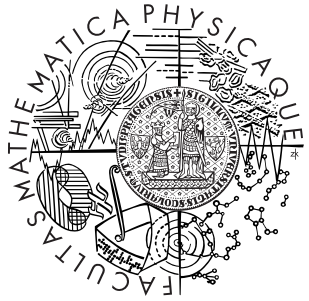
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Gabriela Těthalová

Cyklotomické polynomy

Katedra algebry

Vedoucí bakalářské práce: Dr. Libor Barto
Studijní program: Matematika
Obecná matematika

2010

Děkuji Mgr. Liboru Bartovi, Ph.D. za pomoc při psaní této práce, zejména za jeho čas, který ochotně věnoval přínosným konzultacím.

Prohlašuji, že jsem svou bakalářskou práci napsala samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne 28. července 2010 Gabriela Těthalová

Obsah

Název práce: Cyklotomické polynomy
Autor: Gabriela Těthalová
Katedra (ústav): Katedra algebry
Vedoucí bakalářské práce: Mgr. Libor Barto, Ph.D.
e-mail vedoucího: libor.barto@gmail.com

Abstrakt: Obsahem této práce jsou řešená cvičení týkající se cyklotomických polynomů. Úlohy se většinou věnují dané problematice nad konečnými tělesy. Předvedeny jsou jak některé početní příklady, jako nalezení primitivních n-tých odmocnin z jedné nebo spočítání či rozklad n-tého cyklotomického polynomu, tak i důkazy vybraných vlastností cyklotomických polynomů. Dva užitečné vzorce jsou dokázány dvojím způsobem, podle definice n-tého cyklotomického polynomu a s využitím Möbiovy inverzní formule. Důležitou součástí této práce je i soupis potřebných teoretických výsledků, které při řešení cvičení používáme. Jde většinou o poznatky z konečných těles a teorie čísel.
Klíčová slova: Cyklotomické polynomy, primitivní odmocnina z jedné, konečné těleso

Title: Cyclotomic polynomials
Author: Gabriela Těthalová
Department: Department of Algebra
Supervisor: Mgr. Libor Barto, Ph.D.
Supervisor's e-mail address: libor.barto@gmail.com

Abstract: The thesis consists of exercises regarding cyclotomic polynomials. The exercises discussed deal mostly with problems over finite fields. Examples of arithmetical problems such as determining the primitive nth root of unity or calculation and decomposition of the nth cyclotomic polynomial are provided, as well as proofs of selected characteristics of cyclotomic polynomials. Two useful formulas are both proved in two ways: first, according to the definition of the nth cyclotomic polynomial; secondly, by an application of the Moebius Inversion Formula. The thesis also contains a list of needed theoretical results which were used as the basis of the exercises discussed. These are mostly findings concerning finite fields and number theory.

Keywords: Cyclotomic polynomials, primitive nth root of unity, finite field

Kapitola 1

Úvod

Co jsou to cyklotomické polynomy, jak definujeme cyklotomické těleso a primitivní odmocniny z jedné, jakým způsobem lze cyklotomické polynomy spočítat a co víme o jejich vlastnostech, to jsou jen některé otázky, na něž odpovědět je smyslem této práce. Proč se těmito záležitostmi zabývat a jak k problematice přistupovat?

1.1 Motivace

Cyklotomické polynomy mezi řadou matematických pojmů jistě nezaujmou pouze pozoruhodným názvem. Tyto poutavé úkazy nad konečnými tělesy právem budí zvědavost. My se na ně nyní podíváme zblízka. Přiblížíme definice, důležité termíny a nastíníme hlavní rysy teorie cyklotomických polynomů a cyklotomických těles v matematických větách, ale především v poučných příkladech a cvičeních, jež tvoří jádro této práce.

Definice, výpočty nebo ukazování na zajímavé vlastnosti cyklotomických polynomů spolu propojují některé poznatky z teorie čísel a nauky o konečných tělesech. Je tedy přirozené dívat se na danou problematiku z několika různých úhlů a pokoušet se v důkazech některých cvičení uplatnit vícero různých postupů. V této souvislosti nelze nezmínit Möbiovu inverzní formuli, již jsme si pro tuto příležitost vypůjčili z kombinatoriky. Uvidíme, že nám většinou velice usnadní počítání.

Navíc, věnovat pozornost cyklotomickým polynomům a primitivním odmocninám z jedné se velice vyplatí, neboť tyto poznatky můžeme dále uplatnit v jiných oborech. Studenti příslušných zaměření s nimi například přišli do styku v kurzech pokrývajících témata jako rychlá Fourierova transformace

nebo cyklické kódy.

Na závěr ještě jeden důvod proč se pouštět do počítání příkladů a ověřování vztahů mezi různými typy cyklotomických polynomů. Zadání příkladů jsou převzata ze skript Mgr. Libora Barta, Ph.D. a Doc. RNDr. Jiřího Tůmy, DrSc "Konečná tělesa" (viz Literatura). Autoři do budoucna počítají s jejich rozšířením a vydáním. Tato plánovaná verze bude obsahovat vyřešená cvičení, což budoucím čtenářům usnadní pochopení výkladu. Některá z těchto řešení mohou být převzata z této práce.

1.2 Cíl

Nyní se podívejme konkrétně na obsah této práce. Jak již bylo zmíněno výše, hlavním cílem je vyřešit vybraná cvičení dle [2]. Mezi nimi jsou příklady jak početní, tak teoretické, ve kterých se většinou zkoumají vztahy mezi n-tými cyklotomickými polynomy pro různá n.

Přirozeně začneme seznámením s potřebnou teorií. Nejvíce prostoru věnujeme partiím, které byly volně převzaty z [2] nebo z [1]. Přesněji řečeno, pokud bude použito doslovné znění vět, tvrzení a definic, bude vždy uvedeno odkud pochází. V případě, že bude vyložen důkaz, bude psán dle předlohy v [2], ovšem přeformulován.

Zadání příkladů se shodují se cvičeními v [2]. Ukážeme si, jak spočítat n-tý cyklotomický polynom využitím rozkladu polynomu $x^n - 1$. Tento polynom hraje klíčovou roli v teorii cyklotomických polynomů a cyklotomických těles vůbec, neboť jeho kořeny jsou zřejmě n-té odmocniny z jedné a n-té cyklotomické těleso není nic jiného než rozkladové rozšíření nějakého tělesa $\mathbf{K}$ dané právě polynomem $x^n - 1$ z $\mathbf{K}[x]$. Dále se podíváme na primitivní n-té odmocniny z jedné, budeme zkoumat vlastnosti n-tých cyklotomických polynomů jako je rozložitelnost nebo nerozložitelnost nad konečným tělesem, vyšetříme jejich koeficienty nebo spočítáme některé hodnoty v zajímavých bodech pro různá n. Na závěr dokážeme několik dalších vlastností cyklotomických polynomů.

Zde jsme si tedy zhruba vymezili pole působnosti a osvětlili hlavní myšlenku této práce. Následuje již formální text, jenž nám poskytne potřebnou teoretickou průpravu.

Kapitola 2

Teorie

2.1 Konečná tělesa

Abychom se mohli věnovat studiu cyklotomických polynomů, je nezbytné definovat n-té cyklotomické těleso. Připomeneme nejprve několik potřebných pojmů a tvrzení a zavedeme konečná tělesa.

Definice. Uvažujme libovolné těleso $\mathbf{T}$.

- $\mathbf{T}^*$ značí množinu všech invertibilních prvků z $\mathbf{T}$.
- Řád prvku a z $\mathbf{T}^*$ se značí $\mathrm{ord}(a)$ a je definován jako nejmenší přirozené číslo d takové, že $a^d = 1$ v $\mathbf{T}^*$.

Za povšimnutí stojí jednoduchý a užitečný fakt, který budeme používat, a sice: pokud pro $a \in \mathbf{T}^*$ je $a^l = 1$ v $\mathbf{T}^*$ pro nějaké l, platí $\mathrm{ord}(a) \mid l$. Dále je dobré si uvědomit, že v libovolném tělese jsou invertibilní všechny prvky kromě nulového prvku, tedy platí $\mathbf{T}^* = \mathbf{T} \setminus \{0\}$.

Následující větu využijeme při popisu struktury konečných těles.

Věta 2.1.1. *([4], Tvrz. 2.6) Každá konečná multiplikativní podgrupa komutativního tělesa je cyklická.*

Nejčastěji budeme počítat v konečných tělesech. Podívejme se tedy podrobněji na jejich charakterizaci.

Nejprve ukážeme, jak vypadá mocnění prvků v tělese charakteristiky p.

Lemma 2.1.2. *([2], Lemma* 2.5.*) Nechť* $\mathbf{F}$ *je těleso charakteristiky* $p > 0$. *Pak pro libovolné* $a, b \in \mathbf{F}$ *a libovolné přirozené číslo* $k > 0$ *platí*

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}.$$

Dále se hodí připomenout, jak vypadá rozkladové rozšíření tělesa, tj. rozšíření, ve kterém se nějaký daný polynom rozkládá na lineární činitele. Před tím zmíníme jednu pomocnou definici.

Definice. ([2], Kap. 2) Nechť $\mathbf{F}$ je těleso, $\mathbf{K} \leq \mathbf{F}$ a $\alpha_1, \ldots, \alpha_n \in \mathbf{F}$. Nejmenší podtěleso tělesa $\mathbf{F}$ (vzhledem k inkluzi), které obsahuje $\mathbf{K}$ a prvky $\alpha_1, \ldots, \alpha_n$, značíme $\mathbf{K}(\alpha_1, \ldots, \alpha_n)$.

Definice. ([2], Kap. 2) Nechť $\mathbf{K}$ je těleso, $f(x) \in \mathbf{K}[x]$. Rozšíření $\mathbf{E}$ tělesa $\mathbf{K}$ nazýváme *rozkladové rozšíření* tělesa $\mathbf{K}$ určené polynomem $f(x)$, pokud

- $\mathbf{K} \leq \mathbf{E}$,
- Polynom $f(x) \in \mathbf{E}[x]$ se v $\mathbf{E}$ rozkládá na součin lineárních činitelů, neboli $f(x) = l_c \cdot (x - \theta_1) \ldots (x - \theta_m)$, kde $\theta_1 \ldots \theta_m \in \mathbf{E}$ a l_c je vedoucí koeficient polynomu f a
- $\mathbf{K}(\theta_1 \ldots \theta_m) = \mathbf{E}$ (minimalita).

Buď nyní $\mathbf{F}$ konečné těleso s q prvky. Multiplikativní grupa obsažená v tělese $\mathbf{F}$, tj. grupa invertibilních prvků $(\mathbf{F}^*, \cdot, 1)$, má $q-1$ prvků a podle Věty 2.1.1 je cyklická. Z Lagrangeovy věty musí řád každého prvku grupy $\mathbf{F}^*$ dělit $q-1$, a tedy pro všechna $a \in \mathbf{F}$ je $a^{q-1} = 1$, neboli $a^q = a$ (což pro $a = 0$ zřejmě platí).

Z minulého odstavce pro každé $a \in \mathbf{F}$ máme $a^q - a = 0$. Z tohoto důvodu jsou všechna $a \in \mathbf{F}$ kořeny polynomu $x^q - x$, a proto $(x - a) \mid (x^q - a)$. Pro různá a jsou ale polynomy $(x - a)$ po dvou nesoudělné, a tedy

$$\prod_{a \in \mathbf{F}} (x - a) \mid (x^q - x).$$

Stupeň obou polynomů je zřejmě q a vedoucí člen je v obou případech x^q. Díky tomu a z výše uvedeného dostáváme následující větu.

Věta 2.1.3. *([2], Kap. 2) Nechť* $\mathbf{F}$ *je konečné těleso s* q *prvky. Potom platí následující rovnost polynomů z* $\mathbf{F}[x]$*:*

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

Dále připomeneme velice důležitou větu popisující podobu a vlastnosti konečných těles.

Věta 2.1.4. *([2], Kap. 2) (O existenci a jednoznačnosti konečných těles). Každé konečné těleso má* p^n *prvků, kde* p *je prvočíslo a* n *je přirozené číslo.*

Pro každé prvočíslo p *a přirozené číslo* n *existuje těleso s* $q = p^n$ *prvky.*

Libovolná dvě tělesa s p^n *prvky jsou izomorfní (a jsou izomorfní rozkladovému rozšíření tělesa* $\mathbb{Z}_p$ *určeného polynomem* $x^q - x \in \mathbb{Z}_p[x]$*).*

Definice. ([2], Kap. 2) Těleso s q prvky značíme $\mathbf{F}_q$.

Podívejme se nyní na situaci, kdy q je prvočíslo. Potom je $\mathbb{Z}_q$ těleso a ${\mathbb{Z}^*}_q$ cyklická grupa řádu $q - 1$. V tom případě z charakterizace cyklických grup dostáváme ${\mathbb{Z}^*}_q(\cdot) \simeq \mathbb{Z}_{q-1}(+)$.

Z Věty 2.1.4 jsou každá dvě tělesa se shodným počtem prvků izomorfní. Pro q prvočíslo tedy platí, že $\mathbf{F}_q \simeq \mathbb{Z}_q$, protože obě tato tělesa mají q prvků. Dohromady z předchozích úvah vyplyne následující důsledek.

Důsledek 2.1.5. *Nechť* $\mathbf{F}_q$ *je těleso, kde* q *je prvočíslo. Potom platí*

$$\begin{aligned} {\mathbf{F}^*}_q(\cdot) &\simeq \mathbb{Z}_{q-1}(+) \\ a^k &\to k, \end{aligned}$$

kde a *je libovolný generátor grupy* ${\mathbf{F}^*}_q$*.*

Tento izomorfismus využijeme ve cvičeních. Postup předvedeme na výpočtu primitivních n-tých odmocnin z jedné poté, co tento pojem definujeme.

Definice. Buď $\mathbf{T}$ libovolné těleso. Řekneme, že prvek ξ z $\mathbf{T}$ je primitivní n-tá odmocnina z 1, pokud $\mathrm{ord}(\xi) = n$ v $\mathbf{T}^*$.

Pokud je $\mathrm{ord}(\xi) = n$, platí jistě také $\mathrm{ord}(\xi^s) = n$ pro $\mathrm{NSD}(s, n) = 1$. Pro dané n tedy existuje $\varphi(n)$ primitivních n-tých odmocnin z jedné, kde φ je Eulerova funkce.

Příklad 1. Určete primitivní čtvrté odmocniny z jedné v tělese $\mathbf{F}_{17}$.

Řešení. Máme $n = 4$, $q = 17$. Podle Důsledku 2.1.5 je multiplikativní grupa $\mathbf{F}^*{}_{17}$ řádu 16, a tedy všechny invertibilní prvky tělesa $\mathbf{F}_{17}$ mají řád $1, 2, 4, 8$ nebo 16. Nejprve nalezneme generátor $\mathbf{F}^*{}_{17}$, tj. takové a, pro které platí $\mathrm{ord}(a) = 16$ v $\mathbf{F}^*{}_{17}$. Zkusme položit $a = 3$. Musíme ověřit, že a nemá řád nižší než 16, tzn. $\mathrm{ord}(a) \neq 1, 2, 4, 8$. Stačí ukázat, že $3^8 \not\equiv 1 \pmod{17}$, neboli že řád trojky není dělitelný osmi: $3^8 \equiv 3^4 \cdot 3^4 \equiv (-4)^2 \equiv -1 \pmod{17}$. Tedy trojka je primitivní prvek modulo 17.

Prvek řádu čtyři v grupě $\mathbb{Z}_{16}(+)$ je například čtyřka. Z Důsledku 2.1.5 plyne, že hledaný prvek řádu čtyři je $3^4 \equiv -4 \pmod{17}$. Protože $\varphi(4) = 2$, existuje ještě jeden takový prvek, a to $(-4)^3 \equiv 4 \pmod{17}$, neboť $\mathrm{NSD}(3, 4) = 1$. Celkem tedy v tělese $\mathbf{F}_{17}$ existují dvě primitivní čtvrté odmocniny z jedné, a jsou to prvky 4 a -4.

K primitivním n-tým odmocninám z jedné se ještě později vrátíme, až budeme definovat n-té cyklotomické těleso, a uvedeme tento pojem do dalších souvislostí.

Poznámka. Ještě se pro úplnost zmíníme o konečných tělesech $\mathbf{F}_q$ pro $q = p^n$, tj. o tělesech s počtem prvků rovných mocnině prvočísla. Konstrukce takových konečných těles se provádí pomocí ireducibilního polynomu stupně n ze $\mathbb{Z}_p[x]$ a příslušného rozkladového rozšíření tělesa $\mathbb{Z}_p$.

Například těleso $\mathbf{F}_{27} = \mathbf{F}_{3^3}$ je rozkladovým rozšířením tělesa $\mathbb{Z}_3$ určené ireducibilním polynomem $x^3 + 2x + 1 \in \mathbb{Z}_3[x]$.

Nakonec uvedeme tvrzení o vlastnosti Eulerovy funkce, které později využijeme.

Tvrzení 2.1.6. *([4], Kap. 2.5) Pro každé $n \geq 1$ je $n = \sum_{d|n} \varphi(d)$.*

2.2 n-té cyklotomické těleso a n-tý cyklotomický polynom

Jak již bylo nastíněno v úvodu, bude pro nás nyní důležitý polynom $x^n - 1$. Mimo jiné se teď podíváme na to, kde a jak se tento polynom rozkládá.

Kořeny polynomu $x^n - 1$ jsou zřejmě n-té odmocniny z jedné. Kde tyto kořeny leží? Tato otázka vede k definici n-tého cyklotomického tělesa.

Definice. ([2], Kap. 4) Buď $\mathbf{K}$ libovolné těleso.

- Symbolem $\mathbf{K}^{(n)}$ označme rozkladové rozšíření tělesa $\mathbf{K}$ určené polynomem $x^n - 1$ z $\mathbf{K}[x]$. Toto rozkladové rozšíření nazveme n-té cyklotomické těleso nad $\mathbf{K}$.
- Množina všech n-tých odmocnin z jedné, tj. kořenů $x^n - 1$ v $\mathbf{K}^{(n)}$, se značí $\mathbf{E}^{(n)}$.

Uvažujme nyní $n > 0$ a $\mathbf{K}$ těleso charakteristiky p, kde $p \nmid n$. Podívejme se na derivaci polynomu $x^n - 1 \in \mathbf{K}[x]$: $(x^n - 1)' = (n \mod p)x^{n-1}$. Ale $p \nmid n$, a tedy $n \not\equiv 0 \pmod p$ a jediný kořen $(x^n - 1)'$ je nula. Z toho dostáváme, že $\mathrm{NSD}(x^n - 1, (x^n - 1)') = 1$, a proto kořeny $x^n - 1$ jsou v $\mathbf{K}^{(n)}$ jednoduché a navzájem různé (je jich právě n) a platí:

$$x^n - 1 = \prod_{\xi \in \mathbf{E}^{(n)}} (x - \xi).$$

Pro $p \mid n$, kde $n = p^l m,\ p \nmid m$, platí $x^n - 1 = (x^m - 1)^{p^l}$. Tato rovnost nám dává, že kořeny polynomu $x^n - 1$, leží v $\mathbf{E}^{(m)}$ a násobnost každého z nich je p^l, a $\mathbf{K}^{(n)} = \mathbf{K}^{(m)}$ ([2], Věta 4.1.).

V souvislosti s definicí n-tého cyklotomického tělesa můžeme říci, že ξ, libovolná primitivní n-tá odmocnina z jedné nad tělesem $\mathbf{K}$ charakteristiky $p,\ p \nmid n$, je generátor $\mathbf{E}^{(n)}$. To znamená, že $\mathbf{E}^{(n)} = \{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$. Všechny generátory $\mathbf{E}^{(n)}$ neboli primitivní n-té odmocniny z 1 jsou tvaru $\{\xi^s,\ \mathrm{NSD}(s, n) = 1\}$, jejich počet je $\varphi(n)$.

Každá n-tá odmocnina z 1 je zároveň i primitivní d-tá odmocnina z 1 pro nějaké $d \mid n$. Pokud je ξ primitivní n-tá odmocnina z jedné, mají všechny primitivní d-té odmocniny z jedné, kde $d \mid n$, tvar $\left\{\xi^{\frac{kn}{d}} :\ \mathrm{NSD}(k, d) = 1\right\}$.

Poté, co jsme si definovali n-té cyklotomické těleso a ujasnili si vztahy mezi n-tými a primitivními n-tými odmocninami z jedné, navážeme s definicí n-tého cyklotomického polynomu.

Definice. ([2], Kap. 4) Nechť $\mathbf{K}$ je těleso charakteristiky p, $p \nmid n$. Potom polynom

$$Q_n(x) = \prod_{\xi \text{ je primitivní } \sqrt[n]{1} \text{ v } \mathbf{K}^{(n)}} (x - \xi)$$

se nazývá *n-tý cyklotomický polynom nad* $\mathbf{K}$.

Pokud tedy známe všechny primitivní n-té odmocniny z jedné v rozkladovém rozšíření $\mathbf{K}^{(n)}$ nějakého tělesa $\mathbf{K}$, můžeme n-tý cyklotomický polynom spočítat přímo z definice. Tento postup ovšem není nejpříhodnější a časem ukážeme lepší metodu. Nicméně ještě zmíníme vylepšení výše uvedeného vztahu vyplývající z úvah o primitivních odmocninách z jedné. Pro ξ, libovolnou primitivní n-tou odmocninu z jedné, totiž platí([2], Kap. 4):

$$Q_n(x) = \prod_{\substack{0 \le s < n \\ \mathrm{NSD}(s,n)=1}} (x - \xi^s),$$

a stupeň polynomu $Q_n(x)$ je zřejmě $\varphi(n)$.

Podívejme se, jak by se pomocí definice počítaly n-té cyklotomické polynomy v nějakém konkrétním případě.

Příklad 2. Zvolme těleso $\mathbf{F}_5$. Spočítejte první, druhý a čtvrtý cyklotomický polynom z $\mathbf{F}_5[x]$.

Řešení. Řád grupy $\mathbf{F}^*{}_5$ je podle Důsledku 2.1.5 roven čtyřem, a tedy v $\mathbf{F}_5$ existují první, druhé i čtvrté primitivní odmocniny z jedné.

Primitivní první odmocnina z 1 je evidentně jednička a primitivní druhá odmocnina z 1 je $-1 \equiv 4 \pmod 5$.

Nyní spočteme primitivní čtvrté odmocniny z 1. Primitivní prvek modulo 5, tj. prvek řádu 4, je dvojka, neboť $2^2 \equiv 4 \equiv -1 \pmod 5$. Tedy primitivní čtvrté odmocniny z jedné v $\mathbf{F}_5$ jsou prvky 2 a $2^3 \equiv 3 \pmod 5$, protože $\mathrm{NSD}(3,4) = 1$. Nakonec dostáváme:

$$Q_1(x) = x - 1 = x + 4$$
$$Q_2(x) = x + 1$$
$$Q_4(x) = (x-2)(x-3) = x^2 - 5x + 6 = x^2 + 1$$

V dalším příkladu si ukážeme, jak vypadají pojmy, jež jsme zavedli v této sekci v případě, že si za $\mathbf{K}$ zvolíme těleso racionálních čísel.

Příklad 3. Rozeberte situaci, pokud $\mathbf{K} = \mathbb{Q}$ a $n = 8$.

Řešení. V tomto případě bude n-té cyklotomické těleso podtělesem tělesa komplexních čísel. Všechny osmé odmocniny z 1 budou tvaru $e^{\frac{2\pi ik}{8}} = e^{\frac{\pi ik}{4}}$ pro $k \in \{1, 2, \ldots, 8\}$. Vidíme, že osmé odmocniny z 1 jsou vrcholy pravidelného osmiúhelníku vepsaného do jednotkové kružnice. Toto platí pro všechna n.

A jak vypadají primitivní osmé odmocniny z 1? Jedna primitivní osmá odmocnina z 1 je zřejmě prvek $e^{\frac{\pi i}{4}}$, neboť $\left(e^{\frac{\pi i}{4}}\right)^8 = e^{2\pi i} = 1$ a $\left(e^{\frac{\pi i}{4}}\right)^4 = e^{\pi i} = -1$. Proto všechny primitivní osmé odmocniny z 1 mají tvar $\left(e^{\frac{\pi i}{4}}\right)^s$, kde $\mathrm{NSD}(s, 8) = 1$.

Pro zajímavost se ještě podívejme na primitivní čtvrté odmocniny z 1. Jsou to právě $e^{\frac{\pi i}{2}} = i$ a $e^{\frac{-\pi i}{2}} = -i$. Snadno se tedy dá spočítat čtvrtý cyklotomický polynom:

$$Q_4(x) = (x - i)(x + i) = x^2 + 1.$$

Vraťme se ještě k polynomu $x^n - 1$. Nyní si ukážeme, jak se také dá rozložit, a dostaneme tak další způsob počítání cyklotomických polynomů.

Věta 2.2.1. *([2], Věta 4.2.) Nechť $\mathbf{K}$ je těleso charakteristiky $p, p \nmid n > 0$. Potom platí*

- $x^n - 1 = \prod_{d|n} Q_d(x)$
- *koeficienty $Q^n(x)$ leží v prvotělese tělesa $\mathbf{K}$. Je-li $p = 0$, pak koeficienty $Q_n(x)$ jsou celá čísla.*

Důkaz. V dřívějších úvahách o n-tých odmocninách z jedné jsme zmínili fakt, že každá n-tá odmocnina z jedné je zároveň primitivní d-tá odmocnina z jedné pro nějaké $d \mid n$. Této vlastnosti využijeme při rozkladu polynomu $x^n - 1$ na lineární činitele:

$$x^n - 1 = \prod_{\xi \text{ je } \sqrt[n]{1}} (x - \xi) = \prod_{d|n} \left(\prod_{\nu \text{ je primitivní } \sqrt[d]{1}} (x - \nu) \right) = \prod_{d|n} Q_d(x).$$

Podívejme se nyní koeficienty $Q_n(x)$. Předně připomeňme, že prvotěleso tělesa $\mathbf{K}$ je definováno jako nejmenší podtěleso $\mathbf{K}$. Dále použijeme indukci podle n. V případě $n = 1$ máme $Q_1(x) = x - 1$ a koeficienty $-1, 1$ jistě náleží do prvotělesa.

Předpokládejme, že věta platí pro všechna $d < n$ a přejděme k n-tému cyklotomickému polynomu. Ze vztahu ověřeného v předchozím odstavci dostaneme rovnost

$$Q_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} Q_d(x)}.$$

Čitatel má zjevně koeficienty v prvotělese a podle indukčního předpokladu i jmenovatel. Označme toto prvotěleso $\mathbf{P}$. Při dělení dvou polynomů s koeficienty v $\mathbf{P}$ budou koeficienty výsledného polynomu jistě ležet tamtéž. To plyne z podoby mezivýsledků v průběhu algoritmu pro dělení polynomů se zbytkem - jsou to opět polynomy s koeficienty v $\mathbf{P}$.

Nakonec se podívejme na $p = 0$. Koeficienty $Q_1(x) = x - 1$ jsou evidentně celočíselné. Opět uvažujme, že $Q_d(x)$ má celočíselné koeficienty pro každé $d < n$. Ze vztahu

$$Q_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} Q_d(x)}$$

a z indukčního předpokladu dostáváme, že polynom $Q_n(x)$ má také celočíselné koeficienty, neboť je výsledkem dělení monického celočíselného polynomu monickým celočíselným polynomem (a tedy všechny mezivýsledky jsou celočíselné polynomy). □

Právě dokázanou větu předvedeme na příkladu.

Příklad 4. Podívejme se, jak vypadá $Q_p(x)$, kde p je prvočíslo.

Řešení. Jistě $\deg(Q_p(x)) = \varphi(p) = p - 1$. Předchozí věta dává vztah $x^p - 1 = Q_1(x)Q_p(x)$, přičemž z definice máme $Q_1(x) = x - 1$. Tedy

$$Q_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1.$$

Poslední věta této sekce pojednává o struktuře n-tého cyklotomického tělesa, ale především, a to bude pro nás užitečnější, o způsobu, jakým se rozkládá n-tý cyklotomický polynom na ireducibilní činitele.

K pochopení důkazu je třeba připomenout, co je to algebraický prvek a jeho minimální polynom.

Definice. ([2], Kap. 3) Nechť $\mathbf{F} \leq \mathbf{E}$ jsou tělesa. Prvek $\alpha \in \mathbf{E}$ nazýváme *algebraický* nad $\mathbf{F}$, pokud je kořenem nějakého nenulového polynomu nad $\mathbf{F}$.

Definice. ([2], Kap. 3) Nechť $\mathbf{F} \leq \mathbf{E}$ jsou tělesa a α je algebraický prvek nad $\mathbf{F}$. Nenulový monický polynom $m(x) \in \mathbf{F}[x]$ nejmenšího stupně takový, že $m(x) = 0$, nazýváme *minimální polynom* prvku α nad $\mathbf{F}$.

Minimální polynom je ireducibilní a dělí všechny polynomy $f(x) \in \mathbf{F}[x]$ takové, že $f(\alpha) = 0$. Naopak, ireducibilní polynom $f(x) \in \mathbf{F}[x]$ je (po vydělením vedoucím koeficientem, aby byl monický) minimálním polynomem libovolného svého kořene.

Věta 2.2.2. *([2], Věta* 4.3.*) Buď* $\mathbf{K} = \mathbf{F_q}$ *těleso a* $\mathrm{NSD}(q, n) = 1$*. Nechť* d *je nejmenší kladné přirozené číslo takové, že* $q^d \equiv 1 \pmod{n}$*. Potom*

(i) $\mathbf{K}^{(n)} = \mathbf{F}_{q^d}$

(ii) *Polynom* $Q_n(x)$ *se rozkládá na součin* $\dfrac{\varphi(n)}{d}$ *různých monických ireducibilních polynomů téhož stupně* d*.*

Důkaz. (i) Nechť ξ je primitivní n-tá odmocnina z jedné, a tedy $\mathbf{K}^{(n)} = \mathbf{K}(\xi)$ (nejmenší těleso obsahující $\mathbf{K}$ a ξ obsahuje nutně i množinu všech n-tých odmocnin z jedné generovanou prvkem ξ). Chceme ukázat, že ξ leží v $\mathbf{F}_{q^d}$, ale neleží v žádném jeho vlastním podtělese. Potom totiž $\mathbf{F}_{q^d} = \mathbf{K}(\xi) = \mathbf{K}^{(n)}$. Jak na to?

Těleso $\mathbf{F}_{q^d}$ obsahuje prvek ξ právě tehdy, když $\xi^{q^k-1} = 1$, jinými slovy $n \mid q^k - 1$, protože ξ je řádu n. Ekvivalentně $q^k \equiv 1 \pmod{n}$. Nejmenší

kladné přirozené číslo splňující tuto kongruenci je d, a tedy dostáváme, co jsme chtěli.

(ii) Buď $f(x)$ libovolný monický ireducibilní faktor $Q_n(x)$ a ξ nějaký kořen $Q_n(x)$ v $\mathbf{K}^{(n)}$. Tedy ξ je primitivní n-tá odmocnina z jedné a $f(x)$ minimální polynom ξ nad $\mathbf{F}_q$ ($\xi \in \mathbf{F}_{q^d}$ je algebraický prvek nad $\mathbf{F}_q$).

Uvědomme si, že těleso $\mathbf{K}(\xi)$ tvoří vektorový prostor nad tělesem $\mathbf{K}$. Jeho dimenze je rovna d dle (i), ale také stupni minimálního polynomu ξ.

Protože n-tý cyklotomický polynom má pouze jednoduché kořeny a jeho stupeň je $\varphi(n)$, rozkládá se $Q_n(x)$ na součin $\dfrac{\varphi(n)}{d}$ různých monických ireducibilních polynomů stupně d.

□

2.3 Möbiova inverzní formule

Uvedeme variantu Möbiovy inverzní formule pro grupu psanou multiplikativně, protože tento případ budeme potřebovat ve cvičeních. Začneme s definicí Möbiovy funkce.

Definice. ([2], Kap. 5) *Möbiova funkce* je zobrazení $\mu : \mathbb{N} \to \{-1, 0, 1\}$ definované předpisem

$$\mu(n) = \begin{cases} 1 & \text{pokud } n = 1 \\ (-1)^k & \text{pokud } n \text{ je součin } k \text{ různých prvočísel} \\ 0 & \text{pokud } p^2 \mid n \text{ pro nějaké prvočíslo } p \end{cases}$$

Následující pomocné lemma pojednává o vlastnosti Möbiovy funkce a využijeme jej v důkazu Möbiovy inverzní formule.

Lemma 2.3.1. *([2], Lemma* 5.1.*) Pro libovolné přirozené číslo n platí*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{pokud } n = 1 \\ 0 & \textit{pokud } n > 1 \end{cases}$$

Věta 2.3.2. *([2], Věta* 5.2.*) (Möbiova inverzní formule) Nechť $\mathbf{G} = (\mathbf{G}, \cdot)$ je multiplikativní grupa a $H, h : N \to G$ zobrazení. Potom*

$$H(n) = \prod_{d|n} h(d) \quad \textit{pro všechna } n \in \mathbb{N}$$

právě tehdy, když

$$h(n) = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d|n} H(d)^{\mu\left(\frac{n}{d}\right)} \quad \textit{pro všechna } n \in N.$$

Důkaz. Začneme implikací $\Rightarrow$. Je vidět, že $\prod_{d|n} H(d)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)}$. Dále upravujeme (s užitím předpokladu $H(n) = \prod_{d|n} h(d)$):

$$\prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d|n} \left(\prod_{c|\frac{n}{d}} h(c)\right)^{\mu(d)} = \prod_{c|n} \left(\prod_{d|\frac{n}{c}} h(c)^{\mu(d)}\right) =$$
$$= \prod_{c|n} h(c)^{\sum_{d|\frac{n}{c}} \mu(d)} = h(n).$$

V poslední rovnosti využíváme Lemma 2.3.1 (suma v exponentu je rovna jedné pouze v případě, kdy $c = n$, jindy je nulová).

Opačnou implikaci dokážeme podobně. Předpokládejme, že $\prod_{d|n} H(d)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)} = h(n)$. Potom dostáváme:

$$\prod_{d|n} h(d) = \prod_{d|n} \left(\prod_{c|d} H(c)^{\mu\left(\frac{d}{c}\right)}\right) = \prod_{d|n} \left(\prod_{c|\frac{n}{d}} H(c)^{\mu(d)}\right)$$
$$= \prod_{c|n} \left(\prod_{d|\frac{n}{c}} H(c)^{\mu(d)}\right) = \prod_{c|n} H(c)^{\sum_{d|\frac{n}{c}} \mu(d)} = H(n).$$

V posledním kroku jsme opět použili Lemma 2.3.1. □

2.4 Berlekampův algoritmus

Berlekampův algoritmus slouží k nalezení ireducibilních faktorů bezčtvercového polynomu. Budeme ho používat v kapitole s příklady, a proto ho nyní stručně popíšeme.

Definice. ([2], Kap. 6) Nechť $\mathbf{F}$ je těleso. Polynom $f(x) \in \mathbf{F}[x]$ nazýváme *bezčtvercový*, pokud f není dělitelný druhou mocninou nějakého nekonstantního polynomu.

Platí, že polynom $f(x)$ je bezčtvercový, pokud $\mathrm{NSD}(f(x), f'(x)) = 1$. Tento fakt uvádíme bez důkazu.

K popisu Berlekampova algoritmu je třeba znát následující tvrzení.

Tvrzení 2.4.1. *([2], Tvrz.* 6.2.*) Nechť $f(x) \in \mathbf{F}[x]$ je monický bezčtvercový polynom. Nechť $h(x) \in \mathbf{F}_q[x]$ je polynom takový, že $h^q(x) \equiv h(x) \pmod{f(x)}$. Pak*

$$f(x) = \prod_{a \in \mathbf{F}_q} \mathrm{NSD}(f(x), h(x) - a).$$

Nebudeme dokazovat, že Berlekampův algoritmus skutečně funguje. Uvedeme pouze postup, jakým bychom rozložili monický bezčtvercový polynom $f \in \mathbf{F}_q[x]$ stupně n ([3], Alg. 26).

Při popisování algoritmu ztotožníme polynom $a_0 + a_1 x + \ldots a_n x^n$ s vektorem $(a_0, a_1, \ldots, a_n)$.

1. $S :=$ matice se sloupci $x^0 \mod f, x^q \mod f, \ldots, x^{(n-1)q} \mod f$
2. spočteme bázi $h_1 = 1, h_2, \ldots, h_m$ prostoru řešení soustavy rovnic $(S - I)h = 0$
3. položíme $i := 2, M := f$
4. dokud $\mid M \mid < m$, opakujeme:
   - nahradíme každé $g \in M$ netriviálními faktory z rozkladu $g = \prod_{a \in \mathbf{F}_q} \mathrm{NSD}(g, h_i - a)$
   - $i := i + 1$
5. výsledkem je množina ireducibilních faktorů M.

Kapitola 3

Cvičení

V této kapitole vyřešíme úlohy a cvičení zadané v [2], které se týkají zejména výpočtu primitivních n-tých odmocnin z jedné, n-tých cyklotomických polynomů a důkazů jejich vlastností pro různá n.

3.1 Primitivní n-tá odmocnina z jedné

Předvedeme si výpočet n-tých odmocnin z jedné.

Příklad 5. Najděte primitivní deváté odmocniny z jedné v tělese $\mathbf{F}_{19}$.

Řešení. Buď α primitivní devátá odmocnina z jedné v $\mathbf{F}_{19}$. Z Důsledku 2.1.5 plyne, že řád grupy ${\mathbf{F}^*}_{19}$ je 18. Dostáváme, že všechny primitivní deváté odmocniny z jedné jsou tvaru $\alpha^k, (k, 18) = 1$, tj. jde o všechny prvky řádu devět v ${\mathbf{F}^*}_{19}$.

Nalezněme nejprve generátor ${\mathbf{F}^*}_{19}$ a následně prvek α. Pro a generátor ${\mathbf{F}^*}_{19}$ platí $\mathrm{ord}(a) = 18$. Tedy při hledání takového a stačí ověřit, že jeho řád v ${\mathbf{F}^*}_{19}$ není dělitelný dvěma ani devíti. Položme $a = 2$, potom

$$2^2 \equiv 4 \pmod{19}, 2^9 \equiv -1 \pmod{19},$$

tudíž 2 je primitivní prvek modulo 19. Dvojka je prvek řádu devět v $\mathbb{Z}_{18}(+)$ a s použitím Důsledku 2.1.5 nakonec dostáváme $\alpha = 2^2 = 4$.

Všech primitivních devátých odmocnin z jedné je $\varphi(9) = 6$ a jsou to tedy prvky

$$4,\ 4^5 = -2,\ 4^7 = 6,\ 4^{11} = -3,\ 4^{13} = 9,\ 4^{17} = 5.$$

3.2 n-tý cyklotomický polynom nad tělesem

Nyní se mimo jiné podíváme na rozklad cyklotomických polynomů a vlastnosti jejich koeficientů. Také vyšetříme případ, kdy n je prvočíslo.

Příklad 6. Spočítejte $Q_{15}(x)$ nad $\mathbb{Q}$.

Řešení. Z Věty 2.2.1 plyne pro $Q_{15}(x)$ následující vztah:

$$Q_{15}(x) = \frac{x^{15}-1}{Q_1(x)Q_3(x)Q_5(x)}.$$

Máme $Q_1(x) = x - 1$, dále určíme

$$Q_3(x) = \frac{x^3-1}{x-1} = x^2 + x + 1 \text{ a } Q_5(x) = \frac{x^5-1}{x-1}.$$

Tedy po dosazení

$$\begin{aligned} Q_{15}(x) &= \frac{x^{15}-1}{(x-1)(x^2+x+1)\cdot\dfrac{x^5-1}{x-1}} = \frac{x^{15}-1}{(x^2+x+1)(x^5-1)} \\ &= \frac{x^{15}-1}{x^7+x^6+x^5-x^2-x-1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1. \end{aligned}$$

Následující příklad ukazuje, jak vypadají koeficienty n-tého cyklotomického polynomu nad tělesem charakteristiky $p \nmid n$.

Příklad 7. Buď $Q_n(x)$ n-tý cyklotomický polynom nad $\mathbb{Q}$ a $R_n(x)$ n-tý cyklotomický polynom nad tělesem charakteristiky $p \nmid n$. Dokažte, že koeficienty $R_n(x)$ jsou stejné jako koeficienty $Q_n(x)$ modulo p.

Řešení. Provedeme důkaz indukcí podle n. Pro $n = 1$ máme nad libovolným tělesem $Q_1(x) = x - 1$. Uvažujme nyní, že pro všechna $d \mid n, d < n$ předpoklad platí, tj. že koeficienty $R_d(x)$ jsou stejné jako koeficienty $Q_d(x)$ modulo p.

Z Věty 2.2.1 plyne

$$R_n(x) = \frac{x^n-1}{\prod_{\substack{d\mid n\\ d<n}} R_d(x)}.$$

Koeficienty v čitateli jsou zřejmě vždy 1 a -1. Součin cyklotomických polynomů ve jmenovateli má také požadovanou vlastnost, použijeme totiž indukční předpoklad na jednotlivé součinitele:

$$\prod_{\substack{d|n\\d<n}} R_d(x) = \prod_{\substack{d|n\\d<n}} (Q_d(x) \pmod p) = \left(\prod_{\substack{d|n\\d<n}} Q_d(x) \right) \pmod p.$$

Nakonec, podíl dvou polynomů nad tělesem charakteristiky p s koeficienty stejnými, jako bychom počítali v tělese racionálních čísel modulo p, má také dokazovanou vlastnost. Důvod je ten, že při dělení polynomu polynomem nezáleží na tom, zda počítáme modulo p každý mezivýsledek nebo jestli všechny mezivýsledky počítáme v $\mathbb{Q}[x]$ a až u výsledného polynomu přepočítám koeficienty modulo p.

V další úloze si vyzkoušíme rozklad polynomu na ireducibilní činitele pomocí Berlekampova algoritmu. Použijeme také výsledek Příkladu 6.

Příklad 8. Rozložte polynom $Q_{15}(x) \in \mathbf{F}_2[x]$ na ireducibilní činitele.

Řešení. Z Příkladu 6 máme, že $Q_{15}(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$.

$\mathrm{NSD}(2, 15) = 1$ a nejmenší kladné přirozené číslo d takové, že $2^d \equiv 1 \pmod{15}$, je čtyřka. Věta 2.2.2 říká, že se polynom $Q_{15}(x)$ rozkládá na součin $\frac{\varphi(15)}{4} = 2$ různých monických ireducibilních polynomů téhož stupně čtyři.

K nalezení těchto dvou polynomů využijeme Berlekampův algoritmus:

Označme $f(x) := x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$. $\mathrm{NSD}(f(x), f'(x)) = 1$, a proto je f bezčtvercový. Nejdříve spočítáme matici S:

$$\begin{aligned}
x^0 \bmod f(x) &= 1\\
x^2 \bmod f(x) &= x^2\\
x^4 \bmod f(x) &= x^4\\
x^6 \bmod f(x) &= x^6\\
x^8 \bmod f(x) &= x^7 + x^5 + x^4 + x^3 + x + 1\\
x^{10} \bmod f(x) &= x^5 + 1\\
x^{12} \bmod f(x) &= x^{10} \cdot x^2 \bmod f(x) = x^7 + x^2\\
x^{14} \bmod f(x) &= x^{12} \cdot x^2 \bmod f(x) = x^9 + x^4 \bmod f(x) =\\
&= x^7 + x^6 + x^4 + x^3 + x^2 + 1.
\end{aligned}$$

Tedy

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Nyní aplikujeme Gaussovu eliminaci na matici $S - I$:

$$S - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Báze řešení je například $(1,0,0,0,0,0,0,0)$,$(0,0,1,1,0,1,0,1)$ s příslušnými polynomy $h_1(x) = 1$, $h_2(x) = x^2 + x^3 + x^5 + x^7$. Dále

$$\begin{aligned} &\mathrm{NSD}(f(x), h_2(x) - 0) = \\ &= \mathrm{NSD}(x^8 + x^7 + x^5 + x^4 + x^3 + x + 1, x^7 + x^5 + x^3 + x^2) = \\ &= x^4 + x^3 + 1, \\ &\mathrm{NSD}(f(x), h_2(x) - 1) = \\ &= \mathrm{NSD}(x^8 + x^7 + x^5 + x^4 + x^3 + x + 1, x^7 + x^5 + x^3 + x^2 - 1) = \\ &= x^4 + x + 1. \end{aligned}$$

Výsledný rozklad polynomu $f(x) = Q_{15}(x)$ je $x^8+x^7+x^5+x^4+x^3+x+1 = (x^4 + x^3 + 1)(x^4 + x + 1)$.

Příklad 9. Nechť $\mathbf{K}$ je libovolné těleso a $n > 1$. Dokažte, že polynom $x^{n-1} + x^{n-2} + \ldots + 1$ je rozložitelný, kdykoliv n je složené.

Řešení. Označme p charakteristiku tělesa $\mathbf{K}$. Pro $p = 0$ nebo $p \nmid n$ položme $n = ab$, $1 < a \leq b < n$. Ze vzorce pro součet geometrické řady máme

$x^{ab-1} + x^{ab-2} + \ldots + 1 = \frac{x^{ab}-1}{x-1}$.

Dostáváme

$$x^{ab} - 1 = \prod_{d|ab} Q_d(x) = Q_1(x) \ldots Q_a(x) \ldots Q_b(x) \ldots Q_{ab}(x),$$

a tedy

$$x^{ab-1} + x^{ab-2} + \ldots + 1 = \prod_{\substack{d|ab \\ d>1}} Q_d(x)$$

je netriviální rozklad daného polynomu.

V případě $p \mid n$ existuje kladné přirozené číslo l takové, že $n = pl$. V tělese charakteristiky $p > 0$ podle Lemma 2.1.2 platí $x^n - 1 = (x^l)^p - 1 = (x^l - 1)^p$, a tedy dostáváme následující rozklad:

$$\begin{aligned} x^{n-1} + x^{n-2} + \ldots + 1 = \frac{x^n - 1}{x - 1} = \frac{(x^l - 1)^p (x-1)^{p-1}}{(x-1)^p} = \\ = (x^{l-1} + x^{l-2} + \ldots + 1)^p (x-1)^{p-1}. \end{aligned}$$

V další dvojici příkladů se podíváme na podmínky ireducibility n-tých cyklotomických polynomů pro n je prvočíslo nad tělesy s prvočíselným počtem prvků.

Příklad 10. Najděte nejmenší prvočíslo p takové, že $x^{22} + x^{21} + \ldots + 1$ je ireducibilní nad $\mathbf{F}_p$.

Řešení. Platí $x^{22} + x^{21} + \ldots + 1 = \frac{x^{23}-1}{x-1} = Q_{23}(x)$, neboť 23 je prvočíslo. Podle Věty 2.2.2 se polynom $Q_{23}(x) \in \mathbb{Z}_p[x]$ rozkládá na součin $\dfrac{\varphi(23)}{d} = \dfrac{22}{d}$ různých monických ireducibilních polynomů, přičemž d je nejmenší kladné přirozené číslo splňující $p^d \equiv 1 \bmod 23$. Jinými slovy, hledané p je primitivní prvek modulo 23, neboť potom pro polynom $Q_{23}(x)$ nebude v $\mathbb{Z}_p(x)$ existovat netriviální rozklad.

Dle Důsledku 2.1.5 mají prvky grupy $\mathbb{Z}^*{}_{23}$ řád dělící 22, tzn. $2, 11$ nebo 22.

Položme $p = 2$. Máme

$$\begin{aligned} 2^2 \equiv 4 \pmod{23}, 2^{11} \equiv \left(2^5\right)^2 \cdot 2 \equiv 32^2 \cdot 2 \equiv 9^2 \cdot 2 \equiv 81 \cdot 2 \equiv 12 \cdot 2 \equiv \\ \equiv 24 \equiv 1 \pmod{23}, \end{aligned}$$

tím pádem 11 je řád dvojky v $\mathbb{Z}^*_{23}$ a volba $p = 2$ nevyhovuje. Podobně narazíme na problém u $p = 3$, neboť

$$3^{11} \equiv (3^3)^3 \cdot 3^2 \equiv 27^3 \cdot 9 \equiv 4^3 \cdot 9 \equiv 64 \cdot 9 \equiv -5 \cdot 9 \equiv -45 \equiv 1 \pmod{23}.$$

Nyní se podíváme na případ $p = 5$. Platí $5^2 \equiv 25 \equiv 2 \pmod{23}$ a

$$5^{11} \equiv (5^2)^5 \cdot 5 \equiv 2^5 \cdot 5 \equiv 32 \cdot 5 \equiv 9 \cdot 5 \equiv 45 \equiv -1 \pmod{23},$$

tedy 5^{11} je řádu dva v $\mathbb{Z}^*_{23}$ a pětka je hledaný generátor. Máme $d = \mathrm{ord}(5) = 22$ a odpověď zní $p = 5$.

Příklad 11. Najděte nejmenších deset prvočísel p, pro něž je $x^{p-1} + x^{p-2} + \ldots + 1$ ireducibilní nad $\mathbf{F}_2$.

Řešení. V případě $p = 2$ je polynom $x + 1 \in \mathbf{F}_2[x]$ ireducibilní. Proto nám dvojka vyhovuje.

Pro p liché prvočíslo platí $x^{p-1}+x^{p-2}+\ldots+1 = \dfrac{x^p - 1}{x - 1} = Q_p(x)$. Hledáme tedy nejmenších devět lichých prvočísel p takových, že $Q_p(x)$ je ireducibilní nad $\mathbf{F}_2$.

Opět použijeme Větu 2.2.2: $Q_p(x)$ se v tělese $\mathbf{F}_2$ rozkládá na $\dfrac{\varphi(p)}{d} = \dfrac{p-1}{d}$ netriviálních faktorů, přičemž d je nejmenší kladné přirozené číslo takové, že $2^d \equiv 1 \pmod{p}$. Pro důkaz ireducibility tedy hledáme p takové, aby $d = \mathrm{ord}(2) = p - 1$, neboli aby prvek 2 generoval $\mathbb{Z}^*_p$.

Vždy ověříme, zda-li řád dvojky v $\mathbb{Z}^*_p$ není roven nějakému l, kde $l \mid p - 1, l < p - 1$. Potom by zřejmě p nevyhovovalo.

- $p = 3$: $2 \equiv -1 \pmod{3}$ $\surd$
- $p = 5$: $2^2 \equiv 4 \equiv -1 \pmod{5}$ $\surd$
- $p = 7$: $2^3 \equiv 1 \pmod{7}$, a tedy $p = 7$ nevyhovuje
- $p = 11$: $2^2 \equiv 4 \pmod{11}, 2^5 \equiv 32 \equiv -1 \pmod{11}$ $\surd$
- $p = 13$: $2^4 \equiv 16 \equiv 3 \pmod{13}, 2^6 \equiv 64 \equiv -1 \pmod{13}$ $\surd$
- $p = 17$: $2^8 \equiv (2^4)^2 \equiv (-1)^2 \equiv 1 \pmod{17}$, a tedy $p = 17$ nevyhovuje
- $p = 19$: $2^2 \equiv 4 \pmod{19}, 2^6 \equiv 64 \equiv 7 \pmod{19}, 2^9 \equiv 2^6 \cdot 2^3 \equiv 7 \cdot 8 \equiv 56 \equiv -1 \pmod{19}$ $\surd$

- $p = 23$: $2^2 \equiv 4 \pmod{23}, 2^{11} \equiv 1 \pmod{23}$ (dle Příkladu 10), a tedy $p = 23$ nevyhovuje
- $p = 29$: $2^4 \equiv 16 \pmod{29}, 2^{14} \equiv (2^4)^3 \cdot 2^2 \equiv 16^2 \cdot 16 \cdot 4 \equiv 64 \cdot 256 \equiv 6 \cdot (-5) \equiv -30 \equiv -1 \pmod{29}$ $\surd$
- $p = 31$: $2^5 \equiv 32 \equiv 1 \pmod{31}$, a tedy $p = 31$ nevyhovuje
- $p = 37$: $2^{12} \equiv (2^5)^2 \cdot 2^2 \equiv (-5)^2 \cdot 4 \equiv 25 \cdot 4 \equiv 100 \equiv -11 \pmod{37}, 2^{18} \equiv 2^{12} \cdot 2^6 \equiv -11 \cdot 64 \equiv -11 \cdot (-10) \equiv 110 \equiv -1 \pmod{37}$ $\surd$
- $p = 41$: $2^{20} \equiv (2^5)^4 \equiv 32^4 \equiv (-9)^4 \equiv (-9)^2 \cdot (-9)^2 \equiv 81^2 \equiv (-1)^2 \equiv 1 \pmod{41}$, a tedy $p = 41$ nevyhovuje
- $p = 43$: $2^6 \equiv 64 \equiv 21 \pmod{43}, 2^{14} \equiv (2^6)^2 \cdot 2^2 \equiv 21^2 \cdot 4 \equiv 441 \cdot 4 \equiv 11 \cdot 4 \equiv 44 \equiv 1 \pmod{43}$, a tedy $p = 43$ nevyhovuje
- $p = 47$: $2^{23} \equiv (2^6)^3 \cdot 2^5 \equiv 17^2 \cdot 17 \cdot (-15) \equiv 289 \cdot (-255) \equiv 7 \cdot 27 \equiv 189 \equiv 1 \pmod{47}$, a tedy $p = 47$ nevyhovuje
- $p = 53$: $2^4 \equiv 16 \pmod{53}, 2^{26} \equiv (2^6)^4 \cdot 2^2 \equiv (11^2)^2 \cdot 4 \equiv 15^2 \cdot 4 \equiv 225 \cdot 4 \equiv 13 \cdot 4 \equiv -1 \pmod{53}$ $\surd$
- $p = 59$: $2^2 \equiv 4 \pmod{59}, 2^{29} \equiv (2^6)^4 \cdot 2^5 \equiv 5^4 \cdot 32 \equiv 625 \cdot 32 \equiv 35 \cdot 32 \equiv 1120 \equiv -1 \pmod{59}$ $\surd$

Tedy výsledkem jsou následující prvočísla:

$$2, 3, 5, 11, 13, 19, 29, 37, 53, 59.$$

3.3 Vlastnosti cyklotomických polynomů

Nyní dokážeme několik vlastností cyklotomických polynomů. V některých případech si ukážeme dva typy důkazů: s využitím definice a dle Möbiovy inverzní formule. Budeme vždy pracovat nad takovým tělesem, aby cyklotomické polynomy byly definovány.

Příklad 12. Nechť p je prvočíslo a $p \nmid m$. Dokažte, že potom $Q_{mp}(x) = \frac{Q_m(x^p)}{Q_m(x)}$.

Řešení. Chceme dokázat, že $Q_{mp}(x)Q_m(x) = Q_m(x^p)$. Zvolme pevně nějakou primitivní $\sqrt[mp]{1}$ a označme ji α. Zřejmě $\beta = \alpha^p$ bude primitivní $\sqrt[m]{1}$. Z definice n-tého cyklotomického polynomu platí pro levou a pravou stranu výše zmíněné rovnosti následující vztahy:

$$Q_{mp}(x)Q_m(x) = \prod_{\substack{k<mp \\ \mathrm{NSD}(k,mp)=1}} (x-\alpha^k) \prod_{\substack{k<m \\ \mathrm{NSD}(k,m)=1}} (x-\beta^k),$$
$$Q_m(x^p) = \prod_{\substack{k<m \\ \mathrm{NSD}(k,m)=1}} (x^p-\beta^k).$$

Nyní upravíme $Q_m(x^p)$. Povšimněme si, že polynom $x^p-\beta^k$ má pouze jednoduché kořeny, jelikož $\mathrm{NSD}((x^p-\beta^k),(x^p-\beta^k)') = \mathrm{NSD}((x^p-\beta^k),px^{p-1}) = 1$.

Pro ξ libovolný kořen $x^p-\beta^k$ je $\xi^p = \beta^k$ a platí $\xi^{mp} = \beta^{km} = \alpha^{kmp} = 1$. Proto každé takové ξ je mp-tá odmocnina z 1. Ale všechny mp-té odmocniny z 1 mají tvar $\alpha^l,\ l = 0,1,2,\ldots$. Stačí tedy určit, pro která l je α^l kořenem $x^p-\beta^k$.

Jinými slovy chceme, aby $\alpha^{pl} = \beta^k = \alpha^{pk}$, a proto musí platit $pl \equiv pk \pmod{mp}$. Tato kongruence je splněna právě tehdy, když $l \equiv k \pmod{m}$. Z těchto úvah vyplývá

$$Q_m(x^p) = \prod_{\substack{k<m \\ \mathrm{NSD}(k,m)=1}} \left(\prod_{\substack{l<mp \\ l\equiv k \pmod m}} (x-\alpha^l) \right).$$

Oba polynomy $Q_{mp}(x)Q_m(x)$ a $Q_m(x^p)$ jsou součinem navzájem různých lineárních faktorů. Kořeny polynomu $Q_{mp}(x)Q_m(x)$ jsou právě $\left\{\alpha^l, l \in A\right\}$, kde

$$A = \{r : \mathrm{NSD}(r,mp) = 1, r < mp\} \cup \{pr : \mathrm{NSD}(r,m) = 1, r < m\}.$$

Kořeny polynomu $Q_m(x^p)$ jsou právě $\left\{\alpha^l, l \in B\right\}$, kde

$$B = \{l : l < mp, l \equiv k \pmod m, \mathrm{NSD}(k,m) = 1\}.$$

Nyní stačí ukázat, že $A = B$, a důkaz je hotov.

Od začátku předpokládáme, že prvočíslo p nedělí m. Proto je množina A zřejmě rovna množině $\{r : \mathrm{NSD}(r,m) = 1, r < mp\}$. Množina B obsahuje taková l, že $l \equiv k \pmod m$ a $\mathrm{NSD}(k,m) = 1$. Podle Eukleidova algoritmu je $\mathrm{NSD}(k,m) = \mathrm{NSD}(k \bmod m, m) = \mathrm{NSD}(l \bmod m, m) = \mathrm{NSD}(l,m)$, tedy i $\mathrm{NSD}(l,m) = 1$ a $B = A$.

Řešení. Nyní si dokazovaný vztah upravíme s použitím Möbiovy inverzní formule.

Nejprve vyjádříme $Q_m(x)$. Nad tělesem charakteristiky $p, p \nmid m$ podle Věty 2.2.1 platí

$$x^m - 1 = \prod_{d|m} Q_d(x).$$

Nyní použijeme Větu 2.3.2. Uvažujme funkce $H(m) = x^m - 1$ a $h(m) = Q_m(x)$. Potom dostaneme vztah

$$(1) \qquad Q_m(x) = \prod_{d|m} (x^{\frac{m}{d}} - 1)^{\mu(d)}.$$

Podobně ze stejné věty plyne:

$$(2) \qquad Q_{mp}(x) = \prod_{d|mp} (x^{\frac{mp}{d}} - 1)^{\mu(d)}.$$

Podívejme se na dělitele součinu mp. Protože $p \nmid m$, mají dělitelé mp tvar $\{k : k \mid m\}$ nebo $\{kp : k \mid m\}$. Rovnost (2) tedy lze přepsat následovně:

$$(3) \qquad Q_{mp}(x) = \prod_{d|m} (x^{\frac{mp}{d}} - 1)^{\mu(d)} \prod_{k|m} (x^{\frac{mp}{kp}} - 1)^{\mu(kp)}.$$

Nyní si povšimněme, co z definice Möbiovy funkce plyne pro exponent $\mu(kp)$: platí totiž, že $\mu(kp) = (-1)^{c+1}$, pokud k se rovná součinu c různých prvočísel různých od p (ale tato podmínka v našem případě vždy platí, neboť $p \nmid m$), a $\mu(kp) = 0$, pokud existuje prvočíslo a tak, že $a^2 \mid k$. Z těchto úvah snadno plyne, že $\mu(kp) = -\mu(k)$, a tedy

$$(4) \qquad \prod_{k|m} (x^{\frac{mp}{kp}} - 1)^{\mu(kp)} = \prod_{d|m} (x^{\frac{m}{d}} - 1)^{-\mu(d)}.$$

Nyní s využitím (1), (2), (3) a (4) dostaneme

$$\begin{aligned} Q_{mp}(x) Q_m(x) &= \frac{\prod_{d|m} (x^{\frac{mp}{d}} - 1)^{\mu(d)}}{\prod_{d|m} (x^{\frac{m}{d}} - 1)^{\mu(d)}} \prod_{d|m} (x^{\frac{m}{d}} - 1)^{\mu(d)} = \\ &= \prod_{d|m} ((x^p)^{\frac{m}{d}} - 1)^{\mu(d)} = Q_m(x^p), \end{aligned}$$

a dokazovaná rovnost platí.

Příklad 13. Nechť p je prvočíslo a $p \mid m$. Dokažte, že potom $Q_{mp}(x) = Q_m(x^p)$.

Řešení. Tento vztah dokážeme podobně jako předchozí příklad. Opět buď α nějaká pevně zvolená primitivní $\sqrt[mp]{1}$ a $\beta = \alpha^p$ primitivní $\sqrt[m]{1}$. Potom

$$Q_{mp}(x) = \prod_{\substack{k<mp \\ \mathrm{NSD}(k,mp)=1}} (x - \alpha^k).$$

Dle této rovnosti mají kořeny $Q_{mp}(x)$ tvar $\left\{\alpha^l : l \in A\right\}$, kde

$$A = \left\{r : \mathrm{NSD}(r, mp) = 1, r < mp\right\}.$$

Polynom $Q_m(x^p)$ se rozkládá takto:

$$Q_m(x^p) = \prod_{\substack{k<m \\ \mathrm{NSD}(k,m)=1}} (x^p - \beta^k),$$

kde podobně jako v předchozím cvičení jsou všechny kořeny jednoduché. Z minulého příkladu víme, že kořeny polynomu $Q_m(x^p)$ jsou právě $\left\{\alpha^l : l \in B\right\}$, kde

$$B = \left\{r : r < mp, \mathrm{NSD}(r, m) = 1\right\}.$$

Nyní již stačí ověřit, že $A = B$ a důkaz bude hotov.

Protože p je prvočíslo dělící m, je $\mathrm{NSD}(r, m) = 1$ ekvivalentní $\mathrm{NSD}(r, mp) = 1$. Je to z toho důvodu, že pro největší společný dělitel čísel c a d, kde $c = {p_1}^{e_1} \cdots {p_u}^{e_u}, d = {q_1}^{l_1} \cdots {q_v}^{l_v}$ jsou příslušné prvočíselné rozklady, platí

$$\mathrm{NSD}(c, d) = \prod_{\substack{1 \le i \le u, 1 \le j \le v \\ p_i = q_j}} {p_i}^{\min(e_i, l_j)}.$$

Prvočíselné rozklady čísel m a mp se liší pouze v exponentu prvočísla p. Ale protože zřejmě $\mathrm{NSD}(p, r) = 1$, nebude mít p díky výše uvedenému vztahu v žádném z obou případů na největší společný dělitel vliv. Tedy $\mathrm{NSD}(r, m) = \mathrm{NSD}(r, mp) = 1$, a díky tomu $A = B$.

Řešení. Využijeme vztah (2) z minulého příkladu. Co lze říci o dělitelích součinu mp? Nejprve pro ty, kteří jsou dělitelní p^2, platí

$$(5) \qquad \prod_{\substack{d|mp \\ p^2|d}} (x^{\frac{mp}{d}} - 1)^{\mu(d)} = 1.$$

Je tomu tak proto, že exponent každého součinitele je roven nule: $\mu(d) = \mu(p^2c) = 0$ z definice Möbiovy funkce. Zbývající dělitelé mp jsou tvaru buď $\{k : k \mid m \ \& \ p \nmid k\}$ a nebo $\{kp : k \mid m \ \& \ p \nmid k\}$, přičmž využijeme trik jako v předchozím důkazu, tj. že $\mu(kp) = -\mu(k)$. Dostaneme

$$(6) \qquad Q_{mp}(x) = \prod_{\substack{k|m \\ p\nmid k}} (x^{\frac{mp}{k}} - 1)^{\mu(k)} \prod_{\substack{k|m \\ p\nmid k}} (x^{\frac{mp}{kp}} - 1)^{-\mu(k)} = \frac{\prod_{\substack{d|m \\ p\nmid d}} (x^{\frac{mp}{d}} - 1)^{\mu(d)}}{\prod_{\substack{d|m \\ p\nmid d}} (x^{\frac{m}{d}} - 1)^{\mu(d)}}.$$

Nyní se podíváme na polynom $Q_m(x^p)$. Pomocí (1) z minulého příkladu vidíme, že $Q_m(x^p) = \prod_{d|m} (x^{\frac{mp}{d}} - 1)^{\mu(d)}$. Jak vhodně rozepsat tuto rovnost? Provedeme podobné úvahy jako výše. Mezi děliteli m se mohou vyskytovat násobky p a násobky p^2. Tedy

$$Q_m(x^p) = \prod_{\substack{k|m \\ p^2|k}} (x^{\frac{mp}{k}} - 1)^{\mu(k)} \prod_{\substack{k|m, k=cp \\ p\nmid c}} (x^{\frac{mp}{cp}} - 1)^{-\mu(c)} \prod_{\substack{k|m \\ p\nmid k}} (x^{\frac{mp}{k}} - 1)^{\mu(k)}$$

$$(7) \qquad Q_m(x^p) = \frac{\prod_{\substack{d|m \\ p\nmid d}} (x^{\frac{mp}{d}} - 1)^{\mu(d)}}{\prod_{\substack{d|m \\ p\nmid d}} (x^{\frac{m}{d}} - 1)^{\mu(d)}}.$$

Nyní stačí porovnat rovnosti (6) a (7).

S využitím předešlého příkladu dokážeme následující užitečný vztah, který se bude později hodit v dalších cvičeních.

Příklad 14. Nechť p je prvočíslo a k, m jsou libovolná přirozená čísla. Dokažte, že potom $Q_{mp^k}(x) = Q_{mp}(x^{p^{k-1}})$.

Řešení. Budeme postupovat indukcí podle k. Pro $k = 1$ se levá i pravá strana rovnají. Předpokládejme, že platí $Q_{mp^{k-1}}(x) = Q_{mp}(x^{p^{k-2}})$. Je vztah splněn i pro krok k?

Uvažujme $m' = mp^{k-1}$, zřejmě $p \mid m'$. S použitím Příkladu 13 a indukčního předpokladu máme

$$Q_{mp^k}(x) = Q_{m'p}(x) = Q_{m'}(x^p) = Q_{mp^{k-1}}(x^p) = Q_{mp}((x^p)^{p^{k-2}}) = Q_{mp}(x^{p^{k-1}}).$$

Nyní si ukážeme, čemu se rovnají polynomy $Q_n(-x)$ a $Q_n(x^{-1})$.

Příklad 15. Nechť $n \geq 3$ je liché. Dokažte, že $Q_{2n}(x) = Q_n(-x)$.

Řešení. Zvolíme postup indukcí. Pro $n = 1$ platí:

$$Q_1(-x) = -x - 1 = -(x + 1) = -Q_2(x)$$

Pro $n = 3$ máme z Příkladu 6 spočteno $Q_3(x) = x^2 + x + 1$. Čemu se rovná $Q_6(x)$? Z Věty 2.2.1 plyne:

$$\begin{aligned} Q_6(x) &= \frac{x^6 - 1}{Q_1(x)Q_2(x)Q_3(x)} = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = \\ &= \frac{x^6 - 1}{(x^2-1)(x^2+x+1)} = \frac{x^6 - 1}{x^4 + x^3 - x - 1} = \\ &= x^2 - x + 1. \end{aligned}$$

Tedy $Q_3(-x) = x^2 - x + 1 = Q_6(x)$.

Předpokládejme, že pro všechna $d \mid n$, kde n je liché, platí $Q_d(-x) = Q_{2d}(x)$. Podívejme se, že potom vztah platí i pro n. Nejprve si vyjádříme $Q_{2n}(x)$:

$$\begin{aligned} Q_{2n}(x) &= \frac{x^{2n} - 1}{\prod_{\substack{d \mid 2n \\ d < 2n}} Q_d(x)} = \frac{(x^n - 1)(x^n + 1)}{Q_n(x) \prod_{\substack{d \mid n \\ d < n}} Q_d(x)Q_{2d}(x)} = \\ &= \frac{1}{Q_n(x)} \cdot Q_n(x) \cdot \frac{x^n + 1}{\prod_{\substack{d \mid n \\ d < n}} Q_{2d}(x)} = \frac{x^n + 1}{\prod_{\substack{d \mid n \\ d < n}} Q_{2d}(x)}, \end{aligned}$$

tj. stačí nám dokázat, že

$$Q_n(-x) = \frac{x^n + 1}{\prod_{\substack{d \mid n \\ d < n}} Q_{2d}(x)}.$$

S využitím indukčního předpokladu, Věty 2.2.1 a rovnosti $Q_1(-x) = -Q_2(x)$) se přesvědčíme, že je tomu skutečně tak:

$$Q_n(-x) = \frac{(-1)^n(x^n-1)}{Q_1(-x)\prod_{\substack{d\mid n\\1<d<n}} Q_d(-x)} = \frac{-(x^n+1)}{-Q_2(x)\prod_{\substack{d\mid n\\1<d<n}} Q_{2d}(x)} =$$
$$= \frac{-(x^n+1)}{-\prod_{\substack{d\mid n\\d<n}} Q_{2d}(x)} = \frac{x^n+1}{\prod_{\substack{d\mid n\\d<n}} Q_{2d}(x)},$$

a to je přesně ta rovnost, kterou jsme chtěli.

Příklad 16. Dokažte, že pro $n \geq 2$ platí $Q_n(x^{-1})x^{\varphi(n)} = Q_n(x)$, kde $\varphi(n)$ je Eulerova funkce.

Řešení. Nejprve si uvědomme, že je definováno $\varphi(1) = 1$, a tedy

$$Q_1(x^{-1})x^{\varphi(1)} = Q_1(x^{-1})x = (x^{-1}-1)x = 1-x = -Q_1(x).$$

Opět využijeme indukci. Pro $n = 2$ rovnost platí, neboť $Q_2(x^{-1})x^{\varphi(2)} = (x^{-1}+1)x = 1+x = Q_2(x)$.

Předpokládejme tedy, že pro všechna $d \mid n, d < n$ platí $Q_d(x^{-1})x^{\varphi(d)} = Q_d(x)$. Stačí tedy s využitím indukčního předpokladu ověřit, zda-li vztah platí i pro n. Z Věty 2.2.1 s využitím rovnosti $Q_1(x^{-1})x = -Q_1(x)$ dostáváme:

$$Q_n(x) = \frac{x^n-1}{\prod_{\substack{d\mid n\\d<n}} Q_d(x)} = \frac{((x^{-1})^n-1)(-x^n)}{Q_1(x)\prod_{\substack{d\mid n\\1<d<n}} Q_d(x^{-1})x^{\varphi(d)}} =$$
$$= \frac{(x^{-1})^n-1}{Q_1(x^{-1})\prod_{\substack{d\mid n\\1<d<n}} Q_d(x^{-1})} \cdot \frac{-x^n}{-\prod_{\substack{d\mid n\\1<d<n}} x^{\varphi(d)}} =$$
$$= \frac{(x^{-1})^n-1}{\prod_{\substack{d\mid n\\d<n}} Q_d(x^{-1})} \cdot \frac{x^n}{x^{\sum_{\substack{d\mid n\\1<d<n}} x^{\varphi(d)}}} =$$
$$= Q_n(x^{-1}) \cdot \frac{x^n \cdot x^{\varphi(n)}}{x^{\sum_{\substack{d\mid n\\d<n}} x^{\varphi(d)}}} = Q_n(x^{-1})x^{\varphi(n)}.$$

V posledním kroku jsme použili Tvrzení 2.1.6.

3.4 Vybrané hodnoty cyklotomických polynomů

Podívejme se, čemu se rovná hodnota n-tého cyklotomického polynomu v bodech $-1, 0$ a 1 v závislosti na n. Při řešení využijeme výsledky z předchozí sekce.

Příklad 17. Ukažte, že pro $n \geq 2$ platí $Q_n(0) = 1$.

Řešení. Příklad vyřešíme indukcí podle n. Máme $Q_1(0) = -1$ a $Q_2(0) = 1$, a tedy pro $n = 2$ rovnost platí.

Předpokládejme, že daný vztah platí i pro všechna $d \mid n, d < n$.

Z Věty 2.2.1 plyne: $Q_n(x) = \dfrac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} Q_d(x)}$. S využitím indukčního předpokladu a rovnosti $Q_1(0) = -1$ tedy po dosazení nuly dostáváme

$$Q_n(0) = \frac{0 - 1}{(-1) \cdot \prod_{\substack{d|n \\ d<n}} Q_d(0)} = \frac{-1}{(-1) \cdot 1 \cdots 1} = 1.$$

Příklad 18. Dokažte:

$$Q_n(1) = \begin{cases} 0 & \text{pokud } n = 1 \\ p & \text{pokud } n \text{ je mocnina prvočísla } p \\ 1 & \text{pokud } n \text{ má dva různé prvočíselné dělitele} \end{cases}$$

Řešení. Postupně rozebereme jednotlivé případy. Pro $n = 1$ máme $Q_1(x) = x - 1$, a tedy $Q_1(1) = 1 - 1 = 0$.

V případě, že $n = p^e$ pro nějaké e přirozené číslo a p prvočíslo, si nejprve vyjádříme, čemu se rovná $Q_{p^e}(x)$. Z Věty 2.2.1 plyne vztah

$$x^{p^e} - 1 = Q_1(x) \cdot Q_p(x) \cdots Q_{p^{e-1}}(x) \cdot Q_{p^e}(x).$$

Podívejme se, že také platí

$$Q_1(x) \cdot Q_p(x) \cdots Q_{p^{e-1}}(x) = x^{p^{e-1}} - 1.$$

Kombinací předchozích dvou rovností získáme $x^{p^e} - 1 = (x^{p^{e-1}} - 1)Q_{p^e}(x)$, a tedy

$$Q_{p^e}(x) = \frac{x^{p^e} - 1}{x^{p^{e-1}} - 1} = x^{(p-1)p^{e-1}} + \cdots + x^{p^{e-1}} + 1.$$

V tomto vyjádření máme celkem p sčítanců. Po dosazení jedničky nevyjde nic jiného než

$$Q_{p^e}(1) = 1 + \cdots + 1 = p.$$

Nakonec zbývá situace, kdy n má dva různé prvočíselné dělitele. Nechť $n = {p_1}^{e_1} \cdots {p_k}^{e_k}$ je prvočíselný rozklad čísla n. Budeme postupovat indukcí podle k, kde $k \geq 2$.

Pro $k = 2$ máme $n = {p_1}^{e_1} \cdot {p_2}^{e_2}$. Polynom $Q_{{p_1}^{e_1} \cdot {p_2}^{e_2}}(x)$ si upravíme s použitím výsledků Příkladu 14 a Příkladu 12 (předpoklady jsou splněny):

$$Q_{{p_1}^{e_1}{p_2}^{e_2}}(x) = Q_{{p_1}^{e_1}{p_2}}(x^{{p_2}^{e_2-1}}) = \frac{Q_{{p_1}^{e_1}}((x^{{p_2}^{e_2-1}})^{p_2})}{Q_{{p_1}^{e_1}}(x^{{p_2}^{e_2-1}})} = \frac{Q_{{p_1}^{e_1}}(x^{{p_2}^{e_2}})}{Q_{{p_1}^{e_1}}(x^{{p_2}^{e_2-1}})}.$$

Tedy po dosazení jedničky a využití předešlého vztahu pro n mocninu prvočísla dostaneme

$$Q_{{p_1}^{e_1}{p_2}^{e_2}}(1) = \frac{Q_{{p_1}^{e_1}}\left(1^{{p_2}^{e_2}}\right)}{Q_{{p_1}^{e_1}}\left(1^{{p_2}^{e_2-1}}\right)} = \frac{Q_{{p_1}^{e_1}}(1)}{Q_{{p_1}^{e_1}}(1)} = \frac{p_1}{p_1} = 1.$$

Předpokládejme nyní, že platí $Q_{{p_1}^{e_1}\ldots{p_{k-1}}^{e_{k-1}}}(1) = 1$. Implikuje tato rovnost $Q_{{p_1}^{e_1}\ldots{p_k}^{e_k}}(1) = 1$? Podívejme se, že ano. Pro přehlednost označme $m = {p_1}^{e_1} \ldots {p_{k-1}}^{e_{k-1}}$. Nejprve použijeme k úpravám Příklad 14 a Příklad 12 (předpoklady jsou zřejmě splněny):

$$Q_{m{p_k}^{e_k}}(x) = Q_{mp_k}(x^{{p_k}^{e_k-1}}) = \frac{Q_m(x^{{p_k}^{e_k}})}{Q_m(x^{{p_k}^{e_k-1}})}.$$

Nyní stačí dosadit jedničku a použít indukční předpoklad:

$$Q_{m{p_k}^{e_k}}(1) = \frac{Q_m\left(1^{{p_k}^{e_k}}\right)}{Q_m\left(1^{{p_k}^{e_k-1}}\right)} = \frac{Q_m(1)}{Q_m(1)} = \frac{1}{1} = 1.$$

Řešení. Ještě předvedeme jednodušší způsob jak dokázat, že $Q_n(1) = 1$, pokud n má dva různé prvočíselné dělitele. Uvažujme opět $n = {p_1}^{e_1} \cdots {p_k}^{e_k}$ prvočíselný rozklad čísla n. Případ $n = {p_1}^{e_1}{p_2}^{e_2}$ jsme ověřili v minulém řešení. Nyní dokážeme vztah pro libovolné $k > 2$ za předpokladu, že pro všechna $d \mid n, 1 < d < n$ platí:

$$Q_d(1) = \begin{cases} p & \text{pokud } d \text{ je mocnina prvočísla } p \\ 1 & \text{pokud } d \text{ má dva různé prvočíselné dělitele} \end{cases}$$

Z Věty 2.2.1 plyne

$$Q_n(x) = \frac{x^n - 1}{Q_1(x) \prod_{\substack{d|n \\ 1<d<n}} Q_d(x)} = (x^{n-1} + \cdots x + 1) \cdot \frac{1}{\prod_{\substack{d|n \\ 1<d<n}} Q_d(x)}.$$

Dosadíme $x = 1$ a využijeme indukční předpoklad:

$$Q_n(1) = n \cdot \frac{1}{{p_1}^{e_1} \cdots {p_k}^{e_k}} = \frac{n}{n} = 1.$$

Příklad 19. Dokažte:

$$Q_n(-1) = \begin{cases} 0 & \text{pokud } n = 2 \\ -2 & \text{pokud } n = 1 \\ p & \text{pokud } n \text{ je dvojnásobek mocniny prvočísla } p \\ 1 & \text{jinak} \end{cases}$$

Řešení. Pro $n = 1$ a $n = 2$ stačí jednoduše dosadit do rovností $Q_1(x) = x-1$ a $Q_2(x) = x + 1$. Dostaneme

$$Q_2(-1) = -1 + 1 = 0,$$
$$Q_1(-1) = -1 - 1 = -2.$$

Dále vyřešíme případ, kdy $n = 2p^e$ pro p prvočíslo a e přirozené číslo. Nejprve se podívejme na $p = 2$. Budeme postupovat indukcí podle e. Pro $e = 1$ máme z Příkladu 2, že $Q_{2\cdot 2}(x) = Q_4(x) = x^2 + 1$, a tedy $Q_4(-1) = 1 + 1 = 2$.

Předpokládejme, že $Q_{2\cdot 2^{e-1}}(-1) = Q_{2^e}(-1) = 2$. Platí potom, že $Q_{2\cdot 2^e}(-1) = Q_{2^{e+1}}(-1) = 2?\ 2 \mid 2^e$, a tedy lze použít Příklad 13: $Q_{2\cdot 2^e}(x) = Q_{2^e}(x^2)$, a po dosazení

$$Q_{2\cdot 2^e}(-1) = Q_{2^e}((-1)^2) = Q_{2^e}(1) = 2,$$

kde jsme v poslední úpravě použili vztah pro n mocninu prvočísla z Příkladu 18.

Pro p liché použijeme Příklad 15, neboť $p^e \geq 3$ je opět liché číslo:

$$Q_{2\cdot p^e}(-1) = Q_{p^e}(-(-1)) = Q_{p^e}(1) = p,$$

kde jsme opět využili vztah z Příkladu 18 pro n mocninu prvočísla.

Podívejme se na poslední případ, tzn. na jakékoli jiné n, než jsme dosud

diskutovali. Rozlišíme dvě možnosti:

(1) $n = {p_1}^{e_1} \cdots {p_k}^{e_k}$, kde $p_1, \ldots, p_k$ jsou lichá prvočísla,
(2) $n = 2^e \cdot {p_1}^{e_1} \cdots {p_k}^{e_k}$, kde $p_1, \ldots, p_k$ jsou lichá prvočísla a nastane právě jedna z těchto variant: buď $(e = 1 \ \& \ k \geq 2)$ nebo $(e > 1 \ \& \ k \geq 1)$.

(1) Začněme s případem, kdy n je liché. Budeme postupovat indukcí podle k.
Pro $k = 1$ platí z Příkladu 18 $Q_{p^e}(x) = 1 + x^{p^{e-1}} + \cdots + x^{(p-1)p^{e-1}}$. Vidíme, že ve výsledku máme p sčítanců: k jedničce přičítáme dalších $p-1$ sčítanců (sudý počet), kde je u x v exponentu střídavě liché a sudé číslo. Čili po dosazení -1 se posledních $p-1$ členů navzájem odečte a zbyde $Q_{p^e}(-1) = 1$.

Označme $m = {p_1}^{e_1} \ldots {p_{k-1}}^{e_{k-1}}$. Plyne z předpokladu $Q_m(-1) = 1$ rovnost $Q_{m{p_k}^{e_k}}(-1) = 1$?

Nejprve si upravíme $Q_{m{p_k}^{e_k}}(x)$. Použijeme Příklad 14 a Příklad 12 (předpoklady budou splněny):

$$Q_{m{p_k}^{e_k}}(x) = Q_{m{p_k}}\left(x^{{p_k}^{e_k-1}}\right) = \frac{Q_m\left(x^{{p_k}^{e_k}}\right)}{Q_m\left(x^{{p_k}^{e_k-1}}\right)}.$$

Po dosazení -1 a využití indukčního předpokladu dostaneme

$$Q_{m{p_k}^{e_k}}(-1) = \frac{Q_m\left((-1)^{{p_k}^{e_k}}\right)}{Q_m\left((-1)^{{p_k}^{e_k-1}}\right)} = \frac{Q_m(-1)}{Q_m(-1)} = \frac{1}{1} = 1.$$

(2) Nakonec nám zbyly poslední dva případy. Nejprve se podíváme na $e = 1$ a $k \geq 2$. Opět se nám bude hodit Příklad 15 a Příklad 18.

$$Q_{2 \cdot {p_1}^{e_1} \cdots {p_k}^{e_k}}(-1) = Q_{{p_1}^{e_1} \cdots {p_k}^{e_k}}(1) = 1.$$

Dále vyřešíme variantu $e > 1$ a $k \geq 1$ indukcí podle k.

Pro $k = 1$ plyne z Příkladu 14 toto: $Q_{2^e {p_1}^{e_1}}(x) = Q_{2{p_1}^{e_1}}(x^{2^{e-1}})$. Jelikož 2^{e-1} je sudé číslo, máme po dosazení -1 s využitím výsledku z Příkladu 18:

$$Q_{2^e {p_1}^{e_1}}(-1) = Q_{2{p_1}^{e_1}}(1) = 1.$$

Označme $r = 2^e {p_1}^{e_1} \cdots {p_{k-1}}^{e_{k-1}}$ a předpokládejme, že dokazované tvrzení platí pro $k-1$, tj. že $Q_r(-1) = 1$. Ukažme, že potom platí i $Q_{r{p_k}^{e_k}}(-1) = 1$. Nakonec i v tomto případě použijeme Příklad 14 a Příklad 12:

$$Q_{r{p_k}^{e_k}}(x) = Q_{r{p_k}}(x^{{p_k}^{e_k-1}}) = \frac{Q_r\left(x^{{p_k}^{e_k}}\right)}{Q_r\left(x^{{p_k}^{e_k-1}}\right)}.$$

Nyní stačí pouze dosadit za x prvek -1 a s využitím indukčního předpokladu konečně dostáváme

$$Q_{r{p_k}^{e_k}}(-1) = \frac{Q_r\left((-1)^{{p_k}^{e_k}}\right)}{Q_r\left((-1)^{{p_k}^{e_k-1}}\right)} = \frac{Q_r(-1)}{Q_r(-1)} = \frac{1}{1} = 1.$$

Řešení. V předchozím řešení jsme předvedli případy, kdy $n = 1, n = 2$ a n je dvojnásobek mocniny prvočísla p. Nyní ukážeme jednodušší řešení poslední možnosti, která zahrnuje všechny jiné podoby n. Jak jsme si rozebrali výše, jde o body (1) a (2) z předchozího řešení.

(1) : Máme $n > 1$ liché, $n = {p_1}^{e_1} \cdots {p_k}^{e_k}$. V předchozím řešení jsme ověřili případ $k = 1$. Využijeme řešení Příkladu 18 a napíšeme si $Q_n(x)$ takto:

$$Q_n(x) = (x^{n-1} + \cdots x + 1) \cdot \frac{1}{\prod_{\substack{d|n \\ 1<d<n}} Q_d(x)}.$$

Předpokládejme, že pro $d \mid n, 1 < d < n$ platí $Q_d(-1) = 1$. Stačí už jen dosadit $x = -1$. Dostaneme

$$Q_n(-1) = ((-1)^{n-1} + \cdots + (-1) + 1) \cdot \frac{1}{\prod_{\substack{d|n \\ 1<d<n}} Q_d(-1)} = 1 \cdot \frac{1}{1 \cdots 1} = 1.$$

V případě (2) je n vždy sudé. Pokud $e = 1$ a $k \geq 2$, je důkaz, ve kterém využíváme Příklad 15, jednoduchý (byl již předveden výše). Variantu $e > 1$ a $k = 1$ jsme také již ukázali v předchozím řešení. Předpokládejme tedy, že $e > 1, k > 1$ a pro všechna $d \mid n, 2 < d < n$ je

$$Q_d(-1) = \begin{cases} p & \text{pokud } d \text{ je dvojnásobek mocniny prvočísla } p \\ 1 & \text{jinak} \end{cases}$$

Chceme ukázat, že potom i $Q_n(-1) = 1$. S využitím Věty 2.2.1 můžeme říci, že platí

$$\begin{aligned} Q_n(x) &= \frac{x^n - 1}{Q_1(x)Q_2(x)\prod_{\substack{d|n \\ 2<d<n}} Q_d(x)} = \frac{x^n - 1}{(x-1)(x+1)\prod_{\substack{d|n \\ 2<d<n}} Q_d(x)} = \\ &= (x^{n-1} - x^{n-2} + \cdots - x^2 + x - 1) \cdot \frac{1}{(x-1)\prod_{\substack{d|n \\ 2<d<n}} Q_d(x)}. \end{aligned}$$

Nyní stačí dosadit $x = -1$ a s využitím indukčního předpokladu dostáváme

$$Q_n(-1) = ((-1)^{n-1} - \cdots + (-1) - 1) \cdot \frac{1}{-2 \cdot \prod_{\substack{d|n \\ 2<d<n}} Q_d(-1)} =$$
$$= (-n) \cdot \frac{1}{-2 \cdot 2^{e-1} \cdot {p_1}^{e_1} \cdots {p_k}^{e_k}} = \frac{-n}{-n} = 1.$$

Literatura

[1] Lidl, R., Niederreiter, H.: *Finite fields*, Second edition, Cambridge University Press, 1997.

[2] Barto, L., Tůma, J.: *Konečná tělesa*, pouze elektronická podoba, 2008.

[3] Stanovský, D.: *Počítačová algebra*, pouze elektronická podoba, 2010.

[4] Drápal, A.: *Teorie čísel a RSA*, pouze elektronická podoba.