Univerzita Karlova

Pedagogická fakulta

Katedra matematiky a didaktiky matematiky

BAKALÁŘSKÁ PRÁCE

Polynomiální a exponenciální kongruence

Polynomial and exponential congruences

Matěj Kovářík

Vedoucí práce:	JUDr. Mgr. Filip Beran
Studijní program:	Specializace v pedagogice
Studijní obor:	Matematika a Anglický jazyk se zaměřením na vzdělávání

2023

Odevzdáním této bakalářské práce na téma Polynomiální a exponenciální kongruence potvrzuji, že jsem ji vypracoval pod vedením vedoucího práce samostatně za použití v práci uvedených pramenů a literatury. Dále potvrzuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

Praha, 4. 12. 2023

V první řadě chci poděkovat vedoucími této práce, doktoru Filipovi Beranovi, za čas, který mi věnoval při vedení této práce, poskytnuté materiály, podnětné rady a inspirativní výuku. Dále děkuji magistru Jakubovi Michalovi za podnětnou diskuzi k tématu. Děkuji i své sestře za pomoc s prací a jí a své mamince za obrovskou podporu v životě i studiu. V neposlední řadě děkuji svým přátelům, kolegům a své přítelkyni za to, že tu pro mě jsou, když potřebuji.

ABSTRAKT

Tato bakalářská práce pojednává o polynomiálních a exponenciálních kongruencích a o náhledu na ně z hlediska teorie grup. Práce je rozdělena do tří kapitol. První se věnuje polynomiálním kongruencím, zejména kvadratickým. U nich se zabývá určováním kvadratických zbytků a nezbytků a metodám nalezení řešení včetně úpravy kongruence postupně pro modul daný prvočíslem, mocninou prvočísla, speciálně mocniny dvojky a nakonec složeným číslem. Zvláštní pozornost je věnována Legendrovu symbolu a kvadratické reciprocitě. U polynomiálních kongruencí vyšších stupňů načrtává zobecnění některých prezentovaných poznatků o kvadratických kongruencích. Druhá kapitola pojednává o exponenciálních kongruencích, především v návaznosti na tvrzení, která plynou z jejich zkoumání. Těmi jsou Malá Fermatova věta, Eulerova funkce a věta a Carmichaelova funkce a věta. Zároveň se věnuje i jiným aplikacím těchto poznatků, jako např. zjišťování posledních cifer nebo Fermatův test prvočíselnosti. Ve třetí kapitole nabízí rozšiřující a shrnující pohled na předchozí dvě kapitoly pomocí poznatků teorie grup. Hlavními probíranými koncepty jsou zde řády prvků, generátory (alias primitivní prvky) a izomorfismy mezi grupami. Metody řešení a aplikace poznatků jsou v celé práci ilustrovány řešenými úlohami.

KLÍČOVÁ SLOVA

kvadratická kongruence, exponenciální kongruence, Legendrův symbol, kvadratická reciprocita, Malá Fermatova věta, Eulerova funkce, Carmichaelova funkce, multiplikativní grupa $\mathbb{Z}_n^*$

ABSTRACT

This bachelor's thesis deals with polynomial and exponential congruences, and their features from the point of view of group theory. The thesis is divided into three chapters. First chapter concerns itself with polynomial, especially quadratic congruences. It covers classification of quadratic residues and non-residues and methods of solving including simplifications of congruences separately for modulo odd prime, odd prime power, power of two, and composite number. Special attention is given to Legendre symbol and quadratic reciprocity. Generalisations of some of these concepts are mentioned in a part about polynomial congruences of higher degree. Second chapter encompasses exponential congruences and more importantly theorems and functions emerging from observing such congruences. These include Fermat's little theorem, Euler's totient function and Euler's theorem, and Carmichael function and theorem. In addition, it provides further applications of these results, such as finding last digits of numbers or Fermat primality test. Third chapter offers deeper insight into the subject matter of the previous two chapters using concepts of group theory, such as orders of elements, generators (i.e., primitive roots), and isomorphisms between groups. All methods of solving congruences and different applications of presented results are demonstrated through examples.

KEYWORDS

quadratic congruence, exponential congruence, Legendre symbol, quadratic reciprocity, Fermat's little theorem, Euler's totient function, Carmichael function, multiplicative group of integers modulo n

Obsah

Úvod

Po porozumění lineárním rovnicím a jejich soustavám je dalším logickým krokem zkoumání rovnic kvadratických, po nich dále polynomiálních vyšších stupňů. Po porozumění jim je přirozenou otázkou, jak řešit rovnice, kde se neznámá objevuje v exponentu, tedy tzv. exponenciální rovnice. Obě tyto rovnice se řeší jinými způsoby než lineární a dají se považovat za složitější. Jinak tomu není ani v prostředí kongruencí, kde je nárůst obtížnosti oproti lineárním kongruencím možná ještě větší. Právě řešeními takových kongruencí a jejich širšími souvislostmi se v této práci zabývám.

Cílem této práce je podat poznatky o zde zkoumaných kongruencích a matematických strukturách, pokud možno intuitivním až konstruktivistickým způsobem. Ke většině prezentovaných poznatků se tedy snažím čtenáře přivést pomocí intuice a cílených pozorování. Zároveň z poznatků vyvozuji nové a pojím je do souvislostí. I přesto je pro porozumění tématu očekávaná vstupní znalost čtenáře. Kromě ovládání elementární matematiky na úrovni střední školy je k dobrému porozumění všem tématům, kterých se tato práce dotýká, třeba disponovat relativně dobrou úrovní porozumění lineárním kongruencím a základní znalostí pojmů teorie grup (grupa a její axiomy, těleso).

Konstruktivistický přístup ovlivnil členění této práce. První kapitolou jsou polynomiální kongruence, druhou jsou exponenciální a třetí grupový náhled. To se vymyká členění v drtivé většině literatury, kde se začíná s exponenciálními kongruencemi a znalost grupového kontextu se často předpokládá. Mně ovšem toto členění připadá intuitivnější z důvodů, které jsem nastínil v prvním odstavci. Otázka řešení polynomiálních rovnic (potažmo i kongruenčních) mi přijde o mnoho přirozenější než otázka řešení exponenciálních rovnic. Toto členění má ale svá úskalí. Občas je v práci potřeba koncept, nejčastěji pro důkaz nebo lepší názornost, který si nelze intuitivně zavést v danou chvíli. Proto se v práci v několik případech odkazuji na pozdější kapitoly.

Motivací k sepsání této práce byl předmět Číselné obory a teorie čísel, který jsem v rámci svého studia absolvoval. V něm jsme se mimo jiné učili právě o kvadratických a exponenciálních kongruencích a strukturálním náhledu na ně. K těmto tématům ovšem chyběl nějaký souhrnný učební text v českém jazyce a tato práce jako takový text může

sloužit. Další motivací je moje fascinace čistou matematikou a výzva, kterou pro mě napsání matematické práce představuje.

V první kapitole se zabývám polynomiálními kongruencemi, z velké většiny kvadratickými. Tato kapitola je členěna podle povahy modulu, zda je lichým prvočíslem, mocninou lichého prvočísla, mocninou dvojky, nebo složeným číslem. Nejdříve se vždy věnuji způsobům, jak rozhodnout, zda daná kongruence vůbec má řešení a dále způsobům jeho nalezení. Objevují se zde koncepty jako Legendrův symbol a kvadratická reciprocita.

Ve druhé kapitole se zabývám exponenciálními kongruencemi. Ze zkoumání těchto kongruencí plynou důležité věty (Malá Fermatova, Eulerova, Carmichaelova) a funkce (Eulerova, Carmichaelova), které mají širší využití a těm také věnuji notnou pozornost.

Třetí kapitola poskytuje rozšiřující a prohlubující vhled do předchozích dvou kapitol skrz zkoumání množin modulo n ze strukturálního pohledu. Zde se čtenář seznámí s pojmy jako řád grupy, řád prvku, generátor a izomorfismus. Tato kapitola je o něco méně formální než předchozí dvě.

Jedním z hlavních průkopníků problematiky, kterou se zabývá i tato práce, byl dnes již legendární matematik Carl Friedrich Gauss (1777-1855). Proto anglický překlad jeho *Disquisitiones Arithmeticae* (Gauss, 1986), které napsal ve svých 21 letech a vydláždily cestu moderní teorii čísel, patří mezi hlavní zdroje této práce. Mnoho poznatků, kterými se v práci zabývám nicméně objevili již matematici před Gaussem. Čtyři z nich Gauss zmiňuje v předmluvě, jsou jimi neméně legendární Pierre de Fermat (1607-1665), Leonhard Euler (1707-1783), Joseph-Louis Lagrange (1736-1813) a v neposlední řadě Adrien-Marie Legendre (1752-1833). Mezi další hlavní zdroje patří kniha *Kouzlo čísel* (Křížek, 2018) a skripta *Algebra* (Stanovský, 2022). Ještě chci zmínit bakalářskou práci Natálie Kaňákové (2022) *Lineární diofantické rovnice a kongruence*, na kterou moje práce tematicky navazuje a někdy se na ni odkazuji pro vysvětlení konceptů lineárních kongruencí.

1 Polynomiální kongruence

Před započetím našeho zkoumání připomeňme několik základních poznatků o kongruencích; co vlastně kongruencí míníme, co je kongruenční rovnice a jak s nimi pracovat.

Definice 1 (Kongruence)
Nechť $a, b \in \mathbb{Z}$ a $n \in \mathbb{N}$. Říkáme, že a *je kongruentní* b *modulo* n a zapisujeme:

$$a \equiv b \pmod{n}$$

právě tehdy, když $n|a - b$.

Tento koncept zavedl Gauss ve svých *Disquisitiones Arithmeticae* (dále jen DA) a už tehdy ho definoval v podstatě stejným způsobem: „Si numerus a numeronum b, c differentiam metitur. b et c *secundum a congrui* dicuntur, sin minus, *inconguri*." (s. 9).

Pozn. 1: Do přirozených čísel značených $\mathbb{N}$ nepočítáme nulu. V případě, že budeme zohledňovat i nulu, budeme značit $\mathbb{N}_0$. Připouštíme tedy i modul 1, ve kterém jsou ale všechna celá čísla kongruentní 0, takže tvoří triviální a pro nás nezajímavý případ.

Pozn. 2: Je třeba rozlišit mezi pojmy *kongruence* a *kongruenční rovnice*. Pojem kongruence tak, jak jsme ho zavedli, označuje relaci. Kongruenčními rovnicemi chápeme kongruence, ve kterých se vyskytuje neznámá. Zkráceně dále ovšem budeme kongruencemi rozumět kongruenční rovnice, nemůže-li dojít ke zmatení.

Pozn. 3: V případech, kdy bude z kontextu jasné, v jakém modulu se nacházíme, budeme zápis $(\mathrm{mod}\, n)$ vynechávat.

Pro řešení rovnic se užívá tzv. ekvivalentních úprav. Těmi jsou v prostředí kongruencí přičítání stejného čísla k oběma stranám (obdobně pro odčítání), násobení obou stran stejným číslem a speciálně umocnění obou stran stejným exponentem. Podrobněji (Stanovský, 2022, s. 5).

Z tradičních ekvivalentních úprav chybí jen dělení. To lze za určitých podmínek také provést. Můžeme dělit číslem, kterým jsou obě strany dělitelné. V případě, že je tímto číslem dělitelný i modul, musíme vydělit i ten. Podrobněji opět (Stanovský, 2022, s. 5).

Až po těchto znalostech se můžeme vůbec pokoušet řešit kongruenční rovnice. Nejjednodušším případem jsou lineární kongruence, kterým se podrobně věnuje např. (Kaňáková, 2022).

Na lineární kongruence přirozeně navazujeme kongruencemi polynomiálními (též polynomickými). Těmi jsou rovnice kvadratické, kubické, kvartické a obecně polynomiální rovnice stupně n. V této práci budeme používat pro obecný stupeň polynomu spíše k, protože n budeme většinou značit obecný modul. Kvadratické rovnice tvoří standardní součást školské matematiky, žáci se mohou setkat i se speciálními případy polynomiálních rovnic vyšších stupňů. Oproti lineárním rovnicím se liší metody řešení i očekáváný počet řešení. S polynomiální kongruencemi tomu není jinak. Formálně si definujme, jakými kongruencemi se v této kapitole tedy budeme zabývat.

Definice 2 (Kvadratická kongruence)
Kvadratickou kongruencí rozumíme kongruenční rovnici:

$$ax^2 + bx + c \equiv 0 \pmod{n}$$

kde $a, b, c \in \mathbb{Z},\ n \in \mathbb{N}$ a $a \not\equiv 0 \pmod{n}$. a, b, c jsou koeficienty a x celočíselná neznámá.

Pozn.: Jako různá řešení chápeme nekongruentní řešení.

Obecněji:

Definice 3 (Polynomiální kongruence stupně k)
Polynomiální kongruencí rozumíme kongruenční rovnici:

$$a_k x^k + a_{k-1} x^{k-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{n}$$

kde $a_0, \ldots, a_k \in \mathbb{Z}, n \in \mathbb{N}$ a $a_k \not\equiv 0 \pmod{n}$. $a_0, \ldots, a_k$ jsou koeficienty a x celočíselná neznámá.

Stejně jako u rovnic i u kongruencí s rostoucím stupněm polynomu roste obtížnost řešení, byť jsou teoreticky kongruence snazší. Přeci jen existuje vždy pouze konečný počet hodnot, které lze dosadit za x (bez ohledu na to, zda kongruenci splňuje), narozdíl od rovnic nad reálnými či komplexními čísly. To nám ale neříká nic o náročnosti nalezení konkrétních

řešení. Nejjednodušším případem jsou kongruence kvadratické, budeme se proto převážně věnovat právě jim.

Ze zkušenosti s lineárními kongruencemi se budeme zabývat nejprve moduly prvočísel a následně moduly složených čísel. V některých případech se budeme zvlášť zabývat i moduly mocnin prvočísel. Obvykle budeme prvočísla značit p, často pouze lichá, bude vždy upřesněno. Podobně n bude značit někdy složené číslo, někdy jakékoliv přirozené číslo.

1.1 Kvadratické kongruence mod p

Mějme kvadratickou kongruenci $17x^2 + 25x + 7 \equiv 0 \pmod{31}$ a pokusme se ji vyřešit. Můžeme využít intuice a poznatků, které máme o řešení kvadratických rovnic.

Řešení dosazováním

Můžeme systematicky dosazovat čísla, dokud nenajdeme řešení. Modulo 31 potřebujeme v nejhorším případě (tj. že kongruence nemá řešení) dosadit 31 čísel; od 0 do 30. Dosazováním lze tedy zjistit, že řešeními jsou $x_1 \equiv 14$ a $x_2 \equiv 21$. Obecně modulo n je třeba dosadit maximálně n čísel před nalezením řešení (či zjištění, že kongruence nemá řešení), tedy nějaký konečný počet čísel, o kterých navíc víme, že jsou to celá čísla od 0 do $n - 1$. Nevýhodou tohoto postupu je časová náročnost přímo úměrná velikosti modulu. Na druhou stranu se hodí pro malé moduly, např. kongruenci $x^2 + x + 4 \equiv 0 \pmod{5}$ vyřešíme dosazováním velmi rychle. Řešení je jediné a to $x \equiv 2$. Naopak vyřešit kongruenci $x^2 + x + +4 \equiv 0 \pmod{97}$ dosazováním by bylo velmi časově náročné.

Řešení pomocí obecného vzorce

Pro rovnici $ax^2 + bx + c = 0$ má vzorec podobu $x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ (Pozn.: v angličtině se vzorec označuje *quadratic formula*. V češtině pro něj žádný konvenční termín není, nejčastěji se hovoří o výpočtu pomocí diskriminantu). Nejdříve tedy vyřešme rovnici $17x^2 + 25x + 7 = 0$:

$$x_{1,2} = \frac{-25 \pm \sqrt{25^2 - 4 \cdot 17 \cdot 7}}{2 \cdot 17}$$

$$x_{1,2} = \frac{-25 \pm \sqrt{625 - 476}}{34}$$

$$x_{1,2} = \frac{-25 \pm \sqrt{149}}{34}$$

To jsou hledaná řešení (vzhledem k nesoudělnosti 25 a 34 a prvočíselnosti 149 nelze dále zkrátit ani částečně odmocnit). Před aplikací stejného vzorce na kongruenci se zamysleme, v čem by mohl být problém. Kvadratická rovnice nemá (reálné) řešení v případě, že diskriminant vyjde záporný. To ale v kongruenci problém nečiní, stačí nalézt kladné číslo, které je danému zápornému kongruentní, tedy přičíst k němu modul. Co naopak nečiní

problém v rovnici, ale mohlo by v kongruenci je, kdyby jako v tomto případě nešlo celočíselně dělit ani odmocnit. V kongruencích neceločíselné dělení definováno není, ale jsou v nich definovány inverzní prvky. Stačí tedy najít inverzní prvek ke jmenovateli a tím vynásobit součet v čitateli. Pro odmocninu se pokusme najít nějaký konkrétní příklad, aplikujme tedy vzorec na kongruenci:

$$x_{1,2} \equiv \frac{-25 \pm \sqrt{25^2 - 4 \cdot 17 \cdot 7}}{2 \cdot 17}$$

$$x_{1,2} \equiv \frac{6 \pm \sqrt{(-6)^2 - 11}}{3}$$

$$x_{1,2} \equiv \frac{6 \pm \sqrt{25}}{3}$$

$$x_{1,2} \equiv \frac{6 \pm 5}{3}$$

V tomto případě jsme se ovšem vyhnuli tomu, že bychom museli řešit, jak vypadá odmocnina nějakého čísla modulo 31, které nad reálnými čísly nemá celočíselnou odmocninu. $\frac{6}{3}$ můžeme spočítat „běžně“ a 5 vynásobme inverzním prvkem ke 3, tím je 21. Řešení kongruence tedy jsou:

$$x_1 \equiv 2 + 5 \cdot 21 \equiv 2 + 105 \equiv 2 + 12 = 14$$

$$x_2 \equiv 2 - 12 = -10 \equiv 21$$

Tuto kongruenci jsme také vyřešili poměrně rychle. Co když ale odmocnina nevyjde tak jasně? Zkusme stejným způsobem vyřešit zmíněnou kongruenci $x^2 + x + 4 \equiv 0 \pmod{97}$:

$$x_{1,2} \equiv \frac{-1 \pm \sqrt{1^2 - 4 \cdot 4}}{2}$$

$$x_{1,2} \equiv \frac{-1 \pm \sqrt{-15}}{2}$$

$$x_{1,2} \equiv \frac{-1 \pm \sqrt{82}}{2}$$

Jak postupovat v tomto případě již není jasné. Zkoumejme raději nejprve v menším modulu. Místo toho, abychom řešili jinou kongruenci, zkusme řešit $17x^2 + 25x + 7 = 0$ jiným

způsobem, tak ověříme i funkčnost různých metod. Alternativně lze řešit kvadratické rovnice doplněním na čtverec, což je také způsob, jakým se předchozí obecný vzorec odvozuje.

Řešení doplněním na čtverec

Řešme kongruenci $17x^2 + 25x + 7 \equiv 0 \pmod{31}$ doplněním na čtverec. Nejdříve si u x^2 zařiďme koeficient 1:

$$\begin{aligned} 17x^2 + 25x + 7 &\equiv 0 \ /\cdot 2 \\ 3x^2 + 19x + 14 &\equiv 0 \ /\cdot 11 \\ 2x^2 + 23x + 30 &\equiv 0 \\ 2x^2 - 8x + 30 &\equiv 0 \ /:2 \\ x^2 - 4x + 15 &\equiv 0 \end{aligned}$$

Pozn.: Úpravu šlo provést rovnou přenásobením celé kongruence 11, což je inverzní prvek k 17. Prezentovaný postup považujeme za intuitivnější.

Nyní doplňme na čtverec:

$$\begin{aligned} x^2 - 4x + 4 &\equiv -15 + 4 \\ (x-2)^2 &\equiv -11 \\ (x-2)^2 &\equiv 20 \end{aligned}$$

Provedením substituce $y = x - 2$ dostaneme kongruenci:

$$y^2 \equiv 20$$

Teď stačí zjistit, jak vypadá druhá odmocnina z 20 modulo 31.

Pozn.: $\sqrt{a} \pmod{p}$ budeme v prostředí kongruencí formulovat tak, že řešíme kongruenci $x^2 \equiv a$, tedy že hledáme čísla taková, která jsou po umocnění na druhou kongruentní a. Existují ovšem taková x pro všechna a? Pokud ne, za jakých okolností existují? Až po zodpovězení těchto otázek se lze přesunout k hledání řešení.

1.1.1 Kvadratické zbytky a nezbytky mod p

Pozorujme chování druhých mocnin v nějakém malém modulu. Zvolme 11, abychom neměli moc malý vzorek:

$$0^2 \equiv 0 \qquad 6^2 \equiv (-5)^2 \equiv 3$$

$$1^2 = 1 \qquad 7^2 \equiv (-4)^2 \equiv 5$$

$$2^2 = 4 \qquad 8^2 \equiv (-3)^2 \equiv 9$$

$$3^2 = 9 \qquad 9^2 \equiv (-2)^2 \equiv 4$$

$$4^2 = 16 \equiv 5 \qquad 10^2 \equiv (-1)^2 \equiv 1$$

$$5^2 = 25 \equiv 3$$

Pozn.: Lze pozorovat, že nepřekvapivě i v kongruencích platí $a^2 \equiv (-a)^2$.

Kongruence $x^2 \equiv a \pmod{11}$ má tedy řešení právě tehdy, když $a \equiv 0, 1, 3, 4, 5, 9$. Většina z nich byla očekávatelná, jen pro 3 a 5 to nebylo zřejmé. Dále $2, 6, 7, 8$ a 10 nejsou kongruentní žádné druhé mocnině modulo 11, a tudíž je třeba nejdříve rozhodnout o existenci řešení před snahou o nalezení nějakého řešení. Z tohoto pozorování přirozeně vyplývají dva pojmy.

Definice 4 (Kvadratický zbytek, kvadratický nezbytek; *quadratic residue, quadratic non-residue*)
Nechť $n \in \mathbb{N}$ a $a \in \mathbb{Z}$. Pokud existuje x takové, že je řešením kvadratické kongruence $x^2 \equiv$ $\equiv a \pmod{n}$, pak se a nazývá *kvadratický zbytek* (také *kvadratické reziduum*) modulo n. V opačném případě se a nazývá *kvadratický nezbytek* modulo n (Křížek, 2018, s. 76).

Pozn.: 0 a 1 jsou triviálně kvadratickými zbytky pro všechna n.

Pokud nebude řečeno jinak, 0 nebude v dalších pozorováních, tvrzeních a příkladech v celé práci zohledněna, protože častokrát tvoří triviální případy a většinu tvrzení je bez ní jednodušší formulovat. Také se dále budeme omezovat pouze na zbytky a nezbytky od 1 do $n - 1$ modulo n. V této práci budeme používat zkratky KZ pro kvadratický zbytek a KN pro kvadratický nezbytek.

Než budeme pokračovat dále, je namístě poznámka o notaci. Gauss v DA znázorňuje skutečnost, že a je KZ modulo p zápisem $a\ R\ p$ a skutečnost, že a je KN modulo p zápisem $a\ N\ p$ (R jako *residua quadratica* a N jako *non-residua quadratica*) (Gauss, 1801, s. 100).

V práci ale budeme používat značení KZ a KN, protože se jedná pouze o zkratky slov, ne matematický zápis relace, což více vyhovuje našim účelům.

Příklad 1: Rozhodněte, která čísla jsou KZ a která KN modulo 11.

Řešení: Z pozorování a definice:

$$\text{KZ: } \{0, 1, 3, 4, 5, 9\}$$

$$\text{KN: } \{2, 6, 7, 8, 10\}$$

Dále zkoumejme KZ a KN jako takové. Jaký je jejich počet pro dané modulo? Pokud, jak bylo avizováno, vynecháme nulu, pak modulo 11 můžeme z výčtu výše jednoduše vypozorovat, že je počet KZ a KN stejný, tedy obou je přesně polovina všech zbytků po dělení 11. Formulujme obecně.

Tvrzení 1 (Počet kvadratických zbytků a nezbytků modulo p)
Nechť p je liché prvočíslo. Počet kvadratických zbytků a počet kvadratických nezbytků modulo p jsou oba rovny $\frac{p-1}{2}$ (Gauss, 1986, s. 64).

Důkaz: Nejprve připomeňme, že $(p-a)^2 \equiv (-a)^2 = a^2$. KZ tedy může být nejvýše polovina.

Teď dokažme sporem, že druhé mocniny čísel od 1 do $\frac{p-1}{2}$ jsou si všechny navzájem nekongruentní. Předpokládejme z této množiny a, b taková, že $a \not\equiv b \wedge a^2 \equiv b^2$. Z toho vyplývá:

$$a^2 - b^2 \equiv 0$$

$$(a-b)(a+b) \equiv 0$$

Jelikož zbytky po dělení p tvoří obor integrity (Stanovský, 2022, s. 12), pak musí alespoň jeden ze součinitelů být kongruentní 0, takže buď $a \equiv b$, nebo $a \equiv -b$. Pro druhou kongruenci musí platit $b \equiv p - a$, z čehož vyplývá $b > \frac{p-1}{2}$. Oba tyto případy jsou ve sporu s předpokladem. (Gauss, 1986, s. 64).

Pozn.: Toto tvrzení nelze jednoduše zobecnit na složená čísla. Modulo 12 pozorujme, že kongruence $(a-b)(a+b) \equiv 0$ má kromě jiných i řešení $a \equiv 4$, $b \equiv 2$, protože $2 \cdot 6 \equiv 0$ a důkaz by tedy nebyl korektní.

Příklad 2: Určete, jaký je počet KZ a KN modulo 31.

Řešení: Z odvozeného vztahu je počet roven $\frac{31-1}{2} = \frac{30}{2} = 15$.

Vraťme se k současné podobě kongruence, kterou se snažíme vyřešit: $y^2 \equiv 20 \pmod{31}$. Jsme ve fázi, kdy se snažíme rozhodnout, zda je takováto kongruence řešitelná. Z tvrzení 1 plyne, že je poloviční pravděpodobnost, že ano. Jinými slovy se ptáme na otázku, zda je 20 KZ modulo 31. Jak o tom ovšem rozhodnout? 20 je zřejmě složeným číslem, konkrétně $20 = 2^2 \cdot 5$. Triviálně je 2^2 KZ a lze si jednoduše všimnout, že $6^2 = 36 \equiv 5 \pmod{31}$. Lze z tohoto pozorování ale rozhodnout o „zbytkovosti" 20? Lze obecně ze znalosti toho, zda jsou KZ či KN a a b, rozhodnout o tom, zda je KZ či KN ab?

Pro a a b mohou nastat tři možné případy. Buď jsou obě KZ, obě KN, nebo jedno KZ a druhé KN. Proveďme pozorování pro každý případ zvlášť. Pro jednoduchost se vraťme ke známým KZ a KN modulo 11 a součiny pozorujme na nich:

$$\text{KZ: } \{1, 3, 4, 5, 9\}$$

$$\text{KN: } \{2, 6, 7, 8, 10\}$$

Pozorujme, do jakých množin se dostaneme při násobení KZ a KN. Pokud násobíme dva KZ, vždy v množině KZ zůstaneme. Pokud násobíme KZ a KN, vždy skončíme v množině KN. Překvapivý je až poslední případ, pokud násobíme dva KN, vždy skončíme v množině KZ. Formulujme obecně a blíže se podívejme, jak vše odůvodnit.

Tvrzení 2 (Součiny kvadratických zbytků a kvadratických nezbytků)
Nechť $a, b \in \mathbb{Z}$ a $n \in \mathbb{N}$.

(1) Pokud a a b jsou kvadratickými zbytky modulo p, pak ab je také kvadratickým zbytkem modulo n.
(2) Pokud a je kvadratickým zbytkem modulo p a b je kvadratickým nezbytkem modulo p, pak ab je kvadratickým nezbytkem modulo n.

(3) Pokud a a b jsou kvadratickými nezbytky modulo p, pak ab je kvadratickým zbytkem modulo n. (Gauss, 1986, s. 65-66)

Důkaz: Důkaz provedeme pouze pro modulo p, kde p je prvočíslo. Jeho platnost pro všechna přirozená čísla vyplývá z tvrzení 9 a 12.

(1) Jelikož jsou a i b KZ modulo p, pak dokážeme najít taková x a y, že $a \equiv x^2$ a $b \equiv y^2$. Tudíž $ab \equiv x^2y^2 \equiv (xy)^2$.

(2) Dokažme sporem. Pro spor předpokládejme, že existuje takové x, že $a \equiv x^2$ a zároveň platí $ab \equiv y^2$, kde b je KN. Tím pádem $ab \equiv x^2b \equiv y^2$ a z toho vyplývá:

$$b \equiv y^2(x^2)^{-1} \equiv y^2(x^{-1})^2 \equiv (yx^{-1})^2$$

To by znamenalo, že b je KZ, což je ve sporu s předpokladem a musí platit původní tvrzení.

Pozn.: V tomto důkazu bylo použito tvrzení $(x^{-1})^2 \equiv (x^2)^{-1}$, které dokážeme následovně: z definice inverzního prvku $xx^{-1} \equiv 1$, po umocnění na druhou $(xx^{-1})^2 \equiv x^2(x^{-1})^2 \equiv 1$, a tedy $(x^{-1})^2 \equiv (x^2)^{-1}$.

(4) Z (2) plyne $\forall x, y \in \mathbb{Z}$ jsou ax^2 a by^2 KN. Pro libovolně zvolené x dokážeme najít y takové, že $ax^2 \equiv by^2 \equiv c \pmod p$. Z toho vyplývá $ax^2by^2 \equiv c^2$, a tedy:

$$ab \equiv c^2(x^2)^{-1}(y^2)^{-1} \equiv c^2(x^{-1})^2(y^{-1})^2 \equiv (cx^{-1}y^{-1})^2$$

Pozn.: Zaručenou existenci řešení y kongruence $ax^2 \equiv by^2$ pro libovolné x dokažme následnovně: Pro každý jeden případ zvoleného x je tato úloha ekvivalentní hledání řešení z lineární kongruence $mz \equiv n \pmod p$, kde $m \equiv b$, $n \equiv ax^2$ a $z \equiv y^2$ (Gray, 2009, s. 33). Tato kongruence je řešitelná, což plyne z (Kaňáková, 2022, s. 23). To, že z je také druhou mocninou (tj. KZ) vyplývá z toho, že mz musí být KN.

Součin různých kombinací KZ a KN má stejné vlastnosti jako součin různých kombinací 1 a -1, pokud KZ označíme 1 a KN označíme -1. Toto pozorování formalizuje tzv. Legendrův symbol.

Definice 5 (Legendrův symbol)

Nechť $a \in \mathbb{Z}$ a p je liché prvočíslo. Legendrův symbol čteme „a nad p“ a definujeme:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \iff a \equiv 0 \pmod{p} \\ 1 \iff a \not\equiv 0 \pmod{p} \text{ a } a \text{ je KZ modulo } p \\ -1 \iff a \not\equiv 0 \pmod{p} \text{ a } a \text{ je KN modulo } p \end{cases}$$

(Křížek, 2018, s. 76).

Pozn.: Rozšíření hodnot -1 a 1 o hodnotu 0 zachovává všechny multiplikativní vlastnosti, ze kterých jsme symbol vyvodili.

Zápis Legendrova symbolu není ideálním, lze si ho splést se zlomkem nebo kombinačním číslem. V *Essai sur la Théorie des Nombres*, kde Legendre tento symbol poprvé zavedl, se k volbě notace nevyjadřuje. Tato práce byla publikována již roku 1798, tedy 3 roky před DA, v nichž Gauss symbol vůbec nezmiňuje. Je to pravděpodobně proto, že Legendrovou motivací pro zavedení symbolu bylo zjednodušit zápis po aplikaci Eulerova kritéria (tvrzení 3), což také vysvětluje, proč ho definoval pouze pro lichá prvočísla. (Legendre, 1798, s. 186). Gaussovou motivací bylo klasifikovat čísla jako KZ či KN (Gauss, 1986, s. 88).

Příklad 3: Pomocí definice vyčíslete Legendrovy symboly $\left(\frac{5}{11}\right)$, $\left(\frac{2}{11}\right)$ a $\left(\frac{22}{11}\right)$.

Řešení: Už dříve jsme ukázali: $\left(\frac{5}{11}\right) = 1$, $\left(\frac{2}{11}\right) = -1$.$\left(\frac{22}{11}\right) = 0$, protože $22 \equiv 0 \pmod{11}$.

Stále nezodpovězenou otázku, jak jednoudše zjistit, zda je číslo KZ či KN, jsme přetvořili na otázku, jak vyčíslit Legendrův symbol.

Existuje několik metod pro vyčíslení Legendrova symbolu. Nejdříve zmiňme ty, které pro všechna p a $a, b \in \mathbb{Z}$ přímo plynou z tvrzení 1 a 2:

- $\left(\frac{0}{p}\right) = 0$
- $\left(\frac{1}{p}\right) = 1$
- Pokud $a \equiv b \pmod{p}$, pak $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$
- $\left(\frac{a \cdot b^2}{p}\right) = \left(\frac{a}{p}\right)$

Příklad 4: Pomocí součinů výše vyčíslete Legendrovy symboly $\left(\frac{8}{11}\right)$, $\left(\frac{10}{11}\right)$ a $\left(\frac{14}{11}\right)$.

Řešení: $\left(\frac{8}{11}\right) = \left(\frac{2\cdot 4}{11}\right) = \left(\frac{2\cdot 2^2}{11}\right) = \left(\frac{2}{11}\right) = -1.$

$\left(\frac{10}{11}\right) = \left(\frac{2\cdot 5}{11}\right) = \left(\frac{2}{11}\right)\cdot\left(\frac{5}{11}\right) = -1\cdot 1 = -1.$

$\left(\frac{14}{11}\right) = \left(\frac{3}{11}\right) = 1$. Alternativě $\left(\frac{14}{11}\right) = \left(\frac{2\cdot 7}{11}\right) = \left(\frac{2}{11}\right)\cdot\left(\frac{7}{11}\right) = -1\cdot(-1) = 1.$

Než budeme pokračovat ve zkoumání Legendrových symbolů dále, představme si bez pozorování jeden obecný vzorec pro jejich vyčíslení. Ten poprvé formuloval Euler (samozřejmě bez využití zápisu pomocí Legendrova symbolu) a také se po něm jmenuje (Dickson, 1920, s. 231). Koncept, ze kterého lze tento vzorec přirozeně odvodit a dokázat je představen až v druhé kapitole na str. 61.

Tvrzení 3 (Eulerovo kritérium; *Euler's criterion*)
Nechť $a \in \mathbb{Z}$ a p je liché prvočíslo. Pak:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

(Křížek, 2018, s. 77).

Důkaz: str. 63.

Příklad 5: Pomocí Eulerova kritéria vyčíslete Legendrovy symboly $\left(\frac{3}{11}\right)$ a $\left(\frac{7}{11}\right)$.

Řešení: $\left(\frac{3}{11}\right) \equiv 3^{\frac{11-1}{2}} = 3^5 = (3^2)^2\cdot 3 = 9^2\cdot 3 \equiv (-2)^2\cdot 3 = 4\cdot 3 \equiv 1 \pmod{11}.$

$\left(\frac{7}{11}\right) \equiv 7^{\frac{11-1}{2}} = 7^5 = (7^2)^2\cdot 7 = 49^2\cdot 7 \equiv 5^2\cdot 7 \equiv 3\cdot 7 \equiv 10 \equiv -1 \pmod{11}.$

Toto kritérium je užitečné svou přímočarostí a využitím v důkazech, ale při výpočtech se u vyšších čísel rychle stává nepraktickým. To zmiňuje již Gauss, citujme z originálu DA: „At quoties numeri examinandi mediocriter sunt magni, hoc criterium ob calculi immensitatem prorsus inutile erit." (s. 82).

Jedinou výjimkou je -1, pro které je Eulerovo kritérium naopak velmi užitečné. Pro lichá $\frac{p-1}{2}$ je -1 KN a pro sudá KZ. Lze si bez problémů všimnout, že tento výraz je lichý pro prvočísla tvaru $4k+3$, ekvivalentně $p \equiv 3 \pmod 4$ a sudý pro prvočísla tvaru $4k+1$, ekvivalentně $p \equiv 1 \pmod 4$.

Tvrzení 4 (-1 jako kvadratický zbytek či nezbytek)
Nechť $a \in \mathbb{Z}$ a p je liché prvočíslo. Pak:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \Leftrightarrow p \equiv 1 \pmod 4 \\ -1 \Leftrightarrow p \equiv 3 \pmod 4 \end{cases}$$

(Gauss, 1986, s. 72).

Důkaz: Vždy $k \in \mathbb{N}_0$ vyhovující podmínce, že p je prvočíslo.

První případ: $\left(\frac{-1}{p}\right) = \left(\frac{-1}{4k+1}\right) = (-1)^{\frac{4k+1-1}{2}} = (-1)^{2k} = 1$.

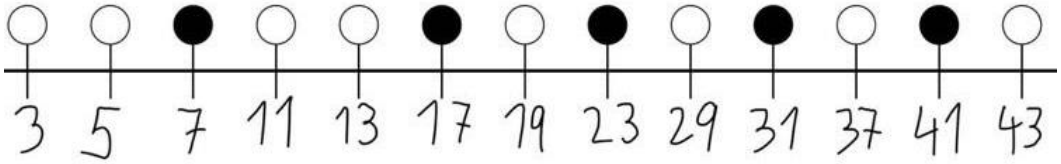
Druhý případ: $\left(\frac{-1}{p}\right) = \left(\frac{-1}{4k+3}\right) = (-1)^{\frac{4k+3-1}{2}} = (-1)^{2k+1} = -1$.

Příklad 6: Vyčíslete Legendrovy symboly $\left(\frac{40}{41}\right)$ a $\left(\frac{46}{47}\right)$.

Řešení: $\left(\frac{40}{41}\right) = \left(\frac{-1}{41}\right) = 1$, protože $41 \equiv 1 \pmod 4$. Alternativně $\left(\frac{40}{41}\right) = \left(\frac{81}{41}\right) = \left(\frac{9^2}{41}\right) = 1$.

$\left(\frac{46}{47}\right) = \left(\frac{-1}{47}\right) = -1$, protože $47 \equiv 3 \pmod 4$.

Lze si všimnout, že pokud známe hodnoty Legendrových symbolů pro všechna prvočísla modulo p, pak dokážeme jednoduše vyčíslit Legendrův symbol i pro všechna složená čísla. Pro prvočísla by se hodilo nalézt méně početně náročné způsoby vyčíslení, než je Eulerovo kritérium. Protože je symbol definován pouze pro moduly lichých prvočísel, pozorujme nejdříve hodnoty $\left(\frac{2}{p}\right)$ pro několik prvních lichých prvočísel p:



Obr. 1: Schéma hodnot $\left(\frac{2}{p}\right)$. Plné kolečko značí $\left(\frac{2}{p}\right) = -1$, prázdné $\left(\frac{2}{p}\right)$.

Podobně jako u -1 se zaměřme na prvočísla určitých tvarů. Pro $p \equiv 1 \pmod 4$ mají symboly $\left(\frac{2}{5}\right)$ a $\left(\frac{2}{13}\right)$ shodnou hodnotu, ale symbol $\left(\frac{2}{17}\right)$ má hodnotu rozdílnou. Stejně je tomu pro $p \equiv 3 \pmod 4$, kde $\left(\frac{2}{7}\right) = \left(\frac{2}{23}\right) \neq \left(\frac{2}{11}\right)$. Zkusme se tedy zaměřit na prvočísla jiných tvarů. Můžeme jít o mocninu dvojky výš a zkoumat prvočísla $\equiv 1, 3, 5, 7 \pmod 8$:

$$p \equiv 1\text{: } \left(\frac{2}{17}\right) = \left(\frac{2}{41}\right) = 1$$

$$p \equiv 3\text{: } \left(\frac{2}{3}\right) = \left(\frac{2}{11}\right) = \left(\frac{2}{19}\right) = \left(\frac{2}{43}\right) = -1$$

$$p \equiv 5\text{: } \left(\frac{2}{5}\right) = \left(\frac{2}{13}\right) = \left(\frac{2}{29}\right) = \left(\frac{2}{37}\right) = -1$$

$$p \equiv 7\text{: } \left(\frac{2}{7}\right) = \left(\frac{2}{23}\right) = \left(\frac{2}{31}\right) = 1$$

Pro tyto tvary prvočísel již pravidelnost zřejmě existuje.

Tvrzení 5 (2 jako kvadratický zbytek či nezbytek)

Nechť p je liché prvočíslo. Pak:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \Leftrightarrow p \equiv \pm 1 \pmod 8 \\ -1 \Leftrightarrow p \equiv \pm 3 \pmod 8 \end{cases}$$

(Gauss, 1986, s. 73-73)

Ekvivalentně:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

(Křížek, 2018, s. 78)

Důkaz: Nejprve dokažme lemma, které budeme používat k důkazu každého případu zvlášť.

Lemma 1 (Gaussovo lemma; Gauss's lemma): $a^{\frac{p-1}{2}} \equiv (-1)^t$, kde t označuje počet všech členů množiny $\left\{a, 2a, 3a, \dots, \frac{p-1}{2}a\right\}$, které jsou větší než $\frac{p}{2}$. Dokažme speciálně pro $a = 2$. Vezměme si všechna sudá přirozená čísla menší než p. Jejich počet se rovná $\frac{p-1}{2}$ a jsou to čísla $\{2, 4, 6, \dots, p-1\}$. Nyní je spolu vynásobme a následně vytkněme 2:

$$2 \cdot 4 \cdot 6 \cdot \dots \cdot (p-1) = 2^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{p-1}{2} = 2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!$$

Teď k této posloupnosti sudých čísel přistupme trochu jinak. Každé sudé číslo větší než $\frac{p-1}{2}$ vyjádřeme záporným číslem jemu kongruentním modulo p. Tedy:

$$\{2, 4, 6, \dots, p-1\} \equiv \left\{-1, (-3), (-5), \dots, 2, 4, 6, \dots, \frac{p-1}{2}\right\} = \left\{-1, 2, (-3), 4, \dots, \frac{p-1}{2}\right\}$$

Počet záporných členů si označme t a všechny členy spolu opět vynásobme. Tím dostaneme:

$$-1 \cdot 2 \cdot (-3) \cdot 4 \cdot \dots \cdot \frac{p-1}{2} = (-1)^t \cdot \left(\frac{p-1}{2}\right)!$$

Tudíž:

$$2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv (-1)^t \cdot \left(\frac{p-1}{2}\right)! \,/ : \left(\frac{p-1}{2}\right)!$$

$$2^{\frac{p-1}{2}} \equiv (-1)^t$$

Užitím lemmatu pro každý případ zvlášť:

- $p \equiv 1 \pmod 8$, ekvivalentně $p = 1 + 8k, k \in \mathbb{Z}$: počet všech čísel menších než p je $8k$, $\frac{p-1}{2} = 4k$ a v tomto případě $t = 2k$. Z lemmatu: $2^{4k} \equiv (-1)^{2k} = 1$.
- $p \equiv 3 \pmod 8$, ekvivalentně $p = 3 + 8k, k \in \mathbb{Z}$: $\frac{p-1}{2} = 4k + 1$. $t = 2k + 1$. $2^{4k+1} \equiv (-1)^{2k+1} = -1$.
- $p \equiv -1 \pmod 8$, ekvivalentně $p = 7 + 8k, k \in \mathbb{Z}$: $\frac{p-1}{2} = 4k + 3$. $t = 2k + 2$. $2^{4k+3} \equiv (-1)^{2k+2} = 1$.
- $p \equiv -3 \pmod 8$, ekvivalentně $p = 5 + 8k, k \in \mathbb{Z}$: $\frac{p-1}{2} = 4k + 2$. $t = 2k + 1$. $2^{4k+2} \equiv (-1)^{2k+1} = -1$. (Silverman, 2012, s. 154-157).

Příklad 7: Vyčíslete Legendrovy symboly $\left(\frac{2}{3}\right), \left(\frac{2}{5}\right), \left(\frac{2}{7}\right)$ a $\left(\frac{2}{17}\right)$.

Řešení: $\left(\frac{2}{3}\right) = -1$, protože $3 \equiv 3 \pmod 8$.

$\left(\frac{2}{5}\right) = -1$, protože $5 \equiv -3 \pmod 8$.

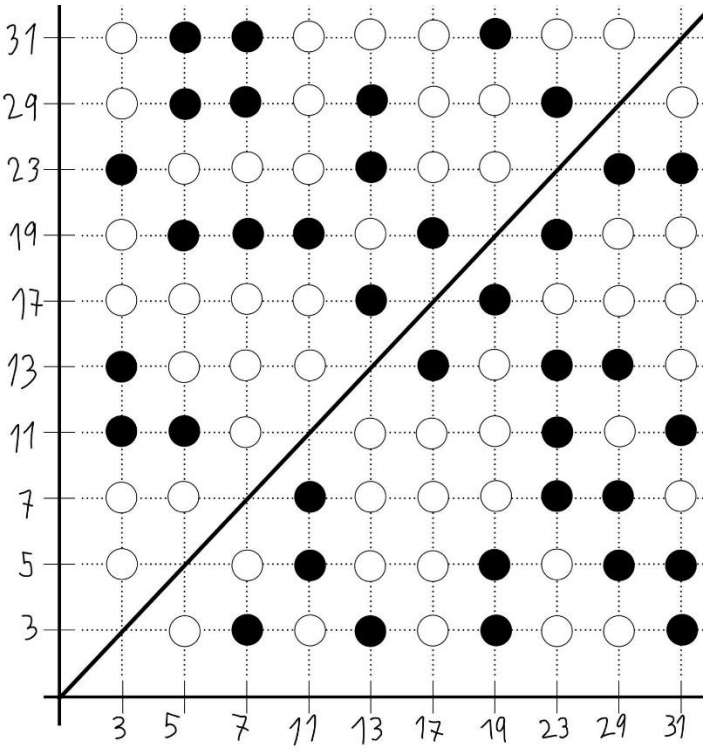
$\left(\frac{2}{7}\right) = 1$, protože $7 \equiv -1 \pmod 8$.

$\left(\frac{2}{17}\right) = 1$, protože $17 \equiv 1 \pmod 8$.

Pozn.: Ekvivalenci formulací ukažme taktéž výčtem všech případů:

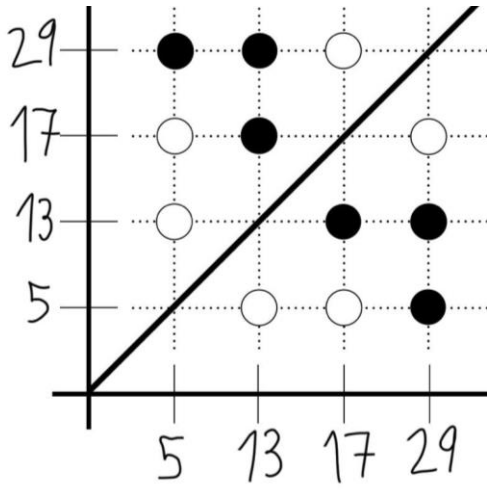
- $p = 8k + 1$: $(-1)^{\frac{(8k+1)^2-1}{2}} = (-1)^{\frac{64k^2+16k+1-1}{8}} = (-1)^{8k^2+2k} = ((-1)^2)^{4k^2+k} = 1$
- $p = 8k + 3$: $(-1)^{\frac{(8k+3)^2-1}{2}} = (-1)^{\frac{64k^2+48k+9-1}{8}} = (-1)^{8k^2+6k+1} = ((-1)^2)^{4k^2+3k} \cdot (-1) = -1$
- $p = 8k - 3$: $(-1)^{\frac{(8k-3)^2-1}{2}} = (-1)^{\frac{64k^2-48k+9-1}{8}} = (-1)^{8k^2-6k+1} = ((-1)^2)^{4k^2-3k} \cdot (-1) = -1$
- $p = 8k - 1$: $(-1)^{\frac{(8k-1)^2-1}{2}} = (-1)^{\frac{64k^2-16k+1-1}{8}} = (-1)^{8k^2-2k} = ((-1)^2)^{4k^2-k} = 1$

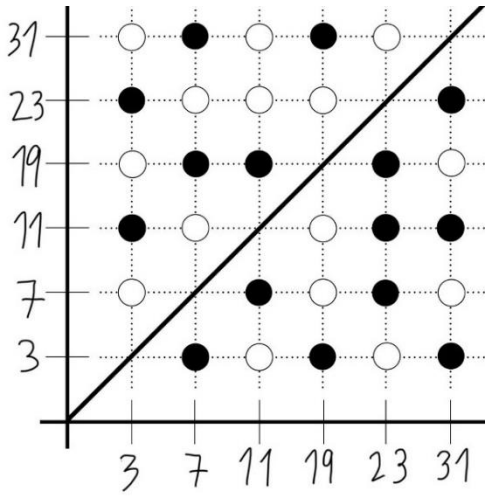
Kombinací tvrzení 4 a 5 bychom mohli formulovat obecné pravidlo pro -2 a podobná pravidla by se dala najít i pro další čísla, nezáporná i záporná. Gauss to provedl až pro ± 7, k nahlédnutí v (Gauss, 1986, s. 73-82). Pokusme se ale spíše nalézt obecnou metody pro symboly lichých prvočísel. Protože je Legendrův symbol definován pouze modulo liché prvočíslo, tak pokud máme symbol $\left(\frac{p}{q}\right)$ (kde p, q jsou lichá prvočísla), má smysl jak symbol $\left(\frac{p}{q}\right)$, tak symbol $\left(\frac{q}{p}\right)$. Otázkou je, zda mezi těmito symboly existuje nějaký užitečný vztah, popřípadě jaký. Nahlédněme do následujícího obrázku:



Obr. 2: Schéma hodnot $\left(\frac{p}{q}\right)$. Čísla na vodorovné ose bereme za p, na svislé za q.

Pozorujme symetrie a antisymetrie v obr. 1. Lze vypozorovat, že pro některá čísla (např. 5) jsou sloupce a řádky celé symetrické. Podobnou úvahou si lze všimnout, že pro žádné číslo nejsou celý řádek a sloupec přesně antisymetrické. Nahlédněme do dvou obrázků, ve kterých jsme znázornili pouze symetrické a pouze asymetrické hodnoty:





Obr. 3 a obr. 4: Schémata hodnot pro symetrické a asymetrické hodnoty $\left(\frac{p}{q}\right)$ a $\left(\frac{q}{p}\right)$.

Co mají všechna prvočísla z obr. 3 společné? Není těžké si všimnout, že jsou všechna tvaru $4k+1, k \in \mathbb{N}_0$, ekvivalentně $\equiv 1 \pmod 4$ a žádná čísla tohoto tvaru jsme z obr. 2 nevynechali. Naopak čísla z obr. 4 jsou všechna $\equiv 3 \pmod 4$. Z toho, že např. pro 5 jsou v obr. 2 celý řádek a sloupec symetrické vyplývá, že stačí, aby alespoň jedno z prvočísel bylo tvaru $4k+1$ a hodnoty symbolů jsou symetrické. Z tohoto pozorování vyplývá jedna z nejdůležitějších vět modulární aritmetiky.

Věta 1 (Zákon kvadratické reciprocity; *law of quadratic reciprocity*)
Nechť p a q jsou lichá prvočísla. Pak:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) \Leftrightarrow p \equiv 1 \pmod 4 \vee q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) \Leftrightarrow p \equiv 3 \pmod 4 \wedge q \equiv 3 \pmod 4 \end{cases}$$

(Gauss, 1986, s. 87-88).

Ekvivalentně:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

(Křížek, 2018, s. 79).

Důkaz: Např. (Gray, 2009, s. 61-64).

Pozn.: Tvrzení o „zbytkovosti" -1 a 2 jsou známá jako *první* a *druhý doplněk kvadratické reciprocity*.

Důkaz zde explicitně neuvádíme, navzdory tomu, že pro kvadratickou reciprocitu existuje nezvykle mnoho důkazů, protože je nad rámec této práce. Sám Gauss publikoval šest různých důkazů kvadratické reciprocity a po jeho smrti byly v jeho poznámkách nalezeny dva další. Zajímavé je, že Gauss považoval kvadratickou reciprocitu za jednu z nejkrásnějších vět v matematice. V DA ji nazývá *základní větou* (*fundamentale theorema*), v soukromí ji nazýval *zlatou větou* (*aureum theorema*) (Gray, 2009, s. 31).

Dokažme alespoň ekvivalenci formulací. Aby byl součin v druhé formulaci roven 1, musí oba symboly mít stejnou hodnotu. V takovém případě musí být -1 umocněna na sudý exponent, pro to musí být alespoň jeden ze součinitelů $\frac{p-1}{2}$ a $\frac{q-1}{2}$ sudý. To nastane, pokud je

alespoň jedno z prvočísel tvaru $4k + 1 \equiv 1 \pmod 4$. V opačném případě, tedy pokud jsou obě prvočísla tvaru $4k + 3 \equiv 3 \pmod 4$ je -1 umocněna na lichý exponent a pro součin symbolů musí platit, že mají rozdílnou hodnotu.

Příklad 8: Pomocí kvadratické reciprocity vyčíslete Legendrův symbol $\left(\frac{47}{53}\right)$.

Řešení: $\left(\frac{47}{53}\right) = \left(\frac{53}{47}\right) = \left(\frac{6}{47}\right) = \left(\frac{2\cdot 3}{47}\right) = \left(\frac{2}{47}\right)\cdot\left(\frac{3}{47}\right) = 1\cdot\left(-\left(\frac{47}{3}\right)\right) = -\left(\frac{2}{3}\right) = -(-1) = 1.$
(S využitím postupně: $53 \equiv 1 \pmod 4$ a $47 \equiv 3 \pmod 4$).

Vraťme se ke kongruenci $17x^2 + 25x + 7 = 0$, kterou jsme upravili na $y^2 \equiv 20$ a kongruenci $x^2 + x + 4 \equiv 0 \pmod{97}$, pro kterou potřebujeme znát $\sqrt{82}$. Ověřme, zda mají řešení.

Příklad 9: Vyčíslete Legendrovy symboly $\left(\frac{82}{97}\right)$ a $\left(\frac{20}{31}\right)$.

Řešení: $\left(\frac{82}{97}\right) = \left(\frac{2\cdot 41}{97}\right) = \left(\frac{2}{97}\right)\cdot\left(\frac{41}{97}\right) = 1\cdot\left(\frac{97}{41}\right) = \left(\frac{15}{41}\right) = \left(\frac{3\cdot 5}{41}\right) = \left(\frac{3}{41}\right)\cdot\left(\frac{5}{41}\right) = \left(\frac{41}{3}\right)\cdot\left(\frac{41}{5}\right) = \left(\frac{2}{3}\right)\cdot\left(\frac{1}{5}\right) = -1\cdot 1 = -1.$

$\left(\frac{20}{31}\right) = \left(\frac{4\cdot 5}{31}\right) = \left(\frac{4}{31}\right)\cdot\left(\frac{5}{31}\right) = \left(\frac{2^2}{31}\right)\cdot\left(\frac{5}{31}\right) = 1\cdot\left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = 1.$

První z původně zkoumaných kongruencí tedy řešení nemá. Druhá je řešitelná i doplněním na čtverec. Teď už jen zbývá takové řešení najít a ověřit, zda se shoduje s řešením pomocí obecného vzorce.

1.1.2 Řešení kvadratické kongruence mod p

V celém tomto oddílu budeme předpokládat, že každá prezentovaná kongruence má řešení, pokud nebude řečeno jinak.

Formulujme nejdříve pár očividných faktů pro modulo p liché prvočíslo:

- kongruenci $x^2 \equiv a^2$ řeší $x \equiv \pm a$,
- kongruenci $x^2 \equiv 0$ řeší $x \equiv 0$,
- kongruenci $(x - a)^2 \equiv 0$ řeší $x \equiv a$,
- kongruenci $x^2 \equiv 1$ řeší $x \equiv \pm 1$,

- kongruenci $x^2 \equiv a^2 b^2$ řeší $x \equiv \pm ab$.

Z prvního tvrzení vyplývá, že stačí vždy najít jen jedno řešení, druhé bude kongruentní jeho opačné hodnotě. Také můžeme pozorovat, že kvadratická kongruence modulo liché prvočíslo má, stejně jako kvadratická rovnice nad reálnými (popřípadě komplexními) čísly, žádné, právě jedno, nebo právě dvě řešení. Z posledního tvrzení vyplývá, že i v prostředí kongruencí platí obdoba částečného odmocňování, což se může v jistých konkrétních případech hodit.

Jak ale nalézt řešení obecně? Žádný obecný vzorec pro každé prvočíslo bohužel nalezen nebyl. V minulém oddílu jsme ale pracovali s prvočísly konkrétních tvarů a pro některé z nich vzorce lze odvodit. Ze všech dosud představených konceptů dává největší smysl využít Eulerovo kritérium.

Předpokládejme řešitelnou kongruenci $x^2 \equiv a \pmod{p}$ postupně pro $p = 4k + 1$ a $p = 4k + 3, k \in \mathbb{N}_0$ a pozorujme, zda lze za využití Eulerova kritéria nalézt výraz umocněný na druhou, který by byl kongruentní a:

$p = 4k + 1$: $a^{\frac{4k}{2}} = a^{2k} \equiv 1 \Rightarrow a^{2k+1} \equiv a$. Nenalezli jsme druhou mocninu kongruentní a.

$p = 4k + 3$: $a^{\frac{4k+2}{2}} = a^{2k+1} \equiv 1 \Rightarrow a^{2k+2} = (a^{k+1})^2 \equiv a$. Nalezli jsme druhou mocninu kongruentní a.

Pro prvočísla druhého tvaru jsme tedy obecný vzorec nalezli.

Tvrzení 6 (Řešení kvadratické kongruence $\mathbf{mod}\ p = 4k + 3$)
Nechť $a \in \mathbb{Z}$ a $p = 4k + 3, k \in \mathbb{N}_0$ je prvočíslem. Řešeními kvadratické kongruence $x^2 \equiv a \pmod{p}$ jsou:

$$x \equiv \pm a^{k+1}$$

Důkaz: $x^2 \equiv (\pm a^{k+1})^2 = a^{2k+2} = a \cdot a^{2k+1} = a \cdot a^{\frac{4k+2}{2}} = a \cdot \left(\frac{a}{p}\right) = a \cdot 1 = a$.

Příklad 10: Nalezněte řešení kongruence $17x^2 + 25x + 7 \equiv 0 \pmod{31}$.

Řešení: Kongruenci jsme již upravili do tvaru $(x - 2)^2 \equiv 20$ a následně zavedli substituci $y = x - 2$. Řešíme $y^2 \equiv 20$. Protože $31 = 4 \cdot 7 + 3$, řešení je tvaru:

$$y \equiv \pm 20^{7+1} = \pm 20^8 = \pm(20^2)^4 \equiv \pm 28^4 = \pm(28^2)^2 \equiv \pm 9^2 \equiv \pm 19$$

Po dosazení jsou řešení:

$$x_1 = y_1 + 2 = 19 + 2 = 21$$

$$x_2 = y_2 + 2 = -19 + 2 \equiv 14$$

Ověřili jsme si tedy, že všechny metody (dosazováním, obecným vzorcem a doplněním na čtverec) vedou ke stejným řešením.

Mohli bychom zkoumat prvočísla dalších tvarů (např. $8k + 5$, $16k + 9$ apod.) a zde by se vzorce obdobným způsobem nalézt podařilo, i když pro ně již vzorce neplynou tak přirozeně, např. Navzdory tomu, že bychom takto množinu prvočísel, pro která vzorec nemáme, postupně více a více zužovali, nepokryli bychom všechna prvočísla. Proto se podívejme na obecný algoritmus, jak nalézt řešení kvadratické kongruence. Odvození algoritmu je poměrně technické, proto jej prezentujeme bez pozorování. Pro pochopení základních principů algoritmu je potřeba dobře rozumět některým poznatkům o cyklických grupách (hlavně řádu prvku a generátoru), proto jejich nastínění necháváme na pozdější část, konkrétně na str. 97.

RESSOL algoritmus

Algoritmus je též znám jako Tonelli-Shanksův algoritmus. Toto jméno má po Albertu Tonellim (1849-1920) a Danielu Shanksovi (1917-1996), kteří jej nezávisle na sobě objevili. Shanks algoritmus nazýval RESSOL jako „*RESidue SOLver*“ („řešitel zbytků“).

Předpokládejme řešitelnou kongruenci $x^2 \equiv a \pmod p$. Opakovaným dělením dvěma mějme $p - 1 = 2^k l$, kde l je liché. Všimněme si, že pokud si zvolíme kandidáta na řešení $y \equiv a^{\frac{l+1}{2}}$, pak $y^2 \equiv a^{l+1} = a \cdot a^l$ a mohou nastat dva případy:

- $a^l \equiv 1$ a tedy $y^2 \equiv a$ a $\pm y$ je řešením.
- $a^l \equiv b \not\equiv 1$ a tedy $y^2 \equiv ab$.

V druhém případě postupujeme následovně:

- Zvolíme si libovolný kvadratický nezbytek c
- Vypočteme c^l
- Opakovaným mocněním b na druhou nalezneme takové n, že $b^{2^n} \equiv 1$
- Vypočteme $c^{l \cdot 2^{k-1-n}} = d$
- Vynásobíme yd, z toho plyne $(yd)^2 \equiv y^2 d^2 \equiv abd^2$
    - Pokud $bd^2 \equiv 1$, řešením je $\pm yd$
    - Pokud $bd^2 \not\equiv 1$, dosadíme $n \to k$, $d^2 \to c^l$, $bd^2 \to b$, $yd \to y$ a od třetího kroku algoritmus opakujeme

Příklad 11: Nalezněte řešení kongruence $x^2 \equiv 43 \pmod{97}$.

Řešení: Nejdříve ověřme, že tato kongruence řešení má:

$$\left(\frac{43}{97}\right) = \left(\frac{97}{43}\right) = \left(\frac{11}{43}\right) = -\left(\frac{43}{11}\right) = -\left(\frac{-1}{11}\right) = -(-1) = 1$$

Řešení tedy existuje. $97 \equiv 1 \pmod 4$, takže se musíme uchýlit k použití RESSOL algoritmu. $97 - 1 = 96 = 2^5 \cdot 3 = 2^k \cdot l$. Kandidátem na řešení je:

$$y \equiv 43^{\frac{l+1}{2}} = 43^{\frac{3+1}{2}} = 43^2 \equiv 6$$

Ale:

$$43^3 \equiv 6 \cdot 43 \equiv 64 = b$$

Takže nejsme hotovi. Zvolme si KN, protože $97 \equiv 1 \pmod 8$, 2 je KZ. $\left(\frac{3}{97}\right) = \left(\frac{97}{3}\right) =$ $= \left(\frac{1}{3}\right) = 1$, takže i 3 je KZ. 4 je triviálně KZ. $\left(\frac{5}{97}\right) = \left(\frac{97}{5}\right) = \left(\frac{2}{5}\right) = -1$. $5 = c$ je KN. Umocněme:

$$5^3 = 125 \equiv 28 = c^l$$

Postupně mocněme $b = 64$ na druhou:

$$64^{2^1} \equiv 22, 64^{2^2} \equiv 22^2 \equiv -1, 64^{2^3} \equiv 1$$

Takže $n = 3$. Dosaďme:

$$28^{2^{k-1-n}} = 28^{2^{5-1-3}} = 28^2 = 8 = d$$

Přenásobme:

$$yd = 6 \cdot 8 \equiv 48$$

$$bd^2 = 64 \cdot 8^2 = 64^2 \equiv 22$$

Stále nejsme hotovi, předefinujme proměnné:

$$3 \to k, 64 \to c^l, 22 \to b, 48 \to y$$

A algoritmus zopakujme:

$$22^{2^1} \equiv -1, 22^{2^2} \equiv 1$$

$n = 2$:

$$64^{2^{3-2-1}} = 64 = d$$

Přenásobme:

$$yd = 48 \cdot 64 \equiv 65$$

$$bd^2 = 22 \cdot 64^2 \equiv 22^2 \equiv 96 \equiv -1$$

Mohli bychom provést ještě jedno opakování, ale všimněme si, že nové $b = -1$ stačí přenásobit -1 pro získání cílené 1. Tedy potřebujeme $d^2 \equiv -1$, z předchozích výpočtů víme, že takovým vyhovujícím d je 22. Tím vynásobme nové $y \to 65$ a řešeními tedy jsou:

$$\pm yd = \pm 65 \cdot 22 \equiv \pm 72$$

1.2 Kvadratické kongruence mod p^k

Začněme pozorováním, zda existuje souvislost mezi řešením kongruence modulo p a modulo p^k.

1.2.1 Kvadratické zbytky a nezbytky mod p^k

Pozorujme, zda řešitelnost kongruence $x^2 \equiv a \pmod 3$ nějak souvisí s řešitelností kongruence $x^2 \equiv a \pmod{27}$.

Předpokládejme, že kongruence modulo 3 řešení má, tedy že a je KZ modulo 3. Pokud vyloučíme triviální nulu, pak a může být jedině 1. Než se dostaneme rovnou ke 27, pozorujme nejdříve modulo $3^2 = 9$. Kongruenci $a \equiv 1 \pmod 3$ splňují modulo 9:

$$a \equiv 1, 4, 7 \pmod 9$$

Zkoumejme, zda jsou tato čísla KZ a jestli se neobjeví nějaké jiné:

$1^2 \equiv 8^2 \equiv 1$ $\quad$ $2^2 \equiv 7^2 \equiv 4$ $\quad$ $3^2 \equiv 6^2 \equiv 0$ $\quad$ $4^2 \equiv 5^2 \equiv 7$

Z tohoto pozorování lze vyvodit rovnou několik důležitých závěrů. Zaprvé, předpokládané KZ opravdu KZ jsou a žádné jiné nenulové se neobjevily. Ovšem kongruence $x^2 \equiv 0$ je zde zajímavější. Nemá pouze jedno triviální řešení, ale mimo něj dvě další (3 a -3), celkem tedy tři. To při bližším pohledu není nijak překvapivé, protože všechna čísla, které ve svém prvočíselném rozkladu obsahují 3 budou po umocnění na druhou násobkem 9. S kongruencemi s pravou stranou nulovou musíme zřejmě pracovat jinak než s nenulovou.

Vraťme se k původnímu pozorování, tentokrát již modulo 27. Analogicky jako pro modulo 9 ověřme, zda jsou všechna $a \equiv 1 \pmod 3$ KZ modulo 27. Musí se nám tedy objevit KZ $a \equiv 1, 4, 7, 10, 13, 16, 19, 22, 25 \pmod{27}$. Mocněme pouze do 13, poté se KZ začnou opakovat. Vynechme $1, 2, 4$ a 5, jejich druhé mocniny ve výčtu očividně nalezneme a také vynechme 9, která bude po umocnění kongruentní 0:

$3^2 \equiv 9$ $\quad$ $7^2 \equiv 22$ $\quad$ $10^2 \equiv 19$ $\quad$ $12^2 \equiv 9$

$6^2 \equiv 9$ $\quad$ $8^2 \equiv 10$ $\quad$ $11^2 \equiv 13$ $\quad$ $13^2 \equiv 7$

Všechny KZ se nám tedy opět objevily, nicméně nám jeden přibyl a opět vyšel více než dvakrát. Tímto KZ je 9. Zřejmě je situace pro soudělná čísla s modulem rozdílná od těch nesoudělných. Zaměřme se tedy nejprve na nesoudělná. Pro ně se zdá, že pokud jsou KZ modulo p, pak jsou KZ i modulo p^2 a výše. Opačně to zdá se platí také. Nikde nám nepřibyl zbytek, který by byl kongruentní 2 modulo 3.

Legendrův symbol je definován pouze pro spodní argument lichého prvočísla, tudíž ho pro klasifikaci KZ a KN zde již nemůžeme využít. Existují jeho zobecnění, ale našim účelům nevyhovuje ani jeden z těchto obecnějších symbolů, proto definujme vlastní. Co se týče notace a nabývaných hodnot, vycházíme z Legendrova symbolu.

Definice 6

Nechť $a \in \mathbb{Z}$ a $n \in \mathbb{N}$. Zápis $\left[\frac{a}{n}\right]$ definujeme:

$$\left[\frac{a}{n}\right] = \begin{cases} 1 \Leftrightarrow a \text{ je KZ modulo } n \\ -1 \Leftrightarrow a \text{ je KN modulo } n \end{cases}$$

Pozn.: Nedefinujeme $\left[\frac{a}{n}\right] = 0$, protože se striktně zabýváme tím, zda je a KZ či KN, nehledě na soudělnost. Pro demonstraci např. $\left(\frac{3}{3}\right) = 0$, ale 3 je KZ modulo 3, protože $3 \equiv 0 \pmod 3$ a $x^2 \equiv 0 \pmod 3$ řešení má, takže $\left[\frac{3}{3}\right] = 3$.

Nyní formulujme závěr předchozího pozorování s využitím našeho symbolu.

Tvrzení 7 (Nesoudělné kvadratické zbytky a nezbytky $\mathbf{mod}\ p^k$)

Nechť $a \in \mathbb{Z}, k \in \mathbb{N}, k \geq 2$, p je liché prvočíslo a $D(a,p) = 1$. Pak a je kvadratickým zbytkem modulo p^k právě tehdy, když a je kvadratickým zbytkem modulo p (Gaus, 1986, s. 67).

Ekvivalentně:

$$\left[\frac{a}{p^k}\right] = \left(\frac{a}{p}\right)$$

Důkaz: Dokážeme první formulaci, ekvivalence obou je zřejmá.

„⇒“ Mějme kongruenci $x^2 \equiv a \pmod{p^k}$, ekvivalentně $p^k | x^2 - a$. Z toho plyne i $p | x^2 - a$, jazykem modulární aritmetiky $x^2 \equiv a \pmod p$.

„⇐“ Mějme kongruenci $x^2 \equiv a \pmod{p}$, ekvivalentně $x^2 = a + lp, l \in \mathbb{Z}$. Tato kvadratická kongruence má z předpokladu řešení, to je tvaru $\pm x + mp, m \in \mathbb{Z}$. Po dosazení:

$$(\pm x + mp)^2 = x^2 \pm 2xmp + (mp)^2 = a + lp \pm 2xmp + (mp)^2 \equiv$$

$$\equiv a + (l + 2xm)p \pmod{p^2}$$

Potřebujeme $l \pm 2xm \equiv 0 \pmod{p}$, ekvivalentně $\pm 2xm \equiv l \pmod{p}$. K $\pm 2x$ existuje inverzní prvek pro násobení, jeho přenásobením máme $m \equiv (\pm 2x)^{-1} l$ a pro každou volbu m nalezneme l, tedy vždy existuje řešení. Pro taková m, l:

$$a + (l \pm 2xm)p \equiv a + p^2 \equiv a \pmod{p}$$

Tímto způsobem můžeme pokračovat pro všechny vyšší mocniny p, až dosáhneme p^k (Gauss, 1986, s. 67-68).

Příklad 12: Rozhodněte, zda je 11 KZ či KN modulo 27.

Řešení: $\left[\frac{11}{27}\right] = \left[\frac{11}{3^3}\right] = \left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1$.

Jak je to se soudělnými KZ? Vyjděme z předchozího pozorování. Nejdříve zmiňme, že ani v jednom z pozorovaných modulů nevyšla 3 jako KZ navzdory tomu, že 3 považujeme za KZ modulo 3. Proto je tvrzení 7 formulováno pouze pro nesoudělné KZ. Jako soudělný KZ nám ovšem vyšla $9 \pmod{27}$. Ta je očividně 3^2, tedy není překvapivé, že je KZ. Obecně p^2 bude triviálně vždy KZ modulo $p^k, k \in \mathbb{N}$. Od této úvahy je již cesta k obecnému závěru krátká. Využitím tvrzení 2 dokážeme rozhodnout o povaze jakéhokoli soudělného čísla. Stačí jen vytknout všechna p^2. Pokud lze vytknout, tak po vytknutí buď zůstane nějaký p-násobek, pak je číslo KN. Pokud zůstane nesoudělné číslo s modulem, pak o něm rozhodneme využitím tvrzení 7. Formulujme využitím symbolu:

Tvrzení 8 (Soudělné kvadratické zbytky a nezbytky mod p^k)
Nechť $a = p^l b, b \in \mathbb{Z}, k, l \in \mathbb{N}, k \geq 2$, p je liché prvočíslo. Platí:

- $\left[\frac{p}{p^k}\right] = -1$
- $\left[\frac{a}{p^k}\right] = \left[\frac{p^l b}{p^k}\right] = \begin{cases} 1 \Leftrightarrow \left(\left[\frac{p}{p^k}\right]^l = 1 \wedge \left[\frac{b}{p^k}\right] = 1\right) \\ -1 \text{ v ostatních případech} \end{cases}$

Důkaz: První část je zřejmě. Druhá část je důsledkem tvrzení 2. Jen pro sudá l platí, že p^l je KZ modulo p^k, protože pro ně $p^l = \left(p^{\frac{l}{2}}\right)^2$ a $\left[\frac{p}{p^k}\right]^l = (-1)^l = 1$. Pro lichá l analogicky $\left[\frac{p}{p^k}\right]^l = -1$.

Podobně odvozeno v (Gauss, 1986, s. 68)

Příklad 13: Rozhodněte, zda je 63 KZ či KN modulo 81.

Řešení: $\left[\frac{63}{81}\right] = \left[\frac{63}{3^4}\right] = \left[\frac{3^2 \cdot 7}{3^4}\right]$

$\left[\frac{3^2}{3^4}\right] = \left[\frac{3}{3^4}\right]^2 = (-1)^2 = 1.$

$\left[\frac{7}{3^4}\right] = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1.$

$\left[\frac{3^2}{3^4}\right] = 1 \wedge \left[\frac{7}{3^4}\right]$, takže $\left[\frac{63}{81}\right] = 1.$

1.2.2 Řešení kvadratické kongruence $\mathbf{mod}\ p^k$

Popsali jsme, jak klasifikovat KZ a KN. Nyní se podívejme na způsob nalezení konkrétních řešení.

Řešení $x^2 \equiv a \pmod{p^k}$ pro nesoudělná a

Nejdříve se vypořádejme s úpravou. Pro nesoudělný koeficient u x^2 je to jednoduché. K tomu vždy existuje inverzní prvek a následně je možné doplnit na čtverec či použít vzorec.

Pozorujme, zda existuje podobná souvislost jako mezi kvadratickými zbytky modulo p a p^k i mezi konkrétními řešeními. Pokusme se tedy vyřešit $x^2 \equiv 13 \pmod{27}$ tak, že nejprve vyřešíme $x^2 \equiv 13 \pmod 3$. Ta je ekvivalentní $x^2 \equiv 1$ a řešení jsou očividně $x \equiv \pm 1$. Zvolme si jedno, pro jednoduchost $x \equiv 1$, ekvivalentně $x = 1 + 3k, k \in \mathbb{Z}$. Použijme stejnou úvahu jako v důkazu tvrzení 7:

$$x^2 = (1 + 3k)^2 = 1 + 6k + 9k^2$$

Pokud bychom chtěli rovnou řešit modulo 27, tak jsme si situaci spíše ztížili. Řešili bychom kvadratickou kongruenci s lineárním i absolutním členem a soudělnými koeficienty. Přejděme tedy prozatím do modulu 9:

$$1 + 6k + 9k^2 \equiv 1 + 6k \pmod 9$$

Zde najednou máme pouze lineární polynom. Položme ho kongruentní 13 a vyřešme:

$$\begin{aligned} 1 + 6k &\equiv 13 \\ 1 + 6k &\equiv 4 \\ 6k &\equiv 3 \;/:3 \\ 2k &\equiv 1 \pmod 3 \;/\cdot 2 \\ k &\equiv 2 \end{aligned}$$

Pak by jedním řešením mělo být $x_1 = 1 + 3 \cdot 2 = 7$, což dřívější pozorování potvrzuje. Druhým řešením je pak $x_2 \equiv -7 \equiv 2 \pmod 9$. Konečně se přesuňme do modulu 27. Opět si zvolme jedno z řešení, třeba znovu menší z nich. $x_2 = 2 + 9l, l \in \mathbb{Z}$, pak:

$$x^2 = (2 + 9l)^2 = 4 + 36l + 81l^2 \equiv 4 + 9l \pmod{27}$$

Řešíme pro 13:

$$\begin{aligned} 4 + 9l &\equiv 13 \\ 9l &\equiv 9 \;/:9 \\ l &\equiv 1 \pmod 3 \end{aligned}$$

Jedním řešením je tedy $x_1 = 2 + 9 = 11$ a obě řešení jsou $x \equiv \pm 11 \pmod{27}$. Zkouškou lze ověřit, že řešení platí. Kdybychom hledali řešení v modulu vyšší mocniny trojky, mohli bychom postupovat dále stejně. Postup shrňme:

- Řešíme $x^2 \equiv a \pmod{p^k}$
- Nejprve vyřešíme $x^2 \equiv a \pmod p$
- Jedním z řešení je $x_1 + lp, l \in \mathbb{Z}$
- Dosadíme $x^2 = (x_1 + lp)^2 = {x_1}^2 + 2x_1lp + (lp)^2 \equiv {x_1}^2 + 2x_1lp \pmod{p^2}$
- Vyřešíme lineární kongruenci ${x_1}^2 + 2x_1lp \equiv a \pmod{p^2}$ s neznámou l
- Nalezené l dosadíme do $x_1 + lp$ a to je jedním řešením $x^2 \equiv a \pmod{p^2}$
- Postup od 3. kroku opakujeme, dokud nedosáhneme modulu p^k. Některé mocniny p lze v postupu přeskočit, vždy se ale musíme zbavit kvadratického členu
- Po nalezení řešení x_k je druhým řešením $-x_k$

Příklad 14: Vyřešte kongruenci $15x^2 - 30x + 60 \equiv 0 \pmod{7^5}$.

Řešení: Nejprve upravme a doplňme na čtverec:

$$\begin{aligned} 15x^2 - 30x + 60 &\equiv 0 \ /: 15 \\ x^2 - 2x + 4 &\equiv 0 \\ x^2 - 2x + 1 &\equiv -4 + 1 \\ (x-1)^2 &\equiv -3 \end{aligned}$$

Zaveďme substituci $y = x - 1$:

$$y^2 \equiv -3$$

Nejdříve řešme modulo 7:

$$\begin{aligned} y^2 &\equiv -3 \pmod 7 \\ y^2 &\equiv 4 \end{aligned}$$

Očividně $y = \pm 2 + 7k, k \in \mathbb{Z}$. Zvolme si jedno z nich a pokračujme modulo 49:

$$\begin{aligned} y^2 = (2 + 7k)^2 &= 4 + 28k + 49k^2 \\ 4 + 28k &\equiv -3 \pmod{49} \\ 28k &\equiv 42 \\ -21k &\equiv 42 \ /: (-21) \\ k &\equiv -2 \pmod 7 \end{aligned}$$

Dosazením máme $y = 37 + 49l, l \in \mathbb{Z}$. Pokračujme:

$$y^2 = (37 + 49l)^2 = 1\,369 + 3\,626l + (49l)^2$$

Všimněme si, že kvadratický člen bude $\equiv 0$ nejvýše modulo $49^2 = 7^4$. Můžeme tedy přeskočit řešení modulo 7^3:

$$\begin{aligned} 1\,369 + 3\,626l &\equiv -3 \pmod{7^4} \\ 1\,225l &\equiv -1\,372 \\ 1\,225l &\equiv 1029 \ /: 49 \\ 25l &\equiv 21 \pmod{49} \ /\cdot 2 \\ l &\equiv 42 \end{aligned}$$

Po dosazení $y = 2\,095 + 7^4 m, m \in \mathbb{Z}$. Konečně řešme modulo 7^5:

$$y^2 = (2\,095 + 7^4 m)^2 \equiv 2\,398 + 9\,604m \pmod{7^5}$$
$$2\,398 + 9\,604m \equiv -3$$
$$9\,604m \equiv -2\,401 \;/ : 2401$$
$$4m \equiv -1 \pmod 7$$
$$4m \equiv 6 \;/ \cdot 2$$
$$m \equiv 5$$

Dosadíme a máme $y = 14\,100 + 7^5 k$, řešení jsou tedy $y \equiv \pm 14\,100 \pmod{7^5}$. Zpětným dosazením do substituční rovnice:

$$x \equiv \pm 14\,101$$

Řešení kvadratické kongruence $\mathbf{mod}\ p^k$ se soudělnými koeficienty s modulem

Podívejme se, jak upravit kongruenci se soudělným koeficientem u x^2 s modulem. Soudělnost jiných koeficientů nás neomezuje. Pozorujme např. $18x^2 + 5x + 10 \equiv$ $\equiv 0 \pmod{27}$. Inverzní prvek k 18 zde neexistuje, musíme zvolit jinou úpravu. V souladu s postupem řešení, které jsme si právě odvodili, zkusme kongruenci nejprve řešit modulo 3:

$$18x^2 + 5x + 10 \equiv 2x + 1 \pmod 3$$

Z kvadratické kongruence se stala lineární. Vyřešme:

$$2x + 1 \equiv 0$$
$$2x \equiv 2$$
$$x \equiv 1$$

Ekvivalentně $x = 1 + 3k, k \in \mathbb{Z}$. Řešení tedy bude jen jediné a nalezneme ho stejným způsobem, který jsme si představili. V tomto případě musíme dosadit do celého neupraveného výrazu:

$$18x^2 + 5x + 10 \equiv 5x + 1 \pmod 9$$
$$5(1 + 3k) + 1 \equiv 0$$
$$5 + 15k + 1 \equiv 0$$
$$6k \equiv -6$$
$$k \equiv -1 \equiv 2 \pmod 3$$

Po dosazení je řešením $x = 7 + 9l, l \in \mathbb{Z}$. Konečně dosaďme do původní neupravené kongruence:

$$18(7 + 9l)^2 + 5(7 + 9l) + 10 \equiv 0 \pmod{27}$$
$$18 \cdot 49 + 18 \cdot 126l + 81l^2 + 35 + 45l + 10 \equiv 0$$
$$9 + 18l \equiv 0$$
$$18l \equiv 18 \,/ : 18$$
$$l \equiv 1 \pmod{3}$$

Dosadíme a máme jediné řešení $x = 16 + 27m, m \in \mathbb{Z}$**.** V případech soudělného koeficientu u x^2 tedy kongruenci řešíme nejdříve modulo p jako v předchozím případě, jen bez předchozího doplnění na čtverec a substituce. Tam se kvadratická kongruence stane lineární už v prvním kroku řešení a výsledné řešení je pouze jedno.

Příklad 15: Vyřešte kongruenci $75x^2 - 12x + 91 \equiv 0 \pmod{625}$.

Řešení: Koeficient u x^2 je soudělný s modulem, bez úpravy řešme modulo 5:

$$3x + 1 \equiv 0 \pmod{5}$$
$$3x \equiv 4 \,/ \cdot 2$$
$$x \equiv 3$$

Řešení je $x = 3 + 5k, k \in \mathbb{Z}$. Postupme o mocninu výš:

$$13x + 16 \equiv 0 \pmod{25}$$
$$13(3 + 5k) + 16 \equiv 0$$
$$39 + 65k + 16 \equiv 0$$
$$15k + 5 \equiv 0 \,/ : 5$$
$$3k + 1 \equiv 0 \pmod{5}$$
$$k \equiv 3$$

Dosazením máme řešení $x = 18 + 25l, l \in \mathbb{Z}$. Pokračujme:

$$75x^2 - 12x + 91 \equiv 0 \pmod{625}$$
$$75(18 + 25l)^2 - 12(18 + 25l) + 91 \equiv 0$$
$$75(324 + 900l + 625l^2) - 216 - 300l + 91 \equiv 0$$
$$325l + 425 \equiv 0 \,/ : 25$$

$$13l + 17 \equiv 0 \pmod{25}$$
$$13l \equiv 8 \,/\cdot 2$$
$$l \equiv 16$$

Výsledné řešení je $x = 418 + 625n, n \in \mathbb{Z}$.

Řešení $x^2 \equiv a \pmod{p^k}$ pro soudělná a

Již jsme vypozorovali, že každý soudělný KZ je modulo 81 součinem 9 a nějakého KZ. Řešitelnou pravou stranu si tedy můžeme představit jako $9k^2$ a řešit pro k. To kongruenci zjednodušuje, protože můžeme vydělit 9 a tím vydělit, a tedy zmenšit, i modul. Zkusme tímto způsobem vyřešit např. $x^2 \equiv 63 \pmod{81}$. Na pravé straně chceme $9k^2$, využijeme tedy substituce $x = 3k$:

$$x^2 = (3k)^2 = 9k^2$$
$$9k^2 \equiv 63 \pmod{81} /: 9$$
$$k^2 \equiv 7 \pmod{9}$$

Řešeními jsou $k \equiv \pm 4 \pmod{9}$. Vzpomeňme si, že pro soudělné zbytky jsme nepozorovali pouze dvě „odmocniny“. Abychom tedy našli všechna řešení, musíme dosadit všechna vyhovující k menší než 81. To je rozdíl oproti předchozímu postupu. Řešení pak jsou:

$$x \equiv 12, 15, 39, 42, 66, 69 \pmod{81}$$

Shrňme a zobecněme:

- Řešíme $x^2 \equiv a \pmod{p^k}$
- Použijeme substituci $x^2 = (pl)^2$, řešíme kongruenci $p^2 l^2 \equiv a$
- Vydělíme p^2 a vyřešíme $l^2 \equiv \frac{a}{p^2} \pmod{p^{k-2}}$
- Do $x = pl$ dosadíme všechna vyhovující $l \in \mathbb{N}_0, l < p^k$

Příklad 16: Vyřešte kongruenci $208x^2 + 97x - 17 \equiv 0 \pmod{243}$.

Řešení: Využijme $243 = 3^5$. Nejprve doplňme na čtverec:

$$208x^2 + 97x - 17 \equiv 0$$
$$-35x^2 + 97x - 17 \equiv 0 \,/\cdot 7$$
$$-2x^2 + 193x - 119 \equiv 0 \,/\cdot (-122)$$

$$x^2 + 25x + 181 \equiv 0$$
$$x^2 - 218x + 181 \equiv 0$$
$$x^2 - 218x + 11\,881 \equiv -181 + 11\,881$$
$$(x - 109)^2 \equiv 36$$

Použijme substituci $y = x - 109$ a řešme $y^2 \equiv 36$. Zde využijme substituci $y = 3k$:

$$9k^2 \equiv 36 \pmod{243} /: 9$$
$$k^2 \equiv 4 \pmod{27}$$

Řešení jsou $k = \pm 2 + 27l$. Dosazením všech vyhovujících k máme:

$$y \equiv 6, 75, 87, 156, 168, 237 \pmod{243}$$

Zpětným dosazením do substituční rovnice:

$$x \equiv 22, 34, 103, 115, 184, 196 \pmod{243}$$

1.3 Kvadratické kongruence mod 2^k

Opět začněme nejdříve klasifikací KZ a KN.

1.3.1 Kvadratické zbytky a nezbytky mod 2^k

Obdobně jako v předchozím oddílu se zaměřme na KZ nesoudělné a soudělné zvlášť. V tomto případě se jednoduše jedná o lichá a sudá čísla. Druhé mocniny lichých čísel jsou tvaru $(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1, k \in \mathbb{Z}$. Všimněme si, že pro všechna k je 4 v tomto výrazu násobena sudým číslem, tudíž je první člen minimálně osminásobkem a všechny druhé mocniny lichých čísel jsou tím pádem $\equiv 1 \pmod 8$. Druhé mocniny sudých čísel jsou tvaru $(2l)^2 = 4l^2, l \in \mathbb{Z}$, tedy analogicky k lichým prvočíslům součinem 2^2 a nějaké jiné druhé mocniny. Formulujme jedním tvrzením s využitím symbolu.

Tvrzení 9 (Kvadratické zbytky a nezbytky mod 2^k)

Nechť $a \in \mathbb{Z}$ a $k \in \mathbb{N}$, platí:

- $\left[\frac{2}{2^k}\right] = -1$ pro $k \geq 2$
- pro lichá a: $\left[\frac{a}{2^k}\right] = \begin{cases} 1 \Leftrightarrow a \equiv 1 \pmod 8 \\ -1 \Leftrightarrow a \not\equiv 1 \pmod 8 \end{cases}$
- pro $a = 2^l b, l \in \mathbb{N}, b$ liché: $\left[\frac{a}{2^k}\right] = \left[\frac{2^l b}{2^k}\right] = \begin{cases} 1 \Leftrightarrow \left(\left[\frac{2}{2^k}\right]^l = 1 \wedge \left[\frac{b}{2^k}\right] = 1\right) \\ -1 \text{ v ostatních případech} \end{cases}$

Odvozeno podobně jako v (Gauss, 1986, 68-69).

Důkaz: První část je zřejmá. Druhá plyne přímo z pozorování druhých mocnin lichých čísel. Důkaz třetí části je analogický k důkazu tvrzení 8.

Příklad 17: Rozhodněte, zda jsou 35 a 68 KZ či KN modulo 128.

Řešení: $\left[\frac{35}{2^7}\right] = -1$, protože $35 \equiv 3 \not\equiv 1 \pmod 8$.

$\left[\frac{68}{2^7}\right] = \left[\frac{2^2 \cdot 17}{2^7}\right]$.

$\left[\frac{2^2}{2^7}\right] = \left[\frac{2}{2^7}\right]^2 = (-1)^2 = 1$, $\left[\frac{17}{2^7}\right] = 1$, protože $17 \equiv 1 \pmod 8$. Takže $\left[\frac{68}{2^7}\right] = 1$.

1.3.2 Řešení kvadratické kongruence $\mathbf{mod}\ 2^k$

Použijeme stejný princip jako pro modulo p^k, tedy postupná konstrukce řešení modulo 2^k ze znalosti řešení modulo všech nižších mocnin dvojky.

Řešení kvadratické kongruence $\mathbf{mod}\ 2^k$ se soudělnými koeficienty a modulem

Modulo nízkých mocnin dvojky se úpravou kongruence není třeba hlouběji zabývat, zde lze kongruenci velmi rychle vyřešit dosazováním. (Pozn.: Zajímavé je, že navzdory tomu, že každé číslo je KZ modulo 2, kongruence $x^2 + x + 1 \equiv 0 \pmod 2$ očividně nemá řešení). Obecný vzorec nelze použít nikdy, protože se v něm vždy dělí sudým číslem a pro ty zde neexistují inverzní prvky. Při doplnění na čtverec se pro vyšší mocniny už nestačí řídit pouze koeficientem u x^2, nýbrž i koeficientem u x. U x^2 opět záleží, zda ke koeficientu existuje inverzní prvek, u x záleží, zda je koeficient sudý nebo lichý. Modulo 2^k pro každé liché číslo totiž platí, že i jemu kongruentní záporné číslo je liché. V případech, kdy kongruenci nelze jednoduše upravit ji budeme bez úpravy řešit v modulech nižších mocnin, jako v případě modulo p^k.

Příklad 18: Vyřešte kongruenci $10x^2 + 3x + 4 \equiv 0 \pmod{16}$.

Řešení: Řešme nejprve modulo 2:

$$x \equiv 0 \pmod 2$$

Řešení je $x = 2k, k \in \mathbb{Z}$. Pokračujme modulo 4:

$$\begin{aligned} 2x^2 + 3x &\equiv 0 \pmod 4 \\ 2(2k)^2 + 3 \cdot 2k &\equiv 0 \\ 2k &\equiv 0 \ /:2 \\ k &\equiv 0 \pmod 2 \end{aligned}$$

Dosazením máme řešení $x = 4l, \in \mathbb{Z}$. Pokračujme:

$$\begin{aligned} 2x^2 + 3x + 4 &\equiv 0 \pmod 8 \\ 2(4l)^2 + 3 \cdot 4l + 4 &\equiv 0 \\ 4l + 4 &\equiv 0 \ /:4 \\ l + 1 &\equiv 0 \pmod 2 \\ l &\equiv 1 \end{aligned}$$

Dosaďme a řešení je $x = 4 + 8m, m \in \mathbb{Z}$. Dokončeme:

$$10x^2 + 3x + 4 \equiv 0 \pmod{16}$$
$$10(4 + 8m)^2 + 3(4 + 8m) + 4 \equiv 0$$
$$10(16 + 64m + 64m^2) + 12 + 24m + 4 \equiv 0$$
$$8m \equiv 0 \ /:8$$
$$m \equiv 0 \pmod{2}$$

Řešením tedy je $x = 4 + 16n, n \in \mathbb{Z}$.

Dále pozorujme $x^2 \equiv a \pmod{2^k}$ pro lichá a sudá a zvlášť.

Řešení $x^2 \equiv a \pmod{2^k}$ pro sudá a

Pro sudá a stačí obdobně jako modulo p^k využít substituci $x = 2k$ a tedy řešit kongruenci $4k^2 \equiv a$. I nadále je postup analogický.

Příklad 19: Vyřešte kongruenci $x^2 \equiv 100 \pmod{256}$

Řešení: Použijme substituci $x = 2k$:

$$4k^2 \equiv 100 \ /:4$$
$$k^2 \equiv 25 \pmod{64}$$

Řešením je $k = 5 + 64l, l \in \mathbb{Z}$. Dosazením všech vhodných k máme řešení:

$$x \equiv 10, 54, 74, 118, 138$$

Řešení $x^2 \equiv a \pmod{2^k}$ pro lichá a

Kongruence $x^2 \equiv a \pmod{2}$ je ekvivalentní kongruenci $x^2 \equiv 1$ a ta má řešení $x \equiv 1$. Modulo 4 jsou lichými KZ: $1^1 = 1$ a $3^2 = 9 \equiv 1$, takže $x^2 \equiv a \pmod{4}$ má řešení pouze pokud $a \equiv 1$ a řešení jsou $x \equiv \pm 1$, tedy jak jsme zvyklí. Modulo 8 jsou lichými KZ:

$$1^1 = 1 \qquad 3^2 = 9 \equiv 1 \qquad 5^2 = 25 \equiv 1 \qquad 7^2 \equiv (-1)^2 = 1$$

Situace je tedy stejná, řešení jsou ovšem 4. Modulo 16 již přibude nový lichý KZ, tím je očividně $3^2 = 9$. Z tohoto pozorování vyplývá, že pro budování řešení z modulů nižších mocnin dvojky můžeme začít od čtyř řešení modulo 8, namísto modulu 2.

Příklad 20: Vyřešte kongruenci $x^2 \equiv 25 \pmod{32}$.

Řešení: Řešení budujme postupně od čtyř řešení $x^2 \equiv 1 \pmod{8}$.

Prvním je $x = 1 + 8k, k \in \mathbb{Z}$. Dosazením máme:

$$x^2 = (1 + 8k)^2 = 1 + 16k + 64k^2 \equiv 1 + 16k \pmod{32}$$
$$1 + 16k \equiv 25$$
$$16k \equiv 24 \;/:8$$
$$2k \equiv 3 \pmod{4}$$

Tato kongruence nemá řešení, protože sudé číslo nemůže být kongruentní lichému modulo 2^k. Druhým řešením je $x = 3 + 8k$, dosaďme:

$$x^2 = (3 + 8k)^2 = 9 + 48k + 64k^2 \equiv 9 + 16k \pmod{32}$$
$$9 + 16k \equiv 25$$
$$16k \equiv 16 \;/:16$$
$$k \equiv 1 \pmod{2}$$

Dosazením všech vyhovujících k máme prozatím dvě řešení $x \equiv 11, 27 \pmod{32}$. Pokračujme dále s $x = 5 + 8k$:

$$x^2 = (5 + 8k)^2 = 25 + 80k + 64k^2 \equiv 25 + 16k \pmod{32}$$
$$25 + 16k \equiv 25$$
$$16k \equiv 0 \;/:16$$
$$k \equiv 0 \pmod{2}$$

Dosadíme všechny vyhovující k a máme dvě další řešení $x \equiv 5, 21$. Konečně dosazením $x = 7 + 8k$ máme:

$$x^2 = (7 + 8k)^2 = 49 + 112k + 64k^2 \equiv 17 + 16k \pmod{32}$$
$$17 + 16k \equiv 25$$
$$16k \equiv 8 \;/:8$$
$$2k \equiv 1 \pmod{4}$$

Tato kongruence také nemá řešení. Řešení původní kongruence jsou tedy čtyři a jsou jimi $x \equiv 5, 11, 21, 27 \pmod{32}$.

Z příkladů je zřejmé, že takové kongruence budou mít čtyři řešení, namísto obvyklých dvou. Nikdy jich nebude více, protože pokud budeme postupovat od řešení modulo 8, pak modulo 16 máme $1^2 \equiv 7^2 \equiv 1$ a $3^2 \equiv 5^2 \equiv 9$ a každý lichý KZ v modulu vyšší mocniny dvojky bude kongruentní jen jednomu z těchto dvou KZ modulo 16. Podotkněme, že stačí nalézt pouze jednu dvojici těchto řešení a druhou dvojící budou jejich opačné hodnoty. Postup je analogický k postupu modulo p^k s tím rozdílem, že nemusíme začínat od nejnižší mocniny dvojky, ale začínáme modulo 8. Také nepracujeme s jedním řešením, ale se všemi čtyřmi.

1.4 Kvadratické kongruence mod n

V případě, že známe prvočíselný rozklad n (což zde předpokládáme), můžeme kongruenci jednoduše rozložit využitím čínské věty o zbytcích (dále jen ČVZ), o ní např. (Křížek, 2018, s. 44).

1.4.1 Kvadratické zbytky a nezbytky mod n

Z ČVZ přirozeně plyne tvrzení o KZ modulo n.

Tvrzení 10 (Kvadratické zbytky a nezbytky mod n)

Nechť p_i je prvočíslo, $a \in \mathbb{Z}$, $k_i \in \mathbb{N}$ a $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$. Pak a je KZ modulo n právě tehdy, když je KZ modulo p_i pro všechna prvočísla, ze kterých je n složeno (Gauss, 1986, s. 70-71). Ekvivalentně:

$$\left[\frac{a}{n}\right] = \begin{cases} 1 \Leftrightarrow \left(\left[\frac{a}{p_1^{k_1}}\right] = 1 \wedge \left[\frac{a}{p_2^{k_2}}\right] = 1 \wedge \dots \wedge \left[\frac{a}{p_m^{k_m}}\right] = 1\right) \\ -1 \text{ v ostatních případech} \end{cases}$$

Důkaz: Tvrzení vyplývá z ČVZ.

„⇐“ a je zbytkem všech mocnin prvočísel, ze kterých je n složeno, jinými slovy kongruence $x^2 \equiv a$ má řešení ve všech těchto modulech. Podle ČVZ tedy také existuje jednoznačné řešení kongruence $x^2 \equiv a \pmod{p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} = n}$.

„⇒“ Plyne z ekvivalence ČVZ.

Příklad 21: Rozhodněte, zda je 2 KZ nebo KN modulo 15.

Řešení: $15 = 3 \cdot 5$, musíme vyčíslit Legendrovy symboly $\left(\frac{2}{3}\right)$ a $\left(\frac{2}{5}\right)$. Protože $3 \equiv 3 \pmod 8$, již první z nich je roven -1, a tedy $\left[\frac{2}{15}\right] = -1$.

Zmiňme také často používané zobecnění Legendrova symbolu.

Definice 6 (Jacobiho symbol)

Nechť p_i je liché prvočíslo, $a \in \mathbb{Z}$, $k_i \in \mathbb{N}$, $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ a $\left(\frac{a}{p_i}\right)$ je Legendrův symbol. Jacobiho symbol definujeme:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \left(\frac{a}{p_2}\right)^{k_2} \dots \left(\frac{a}{p_m}\right)^{k_m}$$

(Křížek, 2018, s. 79).

Příklad 22: Určete hodnotu Jacobiho symbolu $\left(\frac{2}{15}\right)$.

Řešení: $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = -1 \cdot (-1) = 1$

Jak lze na tomto příkladu vidět, Jacobiho symbol může nabývat hodnoty 1 navzdory tomu, že a je KN modulo n. Také je definován pouze pro lichá n. Proto se pro naše účely nehodí.

1.4.2 Řešení kvadratické kongruence $\mathbf{mod}\ n$

Předpokládejme, že jsme vyřešili všechny kongruence v modulech mocnin prvočísel, ze kterých je n složeno. Pokud vyřešíme všechny různé soustavy kongruencí tvořených všemi řešeními (tzn. všechny různé soustavy, kdy si každé modulo vybereme jednu kongruenci), nalezneme všechna řešení původní kongruence. Z toho plyne následující tvrzení.

Tvrzení 11 (Počet řešení kvadratické kongruence modulo n)

Nechť $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$. Počet řešení kongruence $x^2 \equiv a \pmod{n}$ je roven součinu počtů řešení stejné kongruence v modulech $p_1^{k_1}, p_2^{k_2}, \dots, p_m^{k_m}$.

Důkaz: Pro řešení $x^2 \equiv a \pmod{n}$ musíme vyřešit soustavu lineárních kongruencí, které označují řešení stejné kongruence v modulech mocnin prvočísel, ze kterých je n složeno. Počet řešení této kongruence $\mathrm{mod}\ p_1^{k_1}$ si označme l_1, počet řešení $\mathrm{mod}\ p_2^{k_2}$ označme l_2 atd. Počet všech řešitelných soustav takových kongruencí (tj. takových soustav, kde pro každé modulo vybíráme právě jednu kongruenci) je podle kombinatorického pravidla součinu roven $l_1 \cdot l_2 \cdot \dots \cdot l_2$.

Příklad 23: Vyřešte kongruenci $2x^2 + 13x - 9 \equiv 0 \pmod{15}$.

Řešení: Nejprve vyřešme kongruenci $2x^2 + 13x - 9 \equiv 0 \pmod{3}$:

$$2x^2 + x \equiv 0$$
$$x(2x + 1) \equiv 0$$

Z prvního součinitele $x \equiv 0$, z druhého $x \equiv 1$. Nyní řešme $2x^2 + 13x - 9 \equiv 0 \pmod{5}$:

$$2x^2 + 3x + 1 \equiv 0 \,/\cdot 3$$
$$x^2 + 4x + 3 \equiv 0$$
$$x^2 + 4x + 4 \equiv -3 + 4$$
$$(x + 2)^2 \equiv 1$$

A řešení jsou $x \equiv 2$ a $x \equiv 4$. Musíme vyřešit soustavy:

$x \equiv 1 \pmod{3}$	$x \equiv 1 \pmod{3}$	$x \equiv 0 \pmod{3}$	$x \equiv 0 \pmod{3}$
$x \equiv 4 \pmod{5}$	$x \equiv 2 \pmod{5}$	$x \equiv 4 \pmod{5}$	$x \equiv 2 \pmod{5}$

Ptáme se, jaká čísla modulo 15 mají po dělení 3 takový zbytek a po dělení 5 takový zbytek. Zapišme do tabulky:

mod 5 / **mod 3**	**2**	**4**
0	12	9
1	7	4

Tab. 1: Řešení soustavy lineárních kongruencí.

Řešení soustav postupně tedy jsou: $x \equiv 4, 7, 9, 12 \pmod{15}$. To jsou i řešení původní kongruence.

1.5 Polynomiální kongruence vyšších stupňů

V tomto oddílu postupujme obdobně jako v předchozí. Začněme tedy zobecněním základní definice.

Definice 7 (Zbytek/reziduum a nezbytek stupně k)

Nechť $k, n \in \mathbb{N}$ a $a \in \mathbb{Z}$. Pokud existuje x takové, že řeší kongruenci $x^k \equiv a \pmod{n}$, pak říkáme, že číslo a je *zbytek* (nebo *reziduum*) *stupně k modulo n*. V opačném případě říkáme, že číslo a je *nezbytek stupně k modulo n*.

Pozn.: Pro $k = 3$ nazýváme a kubickým zbytkem, pro $k = 4$ kvartickým zbytkem. Dále v tomto oddílu budeme používat pouze termín *zbytek*, bude-li myšlen obecně, či bude-li z kontextu jasné, jakého stupně.

Pozorování: Můžeme předpokládat, že obdobně jako kvadratických zbytků je polovina všech čísel $\bmod p$, tak kubických zbytků bude třetina, kvartických čtvrtina atd. Pozorujme, zda je tato domněnka pravdivá. Již modulo 3 nastává problém, protože $1^3 \equiv 1$ a $2^3 \equiv 2$, tedy všechna čísla modulo 3 jsou kubickými zbytky, tento modul ale může být speciálním případem. Pozorujme dále modulo 5:

$$1^3 = 1 \qquad 3^3 \equiv 2$$

$$2^3 \equiv 3 \qquad 4^3 = (2^2)^3 = (2^3)^2 \equiv 3^2 \equiv 4$$

Opět jsou všechna čísla kubickými zbytky. Všimněme si ovšem, že ani v jednom z těchto pozorování nebyl počet zkoumaných čísel dělitelný třemi. Pro modulo 7 musíme prozkoumat 6 čísel. Tento počet je dělitelný třemi, možná se situace bude lišit:

$$1^3 = 1 \qquad 3^3 \equiv 6 \qquad 5^3 \equiv 6$$

$$2^3 \equiv 1 \qquad 4^3 = (2^2)^3 = (2^3)^2 \equiv 1 \qquad 6^3 \equiv (-1)^3 = -1 \equiv 6$$

Nyní jsou kubickými zbytky pouze 1 a 6, tedy jsou pouze dva a v tomto případě je jich, v souladu s předpokladem, třetina. Pro modulo 5 a 7 proveďme ještě pozorování kvartických zbytků. V prvním případě lze na základě pozorování kubických zbytků předpokládat, že budeme mít jen jeden kvartický zbytek, v druhém zase šest.

$\mathrm{mod}\ 5\colon 1^4 = 1$

$2^4 \equiv 1$

$3^4 \equiv (-2)^4 = 2^4 \equiv 1$

$4^4 \equiv (-1)^4 = 1$

$\mathrm{mod}\ 7\colon 1^4 = 1$

$2^4 \equiv 2$

$3^4 \equiv 4$

$4^4 \equiv (-3)^4 = 3^4 \equiv 4$

$5^4 \equiv (-2)^4 \equiv 2$

$6^4 \equiv (-1)^4 = 1$

V prvním případě se naše domněnka potvrdila, v druhém ne. Namísto očekávaných šesti zbytků máme pouze tři. Na první pohled je to jasné z obecné vlastnosti sudých mocnin, tedy že $a^{2l} = (-a)^{2l}$, zbytků sudého stupně bude tedy vždy maximálně polovina. Pozorujme ještě dále, již jsme pozorovali pro prvočíslo a sudé číslo, tak zvolme liché neprvočíslo, nejmenším takovým je 9:

$\mathrm{mod}\ 5\colon 1^9 = 1$

$2^9 = (2^4)^2 \cdot 2 \equiv 1 \cdot 2 = 2$

$3^9 = (3^4)^2 \cdot 3 \equiv 3$

$4^9 \equiv (-1)^9 = -1 \equiv 4$

$\mathrm{mod}\ 7\colon 1^9 = 1$

$2^9 = (2^4)^2 \cdot 2 \equiv 4 \cdot 2 \equiv 1$

$3^9 = (3^4)^2 \cdot 3 \equiv 4^2 \cdot 3 \equiv 6$

$4^9 = (2^9)^2 \equiv 1$

$5^9 = (5^4)^2 \cdot 5 \equiv 2^2 \cdot 5 \equiv 6$

$6^9 \equiv (-1)^9 = -1 \equiv 6$

V prvním případě jsou opět všechna čísla zbytky stupně 9, v druhém jsou jimi pouze dvě čísla, tedy třetina všech. Domněnka o dělitelnosti se znovu potvrzuje. 6 sice dělitelné 9 není, nicméně tato čísla jsou soudělná a $\mathrm{D}(6,9) = 3$, což koresponduje se skutečností, že zbytků stupně 9 modulo 7 je třetina všech (šesti) zbytků po dělení 7. Shrňme.

Tvrzení 12 (Počet zbytků a nezbytků stupně k modulo p)

Nechť $k \in \mathbb{N}$ a p je liché prvočíslo. Počet zbytků stupně k modulo p se rovná $\frac{p-1}{D(p-1,k)}$.

Důkaz: Str. 96

Příklad 24: Určete počet zbytků stupně 15 postupně modulo $3, 7, 11$ a 31.

Řešení: mod 3: $\frac{3-1}{D(3-1,15)} = \frac{2}{1} = 2$

mod 7: $\frac{7-1}{D(7-1,15)} = \frac{6}{3} = 2$

mod 11: $\frac{11-1}{D(11-1,15)} = \frac{10}{5} = 2$

mod 31: $\frac{31-1}{D(31-1,15)} = \frac{30}{15} = 2.$

Pozn.: Toto tvrzení je zobecněním tvrzení 1. Důležitým důsledkem tohoto tvrzení je, že zbytků sudého stupně je vždy maximálně polovina, protože $p-1$ je sudé. Další užitečné důsledky jsou, že pokud je modulo p pouze jeden zbytek stupně k, je jím triviálně 1 a pokud dva zbytky, pak jsou jimi 1 a -1. To je zřejmé pro zbytky lichého stupně ($(-1)^{2k+1} = -1$), ale ne pro zbytky stupně sudého. Pro ně to plyne z tvrzení 14.

Pozorování: V předchozím oddílu jsme se dále zabývali součiny zbytků a nezbytků různě mezi sebou. Je zjevné, že součinem dvou zbytků stejného stupně je také zbytek tohoto stupně a součinem zbytku nějakého stupně a nezbytku je nezbytek. Jen pro součiny dvou nezbytků obecného stupně neplatí to samé jako pro součin dvou kvadratických nezbytků. Protipříklady lze nalézt v modulech, kde je zbytků daného stupně relativně málo, např. $3 \cdot 4 \equiv 5 \pmod 7$ pro zbytky stupně 9. Nicméně se může stát, že součinem dvou nezbytků bude zbytek, např. $2 \cdot 3 = 6 \pmod 7$ taktéž pro zbytky stupně 9.

Tvrzení 13 (Součiny zbytků a nezbytků stupně k modulo n)
Nechť $k, n \in \mathbb{N}$ a $a, b \in \mathbb{Z}$.

(1) Pokud jsou a, b zbytky stupně k modulo n, pak i ab je zbytkem.
(2) Pokud a je zbytkem a b nezbytkem stupně k modulo n, pak ab je nezbytkem.

Důkaz: Analogicky jako v tvrzení 2, jen nedokazujeme pro druhou mocninu, ale pro obecnou k-tou mocninu.

Dále jsme zavedli Legendrův symbol. Jeho zobecnění na zbytky vyšších stupňů sice existují, nicméně se definují a vyčíslují za využití oboru Eisensteinových či Gaussových celých čísel, které jsou nad rámec této práce. O kubických a kvartických např. v bakalářské práci *Kubická a bikvadratická reciprocita* (Staško, 2019).

Jak lze tedy za použití elementárnější matematiky zjistit, zda je dané číslo zbytkem $\mathrm{mod}\, p$, respektive jestli má kongruence $x^k \equiv a \pmod p$ řešení? Nejprve zmiňme pár triviálních poznatků. Jak již bylo zmíněno, pokud je zbytek stupně k pouze jeden, pak je jím 1, pokud jsou dva, jsou jimi 1 a -1. Při vyšším počtu se ale situace už dosti komplikuje. Nicméně, -1 je vždy zbytkem lichého stupně. Naopak pro sudé stupně platí $x^{2l} = (-x)^{2l}$.

Jako jeden z prvních obecných závěrů v této oblasti jsme zmínili Eulerovo kritérium, v němž se umocňuje zkoumané číslo na počet všech kvadratických zbytků modulo p. To se dá přímo zobecnit.

Tvrzení 14 (Zobecněné Eulerovo kritérium)
Nechť $a \in \mathbb{Z}, k \in \mathbb{N}$ a p je liché prvočíslo. a je zbytkem stupně k modulo p právě tehdy, když:

$$a^{\frac{p-1}{\mathrm{D}(p-1,k)}} \equiv 1 \pmod p$$

Důkaz: (Volkaner, 2011)

Příklad 24: Určete, zda jsou 5 a 7 kubickými zbytky modulo 13.

Řešení: $5^{\frac{13-1}{\mathrm{D}(13-1,3)}} = 5^{\frac{12}{3}} = 5^4 \equiv 1$: Ano

$7^4 \equiv 9$: Ne.

Pozn.: Všimněme si rozdílu mezi Eulerovým kritériem pro kvadratické zbytky a jeho zobecněním. V zobecněném případě již neplatí, že pro nezbytky se použitím kritéria počítaná mocnina musí rovnat -1 (ale může, např. 2 je nezbytkem stupně 4 modulo 17 a $2^{\frac{17-1}{\mathrm{D}(17-1,4)}} = 2^{\frac{16}{4}} = 2^4 \equiv -1 \pmod{17}$).

I zde ovšem platí, že počítání vysokých mocnin může být zdlouhavé a nepraktické. Pro kvadratické zbytky a nezbytky je užitečným pomocníkem zákon kvadratické reciprocity, a i ten lze zobecnit. S nimi ovšem úzce souvisí obecný zbytkový symbol a pro použití

kubické, resp. bikvadratické reciprocity je potřeba pracovat s Eisensteinovými a Gaussovými celými čísly. O těchto reciprocitách více v (Staško, 2019).

O zbytcích neprvočíselných modulů a obecně řešení polynomiálních kongruencí už jen krátce. Podobně jako nalezení řešení obecné polynomiální rovnice nad komplexními čísly či obecné kvadratické kongruence modulo p je nalezení řešení obecné polynomiální kongruence modulo p laicky řečeno poměrně obtížné, ba dokonce obtížnější než u obou zmíněných. Existují algoritmy umožňující faktorizaci polynomů splňujících nějaké podmínky nad konečnými tělesy (což čísla modulo p tvoří). Takové algoritmy tedy odhalí i řešení polynomiální kongruence, ale jsou vysoce nad rámec této práce. Dále platí o polynomiálních kongruencích obdoba základní věty algebry. Nazývá se *Lagrangeova věta* a říká, že kongruence stupně k má nejvýše k řešení. O zbytcích modulo p^l platí zobecněné tvrzení 7 a řešení $x^k \equiv a \pmod{p^l}$ se buduje z řešení $x^k \equiv a \pmod{p}$ analogicky jako pro kvadratické kongruence. V důkazu tohoto tvrzení figuruje tzv. *Henselovo lemma*. $x^k \equiv$ $\equiv a \pmod{n}$ se také řeší obdobně využitím ČVZ a následným řešením soustavy lineárních kongruencí.

2 Exponenciální kongruence

Prvním typem nealgebraických rovnic, se kterými se žáci nejčastěji setkají jsou rovnice exponenciální. Jak název napovídá, neznámá se v těchto rovnicích nachází v exponentu. S mocněním modulo n jsme se v této práci již setkali a smysl tedy mají i exponenciální kongruenční rovnice. Definujme.

Definice 8 (Exponenciální kongruence)
Exponenciální kongruencí rozumíme kongruenční rovnici:

$$a^x \equiv b \pmod{n}$$

kde $a, b \in \mathbb{Z}$ a x je neznámá, často nazývána *diskrétní logaritmus b o základu a modulo n.*

Pozn.: Běžně se hledá řešení, které je přirozeným číslem. Tak tomu bude i v této práci.

Zkusme nejdříve vyřešit dvě jednoduché exponenciální kongruence. Začněme s:

$$3^x \equiv 5 \pmod{11}$$

Modul je relativně malý, zkusme řešit dosazováním:

$$3^2 = 9$$
$$3^3 = 27 \equiv 5$$

To navádí na závěr, že řešením je $x = 3 + 11k, k \in \mathbb{Z}$. Všimněme si ale, že pro $k = 1$:

$$3^{14} = (3^3)^4 \cdot 3^2 \equiv 5^4 \cdot 9 = 25^2 \cdot 9 \equiv 3^2 \cdot 9 = 3^4 \equiv 5 \cdot 3 \equiv 4 \not\equiv 5$$

To znamená, že 11 není správnou periodou řešení. Pozorujme, pro jaký nejmenší exponent je 3 kongruentní 1 modulo 11:

$$3^4 = 81 \equiv 4$$
$$3^5 \equiv 4 \cdot 3 = 12 \equiv 1$$

Správným řešením je tedy $x = 3 + 5k, k \in \mathbb{Z}$.

Zkusme vyřešit kongruenci bez dosazování:

$$5^x \equiv 25 \pmod{31}$$

Řešení je jasné, ale pro názornost převeďme na stejný základ:

$$5^x \equiv 5^2$$

Jedním řešením je $x = 2$. Jak to bude s periodou v tomto případě? Zde opět dosazujme:

$$5^3 = 125 \equiv 1$$

Takže řešením je $x = 2 + 3k$.

Nalezení řešení exponenciální kongruence, kde na pravé straně nemáme číslo, které lze jednoduše převést na stejný základ jako na levé straně a modul je moc velký na dosazování, je obecně velmi nesnadné. Obecně je nalezení diskrétního logaritmu tak obtížné, že je na tomto problému založeno několik šifrovacích metod. Z příkladů je vidět, že otázka, jaká bude perioda řešení, také není úplně triviální.

Pozorujme tedy, jak se vlastně mocniny modulo n chovají. Začněme pozorováním pro prvočíslo. Zvolme 7, protože je relativně malým prvočíslem, ale poskytne nám pro zkoumání větší vzorek, než 3 a 5. Pozorujme a^k pro a i k od 0 do 6. Exponenty sice mohou nabývat i větších hodnot a jejich cykly nejsou tak jasné, ale přeci jen, pro 6 různých umocnění vyjde maximálně 6 různých výsledků, což je počet všech zbytků po dělení 7:

a \ k	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0		0	0	0	0	0	0
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

Tab. 2: Mocniny modulo 7.

Nejdříve se vypořádejme s očekávatelnými závěry. 0^0 je nedefinované. Ve zbylých buňkách prvního řádku se nacházejí samé nuly, 0 je tedy agresivním prvkem zleva. Podobná situace nastává v prvním sloupci, kde máme samé jedničky a 0 je „agresivním prvkem“ i zprava (v uvozovkách, protože ze všech čísel nedělá nuly, tedy samu sebe, ale jedničky). Podobně nepřekvapivý je druhý řádek a sloupec. Z druhého řádku vidíme, že 1 je také agresivním prvkem zleva a z druhého sloupce vyplývá, že je neutrálním prvkem zprava. Zajímavá situace je v posledním sloupci, kde se kromě buňky s nulou nachází jen jedničky. Platí tedy:

$$\forall a \in \mathbb{Z}, a \not\equiv 0: a^6 \equiv 1 \pmod 7$$

Ovšem všimněme si, že některá čísla jsou kongruentní 1 už při své nižší mocnině, nejextrémnějším případem je 6. Vzhledem k tomu, že $6 \equiv -1$, je 6 kongruentní 1 dokonce pro každou svou sudou mocninu. Ostatní čísla, která dosáhnou 1 dříve jí dosáhnou po umocnění na třetí. To vyplývá z Eulerova kritéria a tato čísla jsou kvadratickými zbytky. Opravdu všechna čísla ale dosáhnou 1 až při umocnění na šestou. Zopakujme pozorování modulo jiné prvočíslo, nejbližší větší je 11.V pozorování teď vynechme 0, ale ponechme 1:

a \ k	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9	1	5	3	4	9	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
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1

Tab. 3: Mocniny modulo 11.

V posledním sloupci opět máme samé jedničky, a zdá se, že platí:

$$\forall p \text{ prvočísla a } a \not\equiv 0 \pmod{p}: a^{p-1} \equiv 1 \pmod{p}$$

Pozorujme, zda podobný vztah platí i pro mocninu prvočísla, či složené číslo. Sestavme si tedy obdobnou tabulku modulo 9:

a \ k	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	1	1	1	1	1	1	1	1
2	2	4	8	7	5	1	2	4
3	3	0	0	0	0	0	0	0
4	4	7	1	4	7	1	4	7
5	5	7	8	4	2	1	5	7
6	6	0	0	0	0	0	0	0
7	7	4	1	7	4	1	7	4
8	8	1	8	1	8	1	8	1

Tab. 4: Mocniny modulo 9.

A modulo 10:

a \ k	1	2	3	4	5	6	7	8	9
1	1	1	1	1	1	1	1	1	1
2	2	4	8	6	2	4	8	6	2
3	3	9	7	1	3	9	7	1	3
4	4	6	4	6	4	6	4	6	4
5	5	5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6	6	6
7	7	9	3	1	7	9	3	1	7
8	8	4	2	6	8	4	2	6	8
9	9	1	9	1	9	1	9	1	9

Tab. 5: Mocniny modulo 10.

Ani v jednom případě nemáme v posledním sloupci samé jedničky. Zároveň můžeme pozorovat, že pro čísla soudělná s modulem nevyjde při mocnění 1 nikdy. Tak tomu bylo ostatně i modulo prvočíslo, protože $a \equiv 0 \pmod{p} \Leftrightarrow D(a,p) \neq 1$, zde je soudělných čísel více. Pokud ignorujeme soudělná čísla, pak ale také nalezneme sloupce, ve kterých jsou samé jedničky. Modulo 9 je to po umocnění na šestou, modulo 10 po umocnění na čtvrtou. Zřejmě tedy existuje i jakýsi vztah pro složená čísla, jen je jiný než pro prvočísla. Nejdříve se tedy opět věnujme nejdříve prvočíselným modulům a následně těm neprvočíselným.

2.1 Malá Fermatova věta

Z pozorovaného vztahu v tab. 1 a tab. 2 plyne jedna z nejdůležitějších vět teorie čísel.

Věta 2 (Malá Fermatova věta; *Fermat's little theorem*)

Nechť p je prvočíslo. Pak pro všechna celá čísla a, která jsou nesoudělná s p platí:

$$a^{p-1} \equiv 1 \pmod{p}$$

(Gauss, 1986, s. 31).

Formálněji:

$$\forall p \text{ prvočísla } \forall a \in \mathbb{Z}, D(a,p) = 1 \colon a^{p-1} \equiv 1 \pmod{p}$$

Přenásobením kongruence a lze vynechat podmínku nesoudělnosti:

$$\forall p \text{ prvočísla } \forall a \in \mathbb{Z} \colon a^{p} \equiv a \pmod{p}$$

Uveďme dva důkazy. První názornější, druhý spíše technický. Před druhým důkazem nejprve dokážeme lemma, kterého se v něm využívá.

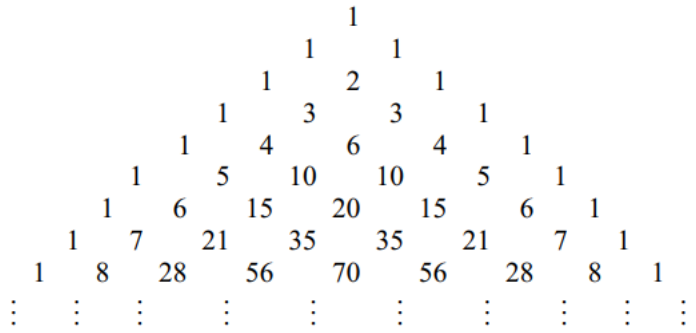
Důkaz 1 (kombinatorický): Mějme p korálků v a různých barvách. Počet všech takových řad, kde se barvy korálků mohou opakovat je a^p. Pokud vyloučíme všechny jednobarevné řády, máme $a^p - a$ různých řad. Nyní chceme ze všech zbylých řad korálků vytvořit náramky, tedy je spojit. Tím se z některých řad stanou stejné náramky. Jako stejné náramky můžeme chápat takové náramky, které můžeme jeden z druhého dostat otočením náramku o několik pozic. Pozic máme p, tedy z p řad se stane jeden náramek. Počet unikátních náramků (který je samozřejmě přirozeným číslem) se tedy rovná $\frac{a^p - a}{p}$. Takže $p|(a^p - a)$, v jazyce modulární aritmetiky $a^p - a \equiv 0 \pmod{p}$ a tedy $a^p \equiv a$ (Golomb, 1956).

Pozn.: Tento důkaz platí pouze pro prvočísla, protože pro složená čísla n neplatí, že každou skupinu stejných náramků tvoří n náramků. U složených n totiž některé stejné náramky tvoří řady stejných skupinek korálků (po dvou, po třech apod.), namísto řad jednotlivých korálků.

Lemma 2 (Školákův sen; Freshman's dream): $(a+1)^p \equiv a^p + 1$. Rozložme levou stranu podle binomické věty $(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1$. Pozorujme $\forall k \in \mathbb{N}, 0 < k < p \colon \binom{p}{k} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-k+1)}{k \cdot (k-1) \cdot \ldots \cdot 1}$. Protože je p prvočíslem, tak se pro

každé menší k v každém takovém binomickém koeficientu p s ničím nezkrátí, takže každý takový koeficient je násobkem p, v jazyce modulární aritmetiky $\binom{p}{k} \equiv 0 \pmod{p}$.

Pozn.: Toto lemma platí speciálně pro prvočísla. Neplatnost pro složená čísla nastiňme nahlédnutím do Pascalova trojúhelníku:



Obr. 5: Pascalův trojúhelník (Křížek, 2018, s. 107)

Lze vidět, že pro neprvočíselné řádky nejsou všechny koeficienty dělitelné pořadím řádku.

Důkaz 2 (matematickou indukcí): Indukci provedeme podle a. Pro $a = 0$ máme $0^p \equiv \equiv 0 \pmod{p}$ a tvrzení platí. Nyní dokažme $a^p \equiv a \Rightarrow (a+1)^p \equiv a+1$. Z lemmatu 2 vyplývá $(a+1)^p \equiv a^p + 1$, což je podle indukčního předpokladu kongruentní $a+1$.

Existuje mnoho dalších důkazů této věty. Tuto větu poprvé formuloval Fermat, nicméně ji nikdy nedokázal, i když tvrdil, že důkaz zná. První důkaz byl publikován Eulerem (Gauss, 1986, s. 32). Dále budeme na malou Fermatovu větu odkazovat zkratkou MFV.

Pozn.: Přívlastek „malá“ tuto větu odlišuje od slavné velké Fermatovy věty (*Fermat's last theorem)*. Navzdory složitosti důkazu je znění věty dosti srozumitelné. Říká, že rovnice $x^n + y^n = y^n$ nemá žádné celočíselné řešení pro $n \in \mathbb{N}, n \geq 3$. Pro $n = 2$ celočíselných řešení existuje samozřejmě nekonečně mnoho, jsou jimi pythagorejské trojice. Fermat tvrdil, že důkaz znal, ale nikdy jej nesepsal. Větu za použití poznatků matematiky, které přišly dávno po Fermatovi, dokázal až roku 1994 britský matematik Andrew Wiles (*1953) (Křížek, 2018, s. 65).

2.1.1 Některá využití MFV

Důkaz Eulerova kritéria

Nejdříve se vraťme k Eulerovu kritériu. To se ze znalosti MFV dá přirozeně odvodit. Platí $a^{p-1} \equiv 1 \pmod{p}$ a tedy musí platit $a^{\frac{p-1}{2}} \equiv 1 \vee a^{\frac{p-1}{2}} \equiv -1$, protože $\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1}$. Toto jsme ostatně vypozorovali i z tab. 1 na začátku kapitoly. Zároveň se pomocí MFV dá kritérium i dokázat.

Důkaz (Eulerovo kritérium): Z MFV: $a^{p-1} \equiv 1 \pmod{p}$, takže $a^{p-1} - 1 \equiv 0$. Rozložme na součin:

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0$$

Protože se nacházíme v oboru integrity, musí jeden ze součinitelů být nulový. Předpokládejme, že a je KZ, tedy $a \equiv x^2$:

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1}$$

A opět dle MFV $x^{p-1} \equiv 1 \equiv a^{\frac{p-1}{2}}$ a pro KZ je první součinitel nulový. Pro KN musí být nulový druhý součinitel, pro ně tedy musí platit $a^{\frac{p-1}{2}} \equiv -1$.

Zbytek po dělení

MFV lze efektivně využít při hledání zbytku po dělení prvočíslem.

Příklad 25: Zjistěte zbytek po dělení čísla *googol* (10^{100}) číslem 47.

Řešení: Platí $\forall a \in \mathbb{Z}$: $a^{46} \equiv 1 \pmod{47}$:

$$10^{100} = 10^{2\cdot 46+8} = 10^{2\cdot 46} \cdot 10^8 = (10^{46})^2 \cdot (10^2)^4 \equiv 1^2 \cdot 6^4 = (6^2)^2 \equiv (-11)^2 =$$

$$= 121 \equiv 27$$

Inverzní prvek

MFV lze využít i pro nalezení inverzního prvku (navzdory tomu, že v drtivé většině případů bude jednodušší využít např. rozšířený Eukleidův algoritmus). To lze odvodit následovně:

$$a^{p-1} \equiv 1 \pmod{p} \;/\cdot a^{-1}$$
$$a^{p-2} \equiv a^{-1}$$

Příklad 26: Nalezněte inverzní prvek k 5 modulo 17.

Řešení: Ze vztahu výše $5^{15} \equiv 5^{-1} \pmod{17}$:

$$5^{15} = (5^3)^5 = 125^5 \equiv 6^5 = 6^2 \cdot 6^2 \cdot 6 = 36 \cdot 36 \cdot 6 \equiv 2 \cdot 2 \cdot 6 = 24 \equiv 7$$

Pozn.: Lze vyřešit jednoduše úvahou: $2 \cdot 17 = 34$ a $5 \cdot 7 = 35 \equiv 1$.

Exponenciální kongruence

Při řešení exponenciálních kongruencí lze MFV využít pro určení periody řešení. Nicméně jak lze z pozorování a příkladů na začátku tohoto oddílu nahlédnout, tato perioda není pro každé číslo nutně ta nejmenší, a tudíž využitím pouze této věty nemusíme pokrýt celou množinu řešení. S čím nám MFV ovšem nepomůže je nalezení samotného jednoho konkrétního řešení dané kongruence.

2.1.2 Fermatův test prvočíselnosti (*Fermat primality test*)

Pro osvětlení principu tohoto testu si nejprve formulujme MFV pomocí implikace:

$$p \text{ je prvočíslo} \Rightarrow \forall a \in \mathbb{Z}\colon a^p \equiv a \pmod{p}$$

Tento test pak vychází z obměněné implikace tohoto tvrzení:

$$\exists a \in \mathbb{Z}\colon a^n \not\equiv a \pmod{n} \Rightarrow n \text{ je složené číslo.}$$

Pozn. 1: Obměněná implikace $A \Rightarrow B$ má podobu $\neg B \Rightarrow \neg A$.

Pozn. 2: Změna zápisu z p v původním znění věty na n reflektuje, že n má být složené.

Je třeba zdůraznit, že tato obměněná implikace říká, že pokud nalezneme číslo a, které nesplňuje vztah uvedený ve znění MFV, pak je dané n složeným číslem, nikoliv že daný vztah pro složená n nesplňuje žádné a. Výrok, který by toto tvrdil by měl podobu:

$$n \text{ je složené číslo} \Rightarrow \forall a \in \mathbb{Z}\colon a^n \not\equiv a \pmod{n}$$

Který neplatí. Demonstrujme na jednoduchých příkladech.

$$2^6 = 64 \equiv 4 \pmod{6}$$
$$3^6 = 729 \equiv 3 \pmod{6}$$

Není třeba zdůrazňovat, že 6 je složeným číslem. Je tedy patrné, že tento test jednoznačně rozhoduje o složenosti čísla, namísto prvočíselnosti. Číslo 2 potvrdilo složenost čísla 6 a je

tvz. *Fermatovým svědkem* složenosti 6, zatímco číslo 3 by při nesprávném porozumění fungování testu potvrdilo prvočíselnost čísla 6. Ve skutečnosti nám výsledek testu při použití 3 nic neřekl. 3 je tedy *Fermatovým lhářem* a 6 je *pseudoprvočíslem* vzhledem k 3. Přesnější pojmenování testu by bylo spíše „Fermatův test složenosti." Pro každé n můžeme všechna čísla rozdělit na svědky a lháře.

Definice 9 (Fermatovi svědci a lháři, pseudoprvočíslo; *Fermat witnesses and liars, pseudoprime*)
Nechť $a \in \mathbb{Z}$ a $n \in \mathbb{N}$ je složené číslo.

Taková a, pro která platí $a^n \not\equiv a \pmod{n}$, se nazývají *Fermatovi svědci složenosti* n.

Taková a, pro která platí $a^n \equiv a \pmod{n}$, se nazývají *Fermatovi lháři*. n se nazývá *pseudoprvočíslo* vzhledem k a.

Příklad 27: Určete všechny Fermatovy svědky a lháře pro 15.

Řešení: Umocněme všechna čísla modulo 15 na čtrnáctou:

$$1^{14} = 1$$
$$2^{14} = (2^4)^3 \cdot 2^2 \equiv (-1)^3 \cdot 4 = -4 \equiv 11$$
$$3^{14} = (3^2)^7 = 9^7 = (9^2)^3 \cdot 9 \equiv 6^3 \cdot 9 = 6^2 \cdot 6 \cdot 9 \equiv 6 \cdot 6 \cdot 9 \equiv 6 \cdot 9 \equiv 9$$
$$4^{14} = (2^2)^{14} = (2^{14})^2 \equiv 11^2 \equiv 1$$
$$5^{14} \equiv (5^2)^7 \equiv (-5)^7 \equiv -5 \equiv 10$$
$$6^{14} = 2^{14} \cdot 3^{14} \equiv 11 \cdot 9 \equiv 9$$
$$7^{14} = (7^2)^7 \equiv 4^7 = (2^2)^7 = 2^{14} \equiv 11$$
$$8^{14} = (2^3)^{14} = (2^{14})^3 \equiv 11^3 \equiv 11$$
$$9^{14} = (3^{14})^2 \equiv 9^2 \equiv 6$$
$$10^{14} = 2^{14} \cdot 5^{14} \equiv 11 \cdot 10 \equiv 5$$
$$11^{14} = (11^2)^7 \equiv 1^7 = 1$$
$$12^{14} = 3^{14} \cdot 4^{14} \equiv 9 \cdot 1 = 9$$
$$13^{14} \equiv (-2)^{14} = 2^{14} \equiv 11$$
$$14^{14} \equiv (-1)^{14} = 1$$

Svědci jsou: $2, 3, 5, 6, 7, 8, 9, 10, 12$ a 13. Lháři jsou: $1, 4, 11$ a 14.

Pozn.: Jak si lze v tomto příkladu všimnout, 1 je Fermatovým lhářem pro všechna n, proto nemá smysl ho pro test využívat.

Příklad 28: Zjistěte, zda je 4 294 967 297 prvočíslem nebo složeným číslem.

Řešení: Využijme Fermatova testu. Pro velká čísla lze využít pomoc kalkulačky:

$$2^{4\,294\,967\,296} \equiv 1, \text{ nelze rozhodnout.}$$

$$3^{4\,294\,967\,297} \equiv 3\,029\,026\,160, \text{ je složený číslem.}$$

A tedy 2 je Fermatovým lhářem a 3 Fermatovým svědkem.

Carmichaelova čísla

Existence Fermatových lhářů navádí na otázku, jestli existuje složené n takové, že všechna celá čísla jsou pro něj Fermatovými lháři. Pokud ano, pak je tento test poměrně nespolehlivý. Jejich existenci nepopírá MFV v podobě implikace. Zakazovala by ji pouze, kdyby byla v podobě ekvivalence, tedy by platila i obrácená implikace:

$$\forall a \in \mathbb{Z}\colon a^n \equiv a \pmod{n} \Rightarrow n \text{ je prvočíslo}$$

Obměněnou implikací:

$$n \text{ je složené číslo} \Rightarrow \exists a \in \mathbb{Z}\colon a^n \not\equiv a \pmod{n}$$

Ta ovšem neplatí a taková čísla opravdu existují.

Definice 10 (Carmichaelovo číslo; *Carmichael number*)

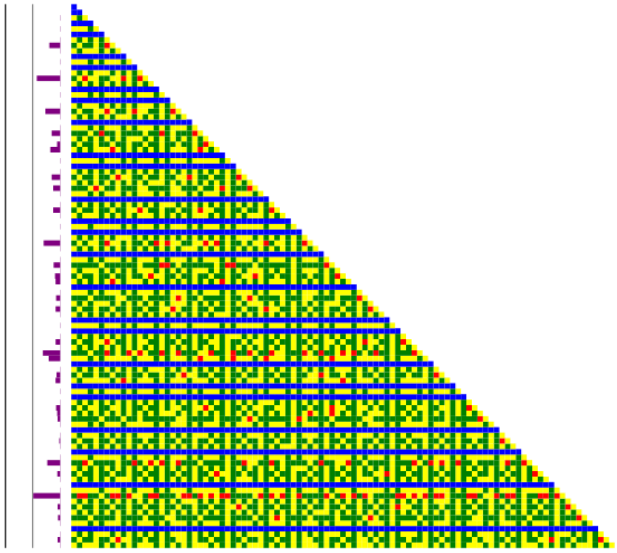
Nechť $a \in \mathbb{Z}$ a $n \in \mathbb{N}$ je složené číslo. Pokud pro všechna a platí:

$$a^n \equiv a \pmod{n}$$

pak se n se nazývá *Carmichaelovo číslo* (Křížek, 2018, s. 218).

Je dokázáno, že takových čísel existuje nekonečně mnoho, což činí Fermatův test prvočíselnosti nespolehlivým (Alford, 1994). Prvních 7 Carmichaelových čísel objevil již roku 1885 český matematik Václav Šimerka (1819-1887), jeho práce se ovšem nedočkala velké pozornosti (Lemmermeyer, 2013). Proto jsou čísla pojmenována po americkém matematikovi Robertu Carmichaelovi (1879-1967), který nezávisle na Šimerkovi v roce 1910 objevil nejmenší takové číslo, kterým je $561 = 3 \cdot 11 \cdot 17$.

Na závěr tohoto oddílu si ukažme schéma Fermatových svědků a lhářů pro prvních 100 přirozených n:



Obr. 6: Fermatovi svědci a lháři pro prvních 100 přirozených čísel (z https://mathlesstraveled.com/2019/01/18/fermat-witnesses-and-liars-some-words-on-pww-24/)

Modrá znázorňuje, že n je prvočíslo, žlutá soudělná čísla s n, zelená svědky a červená lháře. Fialové sloupečky po stranách značí, jaký je poměr lhářů a svědků pro dané n.

2.2 Eulerova funkce a Eulerova věta

Vraťme se k tab. 3 a tab. 4. Zaměřme se na nesoudělná čísla s modulem. Můžeme pozorovat, že všechna taková také sdílí sloupec, v němž jsou samé jedničky, jen jím není sloupec poslední. Modulo 9 je to pro šestou mocninu, modulo 10 pro čtvrtou. Proč zrovna tyto mocniny? Souvisí to nějak s MFV? Pokud se vrátíme ještě dále, k tab. 1 a tab. 2, pak je vlastně pořadí sloupce, kde se nachází samé jedničky pro nesoudělná a shodné s počtem těchto jedniček. Tuto vlastnost sdílí i tab. 3 a tab. 4. Jinými slovy, pokud $a \in \mathbb{Z}$ a k označuje počet všech přirozených čísel menších než $n \in \mathbb{N}$, nesoudělných s n, pak $a^k \equiv 1 \pmod{n}$. Tento vztah poprvé popsal Euler a také se po něm dnes jmenuje (Křížek, 2018, s. 70). Nejprve si formalizujme a zodpovězme otázku, jak taková k jednoduše najít.

Definice 11 (Eulerova funkce; *Euler's totient function*)

Nechť $a, n \in \mathbb{N}$. Eulerova funkce $\varphi(n)$: $\mathbb{N} \to \mathbb{N}$ označuje počet všech přirozených čísel a, která jsou menší než n a nesoudělná s n.

Formálněji:

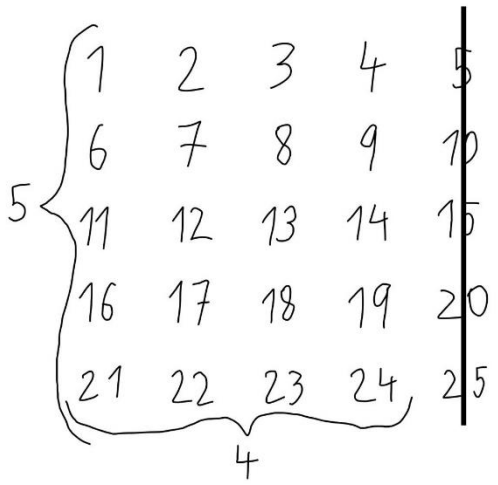
$$\varphi(n) = |\{\forall a \in \mathbb{N}: 0 \leq a \leq n \text{ a } D(a,n) = 1\}|$$

(Křížek, 2018, s. 70).

Pozn. 1: Z definice prvočísla p je $\varphi(p) = p - 1$.

Pozn. 2: Ve druhé formulaci nezávisí na ostrosti nerovností, protože 0 a n jsou s n soudělná vždy pro všechna n.

Z pozorování tab. 3 je patrné, že $\varphi(9) = \varphi(3^2) = 6$. Zkusme funkci intuitivně vyčíslit pro jinou mocninu prvočísla a zobecnit pro všechny mocniny prvočísel. Zkusme určit $\varphi(5^2) = = \varphi(25)$. Vypišme si čísla od 1 od 25 a vyškrtejme všechna soudělná s 25.



Obr. 7: $\varphi(25)$.

Tímto způsobem můžeme hodnotu Eulerovy funkce určit jako $\varphi(25) = \varphi(5^2) = 5 \cdot 4$. Takovéto schéma se dá podobným způsobem sepsat pro libovolné p^k. Mělo by p^{k-1} řádků a p sloupců, takže by bylo vypsáno skutečně všech p^k čísel. Poslední sloupec by obsahoval všechny násobky p, byl by tedy škrtnutý a tabulka, kde zbyla všechna ostatní nesoudělná čísla s p by měla $p - 1$ sloupců. Z toho vyplývá:

$$\varphi(p^k) = p^{k-1} \cdot (p - 1)$$

Hodnotu $\varphi(25)$ lze intuitivně vyčíslit i jinou úvahou. Z celkového počtu přirozených čísel od 1 do 25 potřebujeme odečíst všechna soudělná s 25. To jsou všechny násobky 5, tedy každé páté číslo, ještě jinak jednu pětinu všech čísel. Takže:

$$\varphi(25) = 25 - \frac{1}{5}25 = 25 - 5 = 20$$

Obecně:

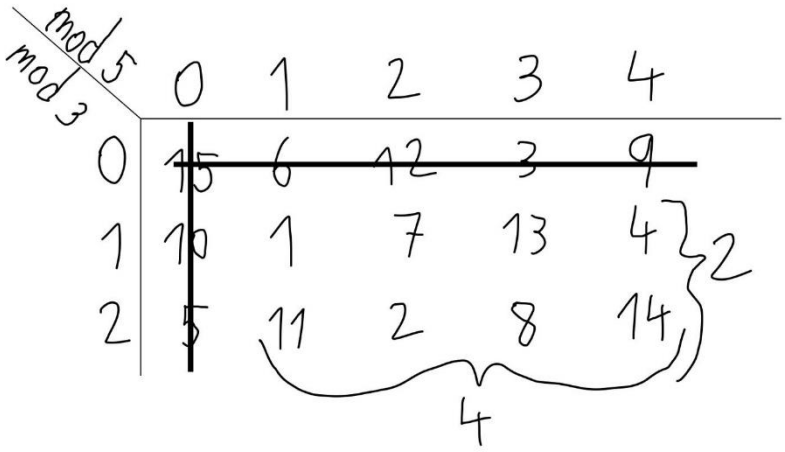
$$\varphi(p^k) = p^k - \frac{1}{p} \cdot p^k$$

Výraz upravme:

$$p^k - \frac{1}{p}p^k = p^k - p^{k-1} = p^k \cdot (p - 1)$$

Vidíme, že obě úvahy vedou v konkrétním příkladu i obecně ke stejnému závěru.

Zbývá hodnota funkce pro složená čísla. Přirozené číslo je se složeným číslem n nesoudělné právě tehdy, když je nesoudělné se všemi prvočísly, ze kterých je n složeno. Z tab. 4 plyne $\varphi(10) = \varphi(2 \cdot 5) = 4$. Vytvořme si schéma opět pro jiné n, např. $n = 15 = 3 \cdot 5$ s ohledem na soudělnost s prvočíselným rozkladem.



Obr. 8: $\varphi(15)$.

Schéma má po vyškrtnutí 2 řádky a 4 sloupce, takže $\varphi(15) = 2 \cdot 4 = 8$. Podobně lze tabulku sestavit pro jakékoli jiné číslo složené ze dvou nesoudělných čísel. Všimněme si, že $\varphi(3) = 2$ a $\varphi(5) = 4$, takže $\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5)$. Předpokladem tedy je:

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n), m, n \in \mathbb{N}$$

Pokusme se na hodnotu $\varphi(15)$ přijít stejnou alternativní úvahou. Z celkového počtu musíme odečíst každé třetí a zároveň každé páté číslo. Tedy jak třetinu, tak pětinu. V této úvaze si ovšem musíme dát pozor, abychom některá čísla neodečetli dvakrát. Proto odečtěme nejdříve třetinu a až z tohoto počtu pětinu. Nejdříve spočtěme $15 - \frac{1}{3} \cdot 15 = 15 - 5 = 10$. A tedy $\varphi(15) = 10 - \frac{1}{5} \cdot 10 = 10 - 2 = 8$. Opět jsme došli ke stejnému výsledku. Zobecněním tohoto postupu ovšem dojdeme k jinému závěru než zobecněním předchozího. Pro n složené z mocnin prvočísel $p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ musíme od n nejdříve odečíst každé p_1-té číslo, tedy $\frac{1}{p_1} n$. Každé p_i-té číslo odečítáme až z této části. Menší výzvu činí takový vztah správně a přehledně zapsat, lze to provést takto:

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_m}\right)$$

Tento vztah byl známý již Eulerovy (Gauss, 1986, s. 21). Zmiňme, že nezávisí na tom, jakých mocnin jsou prvočísla v rozkladu n. Všech čísel soudělných s danou mocninou prvočísla se zbavíme tak, že se zbavíme všech násobků tohoto prvočísla. Také tento vzorec funguje i pro prvočísla a jejich mocniny, takže je univerzální. Všechna pozorování shrňme.

Tvrzení 15 (Výpočet hodnoty Eulerovy funkce)
Nechť p je prvočíslo a $k, m, n, \in \mathbb{N}$. Pak:

(1) $\varphi(p) = p - 1$
(2) $\varphi(p^k) = p^{k-1} \cdot (p - 1) = p^k - p^{k-1}$
(3) pro $D(m, n) = 1$: $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

Univerzálně pro $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$:

(4) $\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_m}\right)$

(Křížek, 2018, s. 70-71).

Důkaz: (1) je patrné z definice prvočísla a (2) z pozorování výše.

(3) Dokážeme pomocí ČVZ. Nejdříve zopakujme, že $\forall l \in \mathbb{N}: \mathrm{D}(l, mn) = 1 \Leftrightarrow (\mathrm{D}(l, m) = = 1 \wedge \mathrm{D}(l, n) = 1)$. Každé takové $l \pmod{mn}$ je kongruentní nějakému číslu $\bmod m$ a nějakému číslu $\bmod n$. Pro všechna l, existuje modulo m $\varphi(m)$ možných kongruencí, modulo n obdobně $\varphi(n)$. Podle ČVZ existuje pro každý pár takových kongruencí jednoznačné řešení $\bmod mn$. Počet všech možných párů je $\varphi(m) \cdot \varphi(n)$. (Gauss, 1986, s. 20-21)

(4) Z (2) a (3) plyne:

$$\varphi(n) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdot \ldots \cdot \varphi(p_m^{k_m})$$
$$\varphi(n) = p_1^{k_1 - 1} \cdot (p_1 - 1) \cdot p_2^{k_2 - 1}(p_2 - 1) \cdot \ldots \cdot p_m^{k_m - 1} \cdot (p_m - 1)$$
$$\varphi(n) = p_1^{k_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdot p_2^{k_2} \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot p_m^{k_m} \cdot \left(1 - \frac{1}{p_m}\right)$$

$$\varphi(n) = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_m}\right)$$

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_m}\right)$$

Pozn. 1: Často se definuje ještě $\varphi(1) = 1$.

Pozn. 2: (1) je speciálním případem (2), ale pro přehlednost jsme (1) formulovali zvlášť. Je zřejmé, že pokud známe prvočíselný rozklad n, dokážeme určit $\varphi(n)$ pro všechna n.

Příklad 29: Určete počet všech přirozených čísel menších než 56, nesoudělných s 56.

Řešení:

$$\varphi(56) = \varphi(7 \cdot 8) = \varphi(7) \cdot \varphi(8) = \varphi(7) \cdot \varphi(2^3) = 6 \cdot 2^{3-1} \cdot (2-1) = 6 \cdot 2^2 \cdot 1 = 24$$

Alternativně:

$$\varphi(56) = \varphi(7) \cdot \varphi(8) = \varphi(7) \cdot \varphi(2^3) = 56 \cdot \left(1 - \frac{1}{7}\right) \cdot \left(1 - \frac{1}{2}\right) = 56 \cdot \frac{6}{7} \cdot \frac{1}{2} = 4 \cdot 6 = 24$$

Příklad 30: Zkoumejte vlastnosti Eulerovy funkce:

a) Je prostá (injektivní)?
b) Je na (surjektivní)?
c) Je bijektivní?
d) Je rostoucí či klesající?

Řešení: a) Funkce prostá není, protipříkladem může být $\varphi(3) = \varphi(4) = 2$.

b) Pro zodpovězení této otázky musíme zodpovědět, zda existují hodnoty, kterých funkce nemůže nabývat. Při výpočtu hodnoty $\varphi(n)$ vycházíme z prvočíselného rozkladu n. Hodnota pro mocninu prvočísla (včetně první) obsahuje součinitel $p - 1$, který je pro lichá prvočísla sudý. Pro $p = 2^k$ je sudost zaručena součinitelem 2^{k-1}. Jedinými speciálními případy jsou $\varphi(2) = \varphi(1) = 1$. Až na ty nemůže $\varphi(n)$ nabývat lichých hodnot pro žádná n.

Jsou i sudé hodnoty, kterých funkce nemůže nabývat, nejmenší je 14. $14 + 1 = 15$ není prvočíslem, tudíž záleží na rozkladu. $14 = 2 \cdot 7$, 2 je hodnotou $\varphi(4)$ nebo $\varphi(3)$, ale 7 je lichým číslem, takže není možnou hodnotou. Obdobnou úvahou ani $21 = 3 \cdot 7$ není možnou hodnotou, protože ani jeden ze součinitelů není možnou hodnotou a $21 + 1 = 22$ není

prvočíslem. Ovšem $28 = 4 \cdot 7$ také není součinem dvou hodnot Eulerovy funkce, ale $28 + +1 = 29$ je prvočíslo, takže 28 je hodnotou funkce, konkrétně $\varphi(29) = 28$. Analogicky $35 = 5 \cdot 7$ není hodnotou, ale $42 = 6 \cdot 7$ ano, protože 7 je mocnina prvočísla a 6 je o 1 menší než to samé prvočíslo, konkrétně $\varphi(49) = \varphi(7^2) = 7 \cdot 6$. Obecně $m \in \mathbb{N}$ je možnou hodnotou $\varphi(n)$ právě tehdy, když je sudé a buď $m + 1$ je prvočíslo, m lze vyjádřit jakou součin dvou hodnot Eulerovy funkce, nebo lze m vyjádřit jakou součin mocniny prvočísla p a $p - 1$.

c) Funkce není ani prostá, ani na, takže není bijektivní.

d) Není ani rostoucí, ani klesající. Protipříklad:

$$\varphi(4) = 2 \qquad \varphi(5) = 4 \qquad \varphi(6) = \varphi(2) \cdot \varphi(3) = 2$$

Nyní když máme definované postupy pro vypočtení hodnoty $\varphi(n)$ pro libovolné n, vraťme se k původnímu pozorování a souvislosti Eulerovy funkce s umocňováním.

Věta 3 (Eulerova věta; *Euler's theorem*)
Nechť $a \in \mathbb{Z}$, $n \in \mathbb{N}$ a $D(a, n) = 1$. Pak $a^{\varphi(n)} \equiv 1 \pmod{n}$. (Křížek, 2018, s. 70).

Důkaz: Mějme množinu všech přirozených čísel menších než n nesoudělných s n. Počet prvků takové množiny je $\varphi(n)$, označme $\{b_1, b_2, \ldots, b_{\varphi(n)}\}$. Každý prvek této množiny je modulo n kongruentní různému prvku množiny $\{ab_1, ab_2, \ldots, ab_{\varphi(n)}\}$ (jinými slovy mezi těmito množinami existuje bijekce, ekvivalentně je druhá množina permutací první). Z toho vyplývá:

$$b_1 \cdot b_2 \cdot \ldots \cdot b_{\varphi(n)} \equiv ab_1 \cdot ab_2 \cdot \ldots \cdot ab_{\varphi(n)}$$

$$b_1 \cdot b_2 \cdot \ldots \cdot b_{\varphi(n)} \equiv a^{\varphi(n)}\left(b_1 \cdot b_2 \cdot \ldots \cdot b_{\varphi(n)}\right) /: (b_1 \cdot b_2 \cdot \ldots \cdot b_{\varphi(n)})$$

$$a^{\varphi(n)} \equiv 1$$

(Gauss, 1986, s. 22).

Pozn. 1: To, že jsou si obě množiny v důkazu nekongruentní dokažme následovně: součinem dvou nesoudělných čísel s modulem bude znovu nesoudělné číslo s modulem. V druhé

množině si nejsou žádné dva prvky kongruentní, protože $ax \equiv ay \pmod{n} \Leftrightarrow x \equiv$ $\equiv y \pmod{n}$ a v první množině předpokládáme všechny prvky nekongruentní.
Pozn. 2: Jelikož $\varphi(p) = p - 1$, je EV zobecněním MFV na všechna přirozená čísla, respektive je MFV speciálním případem EV.

Dále budeme Eulerovu větu značit zkratkou EV.

2.2.1 Využití EV

EV se dá pro nesoudělná a a n využít obdobně jako MFV pro zjištění zbytku a po dělení n a inverzního prvku $a^{-1} \pmod{n}$. Důsledkem je, že EV lze využít pro zjištění libovolného počtu posledních číslic jakéhokoli čísla.

Příklad 31: Určete poslední dvojčíslí čísla $219^{83^{37}}$.

Řešení: Hledáme zbytek po dělení 100, takže počítáme modulo 100:

$$\varphi(100) = \varphi(4 \cdot 25) = \varphi(4) \cdot \varphi(25) = \varphi(2^2) \cdot \varphi(5^2) = 2^1 \cdot 1 \cdot 5^1 \cdot 4 = 40$$

Takže:

$$219^{83^{37}} \equiv 19^{83^{37} \bmod 40} = 19^{3^{37} \bmod 40} \pmod{100}$$

Kde mod 40 chápeme jako operaci. Spočítejme $\varphi(40)$:

$$\varphi(40) = \varphi(8 \cdot 5) = \varphi(2^3) \cdot \varphi(5) = 2^2 \cdot 4 = 16$$

A tedy:

$$19^{3^{37} \bmod 40} = 19^{(3^{16})^2 \cdot 3^5 \bmod 40} = 19^{3^5} = 19^{3^4 \cdot 3} = 19^{81 \cdot 3} \equiv 19^{1 \cdot 3} \equiv 59 \pmod{100}$$

Poslední dvojčíslí je 59.

Pozn.: Úlohy tohoto typu lze řešit i pomocí ČVZ, i když by to v tomto konkrétním případě bylo pracnější. Tento postup např. v (Kaňáková, 2022, s. 39).

Zbytek po dělení (soudělná a s n)

EV lze ovšem využít i pro zjištění zbytku po dělení pro soudělná a a n. Využívá se faktu, že $x \equiv y \pmod{n} \Leftrightarrow kx \equiv ky \pmod{kn}$

Příklad 32: Zjistěte poslední dvojčíslí čísla $735^{30^{86}}$.

Řešení: Opět počítáme modulo 100. Hledaný zbytek označme a:

$$a \equiv 35^{30^{86}} \pmod{100} \;/:5$$
$$\frac{a}{5} \equiv \frac{35}{5} \cdot 35^{30^{86}-1} \pmod{20}$$
$$\frac{a}{5} \equiv 7 \cdot 15^{30^{86}-1}$$

$\varphi(20) = \varphi(4) \cdot \varphi(5) = 2 \cdot 4 = 8$. Takže:

$$15^{30^{86}-1} \equiv 15^{30^{86}-1 \bmod 8} = 15^{(-2)^{86}-1 \bmod 8}$$

$\varphi(8) = 2^2 = 4$, tedy:

$$15^{(-2)^{86}-1 \bmod 8} = 15^{(-2)^2-1} = 15^{4-1} = 15^3 \equiv 15$$

A tedy:

$$\frac{a}{5} \equiv 7 \cdot 15 \pmod{20} \;/\cdot 5$$
$$a \equiv 25 \pmod{100}$$

Posledním dvojčíslím je 25.

Exponenciální kongruence

Stejně jako využitím MFV lze dle EV určit periodu řešení. Nicméně ani EV s hledáním samotného jednoho konkrétního řešení nepomůže a zároveň pro některá čísla neurčí nejmenší periodu. Navíc ji nelze využít pro řešitelné kongruence se soudělným základem, toto se ovšem dá ošetřit vydělením celé kongruence společným dělitelem a případně následným zavedením substituce.

Příklad 33: Vyřešte kongruenci $2^x \equiv 6 \pmod{10}$.

Řešení: Vydělme 2, abychom zajistili nesoudělnost:

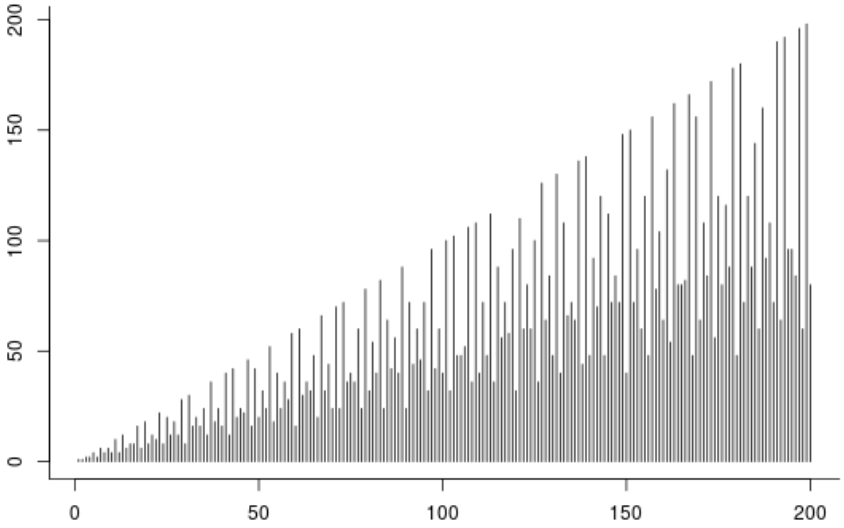
$$2^x \equiv 6 \pmod{10} \;/:2$$
$$2^{x-1} \equiv 3 \pmod{5}$$

Zaveďme substituci $y = x - 1$. Všimněme si, že $2^3 = 8 \equiv 3 \pmod 5$, takže $y \equiv 3$ a tedy $x \equiv 4$. Periodou je $\varphi(10) = \varphi(2 \cdot 5) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4$. Výsledné řešení je:

$$x = 4 + 4k, k \in \mathbb{Z}$$

Pozn.: EV má velké využití v šifrování, jednou z nejznámějších šifer využívající EV je RSA. O něm např. (Křížek, 2018, s. 308-310).

Na závěr graf hodnot $\varphi(n)$ pro prvních 200 n:



Obr. 9: Graf $\varphi(n)$ (svislá osa) pro prvních 200 n (vodorovná osa). Vygenerováno pomocí OEIS (posloupnost A000010).

Nejvyšších hodnot v grafu dosahuje funkce samozřejmě pro prvočísla. Naopak nejnižších hodnot dosahuje pro složená čísla s relativně velkým počtem prvočísel ve svém prvočíselném rozkladu.

2.3 Carmichaelova funkce a Carmichaelova věta

Již víme, že některá čísla jsou kongruentní 1 při nižší mocnině, než určuje hodnota Eulerovy funkce. Může se pro nějaký modul stát, že to bude platit pro všechna čísla? Pozorujme tabulku pro mocniny nesoudělných čísel s 24 modulo 24. $\varphi(24) = \varphi(2^3) \cdot \varphi(3) = 4 \cdot 2 = = 8$, stačí nám tedy 8 řádků i sloupců:

a \ k	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
5	5	1	5	1	5	1	5	1
7	7	1	7	1	7	1	7	1
11	11	1	11	1	11	1	11	1
13	13	1	13	1	13	1	13	1
17	17	1	17	1	17	1	17	1
19	19	1	19	1	19	1	19	1
23	23	1	23	1	23	1	23	1

Tab. 6: Mocniny modulo 24.

Již z druhého sloupce vidíme, že neplatí jen:

$$a^8 \equiv 1 \pmod{24}$$

ale dokonce:

$$a^2 \equiv 1 \pmod{24}$$

Je nějaký vztah mezi očekávanou nejmenší mocninou z využití EV a nejmenší mocninou zde pozorovanou? Na první pohled je 2 dělitelem 8, a dokonce je 2 nejmenším společným násobkem hodnot $\varphi(3)$ a $\varphi(8)$, které byly použity pro určení hodnoty $\varphi(24)$. Výsledky EV jde tedy dále zpřesnit.

Definice 12 (Carmichaelova funkce; *Carmichael function*)

Nechť $a \in \mathbb{Z}, k, n \in \mathbb{N}$ a $D(a,n) = 1$. Hodnota Carmichaelovy funkce $\lambda(n): \mathbb{N} \to \mathbb{N}$ je nejmenší k takové, že $a^k \equiv 1 \pmod{n}$. (Carmichael, 1914, s. 54).

Funkce je pojmenována, stejně jako Carmichaelova čísla, po Robertu Carmichaelovi.

Příklad 34: Z definice určete $\lambda(24)$.

Řešení: Z tab. 5 plyne $\lambda(24) = 2$.

Je zřejmé, že pro všechna prvočísla $\lambda(p) = \varphi(p)$. Jak to bude s hodnotami pro mocniny prvočísel? Využijme vypozorovanou myšlenku nejmenšího společného násobku. Obecně $\varphi(p^k) = p^{k-1} \cdot (p-1)$. Tyto součinitele jsou pro všechna prvočísla nesoudělné, takže lze předpokládat $\varphi(p^k) = \lambda(p^k)$. Tato úvaha je sice správná, ale má výjimku. Vraťme se k pozorování kvadratických kongruencí $\bmod 2^k$. Pro $2, 4$ a 8 je jediným lichým (tedy nesoudělným s modulem) kvadratickým zbytkem 1. To znamená, že pro všechna lichá a platí:

$$a^2 \equiv 1 \pmod{2}$$

Zde ale triviálně platí i $a^1 \equiv 1 \pmod{2}$, a tedy $\varphi(2) = \lambda(2) = 1$. Dále:

$$a^2 \equiv 1 \pmod{4}$$

Takže obdobně $\varphi(4) = \lambda(4) = 2$. Ale:

$$a^2 \equiv 1 \pmod{8}$$

Takže $\lambda(8) = 2$, ale $\varphi(8) = \varphi(2^3) = 2^2 \cdot 1 = 4$. Pro mocniny dvojky se očividně hodnoty Eulerovy a Carmichaelovy funkce vždy nerovnají. Pozorujme ještě modulo 16:

$1^1 = 1$	$9^2 \equiv 1$
$3^2 = 9, 3^3 \equiv 11, 3^4 \equiv 11 \cdot 3 \equiv 1$	$11^2 \equiv 9 \Rightarrow 11^4 \equiv 1$
$5^2 = 25 \equiv 9 \Rightarrow 5^4 \equiv 1$	$13^2 \equiv 9 \Rightarrow 13^4 \equiv 1$
$7^2 \equiv 1$	$15^2 \equiv (-1)^2 = 11$

Tedy $\lambda(16) = 4$. Zdá se, že hodnota Carmichaelovy funkce pro mocniny dvojky (kromě 2 a 4) je o dvě mocniny nižší, ne pouze o jednu, jako v případě Eulerovy funkce.

Věta 4 (Carmichaelova věta; *Carmichael theorem*)

Nechť p je prvočíslo a $k, m \in \mathbb{N}$. Carmichaelova věta určuje způsoby výpočtu hodnot Carmichaelovy funkce:

(1) $\lambda(p) = \varphi(p)$

(2) pro $p \geq 3$: $\lambda(p^k) = \varphi(p^k)$

(3) pro $k \geq 3$: $\lambda(2^k) = 2^{k-2} = \frac{1}{2} \cdot \varphi(2^k)$

(4) $\lambda(2^2) = \lambda(4) = 2$

(5) pro $n = {p_1}^{k_1} \cdot {p_2}^{k_2} \cdot \ldots \cdot {p_m}^{k_m}$: $\lambda(n) = \mathrm{n}\left(\lambda({p_1}^{k_1}), \lambda({p_2}^{k_2}), \ldots, \lambda({p_m}^{k_m})\right)$, kde n značí nejmenší společný násobek

(Carmichael, 1914, s. 39).

Důkaz: (4) lze ověřit jednoduše výčtem. Ostatní tvrzení dokažme tak, že vždy nejprve dokážeme, že $a^{\lambda(n)} \equiv 1 \pmod{n}$ (1. vlastnost) a následně, že je takový exponent opravdu nejmenším (2. vlastnost).

(1) 1. vlastnost plyne z MFV. Pro důkaz 2. vlastnosti vezměme největší menší exponent, který má smysl zvažovat, $\frac{p-1}{2}$ (to, že žádný exponent mezi nimi není třeba zohledňovat plyne z Lagrangeovy věty, které se blíže věnujeme u tvrzení 18). Z Eulerova kritéria pro všechna a, která jsou kvadratickými nezbytky plyne: $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Zvažme případ, že by všechny kvadratické nezbytky dosáhli 1 při umocnění na jiný, lichý dělitel $p-1$. Z Eulerova kritéria ale plyne, že by při takovém umocnění nebyly kongruentní 1 právě kvadratické zbytky.

(2) 1. vlastnost plyne z EV. Pro důkaz 2. vlastnosti se pokusme exponent konstruovat podobně jako řešení kvadratických kongruencí modulo p^k. Z MFV platí $a^{p-1} \equiv 1 \pmod{p}$, ekvivalentně $a^{p-1} = 1 + lp, l \in \mathbb{Z}$. Umocněme obě strany na p-tou:

$$a^{p(p-1)} = 1 + \binom{p}{1} lp + \binom{p}{2} (lp)^2 + \cdots + \binom{p}{p-1} (lp)^{p-1} + (lp)^p$$

Využitím lemmatu 2:

$$a^{p(p-1)} \equiv 1 + (lp)^p \equiv 1 \pmod{p^2}$$

Dalším mocněním na p bychom mohli postupovat pro všechny moduly vyšších mocnin p. Všimněme si, že $\mathrm{mod}\, p^3$ by nezmizel druhý člen rozvoje, zde by tedy exponent $p(p-1)$ nestačil. Protože p nemá žádné dělitele, není třeba zohledňovat jiné exponenty (také plyne z Lagrangeovy věty).

(3) 1. vlastnost dokažme tak, že ukážeme, že pro 3 vždy platí $3^{2^{k-2}} \equiv 1 \pmod{2^k}$. 2. vlastnost tak, že ukážeme, že vždy platí $3^{2^{k-3}} \not\equiv 1 \pmod{2^k}$. Další exponenty netřeba zohledňovat, což opět plyne z Lagrangeovy věty. Důkaz bychom mohli provést i pro 5, a dokonce pro jakékoliv číslo $\equiv 3, 5 \pmod 8$, což lze nahlédnout z pozorování pro modulo 16. Začněme s 1. vlastností:

$$3^{2^{k-2}} \equiv 1 \pmod{2^k}$$

$$3^{2^{k-2}} - 1 \equiv 0$$

$$(3^{2^{k-3}} - 1)(3^{2^{k-3}} + 1) \equiv 0$$

$$(3^{2^0} - 1)(3^{2^0} + 1)(3^{2^1} + 1) \dots (3^{2^{k-3}} + 1) \equiv 0$$

První součinitel je roven 2, druhý je roven 4. Každý další součinitel je násobkem 2, ale ne 4, protože jsou všechny součtem mocniny 9 a 1. Počet všech součinitelů je $k-1$. $k-2$ součinitelů jsou násobkem 2, jeden je násobkem $4 = 2^2$, celá pravá strana je tedy násobkem $2^{k-2} \cdot 2^2 = 2^k$, tedy tvaru $2^k r \equiv 0 \pmod{2^k}$ a předpoklad platí. Podobným způsobem by se dokázalo i pro jiná lichá čísla. Všechna jsou kongruentní 1 nebo 3 modulo 4, takže vždy daný člen o jedna větší nebo o jedna menší bude násobkem 4. Některá lichá čísla (např. 7) by jedničky dosáhla pro nižší exponent ($7 + 1 = 8$), ale nikdy pro vyšší.

Nyní dokažme $3^{2^{k-3}} \not\equiv 1 \pmod{2^k}$ sporem, tedy předpokládejme $3^{2^{k-3}} \equiv 1$:

$$3^{2^{k-3}} - 1 \equiv 0$$

$$(3^{2^{k-4}} - 1)(3^{2^{k-4}} + 1) \equiv 0$$

$$(3^{2^0} - 1)(3^{2^0} + 1)(3^{2^1} + 1) \dots (3^{2^{k-4}} + 1) \equiv 0$$

První součinitel je násobkem 2, druhý násobkem 4 a všechny další násobkem 2, ale ne násobkem 4. Jejich počet je $k-2$ a celá pravá strana je tedy násobkem 2^{k-1} ale není

násobkem 2^k, takže tvaru $2^{k-1}r$, kde r je liché. $2^{k-1}r \not\equiv 0 \pmod{2^k}$, což je ve sporu s předpokladem.

(5) Platí $a^{\lambda\left(p_i^{k_i}\right)} \equiv 1 \left(\mathrm{mod}\, p_i^{k_i}\right)$ pro každou mocninu prvočísla, ze kterých je n složeno. Protože $\lambda(n)$ je násobkem $\lambda\left(p_i^{k_i}\right)$, platí i $a^{\lambda(n)} \equiv 1 \pmod{p_i^{k_i}}$. Z ČVZ plyne $a^{\lambda(n)} \equiv$ $\equiv 1 \pmod{{p_1}^{k_1} \cdot {p_2}^{k_2} \cdot \ldots \cdot {p_m}^{k_m} = n}$. 2. vlastnost plyne z toho, že je $\lambda(n)$ definováno jako nejmenší společný násobek.

Pozn.: Pro výpočet hodnoty Carmichaelovy funkce bohužel neexistuje explicitní vzorec jako pro výpočet hodnoty Eulerovy funkce.

Příklad 35: Určete hodnotu:

a) $\lambda(24)$
b) $\lambda(720)$
c) $\lambda(561)$

Řešení:

a) $\lambda(24) = \mathrm{n}\left(\lambda(3), \lambda(2^3)\right) = \mathrm{n}(2, 2) = 2$

   Naše dřívější pozorování bylo správné.

b) $\lambda(720) = \lambda(5 \cdot 9 \cdot 16) = \mathrm{n}\left(\lambda(5), \lambda(3^2), \lambda(2^4)\right) = \mathrm{n}(4, 6, 2^2) = 12$

   Z toho vyplývá $a^{12} \equiv 1 \pmod{720}$. Pro porovnání:

$$\varphi(720) = \varphi(5) \cdot \varphi(3^2) \cdot \varphi(2^4) = 4 \cdot 3 \cdot 2 \cdot 2^3 \cdot 1 = 192$$

c) $\lambda(561) = \mathrm{n}\left(\lambda(3), \lambda(11), \lambda(17)\right) = \mathrm{n}(2, 10, 16) = 80$

   Můžeme nahlédnout, proč je 561 Carmichaelovým číslem. Je to proto, že $\lambda(561) =$ $= 80$ dělí $561 - 1 = 560$ a při mocnění $a^{560} \pmod{561}$ vlastně mocníme 1^7 pro všechna nesoudělná a.

Carmichael přinesl výsledky, které dále zpřesňují EV. Carmichaelovu lze tedy opět využít na určení inverzního prvku a zjištění zbytku po dělení v mnoha případech efektivněji než Eulerovu funkci.

Příklad 36: Za použití Carmichaelovy věty určete poslední dvojčíslí čísla $219^{83^{37}}$.

Řešení: Počítáme modulo 100:

$$\lambda(100) = \mathrm{n}\big(\lambda(4), \lambda(25)\big) = \mathrm{n}(2, 5 \cdot 4) = 20$$

Takže:

$$219^{83^{37}} \equiv 19^{83^{37} \bmod 20} = 19^{3^{37} \bmod 20} \pmod{100}$$

Spočtěme $\lambda(20)$:

$$\lambda(20) = \mathrm{n}\big(\lambda(4), \lambda(5)\big) = \mathrm{n}(2, 4) = 4$$

Tedy:

$$19^{3^{37} \bmod 20} = 19^{(3^4)^9 \cdot 3 \bmod 20} = 19^3 \equiv 59$$

Příklad 37: Za použití Carmichaelovy věty zjistěte poslední dvojčíslí čísla $735^{30^{86}}$.

Řešení: Úprava je nejdříve stejná jako v příkladu 32:

$$\frac{a}{5} \equiv 7 \cdot 15^{30^{86}-1} \pmod{20}$$

Již víme $\lambda(20) = 4$:

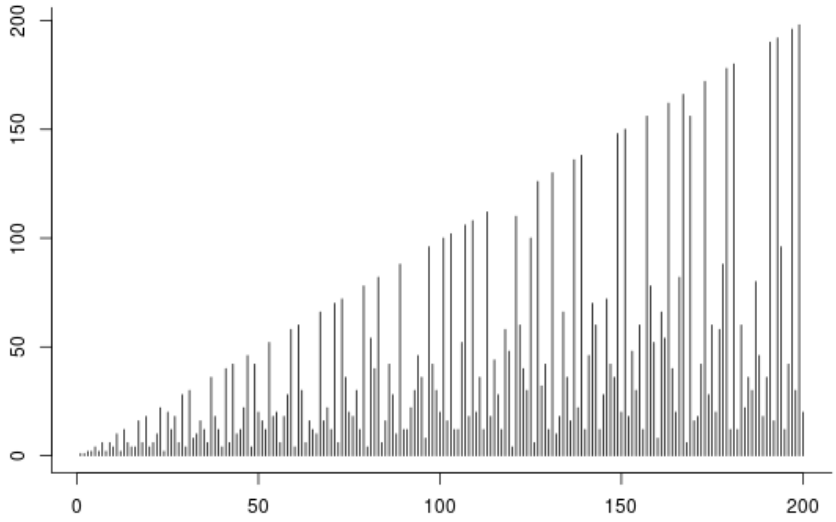
$$15^{30^{86}-1 \bmod 4} = 15^{2^{86}-1 \bmod 4} = 15^{(2^4)^{21} \cdot 2^2 - 1 \bmod 4} = 15^{4-1} = 15^3 \equiv 15$$

Dále již je postup stejný s postupem v příkladu 32.

Využití Carmichaelovy funkce tedy řešení problémů usnadňuje a je přímočařejší než využití Eulerovy funkce.

U exponenciálních kongruencí může opět pomoct s určením periody řešení. Nicméně ani tato funkce zaručeně neurčí nejmenší periodu pro konkrétní číslo a nepomůže s hledáním samotného řešení.

Na závěr opět ukažme graf hodnot $\lambda(n)$ pro prvních 200 n:



Obr. 10: Graf $\lambda(n)$ (svislá osa) pro prvních 200 n (vodorovná osa). Vygenerováno pomocí OEIS (posloupnost A002322).

Můžeme pozorovat stejné fenomény jako u grafu v obr. 9. Oproti němu je tento graf méně „hustý“.

3 Algebraická struktura zbytků po dělení n

V této kapitole se podíváme na kongruence trochu jinou optikou. Co znamená počítat modulo n? Znamená to provádět nějaké operace (používali jsme $+, -$ a $\cdot$) na množině $\{0, 1, \dots, n-1\}$. Naším cílem teď bude zkoumat algebraickou strukturu této množiny se sčítáním a násobením zvlášť. Z toho důvodu budeme dále místo znaku $\equiv$ používat znak $=$. Omezujeme se pouze na struktury s jednou operací a celkově bude tato kapitola o něco méně formální než předchozí dvě. Jde nám spíše o intuitivní výklad ne úplně jednoduchého tématu. Formální výklad může čtenář najít např. v (Stanovský, 2022).

Nejprve si formalizujme množinu našeho zkoumání a operace nad ní.

Definice 13 (Množina $\mathbb{Z}_n$)

Množinou $\mathbb{Z}_n$ rozumíme množinu $\{0, 1, 2, \dots, n-1\}$, kde $n \in \mathbb{N}$.

Formálněji:

$$\mathbb{Z}_n = \{a \in \mathbb{N}_0 : 0 \leq a \leq n-1\}$$

Např. $\mathbb{Z}_5$ je množinou $\{0, 1, 2, 3, 4\}$.

Definice 14 (Sčítání v $\mathbb{Z}_n$)

Sčítání v $\mathbb{Z}_n$ značíme $+_{\mathrm{mod}\, n}$ a definujeme:

$$a +_{\mathrm{mod}\, n} b = (a + b) \bmod n$$

pro $a, b \in \mathbb{Z}_n$, kde $\bmod n$ chápeme jako operaci.

Např. $3 +_{\mathrm{mod}\, 5} 4 = (3 + 4) \bmod 5 = 2$.

Pozn.: Dále budeme značit pouze $+$, protože v této kapitole bude vždy chápáno podle této definice.

Definice 15 (Násobení v $\mathbb{Z}_n$)

Násobení v $\mathbb{Z}_n$ značíme $\cdot_{\mathrm{mod}\, n}$ a definujeme:

$$a \cdot_{\mathrm{mod}\, n} b = (a \cdot b) \bmod n$$

pro $a, b \in \mathbb{Z}_n$, kde $\bmod n$ chápeme jako operaci.

Např. $2 \cdot_{\mathrm{mod}\ 5} 4 = (2 \cdot 4) \bmod 5 = 3$.

Pozn.: Dále budeme značit pouze ·, protože v této kapitole bude vždy chápáno podle této definice.

3.1 Aditivní grupa $\mathbb{Z}_n$

Pozorujme tedy strukturu $\mathbb{Z}_n$ se sčítáním. Množina celých čísel s operací sčítání tvoří komutativní grupu. Na konkrétním příkladu pozorujme, zda by tomu tak mohlo být i pro její podmnožinu $\mathbb{Z}_n$. Pozorujme pro $\mathbb{Z}_{10}$:

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	**0**	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	**0**
2	2	3	4	5	6	7	8	9	**0**	1
3	3	4	5	6	7	8	9	**0**	1	2
4	4	5	6	7	8	9	**0**	1	2	3
5	5	6	7	8	9	**0**	1	2	3	4
6	6	7	8	9	**0**	1	2	3	4	5
7	7	8	9	**0**	1	2	3	4	5	6
8	8	9	**0**	1	2	3	4	5	6	7
9	9	**0**	1	2	3	4	5	6	7	8

Tab. 7: Sčítání v $\mathbb{Z}_{10}$.

Vzhledem k definici operace je vůči ní množina uzavřená. Neutrálním prvkem je očividně stejně jako v množině celých čísel 0. V každém řádku se neutrální prvek objevuje, takže pro každý prvek existuje prvek inverzní. Asociativita z tabulky vidět není, ale plyne z definice sčítání. Konečně, protože je tabulka symetrická podle diagonály, je operace komutativní. Zkoumali jsme pro složené číslo, takže shrňme obecně.

Tvrzení 16 (Aditivní grupa $\mathbb{Z}_n$)

Množina $\mathbb{Z}_n$ s operací sčítání tvoří komutativní grupu.

Bude-li z kontextu jasné, že pracujeme s grupou, ne pouze množinou, budeme značit $\mathbb{Z}_n$.

Důkaz: Z definice sčítání plyne uzavřenost, asociativita a komutativita. Neutrálním prvkem je 0, která náleží $\mathbb{Z}_n$. Pokud se v množině nachází prvek a, pak se v ní nachází i prvek k němu inverzní, tím je $n - a$.

Pozn.: Notace není jednotná, lze se často setkat se zápisem C_n, který má reflektovat, že grupa je cyklická (více na str. 99).

Zdůrazněme, že pro jakékoli přirozené číslo n je struktura $\mathbb{Z}_n$ komutativní grupou. To znamená, že se pro všechna n s takovou grupou velmi jednoduše pracuje a její chování není těžké popsat. Tato skutečnost se nám v našem zkoumání bude brzo hodit.

3.2 Multiplikativní grupa $\mathbb{Z}_n^*$

Nyní pozorujme strukturu $\mathbb{Z}_n$ s násobením. Množina celých čísel bez nuly s násobením tvoří komutativní monoid (tzn. „grupa“ bez inverzních prvků). Pozorujme opět pro $\mathbb{Z}_{10}$, zda se struktura bude shodovat:

·	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	**1**	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	**1**	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	**1**

Tab. 8: Násobení v $\mathbb{Z}_{10}$.

Z tohoto pozorování se i tato struktura zdá komutativním monoidem. Neutrálním prvkem je 1 a tabulka je souměrná podle diagonály. Také zde figuruje 0 jako agresivní prvek, tu ale můžeme pro jednodušší popis struktury bez problémů vynechat. Všimněme si ovšem, že narozdíl od celé množiny celých čísel, kde neexistují žádné inverzní prvky vůči násobení, v $\mathbb{Z}_{10}$ pro některé specifické prvky ano. Na první pohled jsou těmito čísly čísla nesoudělná s 10. Když se tedy omezíme pouze na množinu nesoudělných čísel, dokážeme strukturu zpřehlednit, najednou máme i inverzní prvky ke všem prvkům a struktura se stává komutativní grupou.

Definice 16 (Množina $\mathbb{Z}_n^*$)

Množinou $\mathbb{Z}_n^*$ rozumíme množinu všech $a \in \mathbb{Z}_n$, která jsou nesoudělná s n.

Formálněji:

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : D(a,n) = 1\}$$

S množinou $\mathbb{Z}_n^*$ jsme se vlastně již setkali. Počet prvků $\mathbb{Z}_n^*$ udává $\varphi(n)$.

Příklad 38: Vypište všechny prvky $\mathbb{Z}_{10}^*$.

Řešení: $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$. Můžeme si zkontrolovat, že $\varphi(10) = 4$, což je počet všech prvků.

Popišme tedy strukturu $\mathbb{Z}_n^*$ s násobením.

Tvrzení 17 (Multiplikativní grupa $\mathbb{Z}_n^*$; *multiplicative group of integers* mod n)
Množina $\mathbb{Z}_n^*$ s operací násobení tvoří komutativní grupu.

Bude-li z kontextu jasné, že pracujeme s grupou, ne pouze množinou, budeme značit $\mathbb{Z}_n^*$.

Důkaz: Z definice násobení plyne uzavřenost, asociativita a komutativita. Neutrálním prvkem je 1, která vždy náleží $\mathbb{Z}_n^*$, protože $D(1,n) = 1$ pro všechna n. Existence inverzních prvků vychází z Bézoutovy rovnosti, o ní (Kaňáková, 2022, s. 28). Pro nalezení inverzního prvku k prvku a stačí vyřešit rovnici $ua + vn = 1$ (onen hledaný inverzní prvek je zde u). Tato rovnice má dle Bézoutovy věty celočíselné řešení právě tehdy, když $D(a,n) = 1$, což platí $\forall a \in \mathbb{Z}_n^*$.

Pozn.: Ani v tomto případě není notace jednotná. Je jich celá řad, ale nejčastěji se lze setkat se zápisem $(\mathbb{Z}/n\mathbb{Z})^\times$.

3.3 Řád grupy a řády prvků

Lze v popisu struktury $\mathbb{Z}_n^*$ jít více do hloubky? Zatím jsme zkoumali součiny mezi různými prvky. V souladu s naším zkoumání exponenciálních kongruencí zkusme opakovaně násobit prvky samy se sebou. Pro jednoduchost pozorujme $\mathbb{Z}_7^*$, odkažme se na tab. 1. Z ní pro prvek 2 plyne:

$$2^1 = 2 \qquad 2^2 = 4 \qquad 2^3 = 1$$

Již zde lze pozorovat zajímavý jev. Z MFV platí, že $a^6 \equiv 1 \pmod 7$, nicméně pro 2 stačilo umocnit na třetí. Tento úkaz, se kterým jsme se setkali již v druhé kapitole, formalizujme.

Definice 17 (Řád grupy $\mathbb{Z}_n^*$, řád prvku; *Order of a group, order of element*)
Nechť $k, n \in \mathbb{N}$ a $a \in \mathbb{Z}_n^*$:

- *Řád grupy* $\mathbb{Z}_n^*$ je roven počtu prvků množiny $\mathbb{Z}_n^*$, je tedy tedy:
$$\varphi(n) = |\mathbb{Z}_n^*|$$
- *Řád prvku* a je nejmenší k takové, že $a^k = 1$, značí se $\mathrm{ord}(a) = k$.

(Stanovský, 2022, s. 63).

Pozn.: Řád prvku je unikátní pro každý prvek, nelze ho zjistit obecně např. pomocí vyčíslení Carmichaelovy funkce. Ta obecně neurčuje ani řád grupy, ten je definován jako hodnota Eulerovy funkce.

Příklad 39: Určete řád grupy $\mathbb{Z}_7^*$ a řád jejího prvku 2, tedy $\mathrm{ord}(2)$.

Řešení: Řádem grupy $\mathbb{Z}_7^*$ je $\varphi(7) = 6$.

$\mathrm{ord}(2) = 3$ z definice a pozorování výše.

Když budeme pozorovat mocniny ostatních prvků $\mathbb{Z}_7^*$, zjistíme, že se objevují řády $2, 3$ a 6. To znamená, že všechny řády prvků dělí řád grupy. Všimněme si, že nestačí, aby byly soudělné, neobjevuje se např. řád 4. Toto pozorování formalizuje a zobecňuje na podgrupy, nejen prvky, tzv. *Lagrangeova věta*. O ní více v (Stanovský, 2022, s. 64). My se omezujeme na řády prvků v grupách $\mathbb{Z}_n^*$.

Pozn.: Tato věta je jiná než Lagrangeova věta zmiňovaná v první kapitole. Po Lagrangeovy je pojmenována řada dalších vět, např. Lagrangeova věta o čtyřech čtvercích také z teorie čísel, nebo Lagrangeova věta o střední hodnotě v matematické analýze.

Tvrzení 18 (Řád prvku dělí řád grupy)
Nechť $n \in \mathbb{N}, a \in \mathbb{Z}_n^*$. Pak:

$$\mathrm{ord}(a) | \varphi(n)$$

Důkaz: Z EV platí $a^{\varphi(n)} = 1$, takže $\mathrm{ord}(a) \leq \varphi(n)$. V případě rovnosti tvrzení platí. Pokud pro nějaké a je $\mathrm{ord}(a) < \varphi(n)$, pak musí existovat nějaké $l \in \mathbb{N}$ takové, že $l \cdot \mathrm{ord}(a) = = \varphi(n)$, protože musí platit $(a^{\mathrm{ord}(a)})^l = 1^l = 1 = a^{\varphi(n)}$. V $\mathbb{Z}_n^*$ jsou definovány pouze celočíselné exponenty, takže je tato rovnice řešitelná pouze pokud $\mathrm{ord}(a) | \varphi(n)$. (Gauss, 1986, s. 30-31).

Příklad 40: Vypište všechny řády prvků $\mathbb{Z}_{24}^*$.

Řešení: $\varphi(24) = 8$, což navádí na vypsání všech dělitelů 8. Nicméně již víme, že $\lambda(24) = = 2$, takže všechny prvky jsou maximálně řádu 2, množina řádů je tedy $\{1, 2\}$.

Řády prvků tedy nemusí být všechny dělitele řádů grupy.

Pozn.: Toto tvrzení lze využít pro určení periody řešení exponenciálních kongruencí. Po spočtení $\lambda(n)$ lze určit všechny dělitele této hodnoty a pro konkrétní číslo vyzkoušet pouze tyto dělitele. To situaci značně zjednodušuje, nicméně stále neexistuje žádný obecný algoritmus na určení řádu konkrétního prvku.

3.4 Generátory

Neopouštějme předchozí pozorování. Všimněme si, že v $\mathbb{Z}_7^*$: $\mathrm{ord}(3) = 6$ a umocňováním 3 postupně vyjdou všechny prvky $\mathbb{Z}_7^*$. To znamená, že všechny prvky $\mathbb{Z}_7^*$ lze vyjádřit jako mocninu 3. To může práci s grupou značně zjednodušit.

Definice 18 (Generátor/Primitivní prvek; *Generator/primitive root*)
Nechť $n \in \mathbb{N}$ a $g \in \mathbb{Z}_n^*$. Prvek g se nazývá *generátorem* (také *primitivním prvkem*) grupy $\mathbb{Z}_n^*$, pokud lze každý prvek $\mathbb{Z}_n^*$ vyjádřit jako mocninu g. Skutečnost, že g je generátorem $\mathbb{Z}_n^*$ značíme $\langle g \rangle = \mathbb{Z}_n^*$.

Pozn.: Řád generátoru se očividně musí rovnat řádu grupy.

Pojem generátoru je v teorii grup mnohem obecnější. O nich obecně v (Stanovský, 2022). Naopak pojem primitivní prvek je velmi konkrétní. Tento pojem je přesně definován ve znění této definice. Pojem primitivní prvek zavedl Gauss (latinsky *radice primitiva*) a nepoužívá obecnější pojem generátor jednoduše proto, že obecná teorie grup vznikla až po DA. Dále ale budeme používat termín generátor, protože je obecnější a v kontextu této práce ekvivalentní pojmu primitivní prvek.

Generátory můžeme vztáhnout i k aditivním grupám $\mathbb{Z}_n$, pro které všechny triviálně platí $\langle 1 \rangle = \mathbb{Z}_n$. 3 je generátorem $\mathbb{Z}_7^*$, můžeme zapsat $\langle 3 \rangle = \mathbb{Z}_7^*$, naopak 4 generátorem není, protože např. prvek 3 nelze vyjádřit jako mocninu 4.

K pojmu generátoru se pojí další pojem. Tím je cyklická grupa.

Podívejme se na jednoduché příklady, se kterými nám znalost generátoru může pomoct.

Příklad 41:

a) Dokažte, že 4 není generátorem $\mathbb{Z}_7^*$.
b) Proveďte součin $4 \cdot 5$ v $\mathbb{Z}_7^*$ pomocí generátoru.
c) Využitím generátoru nalezněte inverzní prvek k 2 v $\mathbb{Z}_7^*$.

Řešení:

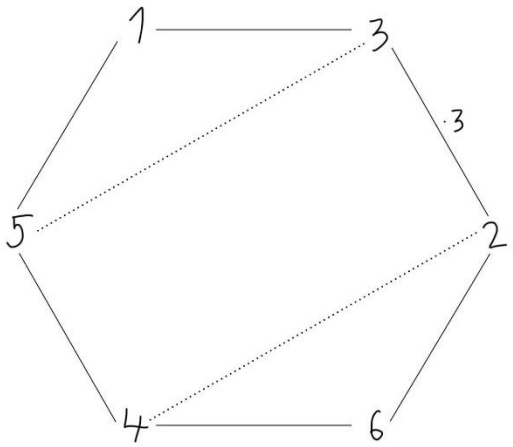
a) 3 je generátorem. $4 = 3^4$ a z umocňování 4 stává umocňování 3^4 a již $(3^4)^3 = 3^{12} = (3^6)^2 = 1$, takže pomocí 4 nevygenerujeme všechny prvky $\mathbb{Z}_7^*$.

b) Oba prvky si zapišme jako mocninu generátoru a z násobení prvků se stane prosté sčítání exponentů:

$$4 \cdot 5 = 3^4 \cdot 3^5 = 3^{4+5} = 3^9 = 3^6 \cdot 3^3 = 1 \cdot 6 = 6$$

c) K prvku vyjádřenému mocninou generátoru je inverzní takový prvek, že se exponenty obou prvků při sečtení rovnají řádu grupy. $2 = 3^2$, inverzním prvkem je tedy $3^{6-2} = 3^4 = 4$.

Všimněme si, že 3 není jediným prvkem, jehož opakovaným mocněním vyšly všechny prvky grupy $\mathbb{Z}_7^*$. To se stalo i pro prvek 5 (tj. i 5 je generátor). Vidíme tedy, že generátor grupy nemusí být určen jednoznačně. Všimněme si, že při generování prvkem 5 jsme generovali prvky grupy v opačném pořadí než při generování trojkou. To vyplývá z faktu, že 5 je inverzním prvkem 3, tedy $3^{-1} = 5$. Generátor tedy nikdy není určen jednoznačně, protože pokud nalezneme generátor, i inverzní prvek k němu bude generátorem. Zvolme si jeden z generátorů, např. 3 a znázorněme strukturu $\mathbb{Z}_7^*$ obrázkem:



Obr. 11: Struktura $\mathbb{Z}_7^*$.

V obr. 11 je znázorněno, že jsme generovali prvkem 3. Přerušované úsečky spojují inverzní prvky.

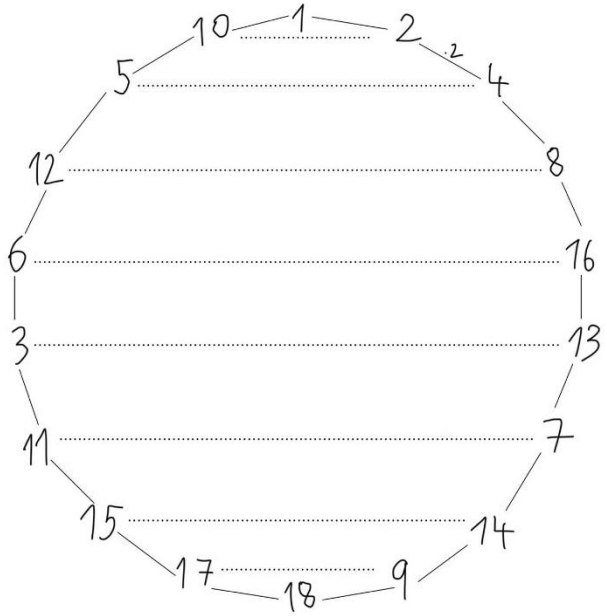
Jak zjistit, kolik generátorů daná grupa má, a popřípadě jak je nalézt? Proveďme pozorování pro grupu s více prvky. Zůstaňme ještě u prvočísel, např. $\mathbb{Z}_{19}^*$. Pokusme se najít generátor tak, že budeme opakovaně umocňovat všechny prvky, dokud nenarazíme na generátor. Důsledkem Lagrangeovy věty stačí umocňovat jen na dělitele 18. Začněme od nejmenšího, u kterého to má smysl, tedy u 2:

$2^1 = 2$ $\qquad$ $2^6 = 8^2 = 7$

$2^2 = 4$ $\qquad$ $2^9 = 2^6 \cdot 2^3 = 7 \cdot 8 = 18 = -1$

$2^3 = 8$

2 tedy generátorem je, protože z pozorování vyplývá $2^{18} = (-1)^2 = 1$ a pro nižší mocninu dvojky 1 nevyjde, takže se řád 2 rovná řádu $\mathbb{Z}_{19}^*$. Tuto grupu generovanou 2 znázorněme obrázkem, ze kterého lépe nahlédneme vlastnosti grupy, a tedy nám zjednoduší i zkoumání generátorů:



Obr. 12: Struktura $\mathbb{Z}_{19}^*$.

V obr. 12 je znázorněno, že jsme generovali prvkem 2. přerušované úsečky opět spojují inverzní prvky.

Začněme nejdříve pozorováním, které prvky nemohou být generátory. V obr. 12 toto můžeme lehce nahlédnout tak, že se podíváme, zda by námi vybraný kandidát na generátor opravdu vygeneroval všechny prvky. Např. lze jednoduše vidět, že $4 = 2^2$ generátorem není, protože při mocnění vynechá každý druhý prvek. Obdobně $8 = 2^3$ vynechá každý třetí. U $16 = 2^4$ už je situace o něco zajímavější, protože sice vynechá každý čtvrtý prvek, nicméně jedním z těchto přeskočených je i prvek 1. Můžeme ovšem „obíhat kolo“ dále,

dokud nenarazíme na 1. Pak vidíme, že ani 16 nevygeneruje všechny prvky. Pokud půjdeme ještě o krok dále a vyzkoušíme $13 = 2^5$, zjistíme, že ta už generátorem je.

Otázkou tedy je, jak zjistit, které prvky při mocnění nevynechají žádný prvek, než narazí na 1 (tyto prvky jsou tedy generátory) a které ne. 4 je druhou mocninou generátoru a 8 třetí. Řád grupy je 18. Oba tyto prvky dosáhli 1 již při jednom „oběhnutí“, což není překvapující, protože oba exponenty generátoru příslušící těmto prvkům dělí řád grupy. Konkrétně 4 vygenerovala 9 prvků, protože $(2^2)^9 = 2^{18}$. 8 obdobně vygenerovala 6 prvků. Pro $16 = 2^4$ už neplatí, že by tento exponent dělil řád grupy, ale je s ním soudělný. 16 vygenerovala také 9 prvků, protože $D(4, 18) = 2$ a $n(4, 18) = 36 = 9 \cdot 4 = 18 \cdot 2$. Až $13 = 2^5$ má exponent nesoudělný s řádem grupy, a tedy vygenerovala všech 18 prvků, protože $\mathrm{n}(5, 18) = 18 \cdot 5$. Takže každá mocnina generátoru, která má nesoudělný exponent s řádem grupy bude také generátorem.

Tvrzení 19 (Počet generátorů $\mathbb{Z}_n^*$)
Nechť $n \in \mathbb{N}$. Počet generátorů $\mathbb{Z}_n^*$ (pokud nějaký existuje) je roven $\varphi(\varphi(n))$.

Důkaz: $\varphi(n)$ označuje počet prvků grupy. Pokud vyjádříme všechny prvky $\mathbb{Z}_n^*$ jako mocninu libovolného generátoru g, pak dalšími generátory budou jen takové mocniny g, pro jejichž exponent $k \in \mathbb{N}$ platí $D\big(k, \varphi(n)\big) = 1$, z čehož triviálně vyplývá $n\big(k, \varphi(n)\big) = k \cdot \varphi(n)$. Tím pádem při postupném mocnění tohoto g^k vyjde $\varphi(n)$ různých prvků (včetně 1 jako poslední), což je počet všech prvků $\mathbb{Z}_n^*$. Pro mocninu generátoru s exponentem $l \in \mathbb{N}$ takovým, že $D\big(l, \varphi(n)\big) > 1$ platí $n\big(l, \varphi(n)\big) < l \cdot \varphi(n)$ a tedy při postupném mocnění vyjde méně než $\varphi(n)$ různých prvků před dosáhnutím 1, což znamená, že l nevygeneruje všechny prvky $\mathbb{Z}_n^*$. Z definice EF je počet k splňujících zmíněnou podmínku $\varphi(\varphi(n))$.

Pozn.: Předpoklad existence generátoru je důležitý. Grupám, které nelze nagenerovat jedním prvkem, tedy necyklickým grupám, se budeme věnovat brzy.

Příklad 42: Určete počet generátorů $\mathbb{Z}_{19}^*$.

Řešení: Počet generátorů $\mathbb{Z}_{19}^*$ je:

$$\varphi\big(\varphi(19)\big) = \varphi(18) = \varphi(2) \cdot \varphi(3^2) = 1 \cdot 3 \cdot 2 = 6$$

Navzdory tomu, že můžeme jednoduše a obecně rozhodnout o počtu generátorů, neexistuje žádný jednoduchý algoritmus pro nalezení konkrétního generátoru. Nejvíce intuitivní metoda pro nalezení generátoru je vyzkoušet všechny přípustné řády prvku (tedy všechny dělitele řádu grupy) postupně od nejmenšího pro všechny prvky grupy, dokud nenarazíme na takový, jehož řád se rovná řádu grupy. Tento prvek bude generátorem.

Příklad 43: Nalezněte generátor $\mathbb{Z}_{23}^*$.

Řešení: $\varphi(23) = 22 = 2 \cdot 11$, prvky tedy mohou být řádu $1, 2, 11$ nebo 22. Exponent 1 není třeba ověřovat:

$$2^2 = 4$$
$$2^{11} = (2^5)^2 \cdot 2 = 9^2 \cdot 2 = 12 \cdot 2 = 1$$
$$3^2 = 9$$
$$3^{11} = (3^2)^5 \cdot 3 = 9^5 \cdot 3 = 12^2 \cdot 9 \cdot 3 = 6 \cdot 4 = 1$$
$$4 = 2^2 \Rightarrow 4^{11} = (2^2)^{11} = (2^{11})^2 = 1$$
$$5^2 = 2$$
$$5^{11} = (5^2)^5 \cdot 5 = 2^5 \cdot 5 = 9 \cdot 5 = -1$$

Nejmenším generátorem je tedy 5.

Na tomto příkladu lze vidět, že nejmenším generátorem může být i větší číslo, než se na první pohled může zdát a jeho nalezení může zabrat nějaký čas.

3.4.1 Polynomiální a exponenciální kongruence a generátory

Koncept generátoru nám může poskytnout hlubší vhled i do abstraktnějších témat předchozích dvou kapitol. Lze jeho využitím dokázat tvrzení o počtu zbytků stupně k (tvrzení 1 a 12), či o součinech různých kombinací zbytků a nezbytků (tvrzení 2 a 13). Také poskytuje vysvětlení fungování RESSOL algoritmu, či možný způsob řešení exponenciálních kongruencí.

Počet zbytků stupně k

Zbytky po dělení p (bez nuly) tvoří prvky $\mathbb{Z}_p^*$, kde si všechny můžeme vyjádřit jako mocniny generátoru. Začněme zbytky kvadratickými. Zřejmě každá sudá mocnina generátoru je kvadratickým zbytkem (protože $g^{2l} = (g^l)^2$) a tedy je jejich počet poloviční oproti počtu

všech prvků $\mathbb{Z}_p^*$. Zároveň se tato úvaha snadno zobecňuje, dokažme analogicky 52: pokud si každý prvek $\mathbb{Z}_p^*$ (jejichž počet je $p-1$) reprezentujeme jako mocninou nějakého generátoru g, pak je zbytkem stupně k každá k-tá mocnina generátoru. Zvolme si nejnižší z nich, tedy g^k. Pokud $D(p-1,k)=1$, pak je g^k také generátorem a každý prvek je tedy nějakou k-tou mocninou. Pokud $D(p-1,k)=2;3;4;...$, pak prvek g^k vygeneruje pouze každý druhý/třetí/čtvrtý/… prvek $\mathbb{Z}_p^*$, tedy pouze polovina/třetina/čtvrtina/… všech prvků je nějakou k-tou mocninou.

Vztah kvadratických zbytků a generátorů

Z $D(p-1,2)=2$ pro všechna p vyplývá, že pokud je prvek kvadratickým zbytkem (a tedy obecně zbytkem sudého stupně), pak nemůže být generátorem. Takže každý generátor je kvadratický nezbytek. To ale neznamená, že každý kvadratický nezbytek je generátor. Počet generátoru $\mathbb{Z}_p^*$ je $\varphi(\varphi(p))=\varphi(p-1)$, což je rovno $\frac{p-1}{2}$ jen pro prvočísla tvaru 2^k+1.

Součiny zbytků a nezbytků

Tvrzení o součinech zbytků a nezbytků je za pomoci mocnin generátoru také jednodušší nahlédnout a dokázat. Principem je rozhodnout, zda bude součet exponentů dělitelný stupněm zkoumaných zbytků. Pro příklad takto alternativně dokažme tvrzení 4: a,b jsou lichými mocninami nějakého generátoru g, tedy:

$$ab = g^{2k+1} \cdot g^{2l+1} = g^{2k+2l+2} = (g^{k+l+1})^2;\ k,l \in \mathbb{N}$$

Tímto způsobem lze obecně ukázat, proč se platnost tohoto tvrzení nepřenáší na všechny nezbytky vyšších stupňů: pro $k \geq 3$: $g^{kl+1} \cdot g^{km+1} = g^{kl+km+2}$, což není k-tou mocninou generátoru, protože $2 < 3$.

Princip RESSOL algoritmu

Hlavním principem fungování algortimů je snižování řádů prvků b a c^l při každém opakování. c^l (kde c je zvolený kvadratický nezbytek) je zaručeně řádu 2^k. Opakovaným mocněním b zjistíme jeho řád a b následně násobíme d^2, které je zkonstruováno jako prvek se stejným řádem. Řád bd^2 je pak menší než řád b a d^2. To ukažme následovně: reprezentujme si b i d^2 jako mocniny nějakého generátoru g. Protože jsou oba prvky stejného řádu a všechny možné řády jsou mocniny dvojky menší než 2^k, musí být oba

mocninou generátoru, jejíž exponent v prvočíselném rozkladu obsahuje stejnou mocniny dvojky, označme $2^l, l < k$. Označme $b = g^{2^l m}$ a $d^2 = g^{2^l n}, m, n$ liché. Pak:

$$bd^2 = g^{2^l m} \cdot g^{2^l n} = g^{2^l m + 2^l n} = g^{2^l (m+n)}$$

Protože jsou m i n obě lichá, pak je jejich součet sudý, takže lze vytknout minimálně první mocninu dvojky součin je nižšího řádu, než byly oba součinitele. Algoritmem tedy dříve či později zákonitě dojdeme k $bd^2 = 1$.

Řešení exponenciální kongruence

Za předpokladu, že známe generátor, si můžeme základy na obou stranách kongruence reprezentovat jako mocniny daného generátoru. Tím převedeme na stejný základ a řešení nalezneme vyřešení lineární rovnice tvořené exponenty. Podotkněme, že v obecném případě tento způsob úplně zjednodušující není. Zaprvé musíme nalézt generátor a zadruhé musíme nalézt, kterými konkrétními mocninami generátoru jsou základy na obou stranách kongruence.

3.5 Cyklické a necyklické grupy $\mathbb{Z}_n^*$

S konceptem generátoru, respektive primitivního prvku úzce souvisí koncept cyklických a necyklických grup. Obě grupy, které jsme zatím znázornili obrázkem byly cyklické, což z jejich tvaru nějakého n-úhelníku intuitivně dává smysl. Zatím jsme ještě nepracovali s grupami, u kterých bychom nenalezli generátor. Existence generátoru je právě klíčová pro to, zda je grupa cyklická či necyklická.

Definice 19 (Cyklická a necyklická grupa; *Cyclic and non-cyclic group*)
Grupa se nazývá *cyklická*, pokud lze všechny její prvky vygenerovat operováním jediným prvkem. Grupa, která není cyklická se nazývá *necyklická*. (Stanovský, 2022, s. 73).

Pozn.: Protože pro všechna n: $\langle 1 \rangle = \mathbb{Z}_n$, je každá grupa $\mathbb{Z}_n$ cyklická.

Zatím jsme zkoumali grupy $\mathbb{Z}_p^*$ pro p prvočíslo. Pozorujme strukturu grup $\mathbb{Z}_{10}^*, \mathbb{Z}_{15}^*, \mathbb{Z}_9^*$ a $\mathbb{Z}_8^*$. Začněme nalezením generátoru:

- $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$. Počet jejích prvků (tzn. řád grupy) je 4 a řády prvků tedy mohou být $1, 2$ nebo 4. Protože $3^2 = -1$, je 3 generátorem.
- $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Řád grupy je 8 a řády prvků mohou být $1, 2, 4$ a 8. Prvky 1 a 14 není potřeba zkoumat. Očividně $2^4 = 1$, tudíž $2, 4$ ani 8 nebudou generátory. Ověřme ostatní prvky:

  $$7^2 = 4 \qquad 11^2 = 1$$
  $$7^4 = 4^2 = 1 \qquad 13^2 = 4$$

  Pro $\mathbb{Z}_{15}^*$ neexistuje jediný generátor.
- $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$. Řád grupy je 6, prvky mohou být řádů $1, 2, 3$ nebo 6. Očividně $2^3 = -1$, takže 2 je generátorem.
- $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. Řád grupy je opět 4. $3^2 = 1$ a $5^2 = 1$, tedy ani $\mathbb{Z}_8^*$ nemá jediný generátor

Příklad 44: Klasifikujte všechny grupy $\mathbb{Z}_n^*$, které jsme zatím pozorovali jako cyklické či necyklické.

Řešení: Všechny grupy, ke kterým jsme nalezli generátor jsou cyklické: $\mathbb{Z}_7^*$, $\mathbb{Z}_9^*$, $\mathbb{Z}_{10}^*$, $\mathbb{Z}_{19}^*$, $\mathbb{Z}_{23}^*$. Necyklické jsou: $\mathbb{Z}_8^*$ a $\mathbb{Z}_{15}^*$.

Toto pozorování situaci značně zkomplikovalo. Vypadá to, že pro některá složená n je $\mathbb{Z}_n^*$ cyklická a pro některá ne. Obdobně pro mocniny prvočísel. Nemusí být hned jasné, jak si necyklické grupy představit a jak jednoduše poznat, které jsou cyklické a které ne.

Uvědomme si, že generátor grupy musí mít řád shodný s řádem grupy. Jinými slovy nesmí existovat $k \in \mathbb{N}$ takové, že:

$$k < \varphi(n) \wedge \forall a \in \mathbb{Z}_n^* : a^k = 1$$

Jinými slovy se alespoň jeden prvek při opakovaném mocnění musí rovnat 1 poprvé až s exponentem $\varphi(n)$. Musí tedy platit $\lambda(n) = \varphi(n)$. Pomocí Carmichaelovy věty můžeme grupy $\mathbb{Z}_n^*$ jednoduše rozdělit na cyklické a necyklické v závislosti na povaze n.

Tvrzení 20 (Klasifikace cyklických a necyklických grup $\mathbb{Z}_n^*$)
Nechť p je liché prvočíslo a n je složené číslo, kromě dvojnásobku mocniny prvočísla. Pak:

- Cyklické jsou grupy $\mathbb{Z}_2^*, \mathbb{Z}_4^*, \mathbb{Z}_p^*, \mathbb{Z}_{2p}^*, \mathbb{Z}_{p^k}^*$ a $\mathbb{Z}_{2p^k}^*$ pro $k \in \mathbb{N}, k \geq 2$
- Necyklické jsou grupy $\mathbb{Z}_{2^k}^*$ pro $k \in \mathbb{N}, k \geq 3$ a grupy $\mathbb{Z}_n^*$ pro všechna ostatní n

Důkaz: Aby grupa $\mathbb{Z}_n^*$ byla cyklická, musí být generována jediným prvkem. Musí pro ni tedy existovat prvek s řádem rovným řádu grupy $\varphi(n)$. Aby takový prvek zaručeně existoval, musí platit $\lambda(n) = \varphi(n)$. Důkaz lze dokončit vypočtením funkčních hodnot pro všechny tvary čísel každého případu zvlášť.

Nyní se přesuňme ke zkoumání, jak popsat strukturu necyklických grup a obecně jako jednoduše popsat strukturu všech grup $\mathbb{Z}_n^*$.

3.6 Izomorfismus $\mathbb{Z}_n^*$

Všimněme si, že v $\mathbb{Z}_{19}^*$ nabývá exponent generátoru hodnot od 1 do 18, což jsou prvky grupy $\mathbb{Z}_{18}$ (kde $18 = 0$, což nic nezmění, protože v $\mathbb{Z}_{19}^*$ $a^0 = a^{18}$). Lze tedy říct, že pokud každý prvek v $\mathbb{Z}_{19}^*$ reprezentujeme mocninou generátoru a každé mocnině přiřadíme prvek $\mathbb{Z}_{18}$ podle jejího exponentu, tak se násobení prvků v $\mathbb{Z}_{19}^*$ chová stejně, jako sčítání prvků v $\mathbb{Z}_{18}$. Přesněji bychom takto provedli zobrazení $\mathbb{Z}_{19}^* \to \mathbb{Z}_{18}$, kterému se říká *izomorfismus*. Abychom si tento koncept dokázali lépe představit, parafrázujme popis z (Stanovský, 2022): Izomorfismus je bijektivní zobrazení mezi dvěma matematickými strukturami, které zachovává jejich základní vlastnosti.

Pozn.: Stanovský definuje izomorfismus pomocí *homomorfismu*, který je obecnější v tom, že nemusí být bijektivní.

S jedním izomorfismem jsme se již setkali. Tím je násobení -1 a 1 a násobení kvadratických zbytků a nezbytků. Znázorněme tabulkou:

·	**KZ**	**KN**
KZ	KZ	KN
KN	KN	KZ

·	**1**	**−1**
1	1	−1
−1	−1	1

Tab. 9 a tab. 10: Izomorfismus mezi kvadratickými zbytky a nezbytky a množinou $\{-1, 1\}$ s násobením.

Obě tabulky se vlastně chovají stejně, jen máme jinak nazvané prvky. Podobným izomorfismus existuje mezi násobením sudých a lichých čísel a násobením 0 a 1:

·	**S**	**L**
S	S	S
L	S	L

·	**0**	**1**
0	0	0
1	0	1

Tab. 11 a tab. 12: Izomorfismus mezi sudými a lichými čísly a množinou $\{0, 1\}$ s násobením.

Co je na izomorfismech zajímavé je to, že může existovat i mezi strukturami s jinými operacemi. To pro naše zkoumání bude velmi užitečné. Dalším jednoduchým izomorfismem, který zmiňuje i Stanovský (s. 72), je mezi strukturami s jinými operacemi. Je jím izomorfismus mezi sčítáním prvků $\mathbb{Z}_2$ a násobením -1 a 1:

$+$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{0}$	0	1
$\mathbf{1}$	1	0

$\cdot$	$\mathbf{1}$	$\mathbf{-1}$
$\mathbf{1}$	1	-1
$\mathbf{-1}$	-1	1

Tab. 13 a tab. 14: Izomorfismus mezi aditivní grupou $\mathbb{Z}_2$ a množinou $\{-1, 1\}$ s násobením.

Dokonce můžeme pozorovat, že protože množina $\{-1, 1\}$ s násobením je izomorfní s grupou $\mathbb{Z}_2$ i násobením KZ a KN, pak je $\mathbb{Z}_2$ také izomorfní s násobením KZ a KN. Můžeme zajít

ještě dále; protože víme, že $\mathbb{Z}_2$ je komutativní grupou, pak i obě struktury, které jsou s ní izomorfní jsou komutativními grupami.

Nyní si ukažme již trochu sofistikovanější izomorfismus mezi strukturami s různými operacemi. S tím jsme se každý setkali na střední škole, je jím logaritmus (pro jednoduchost berme přirozený) a ten je zobrazením z kladných reálných čísel s násobením do reálných čísel se sčítáním. To lze jednoduše nahlédnout ze základních vlastností logaritmů a pomocí jedné z tzv. vět o logaritmech: $\ln(x \cdot y) = \ln x + \ln y$. Zachování struktury můžeme dále pozorovat na tom, že se neutrální prvek zobrazí na neutrální prvek: $\ln 1 = 0$. Také vzájemně inverzní prvky se zobrazí na vzájemně inverzní prvky: k x je inverzním prvkem $\frac{1}{x}$ a $\ln\frac{1}{x} = = -\ln x$, což je inverzním prvkem k $\ln x$.

Všimněme si, že v našem úvodním pozorování k izomorfismu jsme zkoumali vztah mezi prvky a příslušnými mocninami generátoru, což je podobný princip jako zobrazování reálných čísel pomocí logaritmu o daném základu. Dále podotkněme, že motivace pro zavedení logaritmů bylo zjednodušení násobení na sčítání, což se může hodit i v grupách, kterými se zabýváme. Pomocí vlastností, které jsme pozorovali definujme izomorfismus konkrétně pro grupy.

Definice 20 (Grupový izomorfismus)

Nechť G je multiplikativní grupa a H aditivní grupa, $x, y \in G$, 1 je neutrálním prvkem G a 0 je neutrálním prvkem H. Grupovým izomorfismem je bijektivní zobrazení f, pro které platí:

- $f(x \cdot y) = f(x) + f(y)$
- $f(1) = 0$
- $f(x^{-1}) = f(x)^{-1}$

Skutečnost, že G je izomorfní s H se značí $G \cong H$. (Stanovský, 2022)

Pozn.: Definici jsme si zde upravili pro speciální případ grup, kterými se zabýváme, jinak je samozřejmě mnohem obecnější.

Vraťme se zpět k nějaké konkrétní menší grupě; k již pozorované $\mathbb{Z}_7^*$. Jako generátor, podle něhož provedeme zobrazení, si zvolme 3 a znázorněme izomorfismus $\mathbb{Z}_7^* \cong \mathbb{Z}_6$:

$(\mathbb{Z}_7^*, \cdot)$	1	2	3	4	5	6
$(\mathbb{Z}_6, +)$	0	2	1	4	5	3

Tab. 15: Izomorfismus $\mathbb{Z}_7^* \cong \mathbb{Z}_6$. Vrchní řádek obsahuje prvky $\mathbb{Z}_7^*$, spodní příslušnou hodnotu, kterou je třeba umocnit generátor 3 k získání daného prvku.

Příklad 45: Dokažte, že je zobrazení z tab. 15 grupovým izomorfismem.

Řešení: Z tabulky lze rovnou nahlédnout, že se neutrální prvek zobrazil na neutrální prvek. Výčtem můžeme ověřit zachování inverzních prvků (např. $3 \cdot 5 = 1$ a opravdu $1 + 5 = 0$) i obecnou strukturu, např.:

$$\mathbb{Z}_7^*: 3 \cdot 6 = 4$$
$$\mathbb{Z}_6: 1 + 3 = 4$$

3 ale není jediným generátorem $\mathbb{Z}_7^*$. Vytvořme si tabulku izomorfismu $\mathbb{Z}_7^* \cong \mathbb{Z}_6$ podle generátoru 5:

$(\mathbb{Z}_7^*, \cdot)$	1	2	3	4	5	6
$(\mathbb{Z}_6, +)$	0	4	5	2	1	3

Tab. 16: Izomorfismus $\mathbb{Z}_7^* \cong \mathbb{Z}_6$. Vrchní řádek obsahuje prvky $\mathbb{Z}_7^*$, spodní příslušnou hodnotu, kterou je třeba umocnit generátor 5 k získání daného prvku.

Na první pohled je vidět, že spodní řádek tab. 16 se neshoduje se spodním řádkem tab. 15. Takže nejen, že generátor grupy není určen jednoznačně, ani izomorfismus není určen jednoznačně. Přesněji řečeno, jednoznačně určeno je, které grupě je $\mathbb{Z}_7^*$ izomorfní, ale konkrétní zobrazení mezi těmito dvěma grupami jednoznačně určeno není. Obecně lze ale vidět, že pro p prvočíslo:

$$\mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$$

Pro cyklické $\mathbb{Z}_{p^k}^*$ je struktura do jisté míry analogická. Zkoušením dříve či později nalezneme generátor, pomocí něj všechny ostatní prvky a graficky si grupu lze opět

představit jako n-úhelník. Co nemusí být jasné je, které aditivní grupě je taková grupa izomorfní. Zde ovšem úvaha není nikterak složitá. Vzhledem k tomu, že existuje generátor, izomorfismus můžeme analogicky provést podle jeho mocnin. Počet prvků $\mathbb{Z}_{p^k}^*$ a řád generátoru je $\varphi(p^k) = p^{k-1}(p-1)$, takže obecně:

$$\mathbb{Z}_{p^k}^* \cong \mathbb{Z}_{p^{k-1}(p-1)}$$

Nyní se pokusme zjistit, jak si lépe představit právě grupu necyklickou. Ty nejsou generovány jediným prvkem, ale více prvky. Pozorujme blíže $\mathbb{Z}_{15}^*$, zda ji dokážeme nagenerovat více než jedním prvkem, popřípadě kolika. Řád grupy je 8, ale největším možným řádem prvku v této grupě je 4, toho nabývá už prvek 2, který postupně vygeneruje prvky $4, 8$ a 1. Zbývají prvky $7, 11, 13$ a 14. Z nich si zvolme prvek řádu 2, tím je 11. Proč si volíme prvek řádu 2? Protože počet všech kombinací čtyř mocnin prvku 2 a dvou mocnin prvku 11 je 8, což je i řád grupy. Dva prvky řádu 4 by některé prvky vygenerovaly dvakrát. Nyní zbývá operováním s 2 a 11 vygenerovat zbylé 3 prvky:

$$11 \cdot 2 = 7 \qquad 11 \cdot 4 = 14 \qquad 11 \cdot 8 = 13$$

Tím jsou vygenerovány všechny prvky $\mathbb{Z}_{15}^*$ a můžeme zapsat:

$$\mathbb{Z}_{15}^* = \langle 2, 11 \rangle$$

Jsou necyklické grupy vůbec nějaké aditivní grupě izomorfní, a pokud ano, tak jaké? Pokusme se najít příklad konkrétního izomorfismu $\mathbb{Z}_{15}^*$ stejným způsobem, jako pro $\mathbb{Z}_7^*$, tedy pomocí mocnin generátorů. Tímto způsobem ovšem nelze každý prvek zobrazit na jediný prvek, nýbrž na dva, přesněji na dvojici. 11 nabývala své nulté a první mocniny a 2 své nulté až třetí mocniny. Všimněme si, že $\{0, 1\}$ jsou všechny prvky $\mathbb{Z}_2$ a $\{0, 1, 2, 3\}$ jsou všechny prvky $\mathbb{Z}_4$. Tyto dvě grupy tedy spojíme do jedné pomocí operace, kterou si definujeme.

Definice 20 (Direktní součin grup; *Direct product*)

Nechť $G_1, G_2, \dots, G_n$ jsou grupy. Direktním součinem těchto grup rozumíme grupu $G_1 \times G_2 \times \dots \times G_n$, jejíž prvky jsou n-tice tvořené kartézským součinem nosných množin původních grup. V nové grupě provádíme operace po složkách tak, jak byly definovány v původních grupách.

Máme tedy:

$$\mathbb{Z}_{15}^{*} \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

Znázorněme tabulkou:

$\mathbb{Z}_{15}^{*}$	1	2	4	7	8	11	13	14
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$(0,0)$	$(1,1)$	$(0,2)$	$(0,1)$	$(1,3)$	$(1,0)$	$(0,3)$	$(1,2)$

Tab. 17: Izomorfismus $\mathbb{Z}_{15}^{*} \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

Protože je izomorfismus bijektivní, tedy funguje „na obě strany“, lze z předchozích pozorování odvodit, že $\mathbb{Z}_2 \cong \mathbb{Z}_3^{*}$ a $\mathbb{Z}_4 \cong \mathbb{Z}_5^{*}$ a tím pádem tedy:

$$\mathbb{Z}_{15}^{*} \cong \mathbb{Z}_3^{*} \times \mathbb{Z}_5^{*}$$

což koresponduje s faktem, že $15 = 3 \cdot 5$. To hledání izomorfismu složených čísel zjednodušuje, stačí využít prvočíselného rozkladu. Tento konkrétní izomorfismus $\mathbb{Z}_2 \times \mathbb{Z}_4 \cong \mathbb{Z}_3^{*} \times \mathbb{Z}_5^{*}$ lze obdobně zkonstruovat zobrazením exponentu generátoru $\mathbb{Z}_3^{*}$ (tím je pouze prvek 2), respektive $\mathbb{Z}_5^{*}$ (zvolme také 2) na příslušnou mocninu generátoru. Rozšiřme tab. 17:

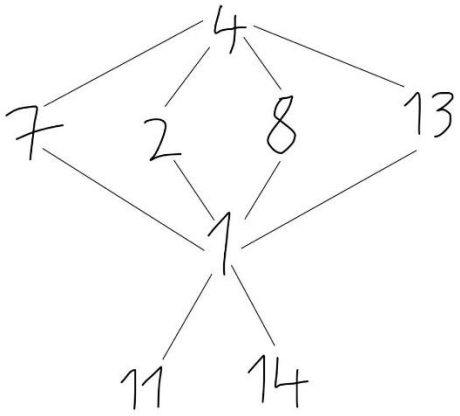
$\mathbb{Z}_{15}^{*}$	1	2	4	7	8	11	13	14
$\mathbb{Z}_3^{*} \times \mathbb{Z}_5^{*}$	$(1,1)$	$(2,2)$	$(1,4)$	$(1,2)$	$(2,3)$	$(2,1)$	$(1,3)$	$(2,4)$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$(0,0)$	$(1,1)$	$(0,2)$	$(0,1)$	$(1,3)$	$(1,0)$	$(0,3)$	$(1,2)$

Tab. 18: Izomorfismus $\mathbb{Z}_{15}^{*} \cong \mathbb{Z}_3^{*} \times \mathbb{Z}_5^{*} \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

Krátce demonstrujme, že se skutečně jedná o izomorfismus. Lze si na první pohled všimnout, že se neutrální prvek pokaždé zobrazil na neutrální prvek. Pozorujme inverzní prvky:

$$\mathbb{Z}_{15}^{*}: 2 \cdot 8 = 1$$
$$\mathbb{Z}_3^{*} \times \mathbb{Z}_5^{*}: (2,2) \cdot (2,3) = (1,1)$$
$$\mathbb{Z}_2 \times \mathbb{Z}_4: (1,1) + (1,3) = (0,0)$$

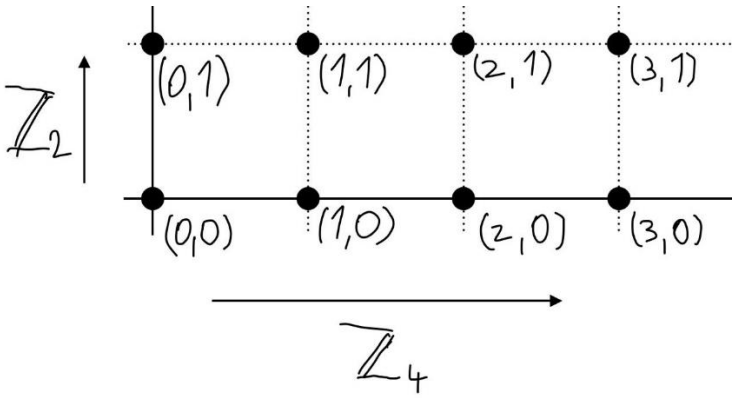
Tuto grupu také znázorněme i obrázkem. V tomto případě nemáme grupu cyklickou, ale z pozorovaní řádů prvků si lze jistých menších cyklů všimnout. Jednou možností je obrázek, ze kterého jsou tyto cykly zřejmé:



Obr. 13: Struktura $\mathbb{Z}_{15}^{*}$.

V obr. 13 je centrem obrázku 1. Z ní vycházejí ostatní prvky a jsou jasně vidět jejich řády a také, které prvky vygeneruje každý prvek sám. Také lze z obrázku nahlédnout, že právě $1, 11, 14$ a 4 jsou Fermatovými lháři pro 15. Všechny se nachází na „kratších“ cyklech. Ostatní prvky jsou Fermatovými svědky.

Druhou možností je souřadnicová reprezentace:



Obr. 14: Souřadnicová reprezentace $\mathbb{Z}_{15}^{*} \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

V té sčítání složek (které je izomorfní násobení prvků) funguje jako posouvání po daných osách o daný počet pozic.

Pozorujme blíže grupu $\mathbb{Z}_8^*$, abychom dosáhli hlubšího porozumění i druhému „typu“ necyklické grupy. Tuto grupu lze také vygenerovat dvěma prvky, těmi jsou 3 a 5, protože $3^2 = 5^2 = 1$ a $3 \cdot 5 = 7$. Oba prvky nabývají své nulté a první mocniny, $\{0, 1\}$ jsou prvky $\mathbb{Z}_2$, grupa bude tedy izomorfní grupě:

$$\mathbb{Z}_2 \times \mathbb{Z}_2$$

Znázorněme tabulkou:

$\mathbb{Z}_8^*$	1	3	5	7
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$(0, 0)$	$(1, 0)$	$(0, 1)$	$(1, 1)$

Tab. 19: Izomorfismus $\mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Zde pozorovaná struktura je poměrně unikátní. Již jsme vypozorovali, že všechny prvky jsou řádu 2. Také jsme vypozorovali, že $3 \cdot 5 = 7$. Protože jsou všechny prvky samy sobě inverzní, tak z tohoto jednoduše plyne, že $7 \cdot 3 = 5$ a $7 \cdot 5 = 3$. Tedy operací s libovolnými dvěma prvky vždy dostaneme ten třetí, který není neutrální. Grupa s takovouto strukturou se nazývá *Kleinova čtyřgrupa (Klein four-group)*. O ní více v (Katrnoška, 2009).

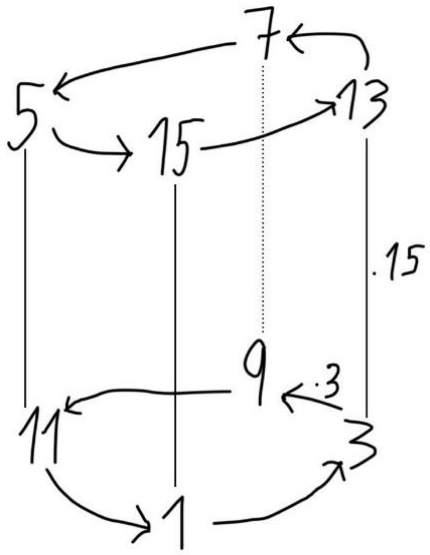
Příklad 46: Klasifikujte všechny grupy $\mathbb{Z}_n^*$ řádu 4 podle toho, zda jsou izomorfní $\mathbb{Z}_4$, nebo $\mathbb{Z}_2 \times \mathbb{Z}_2$ (Kleinově čtyřgrupě).

Řešení: Hledáme grupy $\mathbb{Z}_n^*$ s $\varphi(n) = 4$. Jednou je očividně $\mathbb{Z}_5^*$ a tím pádem i $\mathbb{Z}_{10}^*$. 4 je mocninou dvojky, takže jako hodnotu Eulerovy funkce ji můžeme získat z vyšší mocniny dvojky, konkrétně $\varphi(8)$ pro grupu $\mathbb{Z}_8^*$. Také ale $4 = 2 \cdot 2$. Platí $\varphi(3) = 2$, tím ale nemůžou být oba součinitele, protože pak by se jednalo o mocninu trojky, která se vyčísluje jinak. Dvojku jako hodnotu Eulerovy funkce lze jinak získat už jen ze 4, posledním n je tedy $3 \cdot 4 = 12$ a poslední takovou grupou je $\mathbb{Z}_{12}^*$. Pro jejich rozřazení stačí rozhodnout, které jsou cyklické, takže musíme vyčíslit $\lambda(n)$. Pokud $\lambda(n) = 4$, pak je grupa izomorfní $\mathbb{Z}_4$, pokud $\lambda(n) = 2$, pak je izomorfní $\mathbb{Z}_2 \times \mathbb{Z}_2$. $\lambda(5) = \lambda(10) = 4$ a $\lambda(8) = \lambda(12) = 2$. Takže:

$$\mathbb{Z}_5^* \cong \mathbb{Z}_{10}^* \cong \mathbb{Z}_4$$

$$\mathbb{Z}_8^* \cong \mathbb{Z}_{12}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Dále zkoumejme grupu $\mathbb{Z}_{16}^*$. Ta je řádu 8, ale $\lambda(16) = 4$. Její prvky tedy nabývají nejvýše řádu 4. Triviálně $15^2 = (-1)^2 = 1$, takže stačí naleznout prvek řádu 4 pro vygenerování celé grupy. Z důkazu Carmichaelovy věty vyplývá, že pro každou grupu $\mathbb{Z}_{2^k}^*$ bude prvkem maximálního možného řádu prvek 3. Ten si tedy zvolme jako druhý generátor a znázorněme obrázkem:



Obr. 15: Struktura $\mathbb{Z}_{16}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

Z obr. 15 lze nahlédnout, že se v $\mathbb{Z}_{16}^*$ nachází 2 cykly o 4 prvcích, jedna čtveřice je generovaná prvkem 3, druhá prvkem $-3 = -1 \cdot 3 = 15 \cdot 3 = 13$, takže:

$$\mathbb{Z}_{16}^* = \langle 3, 15 \rangle$$

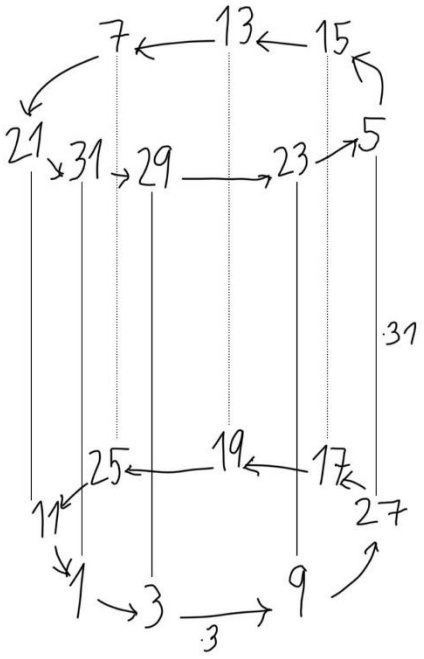
Lze opět sestrojit izomorfismus pomocí mocnin, kterých generátory nabývají, kde začínáme od 0. Pro 15 je to jen 0 nebo 1, prvek 3 nabývá až své třetí mocniny. Z toho vyplývá:

$$\mathbb{Z}_{16}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

Před úplným zobecněním nahlédněme ještě grupu $\mathbb{Z}_{32}^*$, kde je situace obdobná. Řád grupy je 16, ale hodnota $\lambda(16) = 8$. Jedním z generátorů je $-1 = 31$, druhým je opět 3. Analogicky tedy platí:

$$\mathbb{Z}_{32}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_8$$

Znovu ilustrujme obrázkem:



Obr. 16: Struktura $\mathbb{Z}_{32}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_8$.

Situace s izomorfismy $\mathbb{Z}_{2^k}^*$ se již zdá poměrně jasná. Jak ji ale odůvodnit? Řád takové grupy je $\varphi(2^k) = 2^{k-1}$ a $\lambda(2^k) = 2^{k-2}$, stačí tedy umět obecně nalézt v každé takové grupě prvek řádu 2 a prvek řádu 2^{k-2} a ty budou generátory. Nalezení prvku řádu 2 je triviální, vždy $(-1)^2 = 1$. Řádu 2^{k-2} je dle důkazu Carmichaelovy věty vždy prvek 3. Tuto grupu lze tedy pokaždé vygenerovat dvěma generátory: $\{3, 2^k - 1\}$. Všechna tato pozorování konkrétních izomorfismů shrňme a zobecněme.

Věta 5 (Struktura $\mathbb{Z}_n^*$)

(1) pro p prvočíslo; pro $\mathbb{Z}_{2p}^*$ p liché prvočíslo: $\mathbb{Z}_p^* \cong \mathbb{Z}_{2p}^* \cong \mathbb{Z}_{p-1}$

(2) pro p liché prvočíslo a $k \in \mathbb{N}$: $\mathbb{Z}_{p^k}^* \cong \mathbb{Z}_{2p^k}^* \cong \mathbb{Z}_{p^{k-1}} \times \mathbb{Z}_{p-1} \cong \mathbb{Z}_{p^{k-1}\cdot(p-1)}$

(3) pro $k \in \mathbb{N}, k \geq 3$: $\mathbb{Z}_{2^k}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$

(4) $\mathbb{Z}_4^* \cong \mathbb{Z}_2$

(5) pro $m, n \in \mathbb{N}; D(m,n) = 1$: $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$

Důkaz: (4) lze konkrétně, pro (1) a (2) existuje izomorfismus pomocí mocnin generátoru. Pro (3) jsou dvěma generátory $\{3, 2^k - 1\}$, 3 je řádu 2^{k-1} a $2^k - 1$ řádu 2, izomorfismus je opět podle mocnin těchto generátorů. (5) plyne z ČVZ.

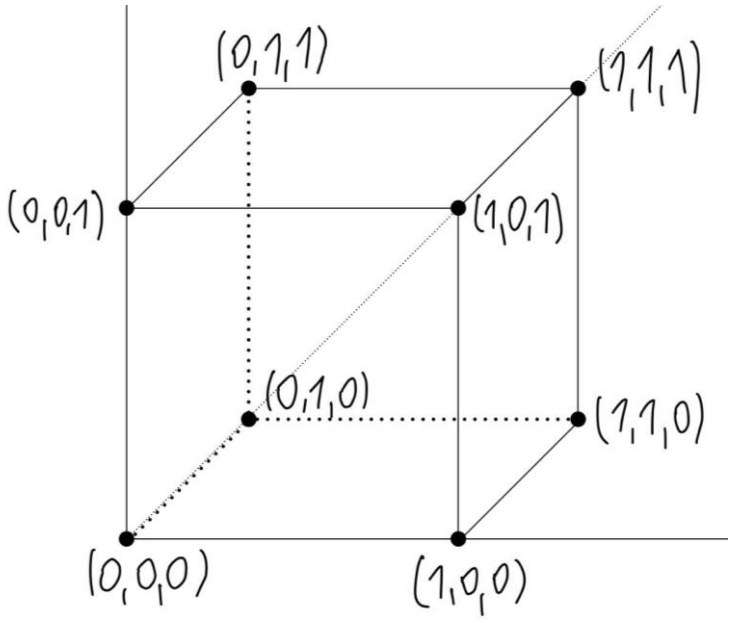
Pozn.: Grupy $\mathbb{Z}_1^*$ a $\mathbb{Z}_1$ jsou triviální a o struktuře grup, které jsou izomorfní nějakému direktnímu součinu grup $\mathbb{Z}_n^*$, mezi nimiž je i $\mathbb{Z}_2^*$ nám nic nového neříkají. Proto pokud se zajímáme o izomorfismy, v direktním součinu grup $\mathbb{Z}_n$ grupu $\mathbb{Z}_1$ nezohledňujeme a proto jsou např. grupy $\mathbb{Z}_p^*$ a $\mathbb{Z}_{2p}^*$ vždy izomorfní.

Příklad 47: Popište strukturu grupy $\mathbb{Z}_{24}^*$ pomocí izomorfismů.

Řešení: Nejdříve určeme prvočíselný rozklad $24 = 2^3 \cdot 3$. Tím pádem:

$$\mathbb{Z}_{24}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Z toho lze i bez určování $\varphi(24)$ určit, jaký je řád grupy $\mathbb{Z}_{24}^*$. Tím je $2 \cdot 2 \cdot 2 = 8$. Zároveň lze obdobně určit největší možný řád prvků grupy, tím je 2. Tato grupa je izomorfní grupě tvořené direktním součinem tří cyklických grup. Jak si ji představit? Nabízí se opět souřadnicová reprezentace:



Obr. 17: Souřadnicová reprezentace $\mathbb{Z}_{24}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Podotkněme, že znalosti izomorfismu je struktura grupy jasná a obr. 17 lze sestavit i bez znalosti konkrétních tří generátorů.

Příklad 48: Rozšiřme předchozí příklad. Určete, které všechny grupy $\mathbb{Z}_n^*$ jsou řádu 8 a které z nich jsou izomorfní: $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ nebo $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Řešení: Hodnotu $\varphi(n) = 8$ lze získat součiny mocnin dvojky s $\varphi(3) = 2$ a $\varphi(5) = 4$. Grupy $\mathbb{Z}_n^*$ řádu 8 jsou tedy $\mathbb{Z}_{15}^*, \mathbb{Z}_{16}^*, \mathbb{Z}_{20}^*, \mathbb{Z}_{24}^*$ a $\mathbb{Z}_{30}^*$. Z prvočíselných rozkladů příslušných n a pravidel pro $\mathbb{Z}_{2^k}^*$:

$$\mathbb{Z}_{16}^* \cong \mathbb{Z}_8$$

$$\mathbb{Z}_{15}^* \cong \mathbb{Z}_{20}^* \cong \mathbb{Z}_{30}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

$$\mathbb{Z}_{24}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Závěr

Jako cíl této práce jsem formuloval snahu shrnout poznatky o polynomiálních a exponenciálních kongruencích a strukturálním pohledu na ně, v rozsahu užitečném pro předmět Teorie čísel a zároveň pokud možno intuitivním a srozumitelným způsobem. Dle mého pohledu jsem tento cíl splnil. V práci je kompletní popis metod určování kvadratických zbytků a nezbytků i řešení kvadratických kongruencí pro jakýkoliv modul. Dále v ní lze nalézt různá využití malé Fermatovy věty, Eulerovy věty a Carmichaelovy funkce a je nastíněna i intuice za nimi. Posledním, co práce nabízí, je intuitivní a čtenářsky přístupný popis algebraické struktury množin zbytků po dělení.

Rezervou by mohlo být to, že v některých částech jsem odkazoval v práci dopředu a výklad není striktně chronologický. Zároveň by v práci mohly být i neřešené úlohy k procvičení a třetí kapitola by mohla být podrobnější. Práce by pak ale nabrala obřích rozměrů.

Jako velký přínos této práce, oproti jiným pracím na dané téma, vidím podrobnější popis řešení některých typů kvadratických kongruencí a elementárnější důkaz výpočtu hodnot Carmichaelovy funkce. Také bych vyzdvihl obrázky v této práci, které ukazují, jak si představit strukturu některých cyklických i necyklických grup.

Seznam použitých informačních zdrojů

ALFORD, W. R., GRANVILLE, A. & POMERANCE, C. (1994). There are infinitely many Carmichael numbers. *Annals of Mathematics*, *140*(3), 703-722. DOI: 10.2307/2118576

CARMICHAEL, R. D. (1914). *The theory of numbers*. John Wiley & Sons. https://gutenberg.org/files/13693/13693-pdf.pdf

DICKSON, L. E. (1920). *History of the theory of numbers: Diophantine analysis*. Carnegie Institution of Washington. https://ia801607.us.archive.org/15/items/historyoftheoryo02dickuoft/historyoftheoryo02dickuoft.pdf

GAUSS, C. (1801). *Disquisitiones Arithmeticae*. DOI: 10.5479/sil.324926.39088000932822

GAUSS, C. (1986). *Disquisitiones Arithmeticae*. Springer. DOI: 10.1007/978-1-4939-7560-0

GOLOMB, S. W. (1956). Combinatorial proof of Fermat's "little" theorem. *The American Mathematical Monthly*, *63*(10), 718. https://www.jstor.org/stable/2309563?origin=JSTOR-pdf

GRAY, J. (2018). *A history of abstract algebra: From algebraic equations to modern algebra*. Springer. DOI: 10.1007/978-3-319-94773-0

KAŇÁKOVÁ, N. (2022). *Lineární diofantické rovnice a kongruence* [Bakalářská práce, Univerzita Karlova]. https://dspace.cuni.cz/bitstream/handle/20.500.11956/175503/130341603.pdf

KATRNOŠKA, F. & KŘÍŽEK, M. (2009). Kleinova čtyřgrupa. *Rozhledy matematicko-fyzikální, 84*(4), 4-9. DML-CZ - Czech Digital Mathematics Library: Kleinova čtyřgrupa

KŘÍŽEK, M., SOMER, L. & ŠOLCOVÁ, A. (2018). *Kouzlo čísel: od velkých objevů k aplikacím* (3. vydání). Academia.

LEGENDRE A.-M. (1798). *Essai sur la Théorie des Nombres*. DOI: 10.1017/CBO9780511693199

LEMMERMEYER, F. (2013). Václav Šimerka: quadratic forms and factorization. *LMS Journal of Computation and Mathematics*, *16*, 118-129. DOI: 10.1112/S1461157013000065

Online encyclopedy of integer sequences. https://oeis.org/

SILVERMAN, J. H. (2012). *A friendly introduction to number theory* (4th edition). Pearson Education. https://www.math.brown.edu/johsilve/frint.html

STANOVSKÝ, D. (2022). *Algebra* [online]. https://www.karlin.mff.cuni.cz/~stanovsk/vyuka/2122/algebra22.pdf

STAŠKO, S. (2019). *Kubická a bikvadratická reciprocita* [Bakalářská práce, Univerzita Karlova]. https://dspace.cuni.cz/bitstream/handle/20.500.11956/107673/130255711.pdf

VOLKANER, H. D. (2011). *Euler's criterion for n:th power residues*. https://www.diva-portal.org/smash/get/diva2:421340/FULLTEXT01.pdf

The math less travelled. (2019). *Fermat witnesses and liars*. https://mathlesstraveled.com/2019/01/18/fermat-witnesses-and-liars-some-words-on-pww-24/