Konečná tělesa a kde je najít

Matěj Doležálek

Abstrakt. Počítat modulo prvočíslo je fajn: skoro všechno má multiplikativní inverz a platí zde spousta užitečných větiček. V tomto příspěvku tyto poznatky zobecníme do pojmu *konečného tělesa* a ukážeme, že ač musíme některé exempláře hledat v exotických místech, stojí to za to. Standardní vysokoškolskou teorii odložíme na závěr, namísto toho se budeme co nejvíce věnovat olympiádním aplikacím.

Definice. *Těleso* je struktura, ve které máme význačné prvky 0, 1 (navzájem různé) a umíme sčítat, odečítat, násobit a nenulovými prvky také dělit za platnosti všech obvyklých pravidel. *Konečné těleso* je těleso, které má jen konečné mnoho prvků.

Úmluva. Je-li F (konečné) těleso, nechť $F^\times$ značí množinu jeho nenulových prvků.

Příklady a základní vlastnosti

Příklad. Pro prvočíslo p tvoří celá čísla modulo p konečné těleso $\mathbb{Z}_p$ s p prvky. Abychom zdůraznili, že se jedná o tělesa, budeme je v tomto příspěvku značit $\mathbb{F}_p$.

Příklad. Je-li $n = ab$ složené číslo, kde $a, b > 1$, pak $\mathbb{Z}_n$ není těleso, např. protože (nenulovými) prvky a, b nelze dělit.

Příklad. Položme $F = \{0, 1, \alpha, \beta\}$ a předepišme na této množině sčítání a násobení následovně:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Všimněte si, že F je čtyřprvkové těleso. Zdůrazněme, že je zcela odlišné od $\mathbb{Z}_4$, což koneckonců ani není těleso.

Pozorování. *Pro každé $a \in F^\times$ je zobrazení $b \mapsto ab$ bijekcí $F^\times \to F^\times$.*

Věta. (malý Fermat) *V konečném tělese o n prvcích splňuje libovolné $a \in F^\times$ rovnost $a^{n-1} = 1$.*

Důsledek. *Nad konečným tělesem F o n prvcích platí rovnost polynomů*

$$x^n - x = \prod_{a \in F} (x - a).$$

Cvičení. (Wilsonova věta) Součin všech prvků konečného tělesa je roven -1.

Úloha 1. Najděte všechna přirozená čísla nesoudělná se všemi členy posloupnosti zadané předpisem $a_n = 2^n + 3^n + 6^n - 1$.

Definice. *Charakteristikou* konečného tělesa F míníme nejmenší přirozené číslo c, pro něž je v F součet c jedniček roven nule.

Cvičení. Charakteristika konečného tělesa musí být prvočíslo.

Tvrzení. *Konečné těleso F charakteristiky p musí mít přesně p^k prvků pro nějaké přirozené k.*

Důkaz. F je vektorový prostor nad $\mathbb{Z}_p$ a musí mít konečnou dimenzi. □

Cvičení. (Frobeniův automorfismus) Buď F konečné těleso charakteristiky p. Potom je zobrazení $\varphi : F \to F$ definované předpisem $\varphi(x) = x^p$ bijekce, která zachovává sčítání i násobení, tj. $\varphi(xy) = \varphi(x)\varphi(y)$ a $\varphi(x + y) = \varphi(x) + \varphi(y)$.

Řády a primitivní prvek

Definice. Buď F konečné těleso. *Řádem* prvku $a \in F^\times$ rozumíme nejmenší přirozené r takové, že $a^r = 1$. Značíme $r = \mathrm{ord}_F(a)$.

Pokud je z kontextu zřejmé, v jakém konečném tělese pracujeme, dovolíme si index F vypustit.

Tvrzení. *Pro $a \in F^\times$ platí $a^e = 1$, právě když* $\mathrm{ord}(a) \mid e$.

Důsledek. *Je-li F těleso s n prvky, pak pro každé $a \in F^\times$ platí* $\mathrm{ord}(a) \mid n - 1$.

Úloha 2. V n-prvkovém tělese nenulová a, b splňují $a^{2^s} + b^{2^s} = 0$. Dokažte, že $n \equiv 1 \pmod{2^{s+1}}$.

Úloha 3. Je dáno prvočíslo p. Dokažte, že existuje nekonečně mnoho prvočísel $q \equiv 1 \pmod{p}$.

Častým začátečnickým omylem kolem malé Fermatovy věty je předpokládat, že $a^e = 1$, právě když $n - 1 \mid e$ (co to říká o řádu a?). To obecně neplatí, triviálním protipříkladem je třeba $a = 1$. Nicméně ta a, která tuto vlastnost mají, jsou význačná a umíme o nich něco říct.

Definice. *Primitivním prvkem* v n-prvkovém tělese F rozumíme takové $g \in F^\times$, že $\mathrm{ord}_F(g) = n - 1$

Jinými slovy: primitivní prvek je takové g, že $F^\times = \{g, g^2, \dots, g^{n-1}\}$. Primitivní prvek není ani zdaleka určen jednoznačně – např. když je primitivním prvkem g, musí jím být také $\frac{1}{g}$.

Věta. *V každém konečném tělese existuje primitivní prvek.*

Důkaz uvaříme z trojice lemmat. Ve všech nechť je F konečné těleso s n prvky.

Lemma A. *Pokud* $\ell \mid \operatorname{ord}(a)$, *pak* $\operatorname{ord}(a^\ell) = \frac{1}{\ell}\operatorname{ord}(a)$.

Lemma B. *Pokud* $r = \operatorname{ord}(a)$, $s = \operatorname{ord}(b)$ *a zároveň jsou* r, s *nesoudělná, pak* $\operatorname{ord}(ab) = rs$.

Lemma C. *V tělese má nenulový polynom stupně* d *nanejvýš* d *různých kořenů.*

Využití primitivního prvku

Cvičení. Nahlédni, že zobrazení $a \mapsto a^m$ je v n-prvkovém tělese bijektivní, právě když je m nesoudělné s $n-1$.

Úloha 4. Buď F těleso s p^k prvky. V závislosti na přirozeném čísle e určete

$$\sum_{a \in F} a^e.$$

Úloha 5. Rozhodni, zda lze tabulku 10×10 vyplnit čísly $1, 2, \dots, 100$ a zvolit $A, B \in \mathbb{Z}_{101}$ tak, aby současně platilo:

(i) Součin prvků libovolného řádku dává po dělení 101 zbytek A.
(ii) Součet prvků libovolného sloupce dává po dělení 101 zbytek B.

Definice. *Multiplikativní množinou*[1] v konečném tělese F budeme rozumět neprázdnou podmnožinu $M \subseteq F^\times$, která je uzavřená na násobení, tedy splňuje $ab \in M$ pro libovolná $a, b \in M$.

Příklad. Mějme n-prvkové těleso F a uvažujme jisté $e \mid n-1$. Potom je

$$M_e = \{a^e \mid a \in F^\times\}$$

multiplikativní množina v F s $\frac{n-1}{e}$ prvky. Navíc platí $b \in M_e \iff b^{\frac{n-1}{e}} = 1$.

Tvrzení. *Každá multiplikativní množina v konečném tělese* F *je tvaru* M_e *pro nějaké* $e \mid n-1$. *Z toho speciálně plyne, že multiplikativní množina je jednoznačně určena svou velikostí.*

Cvičení. (kvadratické zbytky) Buď F konečné těleso liché charakteristiky s n prvky. Kolik prvků $F^\times$ má v F druhou odmocninu? Jak se tyto prvky poznají?

[1] Fajnšmekři mohou multiplikativním množinám říkat *podgrupy* (multiplikativní) *grupy* $F^\times$. My tu však do grup zabíhat nechceme, proto se tomuto – možná správnějšímu – označení vyhneme.

Konečná tělesa ve volné přírodě

Doposud by si z tohoto příspěvku mohl vážený čtenář odnést dojem, že konečná tělesa jsou vlastně jen $\mathbb{Z}_p$ a možná tu a tam nějaký náhodný exemplář jako čtyřprvkové těleso a že pro potřeby olympiádního uplatnění jsou konečná tělesa jen kosmetickou omáčkou k obyčejné modulární aritmetice celých čísel. Zde si dovolíme drahého čtenáře vyvést z těchto hypotetických omylů. Na přednášce bohužel není prostor vše, co zde řekneme, podložit důkazy – laskavý čtenář je snažně žádán, aby to autorovi odpustil.

Úmluva. Když k něčemu připíšeme „$[\alpha]$“, znamená to „přidej α a uzavři na sčítání a násobení“. Připíšeme-li „$/(m)$“, znamená to „dívej se modulo m“. V tomto značení tedy např. $\mathbb{C} = \mathbb{R}[i]$, $\mathbb{F}_p = \mathbb{Z}/(p)$.

Příklad. (Gaussovská čísla) $\mathbb{Z}[i]$ je obor tvořený těmi komplexními čísly $a + bi$, kde $a, b \in \mathbb{Z}$. S využitím imaginární jednotky lze na součin rozložit i některá čísla, u kterých to v $\mathbb{Z}$ nešlo, např. $5 = (2+i)(2-i)$. Modulením zjistíme, že můžeme potkat staré známé v novém hávu, např. $\mathbb{Z}[i]/(2-i)$ je pětiprvkové těleso, které se nijak podstatně neliší od standardního $\mathbb{Z}/(5)$. Podobně se na součin dvou „Gaussovských prvočísel“ rozkládají všechna prvočísla $p \equiv 1 \pmod 4$ (důkaz je netriviální).

Naproti tomu prvočísla $p \equiv 3 \pmod 4$ zůstávají prvočiniteli i v $\mathbb{Z}[i]$, takže při modulení nimi dostaneme tělesa s p^2 prvky. Jelikož $\mathbb{Z}$ bydlí uvnitř $\mathbb{Z}[i]$, i po zmodulení budeme mít přirozeně vnořenou kopii $\mathbb{F}_p = \mathbb{Z}/(p)$ uvnitř $\mathbb{Z}[i]/(p)$. Alternativně se na věc taky můžeme dívat tak, že polynom $x^2 + 1$ neměl v $\mathbb{F}_p$ kořen, tak jsme mu ho přidali pod jménem i a získali tak $\mathbb{F}_p[i]$.

Poznamejme též, že v $\mathbb{Z}[i]$ shodou šťastných okolností funguje jednoznačný rozklad na (Gaussovské) prvočinitele, podobně jako v $\mathbb{Z}$.

Cvičení. Najděte nějaký primitivní prvek v $\mathbb{Z}[i]/(3)$.

Příklad. (zlatý řez a Fibonacciho čísla) Označme jako $\varphi = \frac{1+\sqrt{5}}{2}$ jeden z kořenů polynomu $x^2 - x - 1$, tzv. *zlatý řez*. Druhým kořenem je $1 - \varphi$. Oba kořeny se hodí k explicitnímu vyjádření Fibonacciho čísel (definovaných pomocí $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$), jelikož $F_n = \frac{1}{\sqrt{5}}(\varphi^n - (1-\varphi)^n)$. Aritmetické vlastnosti Fibonacciho čísel proto může pomoci osvětlit pohled v $\mathbb{Z}[\varphi]$. Opět platí, že některá prvočísla se najednou dají rozložit, zatímco jiná nikoliv – ta potom modulením dávají p^2-prvková tělesa.

Dokonce platí, že prvočíslo p zůstává prvočinitelem i v $\mathbb{Z}[\varphi]$ právě tehdy, když polynom $x^2 - x - 1$ nelze nad $\mathbb{F}_p$ rozložit na součin dvou lineárních polynomů. Proto např. $\mathbb{Z}[\varphi]/(2) = \mathbb{F}_2[\varphi]$ je čtyřprvkové těleso. Když pojmenujeme třeba $\alpha = \varphi$, $\beta = \varphi + 1$, zjistíme, že se jedná přesně o čtyřprvkové těleso z příkladu na začátku přednášky. Náhodička, hm?

Příklad. (obecněji) Kdykoliv si vezmeme kořen α ireducibilního monického polynomu $f(x)$ s celočíselnými koeficienty, můžeme se dívat na obor $\mathbb{Z}[\alpha]$. Ten se může chovat v mnoha ohledech zrádně, např. v něm často nebude fungovat jednoznačný rozklad na prvočinitele, ale kdykoliv si vezmeme prvočíslo p takové, že $f(x)$ zůstává ireducibilním i nad $\mathbb{F}_p$, pak bude $\mathbb{Z}[\alpha]/(p) = \mathbb{F}_p[\alpha]$ těleso s $p^{\deg f}$ prvky.

Úloha 6. Nahlédněte, že pro prvočíslo $p \equiv 3 \pmod 4$ se Frobeniův automorfismus v konečném tělese $\mathbb{Z}[i]/(p) = \mathbb{F}_p[i]$ shoduje s komplexním sdružením.

Úloha 7. Buď $p \neq 5$ prvočíslo. Dokažte, že potom p-té Fibonacciho číslo dává po dělení p zbytek ± 1. Od čeho se znaménko odvíjí?

Úloha 8. Buď $p \equiv 3 \pmod 4$ prvočíslo a nechť celá čísla a, b splňují $a^2 + b^2 \equiv 1 \pmod p$. Nahlédněte, že potom lze $a + bi$ modulo p vyjádřit ve tvaru $(c + di)^{p-1}$ pro jistá $c, d \in \mathbb{F}_p$.

Úloha 9. Najděte periodu posloupnosti zbytků Fibonacciho čísel modulo 127.
(HMMT 2017)

Úloha 10. (těžká) Buď posloupnost nezáporných celých čísel zadána pomocí $a_0 = 2$ a $a_{k+1} = 2a_k^2 - 1$. Dokažte, že když liché prvočíslo p dělí nějaké a_n, pak $p \equiv \pm 1 \pmod{2^{n+2}}$. Bonus: na čem závisí znaménko?

Úloha 11. (těžká) Je dáno přirozené číslo k takové, že $p = 4k-1$ je prvočíslo. Dále jsou dána po dvou nesoudělná x, y, z tak, že $x^2+y^2 = z^k$. Dokažte, že $p \mid xy(x^2-y^2)$.
(PraSe 40–2s–3)

Standardní konstrukce a klasifikace konečných těles

Závěrem se sluší trochu poodkrýt vysokoškolskou oponu a říci, co se tu „děje doopravdy“.

Cvičení. Dejme tomu, že jsme v tělese charakteristiky p a podíváme se na množinu S všech kořenů polynomu $x^{p^k} - x$. Nahlédněte, že S tvoří podtěleso (obsahuje 0, 1, je uzavřená na základní operace a dá se v ní dělit).

Definice. Buď K těleso a f nekonstantní polynom s koeficienty z K. Těleso $L \supset K$ nazveme *rozkladovým nadtělesem f nad K*, pokud lze f nad L rozložit na součin lineárních polynomů a zároveň pro kořeny $\alpha_1, \ldots, \alpha_n \in L$ polynomu f platí $L = K[\alpha_1, \ldots, \alpha_n]$.

Tvrzení. *Ke každému nekonstantnímu polynomu nad tělesem existuje rozkladové nadtěleso a všechna taková rozkladová nadtělesa jsou si navzájem izomorfní – liší se jen tím, že jim někdo přejmenoval prvky, ale jejich „skutečná“ struktura je stejná.*

Věta. (velká) *Pro každé prvočíslo p a přirozené k existuje až na izomorfismus právě jedno p^k-prvkové těleso: je to rozkladové nadtěleso polynomu $x^{p^k} - x$ nad $\mathbb{F}_p$ a značíme ho $\mathbb{F}_{p^k}$. Jiná konečná tělesa neexistují a platí $\mathbb{F}_{p^\ell} \subseteq \mathbb{F}_{p^k}$, právě když $\ell \mid k$.*

Úloha 12. Určete, kolik prvků α tělesa $\mathbb{F}_{2^{10}}$ splňuje $\mathbb{F}_{2^{10}} = \mathbb{F}_2[\alpha]$.

Návody

1. $\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=1$.

2. Podmínka ekvivalentně říká, že -1 je 2^s-tá mocnina. Co pak může být řád základu této mocniny?

3. $\frac{p^p-1}{p-1}$.

4. Primitivní prvek dá geometrickou řadu. Alternativně se i bez primitivního prvku dá postupovat přímo z důsledku malého Fermata – je to mnohem techničtější, ale taky poučné.

5. Jak že se tahle kapitolka jmenuje?

6. Nezapomeň, že Frobenius funguje dobře i se sčítáním.

7. Pracuj v $\mathbb{F}_p$ anebo $\mathbb{F}_p[\varphi]$, kde φ je zlatý řez. Frobenius pomůže.

8. Podmínka $a^2+b^2\equiv 1$ určuje multiplikativní množinu v $\mathbb{F}_p[i]$.

9. Ekvivalentně chceš najít řád φ v konečném tělese $\mathbb{Z}[\varphi]/(127)$ (ověř si, že x^2-x-1 skutečně nemá kořen v $\mathbb{F}_{127}$). Frobenius je tvůj kamarád.

10. $a_k=\frac{1}{2}\left(\omega^{2^k}+\omega^{-2^k}\right)$, kde $\omega=2+\sqrt{3}$. Rozliš případy podle toho, zda $\sqrt{3}$ existuje v $\mathbb{F}_p$. Až ti někde bude chybět jedna dvojka, uvědom si, že ω je v příslušném konečném tělese čtverec.

11. S pomocí jednoznačného prvočíselného rozkladu v $\mathbb{Z}[i]$ zjisti, že $x+yi$ je k-tá mocnina. Potom využij toho, že i podmínka $p\mid xy(x^2-y^2)$ určuje v $\mathbb{F}_p[i]$ multiplikativní množinu.

12. Spočítej, kolik prvků $\mathbb{F}_{2^{10}}$ neleží v žádném menším konečném tělese.

Literatura a zdroje

[1] Fíla Čermák a Matěj Doležálek: *Teorie nejen čísel*, seriál MKS, 40. ročník.
[2] Pavel Turek: *Konečná tělesa*, Lysečiny, 2021.
[3] Alexander „Olin“ Slávik: *Konečná tělesa*, Uhelná Příbram, 2014.