

Multiplikativní grupy zbytkových tříd

Pavel Hrubý 2021

Obsah

1	Přehled značení v této publikaci.....	1
2	Úvod	2
3	Základní předpoklady	2
3.1	Grupy zbytkových tříd modulo p	2
3.2	Řád grupy, řád prvku, generátory a Lagrangeova věta	3
3.3	Direktní součin grup	4
3.4	p -grupy a Sylowovy věty.....	4
4	Cyklické grupy.....	5
5	Faktorové grupy cyklických grup	5
6	Primitivní kořeny	6
7	Generátory cyklických grup	8
8	Automorfismy cyklických grup	8
9	Diskrétní logaritmy	15
10	Odmocniny z jedné	16
11	Dirichletovy charaktery	19
12	Fermatova čísla.....	22
12.1	Vlastnosti Fermatových čísel	22
13	Experimenty	23
13.1	Zobrazení grupy na množinu generátorů.....	23
13.2	Symetrie a model čtyř prvků v tělese T_p	27
13.3	Izomorfismy multiplikativních grup se sudými řády.....	34
13.4	Nadgrupy	40
14	Ilustrace	41
15	Závěr	43
16	Literatura	44

1 Přehled značení v této publikaci

p	... prvočíslo
$\mathbf{P}$	... množina všech prvočísel
$\mathbf{Z}$	... množina celých čísel
$\varphi()$	... Eulerova funkce
$\mathbf{Z}_m^+$	... aditivní grupa s m prvky
$\mathbf{Z}_m^*$	... multiplikativní cyklická grupa s $\varphi(m)$ prvky
$\mathbf{Z}_p^*$	... multiplikativní cyklická grupa s $p-1$ prvky
$\mathbf{G}_p$	... množina generátorů grupy $\mathbf{Z}_p^*$
$\langle g \rangle$	... cyklická grupa generovaná prvkem g
$\mathbf{Z}_{n/p}, \mathbf{N}_{n/p}$	... podgrupa řádu n grupy $\mathbf{Z}_p^*$
$\text{ord}(a)$	... řád prvku a
$\text{ord}(\mathbf{N})$	... řád grupy $\mathbf{N}$
$\chi_q(n, \cdot)$	... Dirichletův charakter
$\widehat{\mathbf{G}}_p$	... množina Dirichletových charakterů grupy $\mathbf{Z}_p^*$
ξ_n	... n – tá odmocnina z 1 , $\xi_n = e^{\frac{2\pi}{n}}$
μ_n	... grupa n – tých odmocnin z 1
F_n	... n – té Fermatovo číslo, $F_n = 2^{2^n} + 1$
$\log_g Y$	... diskrétní logaritmus o základu g
$\text{Aut}(\mathbf{Z}_m^*)$	... grupa automorfismů grupy $\mathbf{Z}_m^*$

2 Úvod

Tento text vznikl v rámci mého opakování základů algebry, zejména specializované části Abelových grup. Důkazy vět nepřepisují z původních publikací. Jejich bibliografie je uvedena na konci tohoto textu. Pokud některé tvrzení není v publikacích obsaženo, pak následuje jeho důkaz. Jednotlivé kapitoly jsou uspořádány tak, jak jsem při opakování postupoval a jak jsem se prokousával starými i novými definicemi a pojmy. Kapitoly jsou doplněny ukázkami, zde je nazývám ilustrace, které mi snad pomohli pochopit obsah a vzájemné vztahy matematických abstrakcí.

Celá publikace je zaměřena na porozumění složitosti komutativních cyklických grup zejména ve vyjádření zbytkových tříd celých čísel.

Předpokladem pro porozumění tomuto textu je absolvování některého základního vysokoškolského kurzu algebry s pojmy monoid, grupoid, grupa, okruh, obor integrity, těleso, morfismus a dalšími termíny, které se k těmto matematickým objektům váží. Též se předpokládá znalost základních vztahů z modulární aritmetiky.

3 Základní předpoklady

A teď rychlé shrnutí některých pojmů a tvrzení.

3.1 Grupy zbytkových tříd modulo p

Zbytkové třídy modulo p budeme značit číslicemi $1, 2, 3, \dots, m$, kde příslušná cifra znamená nekonečnou množinu danou předpisem $t = \{a \in \mathbb{Z} : a \equiv t \pmod{p}, 0 \leq t \leq p-1\}$

1. Definice

Zbytkovou třídou modulo n rozumíme množinu všech celých čísel, které při dělení přirozeným číslem n dávají stejný zbytek. Tuto množinu pak můžeme chápat jako jeden celek a celá čísla, která obsahuje, již dále nerozlišovat.

Ilustrace

Zbytkové třídy modulo 5

$$0 = \{0, 5, 10, \dots\}$$

$$1 = \{1, 6, 11, \dots\}$$

$$2 = \{2, 7, 12, \dots\}$$

$$3 = \{3, 8, 13, \dots\}$$

$$4 = \{4, 9, 14, \dots\}$$

$$\text{a pro operaci sčítání zbytkových tříd } 1 + 3 \pmod{5} = \{4, 9, 14, 9, \dots\} \pmod{5} = 4$$

$$\text{a pro operaci násobení zbytkových tříd } 2 * 3 \pmod{5} = \{1, 6, 16, 21, \dots\} \pmod{5} = 1$$

2. Tvrzení

Množina zbytkových tříd modulo p s operacemi sčítání a násobení zbytkových tříd tvoří těleso. Budeme značit T_p .

Ilustrace

Těleso T_5 a vyjádření operací Cayleyho tabulkami:

Aditivní grupa T_5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplikativní grupa T_5

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

kde 0 je neutrální prvek aditivní grupy a 1 je neutrální prvek multiplikativní grupy.

3. Tvzení

T_p je těleso právě tehdy, když p je prvočíslo.

Ilustrace

Pokud by p nebylo prvočíslo, pak se v multiplikativní tabulce objeví dělitelé 0.

4. Definice

Matematický objekt Z_p^* nazveme multiplikativní grupou zbytkových tříd modulo p , kde p je prvočíslo.

5. Definice

Abelova (komutativní) grupa G , která nemá prvky nekonečného řádu, se nazývá periodická (neboli torzní) grupa.

3.2 Řád grupy, řád prvku, generátory a Lagrangeova věta

6. Definice

Řádem grupy G se rozumí počet prvků její nosné množiny, značíme jej $|G|$ (tj., formálně vzato, $|G| = |G|$).

7. Definice

Řádem prvku a v grupě G se rozumí nejmenší $n \in \mathbb{N}$ takové, že $a^n = 1$, pokud takové n existuje. Značíme $\text{ord}(a) = n$.

8. Definice

Uvažujme podmnožinu $X \subset G$ grupy G . Podgrupou generovanou množinou X rozumíme nejmenší podgrupu H (vzhledem k inkluzi) grupy G obsahující podmnožinu X , značíme ji $\langle X \rangle_G$. Prvky množiny X nazveme generátory podgrupy H .

9. Tvzení

Buď G grupa a $a \in G$. Pak řád prvku grupy je roven řádu podgrupy generované tímto prvkem, tj. $\text{ord}(a) = |\langle a \rangle|$.

Ilustrace

* mod 7	1	2	3	4	5	6	řád prvku
1	1	2	3	4	5	6	1
2	2	4	6	1	3	5	3
3	3	6	2	5	1	4	6
4	4	1	5	2	6	3	3
5	5	3	1	6	4	2	6
6	6	5	4	3	2	1	2

Podgrupu $N_{3/7} = \{1, 2, 4\}$ řádu 3 generuje prvek 2, který má řád 3.

10. Věta (Lagrangeova věta)

Buď G konečná grupa a H její podgrupa. Pak řád podgrupy H dělí řád grupy G , tj. $|H| \mid |G|$.

11. Důsledek

Řád prvku grupy dělí řád grupy, tj. $\text{ord}(a) \mid |G|$ pro každé $a \in G$.

12. Důsledek

Řád prvku $a \in H$ podgrupy grupy G dělí řád této podgrupy, tj. $\text{ord}(a) \mid |H|$ pro každé $a \in H$.

13. Lemma

Průnik podgrup je podgrupa.

3.3 Direktní součin grup

14. Definice

Mějme grupy A, B . Množina G všech uspořádaných dvojic (a, b) , $a \in A, b \in B$, spolu s binární operací $(a_1, b_1) \times (a_2, b_2) = (a_1 \circ a_2, b_1 * b_2)$ je opět grupou, kterou nazveme vnější direktní součin grup A, B a značíme ji $A \times B = G$.

15. Definice

Mějme dvě aditivní normální podgrupy A, B grupy G . Pokud $A \vee B = G$, $A \cap B = \{1\}$, řekneme, že G je vnitřním direktním součinem grup A, B , a značíme ho $A \times B = G$.

16. Věta

Direktní součin dvou cyklických aditivních grup Z_m^+, Z_n^+ nesoudělných řádů m, n je cyklickou aditivní grupou řádu mn .

3.4 p-grupy a Sylowovy věty

17. Definice

Konečná grupa řádu p^n , $n \in \mathbb{N}$, kde p je prvočíslo, je nazývána p -grupou.

18. Věta

Každá grupa, která je periodická (cyklická), je direktním součinem svých p -primárních komponent.

19. Definice

Mějme grupu G řádu $p^a \cdot b$, kde $(p, b) = 1$. Potom každá podgrupa grupy G řádů p^a se nazývá Sylowovská p -grupa grupy G .

20. Věta

Nechť aditivní grupa G je konečnou grupou řádu a a p je prvočíslo, které dělí a . Potom G obsahuje sylowovskou p -podgrupu.

21. První Sylowova věta

Každá p -podgrupa A konečné aditivní grupy B je obsažena v některé sylowovské podgrupě grupy B .

22. Druhá Sylowova věta

Každé dvě sylowovské p -podgrupy konečné grupy B jsou konjugované.

23. Třetí Sylowova věta

Mějme konečnou aditivní grupu B a p je prvočíslo, které dělí řád grupy B . Potom počet všech sylowovských aditivních p -podgrup grupy B dělí $o(B)$ (řád grupy B) a je roven $1 + zp$, kde z je nějaké určité nezáporné číslo.

4 Cyklické grupy

24. Definice

Grupa G se nazývá cyklická, pokud je generovaná jedním prvkem, tj. $G = \langle a \rangle$ pro nějaké $a \in G$. Prvky a nazveme generátory grupy G .

Ilustrace

$$\langle 3 \rangle = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\} \bmod 7 = \{3, 2, 6, 4, 5, 1\}$$

25. Tvzení

Každá podgrupa cyklické grupy je cyklická.

26. Tvzení

Buď $G = \langle a \rangle$ cyklická grupa, kde a je generátor grupy. Pokud je nekonečná, generátorem jsou pouze prvky a ; a^{-1} .

Pokud je konečná řádu n , generátory jsou právě prvky a^k pro $k \in \{1; \dots; n-1\}$, kde k je nesoudělné s n .

27. Věta (Cauchyova věta)

Buď G konečná grupa a p prvočíslo, které dělí $|G|$. Pak v G existuje prvek řádu p .

28. Tvzení

Cyklická grupa konečného řádu n obsahuje právě $\varphi(d)$ prvků řádu d pro každé $d \mid n$.

29. Tvzení

Pro každé $n \in \mathbb{N}$ platí $\sum_{d \mid n} \varphi(d) = n$.

30. Tvzení

Nechť $d \mid n$, kde n je řád cyklické grupy G , $n = |G|$. Pak pro každého dělitele d existuje právě jedna podgrupa grupy G řádu d .

31. Tvzení – izomorfismus Z_m^* a $Z_{\varphi(m)}^+$

Nechť Z_m^* je cyklická multiplikativní grupa. Pak je izomorfní s aditivní grupou $Z_{\varphi(m)}^+$.

32. Lemma

Buď G konečná grupa a předpokládejme, že pro každé k existuje v G nejvýše k prvků a splňujících $a^k = 1$. Pak je grupa G cyklická.

33. Tvzení

Nechť Z_m^* je cyklická multiplikativní grupa která obsahuje všechny zbytkové třídy $1, 2, 3, \dots, m-1$. Pak m je prvočíslo.

34. Důsledek

Multiplikativní cyklická grupa Z_p^* , kde p je prvočíslo, má řád $p-1$.

5 Faktorové grupy cyklických grup

35. Definice rozkladové třídy

Buď G grupa a H její podgrupa:

- množiny $aH = \{ah : h \in H\}$, kde $a \in G$, se nazývají (levé) rozkladové třídy podgrupy H ;

- podmnožina $T \subseteq G$ s vlastností $|T \cap aH| = 1$ pro každé $a \in G$ se nazývá **transverzála rozkladu** G podle H .
- počet rozkladových tříd se nazývá index podgrupy H v grupě G a značí se $[G : H] = |\{aH : a \in G\}|$;

36. Lemma

Buď G grupa a H její podgrupa. Pro každé $a, b \in G$ platí buď $aH = bH$, nebo $aH \cap bH = \emptyset$.

37. Lemma (velikost rozkladových tříd).

Buď G grupa a H její podgrupa. Pro každé $a \in G$ platí $|aH| = |H|$.

38. Věta (Lagrangeova věta).

Buď G grupa a H její podgrupa. Pak $|G| = |H| \cdot [G : H]$.

39. Tvzení

Rozkladové třídy podgrupy H grupy G tvoří grupu. Tuto grupu nazýváme faktorová grupa nebo faktorgrupa.

6 Primitivní kořeny

40. Definice Primitivní kořen

Primitivní kořen modulo n je takové číslo g , pokud pro každé celé číslo a nesoudělné s n existuje takové celé číslo k , pro které platí $g^k \equiv a \pmod{n}$.

tj. Necht' $n \in \mathbb{N}$. Celé číslo $g \in \mathbb{Z}$, $(g, n) = 1$ nazveme primitivním kořenem modulo n , pokud je jeho řád modulo n roven $\varphi(n)$.

Ilustrace

Číslo 3 je primitivní kořen modulo 7 protože:

$$3^0 = 1 \equiv 1 \pmod{7}$$

$$3^1 = 3 \equiv 3 \pmod{7}$$

$$3^2 = 9 \equiv 2 \pmod{7}$$

$$3^3 = 27 \equiv 6 \pmod{7}$$

$$3^4 = 81 \equiv 4 \pmod{7}$$

$$3^5 = 243 \equiv 5 \pmod{7}$$

$$3^6 = 729 \equiv 1 \pmod{7}$$

$$3^7 = 2187 \equiv 3 \pmod{7}$$

Vlastnosti:

- s rostoucím k se zbytek $3^k \bmod 7$ opakuje v konečné množině čísel, v tomto případě $\{1, 3, 2, 6, 4, 5\}$.
- jejich počet je konečný, menší než n , nazývá se *perioda* $g^k \bmod n$
- žádný zbytek po dělení není nulový
- 3^k má k modulo 7 statisticky rovnoměrnou distribuci
- vlastnost používaná v šifrování – pouze ze znalosti zbytku po dělení nelze zpětně určit g a k

Poznámka

Primitivní kořen modulo p v multiplikativní cyklické grupě Z_p^* je tedy generátorem této grupy.

41. Lemma

Je-li g primitivní kořen modulo m , pak pro každé číslo $a \in Z$, $(a, m) = 1$ existuje jediné $x_a \in Z$, $0 \leq x_a < \varphi(m)$ s vlastností $g^{x_a} \equiv a \pmod{m}$.

42. Věta

Buď $m \in N$ takové, že modulo m existují primitivní kořeny. Dále nechť $a \in Z$, $(a, m) = 1$. Pak kongruence $x^n \equiv a \pmod{m}$ je řešitelná (tj. a je n -tý mocninný zbytek modulo m), právě když

$a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$, kde $d = (n, \varphi(m))$. Přitom, je-li tato kongruence řešitelná, má právě d řešení.

43. Věta

Buď $m \in N$, $m > 1$. Primitivní kořeny modulo m existují právě tehdy, když m splňuje některou z následujících podmínek:

- $m = 2$ nebo $m = 4$,
- m je mocnina lichého prvočísla
- m je dvojnásobek mocniny lichého prvočísla.

44. Věta

Buď m takové, že modulo m existují primitivní kořeny. Zapišme $\varphi(m) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$. Pak pro libovolné $g \in Z$, $(g, m) = 1$ platí, že g je primitivní kořen modulo m , právě když

$$g^{\frac{\varphi(m)}{p_1}} \not\equiv 1 \pmod{m} \quad \dots \quad g^{\frac{\varphi(m)}{p_k}} \not\equiv 1 \pmod{m}.$$

45. Tvzení

Cyklické grupy jsou pouze grupy izomorfní s grupami $Z_2^*, Z_4^*, Z_{p^k}^*, Z_{2p^k}^*$.

46. Lemma.

Buď p liché prvočíso, $k \geq 2$ libovolné. Pak pro libovolné $a \in Z$ platí $(1 + ap)^{k-2} \equiv 1 + ap^{k-1} \pmod{p^k}$.

47. Tvzení (Henri Cohen)

Buď p liché prvočíso a g primitivní kořen modulo p^k pro $k \in N$. Pak liché z čísel $g, g + p^k$ je primitivním kořenem modulo $2p^k$.

48. Lemma

- Buď $k \in N$, $k \geq 3$. Pak $5^{k-3} \equiv 1 + 2^{k-1} \pmod{2^k}$
- Řád čísla 5 modulo 2^k je 2^{k-2} , $k \geq 3$.
- Primitivní kořeny existují modulo 2^k právě tehdy, když $k \leq 2$.

49. Tvzení

Nechť $m \in N$ je dělitelné alespoň 2 prvočísly a není dvojnásobkem mocniny lichého prvočísla. Pak modulo m neexistují primitivní kořeny.

7 Generátory cyklických grup

50. Tvzení

Nechť g je generátor Z_p^* . Pak g^k je generátor Z_p^* pro $(k, p-1)=1$.

51. Tvzení

Cyklická grupa Z_p^* má právě $\varphi(p-1)$ generátorů. Množinu všech generátorů grupy Z_p^* značíme G_p .

Nejmenší generátor z této množiny označme g_1 .

52. Tvzení

Nechť g je generátor Z_p^* . Pak g^{-1} je generátor Z_p^* .

53. Tvzení

Nechť g je generátor Z_p^* a prvočíslo p je ve tvaru $p=4k+1$. Pak $-g$ je generátor Z_p^* (tj. $-g = p-g$).

Důsledky

Sudé mocniny čísel g nemohou být generátory.

54. Tvzení

Pokud je g generátorem grupy Z_p^* , pak platí $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

55. Tvzení

Nechť $a \in Z_p^*$, $p \in P$ a platí $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Pak buď $a \in G_p$ nebo platí $o = \text{ord}_p a = \frac{p-1}{d}$, kde $o = \text{ord}_p a$ je liché číslo, tj. a je generátor podgrupy $N_{o/p}$.

Důkaz:

Ilustrace

V grupě Z_{37} mají prvky $a = 8, 14, 23, 29$ řád 12 (jsou to generátory podgrupy $N_{12/37}$), $3=36/12$ je liché číslo a platí $8^{\frac{37-1}{2}} \equiv -1 \pmod{37}$.

Důsledek

Pro $p=F_m$ (Fermatovo číslo) je g generátorem grupy Z_p^* právě tehdy, když platí $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

Ilustrace pro F_2

$$3^{\frac{17-1}{2}} \equiv -1 \pmod{17}$$

8 Automorfismy cyklických grup

56. Tvzení

Nechť Z_p^* je multiplikativní grupa a G_p množina jejích generátorů $G_p = \{g_1, g_2, \dots, g_m\}$, kde $m = \varphi(p-1)$. Pak existuje právě m automorfismů $F_i: g_1 \rightarrow g_i$, kde $i=1, 2, \dots, m$.

57. Tvzení

Množina $\{F_1, F_2, \dots, F_m\}$ spolu s operací skládání zobrazení, tvoří grupu $\text{Aut}(Z_p^*)$.

Důsledek: řád grupy $\text{Aut}(Z_p^*)$ je vždy sudé číslo $\varphi(p-1)$.

58. Lemma

Nechť $a \in Z_p^*, g \in G_p, a = g^x$. Pak

$$a^k = (g^x)^k = g^{xk} \bmod p = g^{xk \bmod (p-1)}$$

59. Lemma

Nechť $a, b \in Z_p^*, g \in G_p, a = g^x, b = g^y$. Pak

$$a \cdot b = g^x \cdot g^y = g^{x+y} \bmod p = g^{(x+y) \bmod (p-1)}$$

60. Lemma

Nechť $g, h, a \in G_p, h = g^w, a = h^x, (x, p-1) = 1, (w, p-1) = 1$. Pak

$$a = h^x = (g^w)^x = g^{xw} \bmod p = g^{(xw) \bmod (p-1)} \in G_p$$

61. Lemma

Nechť p je prvočíslo tvaru $p=4k+1$. Pak platí $4 \mid \varphi(p-1)$.

Důkaz:

Prvočíslo p je ve tvaru $p=4k+1$, $\varphi(p-1) = \varphi(4k)$, k je ve tvaru $k = 2^a \cdot p_1^{a_1} \cdot \dots \cdot p_n^{a_n}$, tedy $\varphi(4k) = \varphi(2^{a+2} \cdot p_1^{a_1} \cdot \dots \cdot p_n^{a_n}) = 2^{a+1} \varphi(p_1^{a_1} \cdot \dots \cdot p_n^{a_n}) = 2^{a+1} (p_1 - 1) p_1^{a_1-1} \cdot \dots$ a poněvadž p_1-1 je sudé číslo $= 2^{a+2} \cdot x \cdot p_1^{a_1-1} \cdot \dots = 4 \cdot 2^a x p_1^{a_1-1} \dots$

☺

Pozorování

Pokud $k = 2^a \cdot p_1^{a_1} \cdot \dots \cdot p_n^{a_n}$, pak $2^{(a-1) \cdot n} \mid \varphi(k)$

Ilustrace:

Z_{11}^* s množinou generátorů $G_{11}=\{2,8,7,6\}$

Každý generátor generuje právě jednu uspořádanou množinu $p-1$ prvků, tedy lze definovat zobrazení $\Psi_g: g \rightarrow U_g$, kde U_g je uspořádaná $p-1$ -tice prvků. Těchto zobrazení je právě $\varphi(p-1)$, kde $\varphi()$ je Eulerova funkce. Generátory v $p-1$ -tici jsou ty mocniny generátoru g , kde exponent je nesoudělný s $p-1$. Tedy ostatní generátory dostaneme z nejmenšího generátoru g_1 umocněním na exponent nesoudělný s $p-1$.

	11	exponent									
exp.	Generátor	1	2	3	4	5	6	7	8	9	10
1	2	2	4	8	5	10	9	7	3	6	1
9	6	6	3	7	9	10	5	8	4	2	1
7	7	7	5	2	3	10	4	6	9	8	1
3	8	8	9	6	4	10	3	2	5	7	1
	řád sloupce	10	5	10	5	2	5	10	5	10	1

Při zobrazení generátoru 2 např. na generátor 8 se transformují všechny prvky grupy. Tedy 4 na 9, 8 na 6 atd. Pokud prvek pro generátor 2 je vyjádřen jako 2^k , pak pro generátor 8 je vyjádřen jako $8^3 = (2^k)^3 = 2^{3k} \bmod p = 2^{3k \bmod (p-1)}$.

Skládání jednotlivých automorfismů Ψ_g je tedy možné si představit jako násobení exponentů generátorů (modulo $p-1$), přičemž výsledný exponent je opět nesoudělný s $p-1$ a je to tedy opět některý z generátorů.

Pro generátory g, a, b, c a příslušná zobrazení tedy platí

$$\Psi_a \circ \Psi_b = \Psi_c \text{ a tedy } \Psi_{g^r} \circ \Psi_{g^s} = \Psi_{g^{r \cdot s \bmod (p-1)}}$$

Pro značení automorfismů nám tedy bude stačit uvádět pouze exponenty u základního generátoru g , tedy $A_r \circ A_s = A_{r \cdot s \bmod (p-1)}$

Pro $p=11$ tedy máme v exponentech r, s a generátor $g_1 = 2 \pmod{10}$. Lépe řečeno, na volbě generátoru g zde nezáleží, pro přehlednost volíme vždy nejmenší generátor g_1 .

Tedy zvolme $g=2$, pak generátory Z_{11}^* jsou $2=2^1, 8=2^3, 7=2^7, 6=2^9$, tedy exponenty jsou 1,3,7,9, tedy čísla nesoudělná s $p-1$, tj. zde s číslem 10.

Tabulka automorfismů A_e

Exp.	1	3	7	9
1	A_1	A_3	A_7	A_9
3	A_3	A_9	A_1	A_7
7	A_7	A_1	A_9	A_3
9	A_9	A_7	A_3	A_1

a když použijme pouze exponenty r, s :

Exp. r.s	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

a po přeznačení A_e a přečíslování

$\circ$	F1	F2	F3	F4
F1	F1	F2	F3	F4
F2	F2	F4	F1	F3
F3	F3	F1	F4	F2
F4	F4	F3	F2	F1

Tato grupa je izomorfní s grupou Z_4^+ .

Ilustrace pro $p=17$

Tabulka generátorů a zobrazení na Z_p^* .

Grupa Z_{17}^* má celkem 8 automorfismů. $G_{17}^* = \{3,5,6,7,10,11,12,14\}$

17	exponent															
Generátor	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
5	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1
6	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1
7	7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
10	10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1
11	11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1
12	12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1
14	14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1
řád sloupce	16	8	16	4	16	8	16	2	16	8	16	4	16	8	16	1

Automorfismy - součiny exponentů mod 16

Odpovídající tabulka součinu exponentů generátorů mod 16. Jedná se tedy o komutativní multiplikativní grupu, která není cyklická, řádu 8 a je izomorfní s $G_8 = Z_4^+ \times Z_2^+$.

exponenty	1	3	5	7	9	11	13	15	řád
1	1	3	5	7	9	11	13	15	1
3	3	9	15	5	11	1	7	13	4
5	5	15	9	3	13	7	1	11	4
7	7	5	3	1	15	13	11	9	2
9	9	11	13	15	1	3	5	7	2
11	11	1	7	13	3	9	15	5	4
13	13	7	1	11	5	15	9	3	4
15	15	13	11	9	7	5	3	1	2

$$G_8 = Z_2^+ \times Z_4^+$$

	00	01	02	03	10	11	12	13	řád
00	00	01	02	03	10	11	12	13	1
01	01	03	00	02	11	12	13	10	4
02	02	00	03	01	12	13	10	11	4
03	03	02	01	00	13	10	11	12	2
10	10	11	12	13	00	01	02	03	2
11	11	12	13	10	01	02	03	00	4
12	12	13	10	11	02	03	00	01	2
13	13	10	11	12	03	00	01	02	4

Pro tento izomorfismus lze definovat předpis – přiřazení prvků o stejném řádu. Evidentně lze definovat více izomorfismů.

exponenty	G_8	řád
1	00	1
3	01	4
5	13	4
7	12	2
9	03	2
11	02	4
13	11	4
15	10	2

Ilustrace Z_{29}^*

Existuje celkem 12 automorfismů pro generátory $G_{29} = \{2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27\}$

29	exponent																											
Generátor	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
2	2	4	8	16	3	6	12	24	19	9	18	7	14	28	27	25	21	13	26	23	17	5	10	20	11	22	15	1
3	3	9	27	23	11	4	12	7	21	5	15	16	19	28	26	20	2	6	18	25	17	22	8	24	14	13	10	1
8	8	6	19	7	27	13	17	20	15	4	3	24	18	28	21	23	10	22	2	16	12	9	14	25	26	5	11	1
10	10	13	14	24	8	22	17	25	18	6	2	20	26	28	19	16	15	5	21	7	12	4	11	23	27	9	3	1
11	11	5	26	25	14	9	12	16	2	22	10	23	21	28	18	24	3	4	15	20	17	13	27	7	19	6	8	1
14	14	22	18	20	19	5	12	23	3	13	8	25	2	28	15	7	11	9	10	24	17	6	26	16	21	4	27	1
15	15	22	11	20	10	5	17	23	26	13	21	25	27	28	14	7	18	9	19	24	12	6	3	16	8	4	2	1
18	18	5	3	25	15	9	17	16	27	22	19	23	8	28	11	24	26	4	14	20	12	13	2	7	10	6	21	1
19	19	13	15	24	21	22	12	25	11	6	27	20	3	28	10	16	14	5	8	7	17	4	18	23	2	9	26	1
21	21	6	10	7	2	13	12	20	14	4	26	24	11	28	8	23	19	22	27	16	17	9	15	25	3	5	18	1
26	26	9	2	23	18	4	17	7	8	5	14	16	10	28	3	20	27	6	11	25	12	22	21	24	15	13	19	1
27	27	4	21	16	26	6	17	24	10	9	11	7	15	28	2	25	8	13	3	23	12	5	19	20	18	22	14	1
řád sloupce	28	14	28	7	28	14	4	7	28	14	28	7	28	2	28	7	28	14	28	7	4	14	28	7	28	14	28	1

A příslušná grupa automorfismů $\text{Aut}(Z_{29}^*) \pmod{28}$

exponenty	1	3	5	9	11	13	15	17	19	23	25	27	řád
1	1	3	5	9	11	13	15	17	19	23	25	27	1
3	3	9	15	27	5	11	17	23	1	13	19	25	6
5	5	15	25	17	27	9	19	1	11	3	13	23	6
9	9	27	17	25	15	5	23	13	3	11	1	19	3
11	11	5	27	15	9	3	25	19	13	1	23	17	6
13	13	11	9	5	3	1	27	25	23	19	17	15	2
15	15	17	19	23	25	27	1	3	5	9	11	13	2
17	17	23	1	13	19	25	3	9	15	27	5	11	6
19	19	1	11	3	13	23	5	15	25	17	27	9	6

23	23	13	3	11	1	19	9	27	17	25	15	5	6
25	25	19	13	1	23	17	11	5	27	15	9	3	3
27	27	25	23	19	17	15	13	11	9	5	3	1	2

Tato grupa $\text{Aut}(Z_{29}^*)$ je izomorfní s grupou $G_{12}^+ = Z_6^+ \times Z_2^+$.

Aditivní grupa řádu 12 není cyklická.

$Z_6^+ \times Z_2^+$	00	01	02	03	04	05	10	11	12	13	14	15	řád
00	00	01	02	03	04	05	10	11	12	13	14	15	1
01	01	02	03	04	05	00	11	12	13	14	15	10	6
02	02	03	04	05	00	01	12	13	14	15	10	11	3
03	03	04	05	00	01	02	13	14	15	10	11	12	2
04	04	05	00	01	02	03	14	15	10	11	12	13	3
05	05	00	01	02	03	04	15	10	11	12	13	14	6
10	10	11	12	13	14	15	00	01	02	03	04	05	2
11	11	12	13	14	15	10	01	02	03	04	05	00	6
12	12	13	14	15	10	11	02	03	04	05	00	01	6
13	13	14	15	10	11	12	03	04	05	00	01	02	2
14	14	15	10	11	12	13	04	05	00	01	02	03	6
15	15	10	11	12	13	14	05	00	01	02	03	04	6

Obsahuje tři podgrupy řádu 6 tj. $\langle 01 \rangle$, $\langle 11 \rangle$, $\langle 12 \rangle$.

62. Tvzení

Grupa automorfismů $\text{Aut}(Z_p^*)$ grupy Z_p^* je izomorfní s některou komutativní aditivní grupou $G_{\varphi(p-1)}^+$.

Důsledky

- Tato grupa $G_{\varphi(p-1)}^+$ je cyklická pouze tehdy, je-li $\varphi(p-1) = 2 \cdot p^k$, kde p je liché prvočíslo, a tedy grupa automorfismů $\text{Aut}(Z_p^*)$ grupy Z_p^* je cyklická právě tehdy, když $\varphi(p-1) = 2 \cdot p^k$.
- Grupa automorfismů $\text{Aut}(Z_p^*)$ grupy Z_p^* , kde p je tvaru $p=4k+1$, není cyklická.

63. Tvzení

Grupa automorfismů $\text{Aut}(Z_p^*)$ grupy Z_p^* , kde p je tvaru $p=4k+1$????, je izomorfní s některou komutativní aditivní grupou $G_{\varphi(p-1)/4}^+ \times K_4^+$, kde $\times$ je grupové násobení a K_4^+ je Kleinova grupa.

Důkaz

????????? Pokud má některý prvek grupy $G_{\varphi(p-1)}^+$ řád $\varphi(p-1)$, pak je grupa cyklická. Ale cyklické grupy mohou být pouze grupy řádu 2, 4, p^k a $2p^k$, kde p je liché prvočíslo. $\varphi(p-1)$ je sudé, takže nemůže být typu p^k a navíc platí pro $p=4k+1$, že $4/\varphi(p-1)$, tedy nemůže být ani typu $2p^k$. Poněvadž žádný prvek nemá řád $\varphi(p-1)$, pak největší řád prvku v grupě je $\varphi(p-1)/4$. Existují tedy podgrupy řádu $\varphi(p-1)/4$ grupy $G_{\varphi(p-1)}^+$, označme je $N_{\frac{\varphi(p-1)}{4}}$. (Tyto podgrupy mohou, ale nemusí být cyklické.)

Podgrupa $N_{\frac{\varphi(p-1)}{4}}$ je izomorfní nějaké Z_m^+ kde $m = \frac{\varphi(p-1)}{2} = \frac{\varphi(4k)}{2}$. Necht' $k = 2^a \cdot p_1^{\alpha_1} \dots p_n^{\alpha_n}$, pak

$$\varphi(4k) = \varphi(2^{a+2} \cdot p_1^{\alpha_1} \dots p_n^{\alpha_n}) = 2^{a+1} \cdot \varphi(p_1^{\alpha_1} \dots p_n^{\alpha_n}) \text{ a } m = \frac{\varphi(4k)}{2} = 2^a \cdot \varphi(p_1^{\alpha_1} \dots p_n^{\alpha_n})$$

Pokud je k liché pak $a=0$ a $m = \varphi(p_1^{\alpha_1} \dots p_n^{\alpha_n}) = \varphi(k)$

Podgrupy jsou právě

???????



Tabulka automorfismů grup

p	p-1	Typ	k	Počet automorfismů $\phi(p-1)$	Izomorfní s grupou
5	4	$4k+1$	1	2	Z_2^+
7	6			2	Z_2^+
11	10			4	Z_4^+
13	12	$4k+1$	3	4	Z_4^+
17	16	$4k+1$	4	8	$Z_4^+ \times Z_2^+$
23	22			10	$Z_5^+ \times Z_2^+$
29	28	$4k+1$	7	12	$Z_6^+ \times Z_2^+$
31	30			8	$Z_4^+ \times Z_2^+$
37	36	$4k+1$	9	12	$Z_6^+ \times Z_2^+$
41	40	$4k+1$	10	16	$Z_8^+ \times Z_2^+$
43	42			12	$Z_6^+ \times Z_2^+$
47	46			22	$Z_{11}^+ \times Z_2^+$
53	52	$4k+1$	13	24	$Z_{12}^+ \times Z_2^+$
59	58			28	$Z_{14} \times Z_2^+$
61	60	$4k+1$	15	16	$Z_8^+ \times Z_2^+$
67	66			20	$Z_{10}^+ \times Z_2^+$
...					

9 Diskrétní logaritmy

Nechť p, g, k, Y jsou přirozená čísla, pro něž platí $Y \equiv g^k \pmod{p}$. Potom každé číslo k odpovídající uvedené rovnici nazveme diskrétní logaritmus o základu g z Y vzhledem k modulu p .

$$k = \log_g Y$$

Tato definice nedefinuje číslo k jednoznačně (generátorů grupy je vždy více než jeden), proto se někdy upravuje tak, že ze všech možných diskrétních logaritmů ve smyslu předchozí definice se vybere ten nejmenší generátor.

Poznámka: Obecně se nemusí jednat přímo o přirozená čísla modulo m , diskrétní logaritmus je zobecnění klasického logaritmu pro konečné cyklické grupy.

Poznámka:

V některých publikacích se tato čísla nazývají indexy.

Ilustrace pro $p=11$

11	exponent									
Generátor	1	2	3	4	5	6	7	8	9	10
2	2	4	8	5	10	9	7	3	6	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
řád sloupce	10	5	10	5	2	5	10	5	10	1

$$2^4 = 5 \quad \log_2 5 = 4$$

11	číslo									
Základ log.	1	2	3	4	5	6	7	8	9	10
2	10	1	8	2	4	9	7	3	6	5
6	10	9	2	8	6	1	8	7	4	5
7	10	3	2	6	2	7	1	9	8	5
8	10	7	6	4	8	3	9	1	3	5

10 Odmocniny z jedné

64. Definice n-té odmocniny z jedné

Komplexní čísla z splňující rovnost $z^n = 1$ nazýváme n -té odmocniny z jedné. Množinu všech n -tých odmocnin z jedné budeme značit μ_n .

65. Lemma

Nechť K je konečné rozšíření tělesa $\mathbb{Q}$. Pak množina všech odmocnin z jedné (tj. m -tých odmocnin z jedné pro nějaké $m \in \mathbb{N}$), které leží v K , tvoří konečnou cyklickou multiplikativní grupu řádu m .

66. Lemma

Množina μ_n tvoří cyklickou podgrupu řádu n grupy $\mathbb{C}^*$. Navíc pro $m \in \mathbb{N}$ splňující m/n platí $\mu_m \subset \mu_n$.

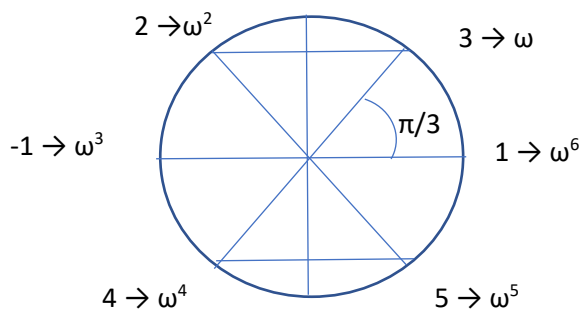
67. Lemma

Ke každé multiplikativní cyklické grupě Z_p^* existuje izomorfní grupa W_{p-1} s prvky μ_{p-1} .

Ilustrace

(pro Z_7^*)

$\omega = e^{\frac{2\pi i}{7-1}} = \xi_6$ je generátor grupy Z_7^*



68. Definice

Pro $n \in \mathbb{N}$ označíme $\xi_n \equiv e^{\frac{2\pi i}{n}} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$

69. Lemma

ξ_{p-1} je generátorem W_{p-1} , kde $p \in \mathbb{P}$. Nechť m je nesoudělné s $p-1$, $m < p-1$. Pak i ξ_{p-1}^m je generátor.

70. Lemma

Označme Ξ_{p-1} množinu všech generátorů W_{p-1} . Pak Ξ_{p-1} je izomorfní s množinou generátorů G_p .

71. Tvzení

Nechť ξ_n je generátor grupy W_{p-1} . Pak i prvek komplexně sdružený $\overline{\xi_n}$ je generátor této grupy.

72. Tvzení

Nechť p je liché prvočíslo. Pak

$$\prod_{i=1}^{p-1} \xi_{p-1}^i = -1 \pmod{p}$$

Důkaz:

p je liché prvočíslo

$$\prod_{i=1}^{p-1} \xi_{p-1}^i = \xi_{p-1}^1 \cdot \xi_{p-1}^2 \cdot \dots \cdot \xi_{p-1}^{p-1} = \xi_{p-1}^{1+2+\dots+p-1} = \xi_{p-1}^{\frac{(p-1)p}{2}} = e^{2\pi i \frac{(p-1)p}{2(p-1)}} = e^{\pi i p} = -1$$

☺

73. Tvzení (Wilsonova věta)

$$(p-1)! = -1 \pmod{p}$$

Důkaz:

Podle (49) jsou grupy Z_p^* a W_{p-1} izomorfní a pořadí násobení v důkazu (54) je komutativní.

☺

Ilustrace

$$(7-1)! = -1 \pmod{7}$$

$$720 = -1 \pmod{7}$$

$$6 = -1 \pmod{7}$$

☺

74. Tvzení

$$\sum_{i=0}^{p-1} \xi_{p-1}^i = 0 \pmod{p}$$

Důkaz:

Pro každé ξ_{p-1}^k existuje číslo opačné $\xi_{p-1}^{k+\frac{p-1}{2}} = -\xi_{p-1}^k$

$$\xi_{p-1}^{k+\frac{p-1}{2}} = e^{\frac{2\pi i}{p-1}(k+\frac{p-1}{2})} = e^{2\pi i \frac{k}{p-1}} \cdot e^{\frac{2\pi i p-1}{2(p-1)}} = \xi_{p-1}^k \cdot e^{\pi i} = -\xi_{p-1}^k$$

☺

Důsledek

$$\sum_{i=1}^{p-1} \xi_{p-1}^i = -1 \pmod{p}$$

$$\sum_{a \in Z_p^*} a = 0 \pmod{p}$$

Ilustrace

$$\sum_{a \in Z_7^*} a = 1 + 2 + 3 + 4 + 5 + 6 = \frac{6 \cdot 7}{2} \pmod{7} = 0$$

☺

11 Dirichletovy charaktery

75. Definice

Nechť n je přirozené číslo, Dirichletův charakter modulo n je pak zobrazení $\chi: \mathbb{Z} \rightarrow \mathbb{C}^*$, které splňuje následující podmínky:

- (i) (úplná multiplikativita) $\chi(a \cdot b) = \chi(a) \cdot \chi(b)$, pro každé $a; b \in \mathbb{Z}$,
- (ii) (periodičnost) $\chi(a + n) = \chi(a)$ pro každé $a \in \mathbb{Z}$,
- (iii) $\chi(a) = 0$ právě když $\gcd(a; n) > 1$.

Dirichletovy charaktery jsou úzce spjaty s charaktery konečných grup. Každý Dirichletův charakter modulo n získáme z charakteru grupy $(\mathbb{Z}/n\mathbb{Z})_*$ a naopak.

Dirichletův charakter $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ modulu $p > 1$ je obsažen v seznamu hodnot $\chi(1)=1, \chi(2), \chi(3), \dots, \chi(p-1), \chi(p)=0$, kde každá z těchto hodnot je kořen jednotky $e(r) := \exp(2\pi i r)$, kde r je racionální číslo.

Conreyovo značení pro Dirichletovy charaktery

Používáme zápis $\chi_q(n, \cdot)$ k identifikaci Dirichletových charakterů $\mathbb{Z} \rightarrow \mathbb{C}$, kde p je modul a n je index, kladné celé číslo nesoudělné s p , které určuje Dirichletův charakter modulu p . LMFDB značení $p.n$ s $1 \leq n < (p, 2)$ jednoznačně identifikuje $\chi_p(n, \cdot)$.

Značení zavedl Brian Conrey. Tento systém notace je základním značením pro explicitní isomorfismus mezi multiplikativní grupou $(\mathbb{Z}/p\mathbb{Z})^\times$ a grupou Dirichletových charakterů s modulem p , což usnadňuje v této notaci určení řádu, konduktoru a parity Dirichletova charakteru nebo usnadňuje i určení charakteru. Například, $\chi_p(1, \cdot)$ je vždy triviální tj. 1, $\chi_p(m, \cdot)$ je reálné číslo jestliže $m^2 \equiv 1 \pmod{p}$ a pro všechna m, n nesoudělná s p máme $\chi_p(m, n) = \chi_p(n, m)$.

Vztah pro výpočet Dirichletova charakteru (p je prvočíslo, g je libovolný generátor)

$$\chi_p(x, y) = \exp\left(2\pi i \frac{\log_g x \cdot \log_g y}{p-1}\right)$$

(v tabulce LMFD vynechávají v zápisu $2\pi i$)

V případě Wikipedie se uvádí symbol ω , pak lze Dirichletův charakter zapsat pro

$$\omega = e^{\frac{2\pi i}{p-1}}$$

jako

ω^k , kde k je $k = \log_g x \cdot \log_g y \pmod{p-1}$

Z Wikipedie pro $p=7$:

Dirichlet	n						
	0	1	2	3	4	5	6 = -1
χ_0	0	1	1	1	1	1	1
χ_1	0	1	ω^2	ω	$-\omega$	$-\omega^2$	-1
χ_2	0	1	$-\omega$	ω^2	ω^2	$-\omega$	1
χ_3	0	1	1	-1	1	-1	-1
χ_4	0	1	ω^2	$-\omega$	$-\omega$	ω^2	1
χ_5	0	1	$-\omega$	$-\omega^2$	ω^2	ω	-1

a v zápisu LMFD

$$\chi_p(x, y) = e\left(\frac{k}{p-1}\right)$$

Tabulky z LMFDB (databáze L-funkcí a modulárních forem)

Orbit label	Conrey labels	Modulus	Conductor	Order	Parity	Primitive
7.a	$\chi_7(1, \cdot)$	7	1	1	even	
7.b	$\chi_7(6, \cdot)$	7	7	2	odd	✓
7.c	$\chi_7(2, \cdot), \chi_7(4, \cdot)$	7	7	3	even	✓
7.d	$\chi_7(3, \cdot), \chi_7(5, \cdot)$	7	7	6	odd	✓

Character	Orbit	Order	Primitive	-1	1	2	3	4	5
$\chi_7(1, \cdot)$	7.a	1	no	1	1	1	1	1	1
$\chi_7(2, \cdot)$	7.c	3	yes	1	1	$e\left(\frac{2}{3}\right)$	$e\left(\frac{1}{3}\right)$	$e\left(\frac{1}{3}\right)$	$e\left(\frac{2}{3}\right)$
$\chi_7(3, \cdot)$	7.d	6	yes	-1	1	$e\left(\frac{1}{3}\right)$	$e\left(\frac{1}{6}\right)$	$e\left(\frac{2}{3}\right)$	$e\left(\frac{5}{6}\right)$
$\chi_7(4, \cdot)$	7.c	3	yes	1	1	$e\left(\frac{1}{3}\right)$	$e\left(\frac{2}{3}\right)$	$e\left(\frac{2}{3}\right)$	$e\left(\frac{1}{3}\right)$
$\chi_7(5, \cdot)$	7.d	6	yes	-1	1	$e\left(\frac{2}{3}\right)$	$e\left(\frac{5}{6}\right)$	$e\left(\frac{1}{3}\right)$	$e\left(\frac{1}{6}\right)$
$\chi_7(6, \cdot)$	7.b	2	yes	-1	1	1	-1	1	-1

Ilustrace pro $\chi_7(2,3)$.

Pro generátor $g=3$, $k = \log_3 2 \cdot \log_3 3 = 2 \cdot 1 = 2$

Pro generátor $g=5$, $k = \log_5 2 \cdot \log_5 3 = 4 \cdot 5 = 20 \bmod 6 = 2$

$$\omega = e^{\frac{2\pi i}{p-1}} = e^{\frac{2\pi i}{7-1}} = e^{\frac{\pi i}{3}}$$

Tedy $\chi_7(2,3) = \omega^2 = e(2/6) = e(1/3)$.

Ilustrace pro $\chi_7(4,3)$.

Pro generátor $g=3$, $k = \log_3 4 \cdot \log_3 3 = 4 \cdot 1 = 4$

Pro generátor $g=5$, $k = \log_5 2 \cdot \log_5 3 = 2 \cdot 5 = 10 \bmod 6 = 4$

Tedy $\chi_7(4,3) = \omega^4 = -\omega = e(4/6) = e(2/3)$.

Vlastnosti Dirichletových charakterů

Pro $a \neq 1$

$$\sum_{i=1}^{p-1} \chi_p(a, i) = 1 \quad \sum_{i=1}^{p-1} \chi_p(i, a) = 1$$

$$\chi_p(a, b) = \chi_p(b, a)$$

Grupa Dirichletových charakterů pro prvočíslo $p=7$

$$(\chi_1 \cdot \chi_2)(a) = \chi_1(a) \cdot \chi_2(a)$$

charaktery	1	2	3	4	5	6	řád
1	1	2	3	4	5	6	1
2	2	4	6	1	3	5	3
3	3	6	2	5	1	4	6
4	4	1	5	2	6	3	3
5	5	3	1	6	4	2	6
6	6	5	4	3	2	1	2

Multiplikativní cyklická grupa modulo 7 zapsaná obecně pomocí generátoru u (za u je možno dosadit buď 3 nebo 5), prvky 3 a 5 jsou vzájemně inverzní.

						řád
1	u	u^2	u^3	u^4	u^5	1
u	u^2	u^3	u^4	u^5	1	6
u^2	u^3	u^4	u^5	1	u	3
u^3	u^4	u^5	1	u	u^2	2
u^4	u^5	1	u	u^2	u^3	3
u^5	1	u	u^2	u^3	u^4	6

Aditivní grupa Z_6 je izomorfní s grupou Z_7^*

	0	1	2	3	4	5	řád prvku
0	0	1	2	3	4	5	1
1	1	2	3	4	5	0	6
2	2	3	4	5	0	1	3
3	3	4	5	0	1	2	2
4	4	5	0	1	2	3	3
5	5	0	1	2	3	4	6

Tabulka 1

12 Fermatova čísla

Fermatovým číslem se v matematice rozumí takové přirozené číslo, které je rovno

$$F_n = 2^{2^n} + 1$$

pro nějaké přirozené číslo n . Svoje jméno tato čísla získala podle matematika Pierra de Fermata, který je zkoumal jako jeden z prvních.

Prvních devět Fermatových čísel je:

$$F_0 = 2^1 + 1 = 3$$

$$F_1 = 2^2 + 1 = 5$$

$$F_2 = 2^4 + 1 = 17$$

$$F_3 = 2^8 + 1 = 257$$

$$F_4 = 2^{16} + 1 = 65\,537$$

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417$$

$$F_6 = 2^{64} + 1 = 18\,446\,744\,073\,709\,551\,617 = 274\,177 \times 67\,280\,421\,310\,721$$

$$F_7 = 2^{128} + 1 = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,211\,457 =$$

$$= 59\,649\,589\,127\,497\,217 \times 5\,704\,689\,200\,685\,129\,054\,721$$

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

12.1 Vlastnosti Fermatových čísel

Snadno nahlédneme, že F_m pro $m \geq 2$ končí na 7, protože 2^{2^m} končí na 6.

Poslední dvojčíslí F_m může končit jen na 17, 37, 57 a 97 pro $m \geq 2$.

Platí rekurentní vztah $F_{m+1} = (F_m - 1)^2 + 1$,

a z toho

$F_{m+1} - 2 = F_m(F_m - 2)$ a indukcí dostáváme

$$F_{m+1} - 2 = F_m F_{m-1} \dots F_1 F_0,$$

ze které plyne, že $F_{m+1} - 2$ je dělitelné všemi menšími Fermatovými čísly. Tedy

$F_{m-k} \mid F_{m+1} - 2$ pro všechna $k = 1, \dots, m$.

76. Tvzení (Goldbachova věta)

Žádná dvě různá Fermatova čísla nemají společného dělitele většího než 1.

77. Tvzení (Lucasova věta)

Jestliže $p \mid F_m$, pak p je tvaru $p = k2^{m+2} + 1$, kde k je přirozené číslo.

78. Tvzení (Pepinův test)

Pro $m \geq 1$ je F_m prvočíslo tehdy a jen tehdy, když $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$

13 Experimenty

13.1 Zobrazení grupy na množinu generátorů

79. Definice zobrazení A grupy Z_p^* na množinu G_p

Nechť Z_p^* je multiplikativní grupa a G_p množina jejích generátorů $G_p = \{g_1, g_2, \dots, g_m\}$, kde $m = \varphi(p-1)$. Pro každý prvek $a \in Z_p^*$ definujeme zobrazení A grupy Z_p^* na množině G_p takto A: $a \rightarrow g^a \pmod{p}$.

80. Tvzení

- Zobrazení A vytvoří $\tau(p-1)$ (tau – aritmetická funkce počtu dělitelů) po dvou disjunktních podmnožinách prvků Z_p^* o stejném řádu r , označme ji M_r . Pro prvek a označme $M_{(a)}$ množinu s pořadím (exponentem) a .
- Podmnožina M_r řádu r je množinou generátorů podgrupy řádu r , tj. podgrupy $N_{r/p}$.
- Každá podmnožina M_r obsahuje spolu s prvkem i jeho inverzní prvek.
- Pokud na množinu G_p působí prvek a soudělný s prvkem $p-1$, výsledkem je skupina M_r kde řád skupiny $r = (p-1)/\text{NSD}(a, p-1)$, tedy pokud na množinu G_p působí prvek nesoudělný je výsledkem opět G_p .
- Pokud vezmeme podmnožinu řádu r a sjednotíme ji s podmnožinami s řádem, který dělí řád této podmnožiny, dostaneme podgrupu grupy Z_p^* řádu r , tj. $\bigcup_{k/r} M_k = N_{r/p}$.
- Existuje přirozená symetrie v pořadí množin $a < p-1$, $M_{(a)} = M_{(p-1-a)}$.
- $\|M_{(a)}\| = \|M_r\| = \varphi\left(\frac{p-1}{\text{NSD}(p-1, a)}\right) = \|G_{r/p}\|$.
- $M_{(a)} = M_{\frac{p-1}{\text{NSD}(p-1, a)}}$.
- $M_2 = M_{(p-1/2)} = \{p-1\}$
- $\forall x \in M_r \exists g \in G_p; x = g^r$.
- Zavedme mocninu $G^e = \{g^e; g \in G\}$ $e=1, \dots, p-1$. Pak $G^1 = G$, $G^{p-1} = \{1\}$, $G^{\frac{p-1}{2}} = \{p-1\}$, $G^e = G_{r/p}$, kde $r = \text{ord}(G^e) = \frac{p-1}{\text{NSD}(e, p-1)}$
- Nechť je p tvaru $p=4l+1$, pak $G^{\frac{p-1}{4}} = \{x, p-1-x = x^{-1}\}$, kde x je generátor $N_{4/p}$.

Důkaz

Pokud je $g \in G_p$, pak každý prvek $a \in Z_p^*$ lze zapsat jako $g^n \pmod{p}$ kde $n \in \{0, \dots, p-1\}$. Generátory jsou ty prvky grupy, kde n je nesoudělné s řádem grupy, tj. $p-1$.

Dále platí, že pokud nějaké s dělí $p-1$, tak pro libovolný generátor $g \in G_p$ je $g^{n/s} \pmod{p}$ je generátor podgrupy řádu $r=n/s$ a všechny prvky podgrupy $N_{r/p}$ lze zapsat jako $g^{\frac{n}{r}k} \pmod{p}$ kde k nabývá hodnot od 1 do r . Generátory této podgrupy jsou ty prvky g^k , kde k je nesoudělné s r .

Důsledky:

- Generátorem grupy Z_p^* nemůže být prvek – úplný čtverec.
- Pokud prvočíslo p je ve tvaru $p=6k+1$, pak generátorem grupy nemůže být ani třetí mocnina čísla.

81. Uspořádané k – tice generátorů

Počet generátorů grupy Z_p^* označme h . Pokud seřadíme množinu generátorů od nejmenšího po největší, pak zobrazení A provede permutaci této h -tice. Počet těchto permutací je právě $\varphi(h)$. Jednotlivé permutace označme H_i .

mod 19

Generátory	H1	H2	H3	H4	H5	H6
2	2	13	14	15	3	10
3	3	15	2	10	14	13
10	10	3	15	14	13	2
13	13	14	10	2	15	3
14	14	10	3	13	2	15
15	15	2	13	3	10	14
i	1	2	3	4	5	6

a přechísľujeme:

	1	2	3	4	5	6
1	1	4	5	6	2	3
2	2	6	1	3	5	4
3	3	2	6	5	4	1
4	4	5	3	1	6	2
5	5	3	2	4	1	6
6	6	1	4	2	3	5
i	1	2	3	4	5	6

Ilustrace:

$$s = 2, r = 18/2 = 9, g = 2$$

$$N_{9/19} = \{1, 4, 5, 6, 7, 9, 11, 16, 17\}$$

$$g^{\frac{18}{9}k}(\text{mod } 19) = g^{2k}(\text{mod } 19) = 2^{2k}(\text{mod } 19) = \{4, 16, 7, 9, 17, 11, 6, 5, 1\}$$

k nesoudělné s 9 jsou čísla 1, 2, 4, 5, 7, 8 a tedy generátory $N_{9/19}$ jsou 4, 16, 9, 17, 6, 5, tedy celkem $\varphi(9) = 6$ generátorů.

Ilustrace na grupě Z_{19}^*

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	řád prvku
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	1
2	2	4	6	8	10	12	14	16	18	1	3	5	7	9	11	13	15	17	18
3	3	6	9	12	15	18	2	5	8	11	14	17	1	4	7	10	13	16	18
4	4	8	12	16	1	5	9	13	17	2	6	10	14	18	3	7	11	15	9
5	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14	9
6	6	12	18	5	11	17	4	10	16	3	9	15	2	8	14	1	7	13	9
7	7	14	2	9	16	4	11	18	6	13	1	8	15	3	10	17	5	12	3
8	8	16	5	13	2	10	18	7	15	4	12	1	9	17	6	14	3	11	6
9	9	18	8	17	7	16	6	15	5	14	4	13	3	12	2	11	1	10	9
10	10	1	11	2	12	3	13	4	14	5	15	6	16	7	17	8	18	9	18
11	11	3	14	6	17	9	1	12	4	15	7	18	10	2	13	5	16	8	3
12	12	5	17	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7	6
13	13	7	1	14	8	2	15	9	3	16	10	4	17	11	5	18	12	6	18
14	14	9	4	18	13	8	3	17	12	7	2	16	11	6	1	15	10	5	18
15	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4	18
16	16	13	10	7	4	1	17	14	11	8	5	2	18	15	12	9	6	3	9
17	17	15	13	11	9	7	5	3	1	18	16	14	12	10	8	6	4	2	9
18	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	2

Podgrupy:

$$N_{9/19} = \{1, 4, 5, 6, 7, 9, 11, 16, 17\} \quad N_{6/19} = \{1, 7, 8, 12, 18\} \quad N_{3/19} = \{1, 7, 11\}$$

Zobrazení grupy Z_{19}^* na G

19	a																	
Generátory	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
10	10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
13	13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
řád M_i	18	9	6	9	18	3	18	9	2	9	18	3	18	9	6	9	18	1

Modře jsou označeny prvky nesoudělné s 18.

$$G_{19} = \{2, 3, 10, 13, 14, 15\}$$

$$M_{18} = \{2, 3, 10, 13, 14, 15\} = G_{19}$$

$$M_9 = \{4, 5, 6, 9, 16, 17\}; \quad r = (19-1)/\text{NSD}(4, 18) = 18/2 = 9$$

$$M_6 = \{8, 12\}; \quad r = (19-1)/\text{NSD}(6, 18) = 18/3 = 6$$

$$M_3 = \{7, 11\}$$

$$M_2 = \{18\}$$

$$M_1 = \{1\}$$

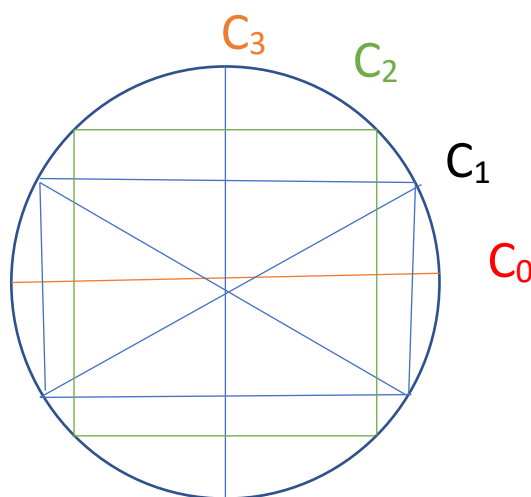
13.2 Symetrie a model čtyř prvků v tělese T_p

82. Tvzení

Nechť T_p je těleso a Z_p^* je jeho multiplikativní grupa. Pak pro každý prvek grupy různý od 1 a -1 existuje čtveřice prvků, který je jednoznačně určen jedním z těchto prvků. Pro prvek a jsou jednoznačně určeny prvky $-a$, a^{-1} , $-a^{-1}$. V případě, že prvočíslo p je ve tvaru $4k+1$ je jedna z těchto čtveřic degenerována na dva prvky pro něž pak platí $b^{-1}=-b$. Vždy existuje degenerovaná čtveřice s prvky 1, -1.

83. Definice

Čtvercem (úplným) prvků nazveme uspořádanou množinu s prvky a , $-a$, a^{-1} , $-a^{-1}$. Pokud $-a = a^{-1}$ nazveme množinu a , $-a$ degenerovaným čtvercem. Tuto množinu označme C_a . Index a je číslován od 1 do $k-1$ podle pořadí prvků v 1 kvadrantu. Degenerovaný čtverec s prvky 1, -1 označme C_0 .



84. Tvzení

Nechť Z_p^* je cyklická komutativní grupa. Pak počet generátorů této grupy je dělitelný 4, počet čtverců generátorů je $\phi(p-1)/4$ (vyjma $p=2q+1$, kde q je prvočíslo, tj. 22, 47, ...).

85. Tvzení

- Nechť T_p je těleso a Z_p^* je jeho multiplikativní grupa a prvočíslo $p > 7$ je ve tvaru $p=4k+1$. Pak existuje právě $k-2$ nezávislých úplných čtverců a degenerovaný čtverec C_{k-1} a C_0 .
- Nechť T_p je těleso a Z_p^* je jeho multiplikativní grupa a prvočíslo $p > 7$ je ve tvaru $p=4k+3$. Pak existuje právě $k-1$ nezávislých úplných čtverců a čtverec C_0 .

Ilustrace

p	$p-1$	$\phi(p-1)$
11	10	4
13	12	4
17	16	8
23	22	10
29	28	12
31	30	16

37	36	12
41	40	20
43	42	12
47	46	22
53	52	24
59	58	28
61	60	16
67	66	20

86. Tvzení

Množiny C_a jsou po dvou disjunktní. Sjednocení všech C_a je množina $1, \dots, p-1$.

87. Tvzení

Nechť prvek $a = g^t$. Pak prvky čtverce jsou $g^t, -g^t, -g^t, g^t$. Pokud t a $t+(p-1)/2$ jsou nesoudělné s $p-1$, pak tento čtverec je čtverec generátorů.

Poznámka

Tedy pro $p=4k+1$, pak $t+(p-1)/2 = t+2k$ a t je nesoudělné s $p-1 = 4k$. Tedy $(t,4k)=1$ a $(t+2k,4k)=1$, tedy pokud $(t,k) \neq 1$ pak podmínka splněna není.

A pro $p=4k+3$, pak $t+(p-1)/2 = t+2k+1$ a t je nesoudělné s $p-1 = 4k+2$. Tedy $(t,4k+2)=1$ a $(t+2k+1,4k+2)=1$, tedy pokud $(t,2k+1) \neq 1$ pak podmínka splněna není.

88. Tvzení

Nechť Z_p^* . Sjednocení všech čtverců generátorů je množina generátorů grupy G_p^* .

89. Tvzení

Pro každé $a < (p-1)/4$ platí

- a) $-C_a = C_a$
- b) $C_a^{-1} = C_a$
- c) $C_a^2 = 1$

90. Tvzení

$$\sum_{a \in C_b} a = 0$$

$$\prod_{a \in C_b} a = 1$$

91. Tvzení

Pro každé a, b platí

- a) $C_a * C_b = 1$
- b) $C_a \pm C_b = 0$

Kde operace $*$ je definována jako součin modulo p všech různých dvojic $x_i * y_j$, kde x_i je libovolný prvek C_a a y_j libovolný prvek C_b .

Kde operace $\pm$ je definována jako součet modulo p všech různých dvojic $x_i * y_j$, kde x_i je libovolný prvek C_a a y_j libovolný prvek C_b .

Ilustrace pro T_{17}

Čtverce C	a	$-a^{-1}$	-a	a^{-1}
1	3	11	14	6
2	9	15	8	2
3	10	5	7	12
4	13	13	4	4
0	16	1	1	16

$C1 * C2 = 3*9 * 11*15 * 14*8 * 6*2 \bmod 17 = 1$, pro libovolné pořadí dvojic prvků

$C1 + C2 = 3+9 + 11+15 + 14+8 + 6+2 \bmod 17 = 0$, pro libovolné pořadí dvojic prvků

Důkaz: operace obyčejné $*$ mod p a $+$ mod p jsou komutativní a asociativní, tj. $C_a \pm C_b = a + b + -a^{-1} + -b^{-1} + -a + -b + a^{-1} + b^{-1} = (a + -a + -a^{-1} + a^{-1}) + (b + -b + -b^{-1} + b^{-1}) = 0 + 0 = 0$

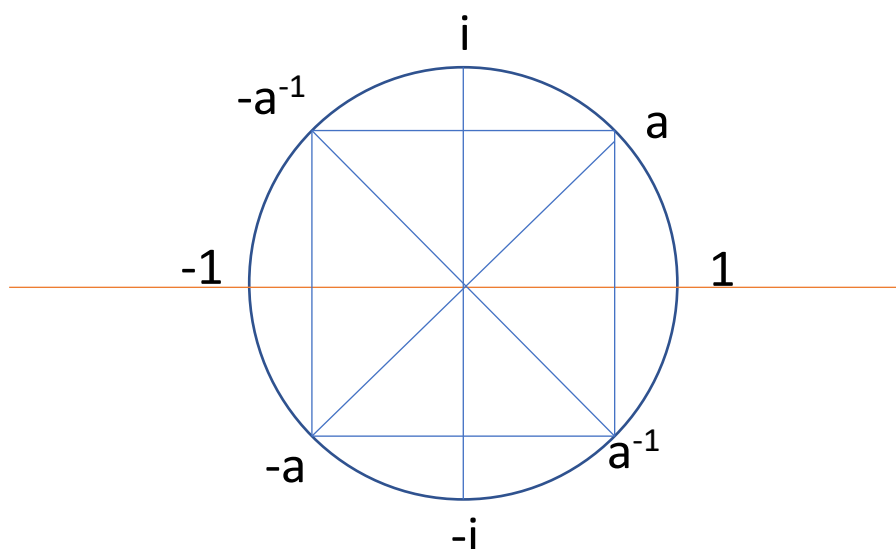
$C_a * C_b = a * b * -a^{-1} * -b^{-1} = -a * -b * a^{-1} * b^{-1} = (a * -a * -a^{-1} * a^{-1}) * (b * -b * -b^{-1} * b^{-1}) = 1 * 1 = 1 \text{ ☺}$

Pozorování

- Prvky a , $-a$ jsou v Gaussově rovině symetrické podle středu, prvky a , a^{-1} jsou symetrické podle reálné osy.
- Nechť g je generátor, pak $i g^{-1}$ je generátor.
- Nechť g je generátor, pak $-g$ je generátor pouze tehdy pokud $-g = g^t$ a t je nesoudělné s $p-1$.
Tedy pro $t=(p-1)/2+1$ je nesoudělné s $p-1$.

Ilustrace:

Obecně pro prvek a z T_p zobrazíme v Gaussově rovině



Ilustrace pro T_7

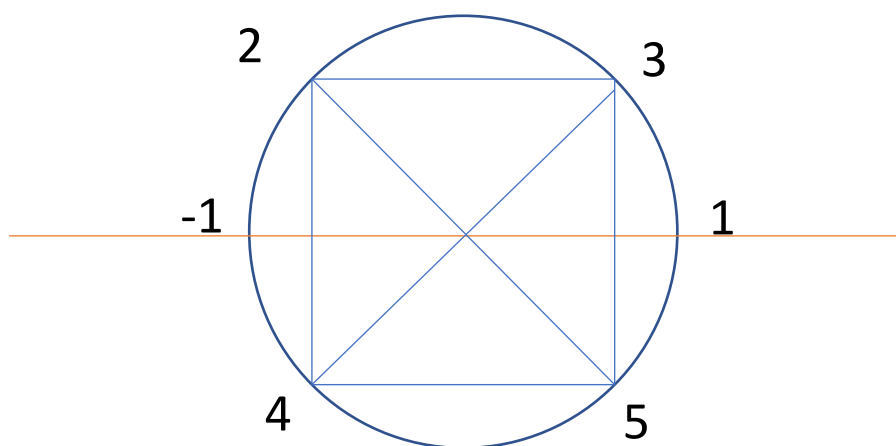
Pro základní mod 7 v tělese T_7 , 7 má tvar $4k+3$, $k=1$.

Pro $a=3$

Značení	a	$-a^{-1}$	-a	a^{-1}	Pozn.
C_1	3	2	4	5	3, 5 jsou generátory grupy
$1 \text{ a } -1$	1	1	6	6	

Pro $a=5$

Značení	a	$-a^{-1}$	-a	a^{-1}	Pozn.
C_1	5	4	2	3	3, 5 jsou generátory grupy
$1 \text{ a } -1$	1	1	6	6	

**Pozorování s Dirichletovy charaktery**

$$\omega = e^{\frac{\pi i}{3}}$$

Dirichlet	n						
	0	1	2	3	4	5	6 = -1
χ_0	0	1	1	1	1	1	1
χ_1	0	1	ω^2	ω	$-\omega$	$-\omega^2$	-1
χ_2	0	1	$-\omega$	ω^2	ω^2	$-\omega$	1
χ_3	0	1	1	-1	1	-1	-1
χ_4	0	1	ω^2	$-\omega$	$-\omega$	ω^2	1
χ_5	0	1	$-\omega$	$-\omega^2$	ω^2	ω	-1

Ilustrace pro T_{13}

Pro základní mod 13 v tělese T_{13} , 13 má tvar $4k+1$, $k=3$

Značení	a	$-a^{-1}$	-a	a^{-1}	Pozn.
C_1	2	6	11	7	2, 6, 11, 7 jsou generátory grupy
C_2	4	3	9	10	
C_3 prvky i a -i	8	8	5	5	degenerovaný čtverec
C_0 prvky 1 a -1	1	1	12	12	degenerovaný čtverec

13	exponent											
Generátor	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	8	3	6	12	11	9	5	10	7	1

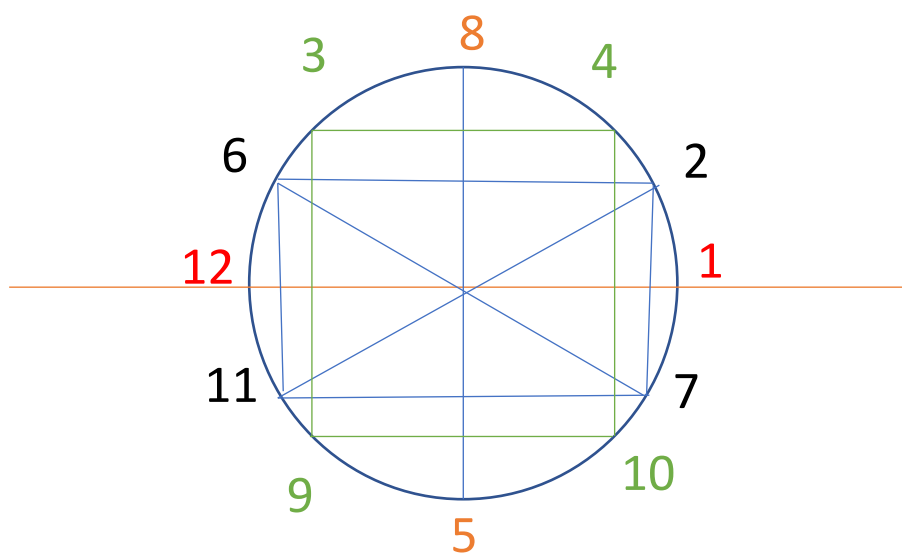
Zvolme generátor 2, $\langle 2 \rangle = Z_{13}^*$.

Prvky 8 a 5 v T_{13} tvoří degenerovaný čtverec a platí $8^{-1} = -8 = 5$.

Prvek 11 je generátor neboť $11 = -2 = 2^7 \pmod{13}$ kde $7 = (13-1)/2+1$ nesoudělné s $13-1 = 12$.

Čtverce	a	$-a^{-1}$	-a	a^{-1}
1	2	6	11	7
2	4	3	9	10
3	8	8	5	5
0	12	1	1	12

gen		
g	g	
g^2		
g^3		k=3
g^4		



Ilustrace pro T_{17}

Tabulka čtverců pro $p=17$ s různými vstupními generátory. $G_{17}=\{3, 5, 6, 7, 10, 11, 12, 14\}$

čtverce	a	$-a^{-1}$	-a	a^{-1}
1	3	11	14	6
2	9	15	8	2
3	10	5	7	12

gen		
g	g	
g^2		
g^3	g	

4	13	13	4	4
0	16	1	1	16

g^4		$k=4$
g^8		

čtverce	a	$-a^{-1}$	$-a$	a^{-1}
1	5	10	12	7
2	8	2	9	15
3	6	14	11	3
4	13	13	4	4
0	16	1	1	16

gen		
g	g	
g^2		
g^3	g	
g^4		$k=4$
g^8		

čtverce	a	$-a^{-1}$	$-a$	a^{-1}
1	6	14	11	3
2	2	8	15	9
3	12	7	5	10
4	4	4	13	13
0	16	1	1	16

gen		
g	g	
g^2		
g^3	g	
g^4		$k=4$
g^8		

17	exponent															
Generátor	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
5	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1
6	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1
7	7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
10	10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1
11	11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1
12	12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1
14	14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1
řád sloupce	16	8	16	4	16	8	16	2	16	8	16	4	16	8	16	1

Ilustrace pro T_{37}

Tabulka čtverců pro $p=37$, $p=4k+1$, $k=9$

$G_{37} = \{ 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35 \}$

Prvek 35 je generátor neboť $35 = -2 = 2^{19} \bmod 37$ kde $19 = (37-1)/2+1$ nesoudělné s $37-1 = 36$.

čtverce	a	$-a^{-1}$	$-a$	a^{-1}
1	2	18	35	19
2	4	9	33	28
3	8	23	29	14

gen		
g	g	
g^2		
g^3		$(3,36) \neq 1$

4	16	30	21	7
5	32	15	5	22
6	27	26	10	11
7	17	13	20	24
8	34	25	3	12
9	31	31	6	6
0	36	36	1	1

g^4		
g^5	g	
g^6		
g^7	g	
g^8		
g^9		$k=9$
36	$p-1$	

.

13.3 Izomorfismy multiplikativních grup se sudými řády

13.3.1 Úvod

V mnoha publikacích se dozvíme, že aditivní a multiplikativní zápis grupy je v podstatě stejný. No, není tomu tak. Evidentně pokud máme zápis grup Z_m^+ a Z_m^* , již se liší jejich vlastnosti včetně jejich řádu. První z nich je aditivní grupa a druhá multiplikativní grupa okruhu $(Z_m, +, *)$. Jistě zápis aditivních grup v multiplikativní notaci je možný, ale pro prvotního čtenáře dosti zmatený. Zde budeme důrazně používat aditivní a multiplikativní notace jen u příslušného druhu grup. Pro aditivní grupy platí mnoho tvrzení, které zde nebudeme všechny vypisovat. Tvrzení a jejich důkazy jsou uvedeny v příslušné literatuře.

13.3.2 Multiplikativní grupy se sudým řádem

Zvolme si nyní multiplikativní grupu Z_m^* , kde m je sudé číslo, $m = 2k = 2^{a+1} \cdot p_1^{a_1} \cdot \dots \cdot p_n^{a_n}$, $a \geq 0$, $a_i \geq 0$ a alespoň jedno a_i je různé od nuly. Dále označme aditivní grupu s n prvky G_n^+ .

Obecné vlastnosti:

- Grupy Z_m^* vesměs nejsou cyklické, vyjma grup typu $m=2p^k$, kde, p je liché prvočíslo, k přirozené číslo větší nebo rovno 1.
- Každá grupa Z_m^* je izomorfní s grupou $G_{\varphi(m)}^+$.
- Řád grupy Z_m^* je vždy omezen $\pi_m \leq \|Z_m^*\| \leq \frac{m}{2}$, kde π_m je počet prvočísel menších než m .
- Prvky v necyklické grupě Z_m^* ($a>0$) mají maximální řád $\frac{\varphi(m)}{4}$.
- Grupy Z_m^* pro $m = 2^{a+1} \cdot p_1^{a_1} \cdot \dots \cdot p_n^{a_n}$ jsou izomorfní direktnímu součinu grup $Z_m^* \cong G_{\varphi(m)}^+ \cong (Z_2^+)^T \times Z_F^+$, kde $T = 2^{n+2}$ a $F = \frac{\varphi(m)}{T}$.
- Počet prvků řádu 2 v grupě Z_m^* pro $m = 2^{a+1} \cdot p_1^{a_1} \cdot \dots \cdot p_n^{a_n}$, $a>1$, je právě $2^{n+2} - 1$.
- Nejvyšší řád prvku v grupě Z_F^+ je $R = Lcm(\varphi(2^a), \varphi(p_1^{a_1}), \dots, \varphi(p_n^{a_n}))$, tedy tato grupa je direktním součinem p -grup.

Řád těchto grup je tedy $\varphi(2k)$ neboli $m = 2k = 2^{a+1} \cdot p_1^{a_1} \cdot \dots \cdot p_n^{a_n}$, $a \geq 0$, $a_i \geq 0$, tedy je možné vybrat z těchto grup některé následující typické skupiny.

S1) Typ Z_m^* , $m=2p^k$, tj. $a=0$ a $m = 2k = 2^1 \cdot p_1^{a_1}$, p je liché prvočíslo, k přirozené číslo, $a_1>0$.

- Tyto grupy jsou cyklické a jsou izomorfní s cyklickou grupou $Z_{\varphi(m)}^+$ a ta je právě jedna.
- Nejvyšší řád prvku v grupě je $p-1$ a těchto prvků je $\varphi(p-1)$.
- V případě že číslo $\varphi(m) + 1$ je prvočíslo, pak je tato grupa izomorfní s multiplikativní grupou $Z_{\varphi(m)+1}^*$.
- Příklady tohoto druhu grup.

$m = 2p^k$	k			
p	1	2	3	4
3	6	18	54	162
5	10	50	250	1250
7	14	98	686	4802
11	22	242	2662	29282

Tyto grupy jsou cyklické.

Ilustrace

Cayleyho tabulka pro Z_{18}^*

Z_{18}^*	1	5	7	11	13	17	řád
1	1	5	7	11	13	17	1
5	5	7	17	1	11	13	6
7	7	17	13	5	1	11	3
11	11	1	5	13	17	7	6
13	13	11	1	17	7	5	3
17	17	13	11	7	5	1	2

Řád grupy je 6. Je izomorfní s cyklickou grupou Z_6^+ a s multiplikativní cyklickou grupou Z_7^* .

S2) Typ Z_m^* , $m=2^a p$, tj. $a>0$ a $m = 2k = 2^{a+1} \cdot p$, p je liché prvočíslo, k přirozené číslo.

- Tyto grupy nejsou cyklické a vzniknou grupovým násobením Kleinovy grupy s cyklickou grupou řádu p .
- Počet prvků řádu 2 je u multiplikativní grupy Z_m^* , kde $m=2^a p$ pro $a>2$ právě 7.

Cayleyho tabulka pro Z_{12}^*

$$12 = 2^2 \cdot 3$$

Z_{12}^*	1	5	7	11	řád
1	1	5	7	11	1
5	5	1	11	7	2
7	7	11	1	5	2
11	11	7	5	1	2

Řád grupy je 4. Je izomorfní s Kleinovou grupou $Z_2^+ * Z_2^+$.

Cayleyho tabulka pro Z_{24}^*

$$24 = 2^3 \cdot 3$$

Z_{24}^*	1	5	7	11	13	17	19	23	řád
1	1	5	7	11	13	17	19	23	1
5	5	1	11	7	17	13	23	19	2
7	7	11	1	5	19	23	13	17	2
11	11	7	5	1	23	19	17	13	2
13	13	17	19	23	1	5	7	11	2
17	17	13	23	19	5	1	11	7	2
19	19	23	13	17	7	11	1	5	2
23	23	19	17	13	11	7	5	1	2

Řád grupy je 8. Je izomorfní s grupou $Z_2^+ * Z_2^+ * Z_2^+$

Cayleyho tabulka pro Z_{56}^*

$$56=2^3 \cdot 7$$

Z_{56}	1	3	5	9	11	13	15	17	19	23	25	27	29	31	33	37	39	41	43	45	47	51	53	55	řád
1	1	3	5	9	11	13	15	17	19	23	25	27	29	31	33	37	39	41	43	45	47	51	53	55	1
3	3	9	15	27	33	39	45	51	1	13	19	25	31	37	43	55	5	11	17	23	29	41	47	53	6
5	5	15	25	45	55	9	19	29	39	3	13	23	33	43	53	17	27	37	47	1	11	31	41	51	6
9	9	27	45	25	43	5	23	41	3	39	1	19	37	55	17	53	15	33	51	13	31	11	29	47	3
11	11	33	55	43	9	31	53	19	41	29	51	17	39	5	27	15	37	3	25	47	13	1	23	45	6
13	13	39	9	5	31	1	27	53	23	19	45	15	41	11	37	33	3	29	55	25	51	47	17	43	2
15	15	45	19	23	53	27	1	31	5	9	39	13	43	17	47	51	25	55	29	3	33	37	11	41	2
17	17	51	29	41	19	53	31	9	43	55	33	11	45	23	1	13	47	25	3	37	15	27	5	39	6
19	19	1	39	3	41	23	5	43	25	45	27	9	47	29	11	31	13	51	33	15	53	17	55	37	6
23	23	13	3	39	29	19	9	55	45	25	15	5	51	41	31	11	1	47	37	27	17	53	43	33	6
25	25	19	13	1	51	45	39	33	27	15	9	3	53	47	41	29	23	17	11	5	55	43	37	31	3
27	27	25	23	19	17	15	13	11	9	5	3	1	55	53	51	47	45	43	41	39	37	33	31	29	2
29	29	31	33	37	39	41	43	45	47	51	53	55	1	3	5	9	11	13	15	17	19	23	25	27	2
31	31	37	43	55	5	11	17	23	29	41	47	53	3	9	15	27	33	39	45	51	1	13	19	25	6
33	33	43	53	17	27	37	47	1	11	31	41	51	5	15	25	45	55	9	19	29	39	3	13	23	6
37	37	55	17	53	15	33	51	13	31	11	29	47	9	27	45	25	43	5	23	41	3	39	1	19	6
39	39	5	27	15	37	3	25	47	13	1	23	45	11	33	55	43	9	31	53	19	41	29	51	17	6
41	41	11	37	33	3	29	55	25	51	47	17	43	13	39	9	5	31	1	27	53	23	19	45	15	2
43	43	17	47	51	25	55	29	3	33	37	11	41	15	45	19	23	53	27	1	31	5	9	39	13	2
45	45	23	1	13	47	25	3	37	15	27	5	39	17	51	29	41	19	53	31	9	43	55	33	11	6
47	47	29	11	31	13	51	33	15	53	17	55	37	19	1	39	3	41	23	5	43	25	45	27	9	6
51	51	41	31	11	1	47	37	27	17	53	43	33	23	13	3	39	29	19	9	55	45	25	15	5	6
53	53	47	41	29	23	17	11	5	55	43	37	31	25	19	13	1	51	45	39	33	27	15	9	3	6
55	55	53	51	47	45	43	41	39	37	33	31	29	27	25	23	19	17	15	13	11	9	5	3	1	2

Řád grupy je 24. Máme zde: 14 prvků řádu 6, 2 prvky řádu 3, 7 prvků řádu 2, 1 prvek řádu 1.

Pokud srovnáme řády prvků, zjistíme, že tato grupa je izomorfní s grupou $K_4^+ * Z_6^+$, kde K_4^+ je Kleinova grupa $Z_2^+ \times Z_2^+$.

Důkaz počtu prvků řádu 2:

	Řády prvků cyklické grupy Z_b^+		
Řády grupy $(Z_2^+)^2$	1	2	...
1	1	2	
2	2	2	
2	2	2	
2	2	2	

S3) Typ $m=2^a p^n$, $a>1$, $k>1$.

a) Počet prvků řádu 2 je u multiplikativní grupy Z_m^* , kde $m=2^a \cdot p^n$ pro $a>2$ právě 7.

Některé možnosti těchto grup

a=2	k			
p	1	2	3	4
3	12	36	108	324
5	20	100	500	2500
7	28	196	1372	9604
11	44	484	5324	58564

a=3	k			
p	1	2	3	4
3	24	72	216	648
5	40	200	1000	5000
7	56	392	2744	19208
11	88	968	10648	117128

Výpis sestavy z programu GAP pro $a=3$, $p=11$, $n=3$, $m=10648$, tedy $m = 2^3 \cdot 11^3$

```
gap> radygr(10648);
Řád grupy je 4840
```

Řád prvku	Počet prvků
1	1
2	7
5	4
10	28
11	10
22	70
55	40
110	280
121	110
242	770
605	440
1210	3080

Nejvyšší řád prvku je $Lcm(\varphi(2^2), \varphi(11^3)) = 1210$

Ilustrace

Ilustrace pro obecný typ pro $m = 2^{a+1} \cdot p_1^{a_1} \cdot \dots \cdot p_n^{a_n}$

$m = 2^5 \cdot 5 \cdot 7 \cdot 11 \cdot 11 \cdot 13 = 1761760$

$a=4$, $n=4$

Řád grupy je 506880

Výpis řádů prvků:

Řád	Počet
1	1
2	63
3	8
4	448
5	4

6	504
8	512
10	252
11	10
12	3584
15	32
20	1792
22	630
24	4096
30	2016
33	80
40	2048
44	4480
55	40
60	14336
66	5040
88	5120
110	2520
120	16384
132	35840
165	320
220	17920
264	40960
330	20160
440	20480
660	143360
1320	163840

Výpočet nejvyššího řádu z GAP: $\text{Lcm}(\Phi(2^4), \Phi(5), \Phi(7), \Phi(11 \cdot 11), \Phi(13)) = 1320$

13.3.3 Multiplikativní grupy řádu mocnin 2

Např. $Z_8, Z_{16}, \dots$

Obecné vlastnosti Z_m^* , $m=2^n$

- Řád grupy je 2^{n-1} .
- Maximální řád prvku grupy je 2^{n-2} .
- Počet prvků řádu 2 je 3.
- Grupa je izomorfní direktnímu součinu grup $Z_2^+ \times Z_{2^{n-2}}^+$, kde druhá grupa je cyklická.
-

Ilustrace Z_{32}^*

Řád grupy je 16.

	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	řád prvku
1	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	1
3	3	9	15	21	27	1	7	13	19	25	31	5	11	17	23	29	8
5	5	15	25	3	13	23	1	11	21	31	9	19	29	7	17	27	8
7	7	21	3	17	31	13	27	9	23	5	19	1	15	29	11	25	4
9	9	27	13	31	17	3	21	7	25	11	29	15	1	19	5	23	4

11	11	1	23	13	3	25	15	5	27	17	7	29	19	9	31	21	8
13	13	7	1	27	21	15	9	3	29	23	17	11	5	31	25	19	8
15	15	13	11	9	7	5	3	1	31	29	27	25	23	21	19	17	2
17	17	19	21	23	25	27	29	31	1	3	5	7	9	11	13	15	2
19	19	25	31	5	11	17	23	29	3	9	15	21	27	1	7	13	8
21	21	31	9	19	29	7	17	27	5	15	25	3	13	23	1	11	8
23	23	5	19	1	15	29	11	25	7	21	3	17	31	13	27	9	4
25	25	11	29	15	1	19	5	23	9	27	13	31	17	3	21	7	4
27	27	17	7	29	19	9	31	21	11	1	23	13	3	25	15	5	8
29	29	23	17	11	5	31	25	19	13	7	1	27	21	15	9	3	8
31	31	29	27	25	23	21	19	17	15	13	11	9	7	5	3	1	2

Izomorfní s grupou $Z_2^+ \times Z_2^3$

	00	01	02	03	04	05	06	07	10	11	12	13	14	15	16	17	řád
00	00	01	02	03	04	05	06	07	10	11	12	13	14	15	16	17	1
01	01	02	03	04	05	06	07	00	11	12	13	14	15	16	17	10	8
02	02	03	04	05	06	07	00	01	12	13	14	15	16	17	10	11	4
03	03	04	05	06	07	00	01	02	13	14	15	16	17	10	11	12	8
04	04	05	06	07	00	01	02	03	14	15	16	17	10	11	12	13	2
05	05	06	07	00	01	02	03	04	15	16	17	10	11	12	13	14	8
06	06	07	00	01	02	03	04	05	16	17	10	11	12	13	14	15	4
07	07	00	01	02	03	04	05	06	17	10	11	12	13	14	15	16	8
10	10	11	12	13	14	15	16	17	00	01	02	03	04	05	06	07	2
11	11	12	13	14	15	16	17	10	01	02	03	04	05	06	07	00	8
12	12	13	14	15	16	17	10	11	02	03	04	05	06	07	00	01	4
13	13	14	15	16	17	10	11	12	03	04	05	06	07	00	01	02	8
14	14	15	16	17	10	11	12	13	04	05	06	07	00	01	02	03	2
15	15	16	17	10	11	12	13	14	05	06	07	00	01	02	03	04	8
16	16	17	10	11	12	13	14	15	06	07	00	01	02	03	04	05	4
17	17	10	11	12	13	14	15	16	07	00	01	02	03	04	05	06	8

13.4 Nadgrupy

92. Definice nadgrupy

Cyklickou multiplikativní grupu G_p^* nazveme nadgrupou multiplikativní grupy H_q^* právě tehdy, když H_q^* je podgrupou grupy G_p^* . Pokud je řád grupy H_q^* nejmenší možný ze všech podgrup G_p^* , nazveme G_p^* minimální nadgrupou grupy H_q^* .

93. Tvzení (bez důkazů)

- Nechť G_p^* je nadgrupou grupy H_q^* . Pak existuje podgrupa $Z_{q(p)}^* \trianglelefteq G_p^*$, která je izomorfní s grupou $H_q^* \cong Z_{q(p)}^*$.
- Nechť $H_q^* \cong Z_{q(p)}^*$ a $\mathbf{v}$ je generátor nadgrupy G_p^* . Pak generátor izomorfní podgrupy $Z_{q(p)}^*$ má $\mathbf{v}$ nadgrupě G_p^* řád $q-1$, a platí $v^{q-1} \equiv 1 \pmod{p}$.
- Nechť $\mathbf{v}$ je generátor nadgrupy G_p^* . Nechť $x = \frac{p-1}{q-1}$. Pak generátor $\mathbf{w}$ podgrupy $Z_{q(p)}^* \trianglelefteq G_p^*$ je určen vztahem $w = v^x \pmod{p}$.
- Nechť $\mathbf{u}$ je generátor grupy H_q^* a $\mathbf{v}$ generátor nadgrupy G_p^* . Nechť $x = \frac{p-1}{q-1}$. Nechť prvek $a \in H_q^*$. Pak existuje prvek b v podgrupě $Z_{q(p)}^* \trianglelefteq G_p^*$ a je určen vztahem $b = v^{x \cdot \log_{u(q)} a} \pmod{p}$.

94. Tvzení (bez důkazů)

- Ke každé multiplikativní grupě H_q^* existuje nekonečně mnoho nadgrup G_p^* z nichž je právě jedna minimální nadgrupou.
- Pro multiplikativní grupu H_3^* je každá grupa G_p^* nadgrupou a $H_3^* \cong Z_{2(p)}^*$ a $Z_{2(p)}^* = \{1, p-1\}$.
- Pro multiplikativní grupu H_5^* je každá grupa G_p^* pro prvočíslo tvaru $p=4k+1$ nadgrupou, tj. $H_5^* \cong Z_{4(p)}^* = \{1, a, b, p-1\}$, $a \cdot b \equiv 1 \pmod{p}$, $a + b \equiv p$ tj. $Z_{4(p)}^* = \{1, a, p-a, p-1\}$.
- Pokud $\mathbf{v}$ je generátor grupy G_p^* , pak $a = v^{\frac{p-1}{4}} \pmod{p}$ a je generátorem $Z_{4(p)}^*$.
- Pokud existuje G_p^* , kde p je prvočíslo takové, že pro prvočíslo q splňuje vztah $p = (q-1) + 1$, pak G_p^* je nadgrupou grupy H_q^* .

14 Ilustrace

Zde jsou uvedeny ilustrace, které se mi nehodilo zařadit do výše uvedeného textu.

Ilustrace pojmů pro grupu Z_7^*

Číselná multiplikativní grupa Z_7^* má řád $\varphi(7)=7-1=6$.

Pro výsledek násobení prvků grupy platí $a \cdot b \pmod{7}$, $a, b \in \{1, 2, 3, 4, 5, 6\}$

Počet generátorů grupy Z_7^* je $\varphi(6) = 2$

Dělitelé čísla 6 jsou čísla $d = 1, 2, 3, 6$

Počty prvků řádu

$1 \rightarrow \varphi(1)=1 \dots 1$ prvek řádu 1

$1 \rightarrow \varphi(2)=1 \dots 1$ prvek řádu 2

$1 \rightarrow \varphi(3)=2 \dots 2$ prvky řádu 3

$1 \rightarrow \varphi(6)=2 \dots 2$ prvky řádu 6 = počet generátorů

Generátory grupy Z_7^* jsou prvky množiny $G_7 = \{3, 5\}$.

Číselná multiplikativní cyklická grupa mod 7						řád prvku
1	2	3	4	5	6	1
2	4	6	1	3	5	3
3	6	2	5	1	4	6
4	1	5	2	6	3	3
5	3	1	6	4	2	6
6	5	4	3	2	1	2

Podgrupy Z_7^*

Dělitelé řádu grupy $n = 6$ jsou 1, 2, 3, 6. Existuje 1 podgrupa řádu 1, 1 podgrupa řádu 2 a 1 podgrupa řádu 3.

Podgrupa řádu 1 má prvek $\{1\}$.

Podgrupa řádu 2 má prvky $N_{2/7} = \{1, 6\}$ neboli $\{1, u^3\}$.

Podgrupa řádu 3 má prvky $N_{3/7} = \{1, 2, 4\}$ neboli $\{1, u^2, u^4\}$.

Budeme faktorizovat podle $N_{3/7} = \{1, 2, 4\}$.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
4	4	1	5	2	6	3

Tedy pokud označíme množiny – rozkladové třídy - $A = \{1, 2, 4\}$ a $B = \{3, 5, 6\}$, pak dostaneme grupu Z_2^+ .

Operace s rozkladovými třídami provádíme modulo 7, tj. $4 \cdot 3 \pmod{7} = 5$ atd.

A	B
B	A

což je faktorgrupa $Z_7^* / N_{3/7}$

A budeme faktorizovat podle $N_{2/7} = \{1, 6\}$

	1	2	3	4	5	6
1	1	2	3	4	5	6
6	6	5	4	3	2	1

Operace s rozkladovými třídami provádíme modulo 7, tj. $6 \cdot 2 \pmod{7} = 5$ atd.

1,6	2,5	3,4
2,5	3,4	1,6
3,4	1,6	2,5

Označme $0 = \{1,6\}$, $1 = \{2,5\}$, $2 = \{3,4\}$, pak

0	1	2
1	2	0
2	0	1

to je grupa Z_3^+

a tedy faktorgrupa $Z_7^*/N_{2/7} \cong Z_3^+$

Generování grupy Z_7^* generátory 3 a 5

Exponent	1	2	3	4	5	6
Generátor						
3	3	2	6	4	5	1
5	5	4	6	2	3	1

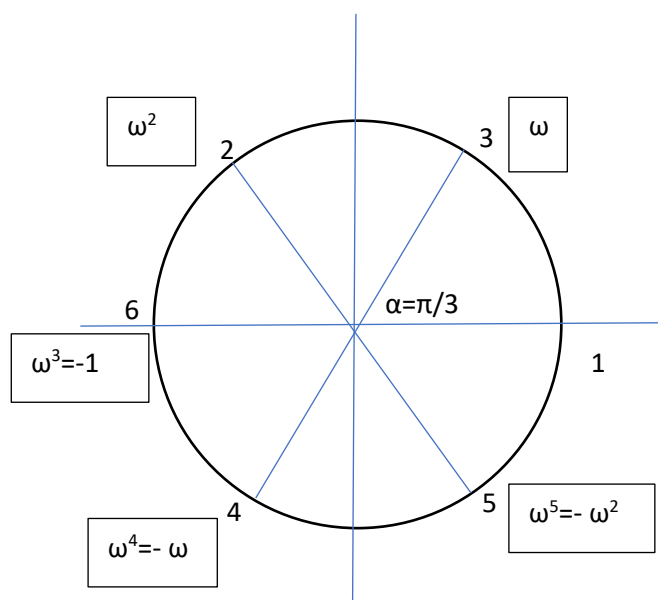
Tabulka diskretních logaritmů pro $p=7$.

7	x					
	1	2	3	4	5	6
$\log_3 x$	6	2	1	4	5	3
$\log_5 x$	6	4	5	2	1	3

Např. $\log_5 4 = 2$ tj. $5^2 = 4$, vše mod 7.

Izomorfní zobrazení Z_7^* na C^*

$$\omega = e^{\frac{2\pi i}{p-1}} = e^{\frac{\pi i}{3}}$$



Kořeny rovnice

$$x^6 - 1 = 0$$

Jsou izomorfní s $1, 2, \dots, 6$.

Pro kořeny $a_1, \dots, a_6$ rovnice platí v tělese T_7

$$a_1 \cdot a_2 \cdot \dots \cdot a_6 = -1$$

$$a_1 + a_2 + \dots + a_6 = 0$$

Tedy mod 7

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \bmod 7 = 720 \bmod 7 = 6 \bmod 7 = -1 \bmod 7$$

$$1 + 2 + 3 + 4 + 5 + 6 \bmod 7 = 21 \bmod 7 = 0$$

15 Závěr

Toto je konec základního přehledu. Pokračování snad někdy dopíšu. Zejména je důležité se seznámit s klasifikací jednoduchých grup, což je jeden z fascinujících vyřešených problémů teorie grup. Tak příště.

16 Literatura

- Bulant, M. (2007). *Teorie čísel*. Načteno z Web MUNI:
<https://is.muni.cz/el/1431/jaro2007/M6520/um/main-print.pdf>
- GAP Group. (29. 2 2020). *The GAP - Groups, Algorithms, Programming - a System for Computational Discrete Algebra*. Načteno z GAP: <https://www.gap-system.org/>
- Halaš, R. (2014). *Úvod do teorie čísel*. Olomouc: Universita Palackého Olomouc, Přírodovědecká fakulta.
- Jahoda, P. (2000). *Základy teorie čísel a jejích aplikací pro nematematické*. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava.
- Křížek, M. (1995). O Fermatových číslech. *Pokroky matematiky, fyziky a astronomie*, stránky Pokroky matematiky, fyziky a astronomie, Vol. 40 (1995), No. 5, 243–253.
- Liczman, P. (2020). *Abelovská tělesa a Dirichletovy charaktery*. Brno: Přírodovědecká fakulta, Masarykova univerzita, Ústav matematiky a statistiky.
- Nejdalková, T. (2018). *Vlastnosti konečných grup s programem GAP*. Načteno z
<https://theses.cz/id/o9h46f/>
- Růžička, P. (2019). *Elementární teorie grup*. Načteno z
<https://www2.karlin.mff.cuni.cz/~ruzicka/ctg/kapitola1.pdf>:
<https://www2.karlin.mff.cuni.cz/~ruzicka/ctg/kapitola1.pdf>
- Stanovský, D. (2009). *Základy algebry*. Načteno z mff.wladik.net:
http://mff.wladik.net/10zs/skripta_zalg.pdf
- Stanovský, D. (10. 6 2019). *Nový text o grupách*. Načteno z
https://www.karlin.mff.cuni.cz/~stovicek/dl/19-20-ls/alg_grupy.pdf
- Stanovský, D. (2021). *Učební text Algebra 2020/21*. Načteno z
<https://www.karlin.mff.cuni.cz/~kala/2021alg/algebra21.pdf>
- Stanovský, D. (2021). *Základy algebry pro informatiky*. Načteno z mff.cuni.cz:
https://www2.karlin.mff.cuni.cz/~stanovsk/vyuka/alginf_text.pdf
- Wikipedie, P. (8. 7 2018). *Fermatovo číslo*. Načteno z Wikipedia:
https://cs.wikipedia.org/w/index.php?title=Fermatovo_%C4%8D%C3%ADslo&oldid=16352190
- Wikipedie, P. (8. 5 2020). *Diskrétní logaritmus*. Načteno z cs.wikipedia.com: Wikipedie: Otevřená encyklopedie: Diskrétní logaritmus [online]. c2020 [citováno 8. 07. 2021]. Dostupný z WWW: <https://cs.wikipedia.org/w/index.php?title=Diskr%C3%A9tn%C3%AD_logaritmus&oldid=18491846>