$ si poručíme $b_i = F(a_i)$. Z Lagrangeovy interpolace plyne, že existuje f splňující tyto požadavky, takže skutečně $F(a) = f(a)$ pro každé $a \in T$.