Kvadratické rovnice v Z_p

J. Nečas

Abstract. "Higher" algebra textbooks usually don't pay closer attention to the counting praxis in the finite fields. This article discusses one sort of counting tasks in the fields of residue systems by prime module: a solution of quadratic equations. At the end of the article is given an example with a module equal to 13.

Klíčová slova: Konečné těleso, zbytkové třídy podle prvočíselného modulu, odmocnina jako množina, kvadratická rovnice, řešení kvadratické rovnice v konečném tělese.

Symbolem Z budeme označovat obor integrity celých čísel a Z_p budeme značit těleso zbytkových tříd podle modulu p, kde p je liché prvočíslo[1]; struktury a jejich nosiče budeme značit stejně, tedy $Z = \{..., -2, -1, 0, 1, 2, 3, ...\}$, $Z_p = \{0, 1, ..., p - 1\}$. Symboly 0, 1, ..., p - 1 tak budou značit jak celá čísla, tak třídy kongruence podle modulu p, tedy prvky tělesa Z_p; kontext bude volen tak, aby nedošlo k nedorozumění. Rovněž pro binární tělesové operace v Z a v Z_p budeme používat stejné symboly.

Ukážeme, že podobně jako v tělese reálných čísel i v Z_p pro každou kvadratickou rovnici

$$x^2 + rx + s = 0 \qquad (1)$$

nastane právě jedna z možností:

a) rovnice má právě jedno řešení,
b) rovnice má právě dvě řešení,
c) rovnice nemá řešení.

Budeme dále dávat přednost množinovému pojetí pojmu řešení, v tomto pojetí zmíněné možnosti vyjádříme takto:

a) řešení rovnice má právě jeden prvek,
b) řešení rovnice má právě dva prvky,
c) řešení rovnice je prázdná množina.

Každý z koeficientů r, s je prvkem množiny množiny Z_p, a tedy může nabývat p různých hodnot. Znamená to, že v Z_p existuje p^2 různých kvadratických rovnic tvaru (1), a tedy (teoreticky; v praxi pro dostatečně malá p) řešení všech takových rovnic lze vyjádřit čtvercovou tabulkou, v níž např. řádky odpovídají různým hodnotám r a sloupce různým hodnotám s. Na závěr výkladu uvedeme takovou tabulku pro těleso Z_{13}. Článek zakončíme zmínkou o kvadratických rovnicích v Z_2, přičemž využijeme toho, že tam existují jen 4 možné dvojice (r, s) koeficientů v rovnici.

[1] V závěru článku rozšíříme některé závěry i na Z_2.

Nechť p je libovolné liché prvočíslo a $0 < m < p/2$. V oboru integrity celých čísel platí $m^2 - (p - m)^2 = p(2m - p)$; rozdíl je dělitelný číslem p, a tedy v Z_p platí identita

$$m^2 = (p - m)^2. \tag{2}$$

Poněvadž každý nenulový prvek tělesa Z_p, který je druhou mocninou nějakého prvku, je druhou mocninou aspoň dvou prvků, rozpadá se $(p - 1)$-prvková množina všech nenulových prvků tělesa Z_p na dvě neprázdné podmnožiny Q_p a Q'_p; v první jsou ty prvky, které jsou druhými mocninami nějakého prvku, v druhé ty, které druhými mocninami nejsou. Prvky množiny Q_p, resp. Q'_p nazýváme **kvadratickými zbytky**, resp. **kvadratickými nezbytky modulo *p***. Pro počty Card Q_p, resp. Card Q'_p prvků těchto množin podle (2) platí

$$\text{Card } Q_p \leq \text{Card } Q'_p .$$

Není obtížné dokázat, že platí-li pro nenulové prvky $x, y \in Z_p$ rovnost $x^2 = y^2$, pak $x = y$ nebo $x = (p - y)$, a tedy platí dokonce rovnost

$$\text{Card } Q_p = \text{Card } Q'_p = (p - 1)/2 \tag{3}$$

V Z_p můžeme ryze kvadratickou rovnici

$$x^2 + s = 0, \tag{4}$$

přepsat ve tvaru

$$x^2 = \backslash s = t, \tag{5}$$

kde symbol \ vyjadřuje unární minus v Z_p; tedy $\backslash s = 0$, pokud $s = 0$, $\backslash s = p - s$ v ostatních případech. Řešení rovnice (5), a tedy i rovnice (4), je prázdná, resp. jednoprvková, resp. dvouprvková množina, právě když t je kvadratický nezbytek, resp. 0, resp. kvadratický zbytek modulo p. Řešení rovnice (5) nazveme **odmocninou** z prvku t a označíme $\sqrt{t}$. V tomto pojetí tedy odmocnina v Z_p je prázdná, jedno nebo dvouprvková množina.

Věnujme se nyní "obecné" kvadratické rovnici (l) pro libovolný okruh Z_p, kde p je liché prvočíslo. Rovnici (1) upravíme obdobně[2], jako se to dělá v tělese reálných čísel:

$$(x + r/2)^2 = (r/2)^2 - s \tag{6}$$

Počet řešení dané rovnice tvaru (1) bude záležet na tom, zda $(r/2)^2 - s$ je kvadratický zbytek, kvadratický nezbytek či 0, tedy pokud

$(r/2)^2 - s$ je kvadratický zbytek, řešení rovnice (1) má právě 2 prvky,

$(r/2)^2 - s$ je kvadratický nezbytek, řešení rovnice (1) je prázdná množina,

$(r/2)^2 = s$, řešení rovnice (1) má právě 1 prvek.

Řešením rovnice (1) je množina

$$\{x \mid \exists w \in \sqrt{((r/2)^2 - s)} : \; x = \backslash(r/2) + w\}. \tag{7}$$

Z uvedeného výkladu je zřejmé, že mezi p^2 různými rovnicemi tvaru (1) v tělese Z_p je

[2] Výraz a/b znamená totéž jako $a.b^{-1}$; v komutativním tělese lze dělení nenulovým prvkem smysluplně definovat. Je zřejmé, že podobnou konstrukci nelze dělat v Z_2, kde nenulový prvek 2 neexistuje. Požadavek, aby p bylo liché prvočíslo, je tedy podstatný.

$p(p-1)/2$ rovnic majících prázdné řešení,

p rovnic majících jednoprvkové řešení a

$p(p-1)/2$ rovnic majících dvouprvkové řešení.

Jako příklad uveďme řešení kvadratických rovnic v Z_{13}.

Kvadratické zbytky modulo 13 jsou 1, 3, 4, 9, 10 a 12 (viz tabulku 1 druhých mocnin modulo 13; z tabulky je vidět, že zde platí vztah (2)).

Tabulka 1

x	0	1	2	3	4	5	6	7	8	9	10	11	12
x^2	0	1	4	9	3	12	10	10	12	3	9	4	1

Tabulka 2 uvádí hodnoty výrazů $(r/2)$, \(r/2), $(r/2)^2$ a $(r/2)^2 - s$ pro různé dvojice (r, s), přičemž typem písma jsou odlišeny kvadratické zbytky, nuly a kvadratické ne-zbytky.

Tabulka 2

				s												
r	r /2	\r /2	(r /2)^2	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	**0**	12	11	10	9	8	7	6	5	4	3	2	1
1	7	6	10	10	9	8	7	6	5	4	3	2	1	**0**	12	11
2	1	12	1	1	**0**	12	11	10	9	8	7	6	5	4	3	2
3	8	5	12	12	11	10	9	8	7	6	5	4	3	2	1	**0**
4	2	11	4	4	3	2	1	**0**	12	11	10	9	8	7	6	5
5	9	4	3	3	2	1	**0**	12	11	10	9	8	7	6	5	4
6	3	10	9	9	8	7	6	5	4	3	2	1	**0**	12	11	10
7	10	3	9	9	8	7	6	5	4	3	2	1	**0**	12	11	10
8	4	9	3	3	2	1	**0**	12	11	10	9	8	7	6	5	4
9	11	2	4	4	3	2	1	**0**	12	11	10	9	8	7	6	5
10	5	8	12	12	11	10	9	8	7	6	5	4	3	2	1	**0**
11	12	1	1	1	**0**	12	11	10	9	8	7	6	5	4	3	2
12	6	7	10	10	9	8	7	6	5	4	3	2	1	**0**	12	11

Zmínili jsme, že řešení kvadratické rovnice (1) může být pro jednotlivé hodnoty uspořádaných dvojic (r, s) vyjádřeno tabulkou; pro Z_{13} je vyjadřuje tabulka 3; složené "množinové" závorky a čárky mezi prvky dvouprvkových množin jsou v ní z grafických důvodů vynechány.

Tabulka 3

s	0		1		2		3		4		5		6		7		8		9		10		11		12	
r																										
0	0		8	5	Ø		7	6	3	10	Ø		Ø		Ø		Ø		11	2	4	9	Ø		1	12
1	12	0	3	9	Ø		Ø		Ø		Ø		8	4	2	10	Ø		5	7	6		1	11	Ø	
2	0	11	12		4	7	Ø		5	6	9	2	Ø		Ø		Ø		Ø		1	10	8	3	Ø	
3	10	0	Ø		11	12	2	8	Ø		Ø		Ø		Ø		7	3	1	9	Ø		4	6	5	
4	0	9	7	2	Ø		10	12	11		6	3	Ø		5	4	1	8	Ø		Ø		Ø		Ø	
5	8	0	Ø		5	3	4		9	12	Ø		10	11	1	7	Ø		Ø		Ø		Ø		6	2
6	0	7	Ø		Ø		Ø		Ø		8	12	1	6	Ø		11	9	10		2	5	Ø		3	4
7	6	0	Ø		Ø		Ø		Ø		1	5	7	12	Ø		4	2	3		8	11	Ø		9	10
8	0	5	Ø		10	8	9		1	4	Ø		2	3	6	12	Ø		Ø		Ø		Ø		11	7
9	4	0	11	6	Ø		1	3	2		10	7	Ø		9	8	5	12	Ø		Ø		Ø		Ø	
10	0	3	Ø		1	2	5	11	Ø		Ø		Ø		Ø		10	6	4	12	Ø		7	9	8	
11	2	0	1		6	9	Ø		7	8	11	4	Ø		Ø		Ø		Ø		3	12	10	5	Ø	
12	0	1	4	10	Ø		Ø		Ø		Ø		9	5	3	11	Ø		6	8	7		2	12	Ø	

Jak jsme již zmínili, článek zakončíme zmínkou o řešení rovnice (1) v Z_2. Koeficienty r a s nabývají hodnot 0 a 1, a tak po jejich dosazení rovnice má jeden ze čtyř tvarů $x^2 = 0$, $x^2 + 1 = 0$, $x^2 + x = 0$, $x^2 + x + 1 = 0$. Řešením těchto rovnic jsou po řadě množiny $\{0\}$, $\{1\}$, $\{0, 1\}$, ø. Uvedené tvrzení o počtu prázdných, jedno a dvouprvkových řešení v Z_p tedy platí i pro $p = 2$.

Literatura

[1] BIRKHOFF, G., BARTEE, T.C.: Sovtremennaja prikladnaja algebra. Moskva, Mir 1976.
[2] KOŘÍNEK, V.: Základy algebry. Praha, NČSAV 1956.
[3] PRIJATELJ, N.: Matematične strukture II. Operacije. Ljubljana, Mladinska knjiga 1967.
[4] PROCHÁZKA, L. aj.: Algebra. Praha, Academia 1990.
[5] RYCHLÍK, K.: Úvod do elementární číselné teorie. Praha, JČMF - Přírodovědecké nakladatelství 1950.
[6] https://cs.wikipedia.org/wiki/Modul%C3%A1rn%C3%AD_aritmetika
[7] http://www.cam.zcu.cz/~ryjacek/students/DMA/skripta/2.pdf
[8] http://math.feld.cvut.cz/demlova/teaching/dml/pred11.pdf

RNDr. Jiří Nečas
Department of Mathematics
University of Economics
Ekonomická 957
148 00 Prague 4
e-mail: *necas@vse.cz*

Opravy typu písma:
07.08.2024