Primitivní kořeny a kvadratické nezbytky

J. Nečas

Abstract. The article deals with the relationship of the primitive roots, the quadratic non-residues and the Fermat primes. It uses some simple knowledge of the algebra of finite fields.

Klíčová slova. Mathematics Eulerova funkce, kvadratické zbytky a nezbytky, primitivní kořeny, Fermatova čísla

1 Úvod

1.1. V tomto článku se budeme pohybovat především v tělesech Z_p zbytkových tříd modulo p, kde p je liché prvočíslo[1], a to především v jejich multiplikativních grupách[2] M_p. Prvky těchto struktur budeme označovat čísly 0, 1, ..., p-1, resp. 1, 2, ..., p-1. Některé závěry pak budeme formulovat "řečí" oboru integrity celých čísel. Nejdříve připomeňme některé pojmy, jimž se dále budeme věnovat.

Nechť tedy p je libovolné liché prvočíslo. V multiplikativní grupě M_p můžeme pracovat s celočíselnými mocninami; pro libovolný prvek a položíme:

$$a^0 = 1,$$
$$a^n = a.a^{n-1} \quad \text{pro } n > 0,$$
$$a^n = (a^{-n})^{-1} \quad \text{pro } n < -1,$$

přičemž a^{-1} je inverzní prvek k prvku a.

Jako příklad v odd. 5 uvádíme tabulky n-tých (n = 0, 1, 2, p-1) mocnin nenulových prvků v grupách M_p pro p = 3, 5, 7, 11, 13 a 17.

1.2. Protože grupa M_p má p-1 prvků, mezi mocninami libovolného prvku a může být nejvýše p-1 různých hodnot. Grupa M_p je cyklická[3]; protože p je liché prvočíslo, má M_p sudý počet prvků. Generátory grupy M_p se nazývají **primitivními kořeny modulo *p*.** Množinu všech primitivních kořenů modulo p označme PK_p.

Příklad (viz tabulku mocnin - odd. 5): $PK_3 = \{2\}$, $PK_5 = \{2, 3\}$, $PK_7 = \{3, 5\}$ $PK_{11} = \{2, 6,7, 8\}$, $PK_{13} = \{2, 6, 7, 11\}$ $PK_{17} = \{3, 5, 6, 7, 10, 11, 12, 14\}$. Primitivní kořeny jsou v levém sloupci vyznačeny polotučnou kurzívou.

[1] Těleso Z_2 z úvah vylučujeme především proto, že jeho multiplikativní grupa je jednoprvková, a tudíž nezajímavá.

[2] Nebudeme rozlišovat označení struktury a jejího nosiče, tedy M_p bude označovat jak multiplikativní grupu, tak (p-1)-prvkovou množinu všech jejích prvků.

[3] Toto není triviální tvrzení; bez použití grupové terminologie je dokázáno např. v knize [3], kap. IV, §2

2 Kvadratické zbytky a kvadratické nezbytky

2.1. Nechť p je liché prvočíslo a $m < p/2$. Platí

$$m^2 = (p - m)^2. \qquad (1)$$

Tuto identitu ověřím snadno, přejdeme-li do oboru integrity celých čísel, kde ověříme, že $m^2 \equiv (p - m)^2 \bmod p$, tedy že $p|(m^2 - (p - m)^2)$, což plyne ze známého vztahu pro rozdíl druhých mocnin $m^2 - (p - m)^2 = p.(2m - p)$.

2.2. Množina všech prvků grupy M_p se tedy rozpadá na dvě 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.** Pro počty Card Q_p,resp. Card Q'_p prvků těchto množin ze vztahu (1) plyne:

$$\text{Card } Q_p \leq \text{Card } Q'_p. \qquad (2)$$

Není obtížné dokázat, že platí-li v M_p rovnost $x^2 = y^2$, pak $x = y$ nebo $x = (p - y)$, a tedy platí dokonce rovnost

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

Příklad (viz druhé mocniny v tabulce mocnin - odd.5): $Q'_3 = \{2\}$, $Q'_5 = \{2, 3\}$, $Q'_7 = \{3, 5, 6\}$, $Q'_{11} = \{2, 6, 7, 8, 10\}$, $Q'_{13} = \{2, 5, 6, 7, 8, 11\}$, $Q'_{17} = \{3, 5, 6, 7, 10, 11, 12, 14\}$.

2.3. Porovnáme-li příklady množin PK_r a Q'_r (r = 3, 5, 7, 11, 13, 17), vidíme, že v uvedených případech platí $PK_r \subseteq Q'_r$, přičemž pro r = 3, 5 a 17 zde platí rovnost, zatímco v případech r = 7, 11 a 13 platí ostrá inkluze. Inkluze $PK_r \subseteq Q'_r$ platí pro všechna lichá prvočísla r, neboť kvadratický zbytek nemůže být primitivním kořenem (a tedy generátorem grupy M_p)[4]. Naším cílem bude odpověď na otázku, pro jaká lichá prvočísla r zde platí rovnost.

3 Eulerova funkce

3.1. Pro kladná přirozená čísla n definujeme **Eulerovu funkci** $\varphi(n)$ tak, že $\varphi(n)$ vyjadřuje počet přirozených čísel, která jsou menší nebo rovna[5] číslu n a s číslem n jsou nesoudělná[6].

3.2. *Některé vlastnosti Eulerovy funkce.* Platí $\varphi(1)$=1. Pro každé prvočíslo p a každé kladné přirozené číslo n je $\varphi(p^n) = (p\text{-}1)p^{n-1}$, speciálně tedy $\varphi(p) = p\text{-}1$. Jsou-li přirozená čísla m a n nesoudělná, platí rovnost $\varphi(mn) = \varphi(m)\varphi(n)$. Pro každé přirozené číslo n>2 je

---

[4] Nechť b je kvadratickým zbytkem v grupě M_p, $b = a$^2. Podle Eulerovy věty musí platit

$$a\text{^}(p-1) = a\text{^}(2*((p-1)/2)) = (a\text{^}2)\text{^}((p-1)/2)) = b\text{^}((p-1)/2)),$$

a tedy b není generátorem grupy M_p (mocnitel $(p-1)/2$ má smysl, protože $p-1$ je sudé číslo). K symbolu ^ viz pozn. 7.

[5] Možnost rovnosti argumentu zde požadujeme kvůli smysluplnosti definice funkce $\varphi(n)$ pro n=1; požadujeme, aby $\varphi(1)$ =1.

[6] Funkce φ se někdy též nazývá Gaussovou funkcí, např. v knize [5].

$\varphi(n)$ sudé číslo. Ze zmíněných vlastností Eulerovy funkce plyne, že pro $n = p_1\text{^}a_1 \ldots p_k\text{^}a_k$ je[7]

$$\varphi(n) = (p_1\text{-}1)p_1\text{^}(a_1\text{-}1) \ldots (p_k\text{-}1)p_k\text{^}(a_k\text{-}1)\,. \tag{4}$$

Z vyjádření $\varphi(n)$ ve tvaru (4) plyne, že hodnota podílu $\varphi(n)/n$ závisí jen na tom, jaká prvočísla se v prvočíselném rozkladu čísla n vyskytují; nezávisí tedy na tom, v jakých mocninách se tam tato prvočísla vyskytují. Pokud se v prvočíselném rozkladu čísla n vyskytují prvočísla $p_1, \ldots, p_k$ a žádné jiné, pak

$$\varphi(n)/n = (1 - p_1^{-1}). \ldots .(1 - p_k^{-1}). \tag{5}$$

Dalším důsledkem vyjádření $\varphi(n)$ ve tvaru (4) (popř. $\varphi(n)/n$ ve tvaru (5)) je, že pro libovolné sudé číslo s platí nerovnost

$$\varphi(s) \leq s/2, \tag{6}$$

přičemž rovnost nastane, právě když s je mocninou čísla 2.

3.3. Eulerova funkce se využívá při studiu primitivních kořenů. Ze základních vlastností cyklických grup totiž plyne tvrzení: Je-li nějaký prvek a generátorem grupy M_p, pak platí, že a^r je také generátorem grupy M_p, právě když čísla r a řád grupy (tedy p-1) jsou čísla nesoudělná. To ovšem znamená, že grupa M_p má právě tolik generátorů, kolik je čísel menších než p - 1 a s p - 1 nesoudělných, tedy

$$\text{Card PK}_p = \varphi(p\text{-}1). \tag{7}$$

4 Fermatova čísla

4.1. n-tým **Fermatovým číslem** nazýváme číslo F_n tvaru $2\text{^}2^n + 1$. Pokud je Fermatovo číslo prvočíslem, mluvíme o **Fermatově prvočísle**.

4.2. Prvních pět Fermatových čísel jsou prvočísla:

$F_0 = 2^1 + 1 = 3$
$F_1 = 2^2 + 1 = 5$
$F_2 = 2^4 + 1 = 17$
$F_3 = 2^8 + 1 = 257$
$F_4 = 2^{16} + 1 = 65\,537$

Jiná Fermatova prvočísla dosud známa nejsou. Pro informaci uveďme další čtyři Fermatova čísla (včetně rozkladu na součin)[8]:

$F_5 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417$
$F_6 = 2^{64} + 1 = 18\,446\,744\,073\,709\,551\,617$
$= 274\,177 \times 67\,280\,421\,310\,721$
$F_7 = 2^{128} + 1 = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,211\,457$
$= 59\,649\,589\,127\,497\,217 \times 5\,704\,689\,200\,685\,129\,054\,721$

[7] Symbolem ^ označujeme (v souladu s běžnou praxí v programovacích jazycích) mocninu; výrazy x^y a $x\text{^}y$ tedy znamenají totéž (včetně vyšší priority mocniny před násobením, a tedy samozřejmě i před sčítáním)
[8] Podle [6]

$F_8 = 2^{256} + 1 = 115\ 792\ 089\ 237\ 316\ 195\ 423\ 570\ 985\ 008\ 687\ 907\ 853\ 269\ 984$
$665\ 640\ 564\ 039\ 457\ 584\ 007\ 913\ 129\ 639\ 937$
$= 1\ 238\ 926\ 361\ 552\ 897 \times 93\ 461\ 639\ 715\ 357\ 977\ 769\ 163\ 558\ 199\ 606\ 896$
$584\ 051\ 237\ 541\ 638\ 188\ 580\ 280\ 321$

4.3. V článku [2] se mluví o Mersennových číslech, resp. o Mersennových prvočíslech, tj. o číslech (resp. prvočíslech) tvaru 2^k-1. Naskýtá se otázka, kdy čísla tvaru 2^k+1 mohou být prvočísly. Pro k=0 a k=1 o prvočísla jde. Nechť tedy k>1. Jestliže k není tvaru 2^n, musí v prvočíselném rozkladu čísla k existovat aspoň jedno liché číslo, tedy $k = u.t$, kde u je liché číslo, $u > 1$ (t může být i 1). Pak

$$2^k + 1 = (2^t)^u + 1 = (2^t + 1)((2^t)^{u-1} - (2^t)^{u-2} + ... + 1) \qquad (8)$$

je rozklad čísla 2^k+1 na součin dvou činitelů větších než 1. Nutnou podmínkou k tomu, aby číslo tvaru 2^k+1 bylo prvočíslem, tedy je, že mocnitel k musí být mocninou čísla 2. To však znamená, že čísla tvaru 2^k+1 jsou prvočísly, právě když jsou Fermatovými prvočísly.

4.4. Uvedli jsme, že pro všechna lichá prvočísla r platí inkluze $PK_r \subseteq Q'_r$. V příkladech, které jsme uvedli, platí rovnost pro r = 3, 5 a 17, tedy pro F_0, F_1, F_2, zatímco pro r = 7, 11 a 13, tedy pro prvočísla, která nejsou prvočísly Fermatovými, nastává ostrá inkluze. To není náhoda. Platí totiž věta, k níž směřuje celý tento článek:

4.5. Nechť r je libovolné liché prvočíslo. Pak $PK_r = Q'_r$, právě když r je Fermatovo prvočíslo.

Větu nyní dokažme. Vzhledem k platnosti inkluze $PK_r \subseteq Q'_r$ stačí dokázat, že rovnost Card PK_r = Card Q'_r platí, právě když r je Fermatovo prvočíslo. Uvedli jsme, že Card $Q'_r = (r-1)/2$, Card $PK_r = \varphi(r-1)$. Jde tedy o to dokázat, že $\varphi(r-1) = (r-1)/2$, právě když r je Fermatovo prvočíslo. Na konci odd. 3.2 jsme ovšem zmínili, že tato rovnost platí, právě když r-1 je mocninou 2, tedy r musí mít tvar 2^k+1, což podle odd. 4.3 je ekvivalentní s podmínkou, že r musí být Fermatovým prvočíslem.

5 Tabulka mocnin prvků ve vybraných grupách M_p

Primitivní kořeny jsou vytištěny polotučně kurzívou; *a* je základ, *n* exponent.

p= 5

n	0	1	2	3	4
a					
1	1	1	1	1	1
2	1	2	4	3	1
3	1	3	4	2	1
4	1	4	1	4	1

p= 3

n	0	1	2
a			
1	1	1	1
2	1	2	1

p= 7

n	0	1	2	3	4	5	6
a							
1	1	1	1	1	1	1	1
2	1	2	4	1	2	4	1
3	1	3	2	6	4	5	1
4	1	4	2	1	4	2	1
5	1	5	4	6	2	3	1
6	1	6	1	6	1	6	1

p= 11

n	0	1	2	3	4	5	6	7	8	9	10
a											
1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	5	10	9	7	3	6	1
3	1	3	9	5	4	1	3	9	5	4	1
4	1	4	5	9	3	1	4	5	9	3	1
5	1	5	3	4	9	1	5	3	4	9	1
6	1	6	3	7	9	10	5	8	4	2	1
7	1	7	5	2	3	10	4	6	9	8	1
8	1	8	9	6	4	10	3	2	5	7	1
9	1	9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1	10	1

p= 13

n	0	1	2	3	4	5	6	7	8	9	10	11	12
a													
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	3	6	12	11	9	5	10	7	1
3	1	3	9	1	3	9	1	3	9	1	3	9	1
4	1	4	3	12	9	10	1	4	3	12	9	10	1
5	1	5	12	8	1	5	12	8	1	5	12	8	1
6	1	6	10	8	9	2	12	7	3	5	4	11	1
7	1	7	10	5	9	11	12	6	3	8	4	2	1
8	1	8	12	5	1	8	12	5	1	8	12	5	1
9	1	9	3	1	9	3	1	9	3	1	9	3	1
10	1	10	9	12	3	4	1	10	9	12	3	4	1
11	1	11	4	5	3	7	12	2	9	8	10	6	1
12	1	12	1	12	1	12	1	12	1	12	1	12	1

p= 17

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a																	
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1
3	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
4	1	4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1
5	1	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1
6	1	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1
7	1	7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
8	1	8	13	2	16	9	4	15	1	8	13	2	16	9	4	15	1
9	1	9	13	15	16	8	4	2	1	9	13	15	16	8	4	2	1
10	1	10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1
11	1	11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1
12	1	12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1
13	1	13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1
14	1	14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1
15	1	15	4	9	16	2	13	8	1	15	4	9	16	2	13	8	1
16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1

Literatura

[1] KŘÍŽEK, M., SOMER, L., ŠOLCOVÁ, A.: Kouzlo čísel. Praha, Academia 2009.
[2] NEČAS, J.: *Some Remarks on Trigonal and Perfect Numbers*. Mundus Symbolicus 23, 2015
[3] MICHELOVIČ, Š. Ch.: Teorija čisel. Moskva, Vysšaja škola 1967.
[4] RYCHLÍK, K.: Úvod do elementární číselné teorie. Praha, JČMF - Přírodovědecké nakladatelství 1950
[5] SIERPIŃSKI, W.: Arytmetyka Teoretyczna. Warszawa, PWN 1968.
[6] https://cs.wikipedia.org/wiki/Fermatovo_%C4%8D%C3%ADslo

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