ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PEDAGOGICKÁ
KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

POLYNOMY PRO DĚLENÍ KRUHU

BAKALÁŘSKÁ PRÁCE

Lenka Němcová

Přírodovědná studia, obor Matematická studia

Vedoucí práce: Doc. RNDr. Jaroslav Hora, CSc.

Plzeň, 2014

Prohlašuji, že jsem bakalářskou práci s názvem „Polynomy pro dělení kruhu“ vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni 25. června 2014 ……..

vlastnoruční podpis

Děkuji vedoucímu mé bakalářské práce Doc. RNDr. Jaroslavu Horovi, CSc. za inspirativní vedení mé práce, cenné rady a připomínky, za jeho ochotu a čas.

Zde se nachází oficiální zadání bakalářské práce.

Obsah

Úvod

Tato bakalářská práce má za úkol zkoumání binomických rovnic a k nim příslušných polynomů pro dělení kruhu, jinými slovy cyklotomických polynomů. Je v ní řešena otázka sestrojitelnosti pravidelných mnohoúhelníků, čímž se už odedávna zabývali velcí matematikové jako například Gauss.

V první kapitole se budeme zabývat binomickými rovnicemi obecně a primitivními n-tými odmocninami. Vysvětlíme si význam algebraického a goniometrického tvaru komplexního čísla. Připomeneme si Moivreovu větu a její odvození z Eulerova vzorce. Dále si připomeneme větu o rovnosti dvou komplexních čísel. Uvedeme speciální případy binomické rovnice a vysvětlíme, v jakém tvaru lze zapsat všechny její kořeny. Dostaneme se k tomu, proč se binomické rovnice nazývají rovnicemi pro dělení kruhu. Dále uvedeme vlastnosti těchto rovnic a vlastnosti jejich kořenů. Důležitou větou pro nás bude věta o primitivních kořenech a zmíníme se také o Eulerově funkci.

V druhé kapitole si vysvětlíme pojem polynomy pro dělení kruhu neboli cyklotomické polynomy. Uvedeme, jak tyto polynomy vypadají, jaký mají tvar a jejich nejdůležitější vlastnosti. V této kapitole se také budeme zabývat otázkou sestrojitelnosti pravidelných mnohoúhelníků pouze s pomocí pravítka a kružítka, protože ne každý mnohoúhelník lze takto zkonstruovat. Vysvětlíme si pojmy eukleidovská konstrukce a Fermatova prvočísla. V této části je text doplněn o ukázky konstrukcí některých jednoduchých mnohoúhelníků. Také podáme návod na přibližnou konstrukci úhlu $10°$. Významným tématem bude německý matematik a fyzik Johann Friedrich Carl Gauss a jeho objev týkající se sestrojení pravidelného sedmnáctiúhelníku. Ukážeme si jeho konstrukci na základě Gaussových period. To ovšem není jediný způsob jeho konstrukce, jako další tedy ukážeme konstrukci Richmondovu. Dále si uvedeme větu týkající se sestrojitelnosti a druhých odmocnin, podmínky, kdy je binomická rovnice a cyklotomický polynom řešitelný pomocí druhých odmocnin. V poslední části této kapitoly je vysvětlen pojem reciproká rovnice a příklad řešení binomické rovnice pomocí převodu na reciprokou.

Ve třetí kapitole se budeme zabývat polynomy pro dělení kruhu a jejich ireducibilitou. Vysvětlíme si pojmy primitivní, normovaný, reducibilní a ireducibilní polynom. Ukážeme si využití Hornerova schématu při rozkladu polynomu na kořenové činitele. Uvedeme

základní vlastnosti ireducibilních polynomů a dokážeme, že všechny cyklotomické polynomy jsou ireducibilní.

V poslední – čtvrté kapitole se budeme zabývat koeficienty cyklotomických polynomů. Ačkoliv by se mohlo na první pohled zdát, že koeficienty polynomů pro dělení kruhu budou vždy rovné jedné, není tomu tak. Uvedeme některé příklady těchto výjimek. Seznámíme se s větami týkajícími se koeficientů a naučíme se metodu určování koeficientů podle Lama a Leunga.

1. BINOMICKÁ ROVNICE, PRIMITIVNÍ N-TÉ ODMOCNINY

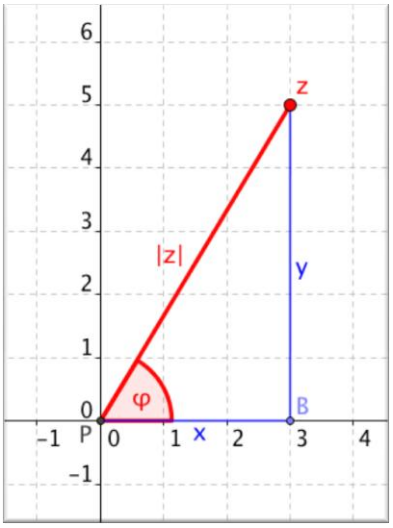
1.1 Algebraický a goniometrický tvar komplexního čísla

Všechna komplexní čísla můžeme zapsat v algebraickém tvaru $z = x + yi$, kde x je reálná část, y je imaginární část a i je imaginární jednotka, pro kterou platí:

- $i^2 = -1$,
- $i^3 = -i$,
- $i^4 = 1$.

Tento tvar poskytuje informace k zaznamenávání komplexních čísel do Gaussovy roviny jako bodů popsaných uspořádanými dvojicemi $[x, y]$, reálná část se zakresluje na osu x a imaginární část na osu y.

K vyjádření komplexního čísla v goniometrickém tvaru potřebujeme znát vzdálenost komplexního čísla od počátku, tedy délku spojnice $|z|$, jejíž hodnota vyjadřuje absolutní hodnotu komplexního čísla, a úhel φ, který svírá kladná poloosa x se spojnicí $|z|$, jak je vidět na obrázku.



Obrázek 1: Grafické znázornění komplexního čísla v goniometrickém tvaru

Absolutní hodnota se vypočte pomocí Pythagorovy věty jako $|z| = \sqrt{x^2 + y^2}$ a pomocí vlastností goniometrických funkcí, tj. $\cos\varphi = \frac{x}{|z|}$, $\sin\varphi = \frac{y}{|z|}$, dopočteme úhel φ, pro který platí, že $0 \leq \varphi \leq 2\pi$. Goniometrický tvar komplexního čísla z pak vypadá následovně:

$$z = |z|(\cos\varphi + i\sin\varphi).$$

[1] [16]

Příklad: Komplexní číslo je dáno v algebraickém tvaru $z = 1 + i$. Převeďte komplexní číslo z do goniometrického tvaru.

Postup převodu je následující. Jako první si vypočteme absolutní hodnotu komplexního čísla z:

$$|z| = \sqrt{x^2 + y^2} = \sqrt{1^2 + 1^2} = \sqrt{2}\,.$$

Dále zjistíme hodnotu úhlu φ:

Platí $\sin\varphi = \frac{y}{|z|} = \frac{1}{\sqrt{2}}$ a $\cos\varphi = \frac{x}{|z|} = \frac{1}{\sqrt{2}}$. Protože $0 \leq \varphi \leq 2\pi, \sin\varphi > 0, \cos\varphi > 0$, je φ úhel z I. kvadrantu a snadno zjistíme, že $\varphi = \frac{\pi}{4}$.

Nyní tedy můžeme zapsat goniometrický tvar komplexního čísla:

$$z = |z|(\cos\varphi + i\sin\varphi) = \sqrt{2}(\cos\tfrac{\pi}{4} + i\sin\tfrac{\pi}{4}).$$

Příklad: Komplexní číslo je dáno v goniometrickém tvaru $z = \frac{\sqrt{2}}{2}(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4})$. Převeďte komplexní číslo z do algebraického tvaru.

Při převodu komplexního čísla z goniometrického tvaru na tvar algebraický se používají pouze dvě aritmetické úpravy, a to takové, že se v komplexním číslu nahradí hodnoty goniometrických funkcí $\cos\varphi$ a $\sin\varphi$ za číselné hodnoty a pak se provede roznásobení závorky:

Výraz $\cos\frac{3\pi}{4}$ je roven $-\frac{1}{\sqrt{2}}$ a výraz $\sin\frac{3\pi}{4}$ je roven $\frac{1}{\sqrt{2}}$.

Dále už jen roznásobíme:

$$z = \frac{\sqrt{2}}{2}\left(-\frac{1}{\sqrt{2}} + i\,\frac{1}{\sqrt{2}}\right) = -\frac{\sqrt{2}}{2\sqrt{2}} + i\,\frac{\sqrt{2}}{2\sqrt{2}},$$

což se po provedení zkrácení odmocnin rovná:

$$z = -\frac{1}{2} + i\,\frac{1}{2}.$$

Věta 1.1.1 (Moivreova věta)

Moivreova věta říká, že pro každé n přirozené a libovolné číslo φ komplexní (nebo reálné, neboť jsou podmnožinou) platí:

$$(\cos\varphi + i\sin\varphi)^n = (\cos(n\varphi) + i\sin(n\varphi)).$$

Věta je odvozena z Eulerova vzorce $e^{ix} = \cos x + i\sin x$ a používá se pro vyjádření n-tých odmocnin z jedné, nebo obecně $\sqrt[n]{z}$, a pro vyjádření $\cos(k\varphi)$ a $\sin(k\varphi)$, $k \in N$, pomocí funkcí $\sin\varphi$ *a* $\cos\varphi$.

[1]

Příklad: Pomocí Moivreovy věty vypočtěte mocninu komplexního čísla:

$$(\cos\frac{3\pi}{2}+i\sin\frac{3\pi}{2})^7=\left(\cos\frac{21\pi}{2}+i\sin\frac{21\pi}{2}\right)=\left(\cos\frac{\pi}{2}+i\sin\frac{\pi}{2}\right)=0+1i=i\,.$$

Věta 1.1.2 (O rovnosti dvou komplexních čísel)

Dvě komplexní čísla vyjádřená v algebraickém tvaru jsou si rovna právě tehdy, když se rovnají jejich reálné části a zároveň se rovnají jejich imaginární části.

Dvě komplexní čísla vyjádřená v goniometrickém tvaru jsou si rovna právě tehdy, když se rovnají jejich absolutní hodnoty a zároveň se rovnají jejich argumenty, popřípadě se liší o celočíselný násobek 2π.

[1]

1.2 Binomická rovnice

Binomickou rovnicí v obecném tvaru rozumíme algebraickou rovnici

$$pz^n+q=0,\quad p,q\neq 0$$

kde p,q jsou reálná nebo komplexní čísla a n je číslo přirozené.

Speciálními případy binomické rovnice jsou:

- lineární rovnice, kde $n=1$: $pz+q=0$,
- kvadratická rovnice, kde $n=2$: $pz^2+q=0$.

Postupnými úpravami binomické rovnice $pz^n+q=0$

$z^n=-\frac{q}{p}$ … substituce $-\frac{q}{p}=a$

$z^n-a=0$ … normovaný tvar bin. rovnice

dostáváme $z=\sqrt[n]{a}\,.$

Každé z řešení uvedené rovnice je n-tou odmocninou z čísla a.

- Je-li $a=0$, pak pro všechna $n\in N$ má rovnice $z^n=0$ právě jedno řešení, a to $z=0$,
- je-li $a\neq 0$, pak je $z\neq 0$ a rovnice $z^n=a$ má právě n řešení.

Obě čísla vyjádříme v goniometrických tvarech:

$$a=|a|(\cos\alpha+i\sin\alpha)$$
$$z=|z|(\cos\beta+i\sin\beta)$$
$$\vdots$$
$$z^n=a$$
$$|z|^n(\cos n\beta+i\sin n\beta)=|a|(\cos\alpha+i\sin\alpha)$$

Z věty o rovnosti dvou komplexních čísel v goniometrickém tvaru víme, že čísla jsou si rovna, pokud se rovnají jejich absolutní hodnoty a jejich argumenty se rovnají nebo liší o celočíselný násobek 2π.

Z toho tedy plyne:

$$|z|^n = |a| \qquad \text{neboli} \qquad |z| = \sqrt[n]{|a|}$$

$$n\beta = \alpha + 2k\pi, k \in Z \qquad \beta = \frac{\alpha+2k\pi}{n}, k \in Z$$

a všechna řešení rovnice $z^n = a$ (tj. tvary všech n-tých odmocnin z čísla a) lze vyjádřit ve tvaru:

$$z_{k+1} = \sqrt[n]{z} = \left\{\sqrt[n]{|a|}\left(\cos\frac{\varphi+2k\pi}{n} + i\sin\frac{\varphi+2k\pi}{n}\right) : 0 \le k \le n-1\right\}, k \in Z, n \in N.$$

Pokud bychom uvažovali $k \ge n$, dostali bychom stejná řešení, která by měla argumenty lišící se o 2π, tedy o periodu jak sinu, tak kosinu.

[2]

Příklad: Vypočti kořeny rovnice $w = \sqrt[4]{v}$, kde $v = 256(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3})$.

Komplexní číslo v je již zadáno v goniometrickém tvaru.

$$w = \sqrt[4]{v} = \sqrt[4]{256(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3})}$$

Všechna řešení budou mít tvar: $w_{k+1} = \sqrt[4]{256}\left(\cos\frac{\frac{4\pi}{3}+2k\pi}{4} + i\sin\frac{\frac{4\pi}{3}+2k\pi}{4}\right), k = 0,1,2,3.$

Vzhledem ke stupni odmocniny má rovnice právě čtyři řešení, a to $w_1, \dots, w_4$.

$$w_1 = 4\left(\cos\frac{\frac{4\pi}{3}}{4} + i\sin\frac{\frac{4\pi}{3}}{4}\right) = 4\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right) = 4\left(\frac{1}{2} + i\,\frac{\sqrt{3}}{2}\right) = 2 + 2\sqrt{3}\,i,$$

$$w_2 = 4\left(\cos\frac{\frac{4\pi}{3}+2\pi}{4} + i\sin\frac{\frac{4\pi}{3}+2\pi}{4}\right) = 4\left(\cos\frac{5\pi}{6} + i\sin\frac{5\pi}{6}\right) = 4\left(-\frac{\sqrt{3}}{2} + i\,\frac{1}{2}\right)$$

$$= -2\sqrt{3} + 2\,i,$$

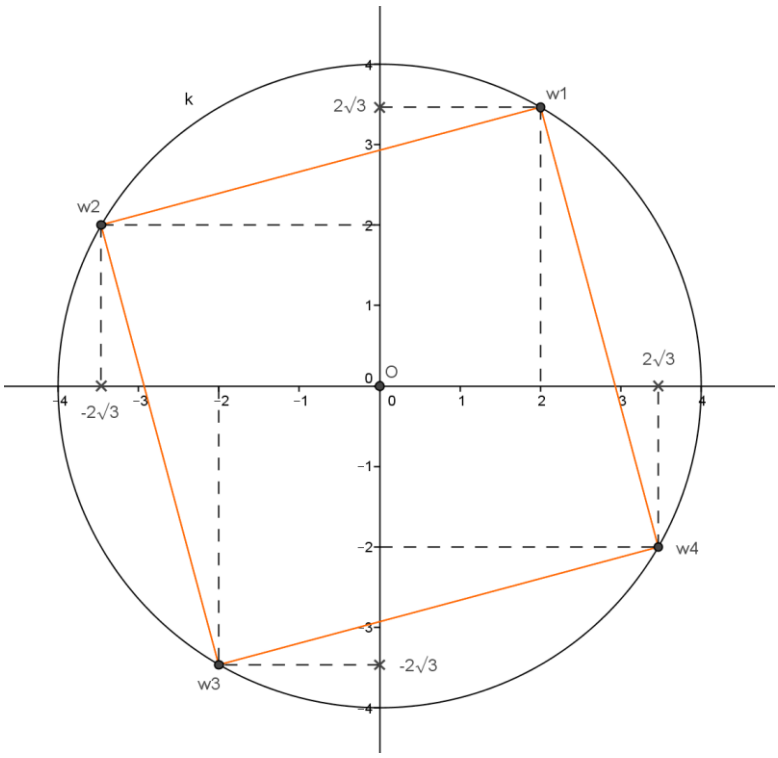
$$w_3 = 4\left(\cos\frac{\frac{4\pi}{3}+4\pi}{4} + i\sin\frac{\frac{4\pi}{3}+4\pi}{4}\right) = 4\left(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}\right) = 4\left(-\frac{1}{2} - i\,\frac{\sqrt{3}}{2}\right)$$

$$= -2 - 2\sqrt{3}\,i,$$

$$w_4 = 4\left(\cos\frac{\frac{4\pi}{3}+6\pi}{4} + i\sin\frac{\frac{4\pi}{3}+6\pi}{4}\right) = 4\left(\cos\frac{11\pi}{6} + i\sin\frac{11\pi}{6}\right) = 4\left(\frac{\sqrt{3}}{2} - i\,\frac{1}{2}\right)$$

$$= 2\sqrt{3} - 2\,i.$$

Lze vyjádřit: $w_1 = [2,2\sqrt{3}], w_2 = [-2\sqrt{3},2], w_3 = [-2,-2\sqrt{3}], w_4 = [2\sqrt{3},-2]$ a zakreslit do Gaussovy roviny:



Obrázek 2: Zakreslení kořenů do Gaussovy roviny - vznik čtverce

Všechny n-té odmocniny z čísla a mají tedy stejnou absolutní hodnotu $\sqrt[n]{|a|}$ a argumenty lišící se o násobek $\frac{2\pi}{n}$. Pokud tyto kořeny znázorníme v Gaussově rovině, dostaneme pravidelný n-úhelník vepsaný do kružnice o poloměru $\sqrt[n]{|a|}$ a se středem v počátku soustavy souřadnic. Smysl to má pouze u $n \geq 3$, pro $n = 2$ jsou komplexními odmocninami dvě opačná komplexní čísla. Rozdělíme-li tento pravidelný n-úhelník na n stejných trojúhelníků, pak jsou tyto trojúhelníky rovnoramenné. Základnu tvoří vždy příslušná strana mnohoúhelníku, ramena mají shodnou délku s poloměrem kružnice. Středový úhel mnohoúhelníku, tedy úhel při hlavním vrcholu rovnoramenného trojúhelníka, je roven $\frac{180°}{n}$. Proto se binomickým rovnicím ve tvaru $z^n - a = 0$ říká rovnice pro dělení kruhu.

[3]

1.3 Rovnice pro dělení kruhu

Uvažujme jednotkovou kružnici. Rovnicí pro dělení kruhu budeme nazývat binomickou rovnici ve tvaru $x^n - 1 = 0$. Číslo x je n-tý kořen z jedné, právě když $x^n = 1$.

Věta 1.3.1 (Kořeny rovnice pro dělení kruhu)

Rovnice pro dělení kruhu neboli binomická rovnice ve tvaru $x^n - 1 = 0$ má právě n kořenů. Ty jsou dány vztahem

$$x_{k+1} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, k = 0, 1, 2, \dots, n-1.$$

Tj.: $x_1 = \cos\frac{0}{n} + i\sin\frac{0}{n} = 1$

$x_2 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} = \varepsilon$

$x_3 = \cos\frac{4\pi}{n} + i\sin\frac{4\pi}{n} = \varepsilon^2$

$x_4 = \cos\frac{6\pi}{n} + i\sin\frac{6\pi}{n} = \varepsilon^3$

$\vdots$

$x_n = \cos\frac{2(n-1)\pi}{n} + i\sin\frac{2(n-1)\pi}{n} = \varepsilon^{n-1}$

Důsledek:

Označíme-li $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, potom podle Moivreovy věty platí

$$\varepsilon^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}.$$

Proto všechny kořeny rovnice $x^n - 1 = 0$ (neboli všechny n-té odmocniny z jedné) můžeme označit takto:

$$1, \varepsilon, \varepsilon^2, \varepsilon^3, \dots, \varepsilon^{n-1}.$$

[4]

Díky číslu $a = 1$ bude mít n-úhelník vzniklý po zakreslení kořenů do Gaussovy roviny vždy jeden vrchol v bodě $[1,0]$.

Příklad: Vypočti kořeny binomické rovnice $x^4 - 1 = 0$.

Kořeny binomické rovnice vypočteme pomocí vzorce v předchozí větě. Máme tedy:

$$x_1 = \cos\frac{0}{4} + i\sin\frac{0}{4} = 1 + 0i,$$

$$x_2 = \cos\frac{2\pi}{4} + i\sin\frac{2\pi}{4} = 0 + 1i,$$

$$x_3 = \cos\frac{4\pi}{4} + i\sin\frac{4\pi}{4} = -1 + 0i,$$

$$x_4 = \cos\frac{6\pi}{4} + i\sin\frac{6\pi}{4} = 0 - 1i.$$

Ověříme ještě platnost umocňování. Označme podle věty $x_2 = \varepsilon = i$, potom:

$$x_3 = \varepsilon^2 = i^2 = -1,$$

$$x_4 = \varepsilon^3 = i^3 = -i.$$

Věta 1.3.2

Vezměme libovolnou konkrétní hodnotu kořene rovnice $x^n - 1 = 0$ a označme ji x_0. Potom všechny další kořeny rovnice $x^n - 1 = 0$ dostaneme jako součin tohoto čísla s mocninou čísla $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, tj.

$$x_1 = x_0\,\varepsilon,$$
$$x_2 = x_0\,\varepsilon^2,$$
$$x_3 = x_0\,\varepsilon^3$$
$$\vdots$$
$$x_n = x_0\,\varepsilon^n.$$

[4]

Příklad: Berme v úvahu výsledky předchozího příkladu.

Vezměme libovolný kořen, například třetí kořen $x_3 = -1$ a označme ho jako x_0, a číslo $\varepsilon = \cos\frac{2\pi}{4} + i\sin\frac{2\pi}{4}$, o kterém víme, že je rovno imaginární jednotce i. Potom všechny ostatní kořeny získáme podle předchozí věty takto:

$$x_0 = -1,$$

$$x_1 = x_3\,\varepsilon = -1.i = -i,$$

$$x_2 = x_3\,\varepsilon^2 = -1.i^2 = 1,$$

$$x_3 = x_0\,\varepsilon^3 = -1.i^3 = i.$$

Příklad:

a) Vypočti kořeny binomické rovnice $x^2 - 1 = 0$.

$x_{1,2} = \pm 1$.

b) Vypočti kořeny binomické rovnice $x^3 - 1 = 0$.

$x_1 = 1$

$(x^3 - 1) : (x - 1) = x^2 + x + 1$

$x^2 + x + 1 = 0$

$D = b^2 - 4ac = 1 - 4 = -3$

$x_{2,3} = \frac{-b \pm \sqrt{D}}{2a} = \frac{-1 \pm \sqrt{3}\, i}{2} = \frac{1}{2}\left(-1 \pm \sqrt{3}\, i\right).$

Věta 1.3.3

Mějme rovnici $x^n - 1 = 0$. Existují-li dvě nesoudělná čísla n_1, n_2, pro která platí

$$n_1 n_2 = n$$

a zároveň platí, že rovnice $x^{n_1} - 1 = 0$ má řešení $\alpha_k, (k = 1,2, \dots, n_1)$, a rovnice $x^{n_2} - 1 = 0$ má řešení $\beta_l, (l = 1,2, \dots, n_2)$, pak hodnota $n_1 n_2$ dává počet součinů čísel α_k, β_l, které udávají všechny kořeny rovnice $x^n - 1 = 0$.

Důkaz:

Rovnice $x^{n_1 n_2} - 1 = 0$ má kořeny x_{kl}, rovnice $x^{n_1} - 1 = 0$ má kořeny α_k, rovnice $x^{n_2} - 1 = 0$ má kořeny β_l, kde $k = 1,2, \dots, n_1$ a $l = 1,2, \dots, n_2$.

$$\alpha_k = \cos\frac{2k\pi}{n_1} + i \sin\frac{2k\pi}{n_1}$$

$$\beta_l = \cos\frac{2l\pi}{n_2} + i \sin\frac{2l\pi}{n_2}$$

$$x_{kl} = \cos\left(\frac{2k\pi}{n_1} + \frac{2l\pi}{n_2}\right) + i \sin\left(\frac{2k\pi}{n_1} + \frac{2l\pi}{n_2}\right)$$

Je zřejmé, že číslo x_{kl} je kořenem rovnice $x^{n_1 n_2} - 1 = 0$. Dále musí platit, že všechny její kořeny jsou navzájem různé. Předpokládejme, že dva kořeny budou shodné, $\alpha_k \beta_l = \alpha_{\acute{k}} \beta_{\acute{l}}$, kde $k, \acute{k} = 1, \dots, n_1$ a $l, \acute{l} = 1, \dots, n_2$. Platí $1 \le k \le \acute{k} \le n_1$ a $1 \le l \le \acute{l} \le n_2$. Platí tedy i $\frac{\alpha_k}{\alpha_{\acute{k}}} = \frac{\beta_l}{\beta_{\acute{l}}}$. Použijme pravidlo o dělení komplexních čísel:

$$\cos\frac{2\pi(k-\acute{k})}{n_1} + i \sin\frac{2\pi(k-\acute{k})}{n_1} = \cos\frac{2\pi(l-\acute{l})}{n_2} + i \sin\frac{2\pi(l-\acute{l})}{n_2}$$

$$\frac{k-\acute{k}}{n_1} = \frac{l-\acute{l}}{n_2}$$

$$(k-\acute{k})n_2 = (l-\acute{l})n_1$$

Z toho plyne, že číslo $(k-\acute{k})n_2$ je dělitelné číslem n_1. Ovšem číslo n_2 je s číslem n_1 nesoudělné, proto musí být $(k-\acute{k})$ dělitelné n_1. Ale $|k-\acute{k}| < n_1$, to znamená, že $k-\acute{k}$

se musí rovnat nule a tedy $k = \acute{k}$ a zároveň i $l = \acute{l}$. Rovnost tedy nastává právě v tom případě, kdy $k = \acute{k}$ a $l = \acute{l}$, čímž je dokázáno, že jsou všechna řešení navzájem různá.

[13]

Příklad: Vypočti kořeny binomické rovnice $x^6 - 1 = 0$.

Exponent $n = 6$ lze rozložit na součin $6 = 2.3$, pak $n_1 = 2, n_2 = 3$. Kořeny rovnic $x^2 - 1 = 0$ a $x^3 - 1 = 0$ jsme zjistili v předchozím příkladě.

Označíme-li $\varepsilon = \frac{1}{2}(-1 + \sqrt{3}\, i)$, pak $a_k = \pm 1, (k = 1, 2)$, $\beta_l = 1, \varepsilon, \varepsilon^2, (l = 1, 2, 3)$.

Všemi kořeny rovnice $x^6 - 1 = 0$ jsou tedy čísla $1, -1, \varepsilon, \varepsilon^2, -\varepsilon, -\varepsilon^2$.

Jak je vidět, kořeny 1 a -1 jsou zároveň kořeny rovnice $x^2 - 1 = 0$, další dva kořeny jsou zároveň kořeny rovnice $x^3 - 1 = 0$. Zbývající kořeny $-\varepsilon, -\varepsilon^2$ vyhovují až řešení zadané rovnice. Takové kořeny se nazývají primitivní.

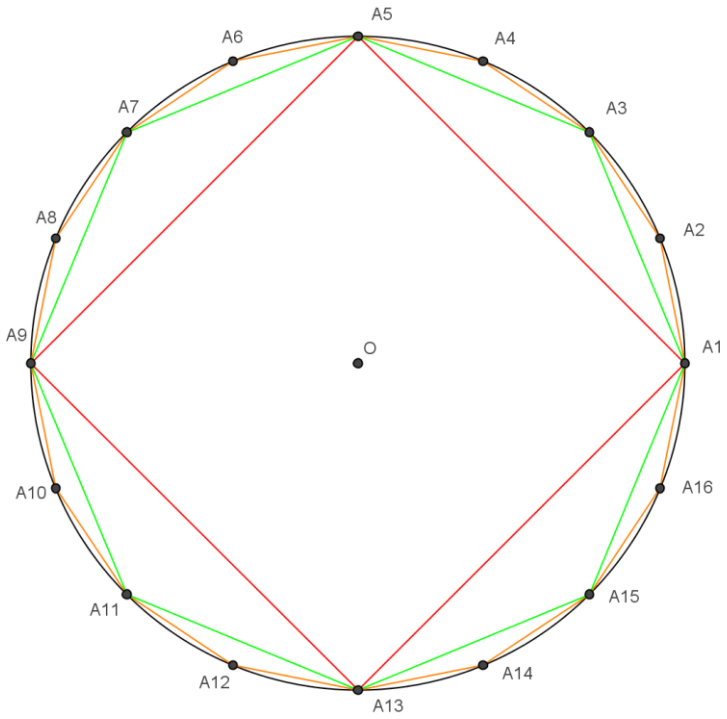
Věta 1.3.4 (Primitivní kořeny)

Kořeny rovnice $x^n - 1 = 0$ nazýváme primitivními kořeny, právě když nejsou řešením žádné rovnice ve tvaru $x^m - 1 = 0$, kde $1 \leq m < n$.

Zároveň platí, že číslo $\varepsilon = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}, n \geq 1$ je vždy primitivním kořenem rovnice $x^n - 1 = 0$.

[13]

Příklad:



Obrázek 3: Pravidelný šestnáctiúhelník a primitivní kořeny

Na obrázku je oranžovou barvou znázorněn pravidelný šestnáctiúhelník. Binomická rovnice $x^{16}-1=0$ má $\varphi(16)=8$ primitivních kořenů, kterým odpovídají vrcholy $A_2, A_4, A_6, A_8, A_{10}, A_{12}, A_{14}, A_{16}$. Ostatní kořeny této binomické rovnice netvoří vlastní vrcholy pravidelného šestnáctiúhelníku. Vrchol A_1 je vrchol, který tvoří počáteční vrchol všech mnohoúhelníků, průměr A_1A_9 dělí kružnici na dvě půlkružnice. Vrcholy A_5, A_{13} náleží již pravidelnému čtyřúhelníku, znázorněnému červenou barvou, a zbylé vrcholy A_3, A_7, A_{11}, A_{15} jsou vlastní pravidelnému osmiúhelníku, znázorněnému zelenou barvou.

Věta 1.3.5

Číslo δ je primitivním kořenem rovnice $x^n-1=0, n\geq 1$ právě tehdy, když všechna čísla $\delta, \delta^2, \delta^3, \dots, \delta^{n-1}, \delta^n$ jsou navzájem různá.

[13]

Věta 1.3.6 (O počtu primitivních kořenů)

Vezměme libovolný primitivní kořen a označme ho δ. Potom mezi čísly $\delta, \delta^2, \delta^3, \dots, \delta^{n-1}, \delta^n$ jsou primitivními kořeny rovnice $x^n-1=0$ právě ta čísla δ^k, jejichž exponent je nesoudělný s číslem n.

Důkaz:

a) sporem: Předpokládejme, že čísla n, k jsou soudělná,

tzn. $D(n,k)=D>1$. Potom platí $(\delta^k)^{\frac{n}{D}}=(\delta^n)^{\frac{k}{D}}=1^{\frac{k}{D}}=1$, z toho plyne, že δ^k je kořenem rovnice $x^{\frac{n}{D}}-1=0$, tedy není primitivním kořenem rovnice $x^n-1=0$.

b) Jsou-li čísla n, k nesoudělná, pak neexistuje žádné číslo t takové, pro které by platilo: $0<t<n$ a zároveň $(\delta^k)^t=1$. Je-li číslo δ primitivním kořenem, pak platí $(\delta^k)^t=\delta^{kt}=1$ právě tehdy, když je číslo kt dělitelné číslem n. Podle uvedené věty je číslo k nesoudělné s číslem n, proto musí být t dělitelné číslem n. Číslo t je podle podmínky menší než n, tedy takové číslo neexistuje.

[13]

Důsledkem tohoto je, že rovnice $x^n-1=0, n>1$ má přesně tolik primitivních kořenů, kolik existuje přirozených čísel menších než číslo n a zároveň nesoudělných s číslem n. Proto je primitivních n-tých kořenů z jedné právě $\varphi(n)$, kde φ je Eulerova funkce.

[13]

1.4 Eulerova funkce

Eulerovou funkcí rozumíme funkci na množině přirozených čísel N_1, přiřazující každému číslu z této množiny číslo představující počet nenulových přirozených čísel menších než toto číslo, která jsou s tímto číslem nesoudělná.

Věta 1.4.1 (Základní vlastnosti Eulerovy funkce)

Pro Eulerovu funkci platí:

1. m_1, m_2 jsou nesoudělná čísla, potom $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$,
2. $\varphi(p) = p - 1$, kde p je prvočíslo,
3. $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, kde p je prvočíslo.

[15]

Příklad: Vypočtěte následující hodnoty Eulerovy funkce.

$\varphi(7) = 7 - 1 = 6,$

$\varphi(16) = \varphi(2^4) = 2^{4-1}.(2-1) = 8,$

$\varphi(15) = \varphi(3)\varphi(5) = (3-1)(5-1) = 2.4 = 8,$

$\varphi(24) = \varphi(3)\varphi(8) = \varphi(3)\varphi(2^3) = (3-1).2^{3-1}.(2-1) = 2.4.1 = 8.$

2. POLYNOMY PRO DĚLENÍ KRUHU A JEJICH VLASTNOSTI

2.1 Cyklotomické polynomy

Zjistili jsme tedy, že k řešení binomické rovnice n-tého stupně $x^n - 1 = 0$ stačí najít alespoň jeden z jeho $\varphi(n)$ primitivních kořenů. Všechny ostatní kořeny dostaneme postupným umocňováním tohoto kořene r:

$$r, r^2, r^3, \dots, r^{n-1}, r^n = 1.$$

Vzhledem k tomu lze otázku řešení binomické rovnice převést na řešení takové rovnice $\phi(x) = 0$ (už ne binomické), jejímiž kořeny by byly primitivní kořeny (a jen tyto kořeny) dané binomické rovnice. Pak by libovolný kořen rovnice $\phi_n(x) = 0$ dával řešení binomické rovnice. Taková rovnice $\phi_n(x) = 0$ se pro souvislost binomických rovnic pro dělení kruhu nazývá polynomem pro dělení kruhu, jinými slovy cyklotomickým polynomem.

[4]

Polynom $\phi_n(x) = 0$ dělí kružnici na n částí, čímž vzniká pravidelný n-úhelník. Jsou-li kořeny takového polynomu všechny primitivní kořeny binomické rovnice $x^n - 1 = 0$, stupeň polynomu musí být roven číslu $\varphi(n)$. Jak tento polynom vypadá?

Věta 2.1.1 (Tvary cyklotomických polynomů)

Mějme $n = p$, kde číslo p je prvočíslo. Potom jsou všechny kořeny binomické rovnice $x^p - 1 = 0$, kromě kořene $x = 1$, kořeny primitivními. Polynom pro dělení kruhu má následující tvar:

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

[4]

V dalším případě mějme stupeň binomické rovnice roven mocnině některého prvočísla, tedy $n = p^\alpha$. Dělitelé čísla p^α jsou jistě čísla:

$$p^{\alpha-1}, p^{\alpha-2}, \ldots, p^2, p, 1.$$

Označíme-li libovolně některé toto číslo jako β, pak kořeny binomické rovnice $x^\beta - 1 = 0$ jsou zároveň kořeny binomické rovnice $x^{p^\alpha} - 1 = 0$. Nejsou tedy primitivními kořeny. Polynom, jehož řešení dávají pouze primitivní kořeny této rovnice, je roven:

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

[4]

Dále pro násobky libovolného lichého prvočísla p platí:

$$\phi_{2p}(x) = \frac{x^{2p} - 1}{x^p - 1} \cdot \frac{x - 1}{x^2 - 1} = x^{p-1} - x^{p-2} + x^{p-3} - \ \ldots - x + 1,$$

$$\phi_{4p}(x) = \frac{x^{4p} - 1}{x^{2p} - 1} \cdot \frac{x^2 - 1}{x^4 - 1} = x^{2p-2} - x^{2p-4} + x^{2p-6} - \ \ldots - x^2 + 1.$$

[10]

Obecně mějme libovolné n, např. $n = 33$.

Víme, že $\phi_1(x) = x - 1$, dále víme, že $x^3 - 1 = \phi_1(x)\phi_3(x)$, odkud získáme $\phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1$. Podobně je $x^{11} - 1 = \phi_1\phi_{11}$, z toho $\phi_{11}(x) = \frac{x^{11} - 1}{x - 1} = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Utvořme tedy rovnost

$$x^{33} - 1 = \phi_1(x)\phi_3(x)\phi_{11}(x)\phi_{33}(x),$$

odkud vyplývá

$$\phi_{33}(x) = \frac{x^{33} - 1}{\phi_1(x)\phi_3(x)\phi_{11}(x)}$$

$$= \frac{x^{33} - 1}{(x - 1)(x^2 + x + 1)(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)}$$

$$= x^{20} - x^{19} + x^{17} - x^{16} + x^{14} - x^{13} + x^{11} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1.$$

Tento postup výpočtu cyklotomického polynomu je jistě velmi srozumitelný a jednoduchý, ovšem je velmi náročný ze strany výpočtu, a to díky násobení ve jmenovali zlomku a následnému dělení polynomů. Proto matematikové hledali jiný obecný způsob nalezení cyklotomického polynomu, který by samotný výpočet co nejvíce zjednodušil. Jeden takový nyní uvedeme. V obecném výkladu může vypadat složitě, proto si tento postup řešení dále vysvětlíme na příkladu, kde uvidíme jeho výhodu.

Obecně mějme libovolné n. Číslo n rozložíme na součin prvočísel.
Polynom pro dělení kruhu vypadá následovně:

$$\phi_n(x) = \frac{\prod(x^{d_1}-1)}{\prod(x^{d_2}-1)}.$$

Čitatel i jmenovatel zlomku se skládá ze součinu dvojčlenů. Číslo d_1 nabývá hodnoty n a jeho dělitelů, které získáme vydělením čísla n sudým počtem prvočísel z rozkladu. Počet těchto dvojčlenů je roven $\alpha = 1 + C_m^2 + C_m^4 + \cdots$, kde m je počet prvočísel rozkladu. Číslo C_k^n je tzv. kombinační číslo, které vyjadřuje počet kombinací k-prvkových podmnožin vybíraných z n-prvkové množiny. Kombinační číslo C_k^n lze zapsat ve tvaru $\binom{n}{k}$ a vypočte se pomocí vzorce $\frac{n!}{k!(n-k)!}, n \geq k \geq 0$, jinak je rovno nule. Číslo d_2 pak nabývá hodnot dělitelů, které dostaneme po vydělení čísla n lichým počtem prvočísel z rozkladu. Tento počet je roven $\beta = C_m^1 + C_m^3 + C_m^5 + \cdots$. Čísla α, β jsou si rovna (podle Newtonova binomického rozvoje, kde součet binomických koeficientů stojících na sudých místech je roven součtu koeficientů stojících na sudých místech). Každý dvojčlen, jehož kořen by byl neprimitivním kořenem rovnice $x^n - 1 = 0$, je vykrácen. Díky tomu ve výrazu zbudou jen ty dvojčleny, jejichž kořeny dávají primitivní kořeny rovnice $x^n - 1 = 0$. Počet těchto dvojčlenů je roven $\varphi(n)$. Proto je pak polynom $\phi_n(x)$ stupně $\varphi(n)$ a jeho kořeny jsou všechny primitivní n-té odmocniny z jedné.

[4]

Příklad: Nalezněte cyklotomický polynom $\phi_{30}(x)$.
Index $n = 30$ rozložíme na součin prvočísel jako 2.3.5. Použijeme vzorec pro obecné n, který jsme si právě vysvětlili.
Jako první určíme počet hodnot, kterých nabývá číslo d_1 (při dělení sudým počtem prvočísel rozkladu):

$$d_1 = 1 + C_3^2 = 1 + \frac{3(3-1)}{2!} = 4.$$

Těmito hodnotami jsou:

$$30, \qquad \frac{30}{2.3} = 5, \qquad \frac{30}{2.5} = 3, \qquad \frac{30}{3.5} = 2.$$

Stejně tak určíme počet hodnot, kterých nabývá číslo d_2 (při dělení lichým počtem prvočísel rozkladu):

$$d_2 = C_3^1 + C_3^3 = 3 + 1 = 4.$$

Těmito hodnotami jsou:

$$\frac{30}{2} = 15, \qquad \frac{30}{3} = 10, \qquad \frac{30}{5} = 6, \qquad \frac{30}{2.3.5} = 1.$$

Nyní dosadíme do vzorce, zkrátíme a získáme požadovaný polynom:

$$\phi_{30}(x) = \frac{(x^{30}-1)(x^5-1)(x^3-1)(x^2-1)}{(x^{15}-1)(x^{10}-1)(x^6-1)(x-1)} =$$

$$= \frac{(x^{15}-1)(x^{15}+1)(x^5-1)(x^3-1)(x-1)(x+1)}{(x^{15}-1)(x^5-1)(x^5+1)(x^3-1)(x^5+1)(x-1)}$$

$$= \frac{(x^{15}+1)(x+1)}{(x^5+1)(x^3+1)} = \frac{x^{10}-x^5+1}{x^2-x+1} = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1.$$

Zde je vidět, jak nám tento postup velmi usnadní výpočet díky krácení výrazů v závorkách.

[4]

Příklad: Nalezněte cyklotomický polynom $\phi_7(x)$.

Index polynomu $n = 7$ je prvočíslo.

$$\phi_7(x) = \frac{x^7-1}{x-1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Příklad: Nalezněte cyklotomický polynom $\phi_4(x)$.

Index polynomu $n = 4 = 2^2$. Index je možné napsat jako mocninu prvočísla. Použijeme tedy vzorec $\phi_{p^\alpha}(x) = \frac{x^{p^\alpha}-1}{x^{p^{\alpha-1}}-1}$.

$$\phi_4(x) = \phi_{2^2}(x) = \frac{x^{2^2}-1}{x^{2^{2-1}}-1} = \frac{x^4-1}{x^2-1} = x^2 + 1.$$

Příklad: Nalezněte cyklotomický polynom $\phi_{26}(x)$.

Index polynomu $n = 26 = 2.13$. Číslo 13 je liché prvočíslo.

$$\phi_{26}(x) = \frac{x^{26}-1}{x^{13}-1}.\frac{x-1}{x^2-1} = \frac{x^{27}-x^{26}-x+1}{x^{15}-x^{13}-x^2+1}$$

$$= x^{12} - x^{11} + x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1.$$

Příklad: Nalezněte cyklotomický polynom $\phi_{44}(x)$.

Index polynomu $n = 44 = 4.11$. Číslo 11 je liché prvočíslo.

$$\phi_{44}(x) = \frac{x^{44}-1}{x^{22}-1}.\frac{x^2-1}{x^4-1} = \frac{x^{46}-x^{44}-x^2+1}{x^{26}-x^{22}-x^4+1}$$
$$= x^{20}-x^{18}+x^{16}-x^{14}+x^{12}-x^{10}+x^8-x^6+x^4-x^2+1.$$

2.2 Sestrojitelnost pravidelných mnohoúhelníků

Eukleidovská konstrukce je obor geometrie, který se zabývá otázkou sestrojitelnosti geometrických útvarů pouze s pomocí obyčejného kružítka a pravítka, při čemž se předpokládá, že pravítko je nekonečné délky a bez jakýchkoliv značek, využíváme pouze jedné jeho hrany, a také kružítko je schopné narýsovat kružnici libovolné velikosti.

Eukleidovská konstrukce k sestrojení geometrických útvarů využívá body, přímky (úsečky) a kružnice. Mezi základní konstrukční úkoly patří:

1. pomocí dvou bodů sestrojit přímku procházející těmito body nebo úsečku ohraničenou těmito body,
2. pomocí dvou bodů sestrojit kružnici takovou, která bude mít v jednom z bodů střed a druhým bude procházet,
3. pomocí dvou přímek sestrojit bod, ve kterém se tyto přímky protínají – tj. jejich průsečík,
4. pomocí kružnice a přímky sestrojit dva body, popřípadě jeden bod, ve kterých se přímka s kružnicí protíná,
5. pomocí dvou kružnic sestrojit dva body, popřípadě jeden bod, ve kterých se spolu protínají tyto kružnice.

[5]

Otázka, které pravidelné mnohoúhelníky lze sestrojit pomocí eukleidovské konstrukce, je spojena s Fermatem a Gaussem. Fermatova prvočísla jsou taková čísla, která lze vyjádřit ve tvaru

$$F_m = 2^{2^m} + 1,$$

tedy jsou to Fermatova čísla, a zároveň je toto číslo F_m prvočíslem. Fermat zemřel v přesvědčení, že všechna Fermatova čísla jsou prvočísla. Až o necelých sto let tuto hypotézu vyvrátil Euler, který přišel na to, že číslo F_5 není prvočíslo, ale je složené. Doposud známá Fermatova prvočísla jsou čísla

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257 \text{ a } F_4 = 65537.$$

A právě Gauss objevil, že pomocí eukleidovské konstrukce lze zkonstruovat pouze takové mnohoúhelníky, u nichž počet vrcholů je roven Fermatovu prvočíslu nebo číslu

$$n = 2^k p_1 p_2 \dots p_l,$$

kde $p_1, \dots, p_l$ jsou si navzájem různá Fermatova prvočísla. Tuto podmínku tedy splňují například $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, \dots$ a naopak nelze sestrojit n-úhelníky, kde $n = 7, 9, 11, 13, 14, \dots$

[6]

Věta 2.2.1 (O eukleidovsky konstruovatelných pravidelných mnohoúhelnících)

Pravidelný mnohoúhelník je eukleidovsky konstruovatelný, jestliže počet jeho vrcholů je roven číslu n, kde

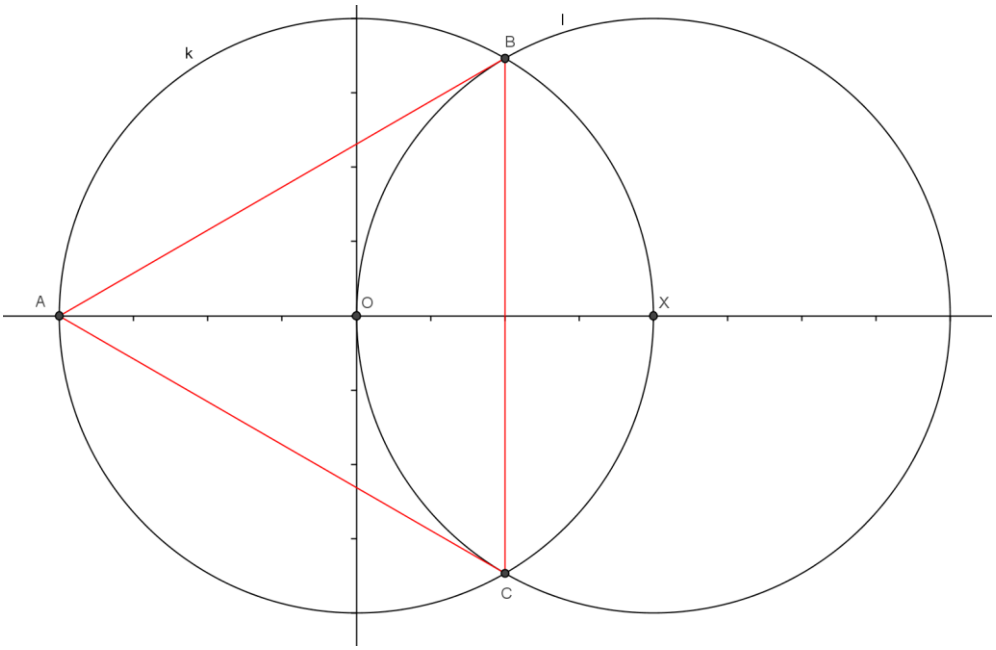
1. $n = 2^k, k > 1$ nebo
2. $n = 2^{2^k} + 1$, tj. n je Fermatovo prvočíslo, nebo
3. $n = 2^k p_1 p_2 \dots p_l$, kde $p_1, p_2, \dots, p_l$ jsou si navzájem různá Fermatova prvočísla.

Příklad: Vezměme například pravidelný trojúhelník, pětiúhelník a sedmiúhelník.

Pravidelný trojúhelník, tj. rovnostranný trojúhelník, má tři vrcholy a $n = 3$ je Fermatovo prvočíslo. Postup konstrukce je následující:

Uvažujme kartézskou soustavu souřadnic s počátkem v bodě $O = [0; 0]$.

1. k: $k(O;\ r)$
2. A, X: body A, X vzniknou jako průsečíky kružnice k se souřadnicovou osou x
3. l: $l(X; r)$
4. B, C: $\{B, C\} = k \cap l$



Obrázek 4: Konstrukce pravidelného trojúhelníku

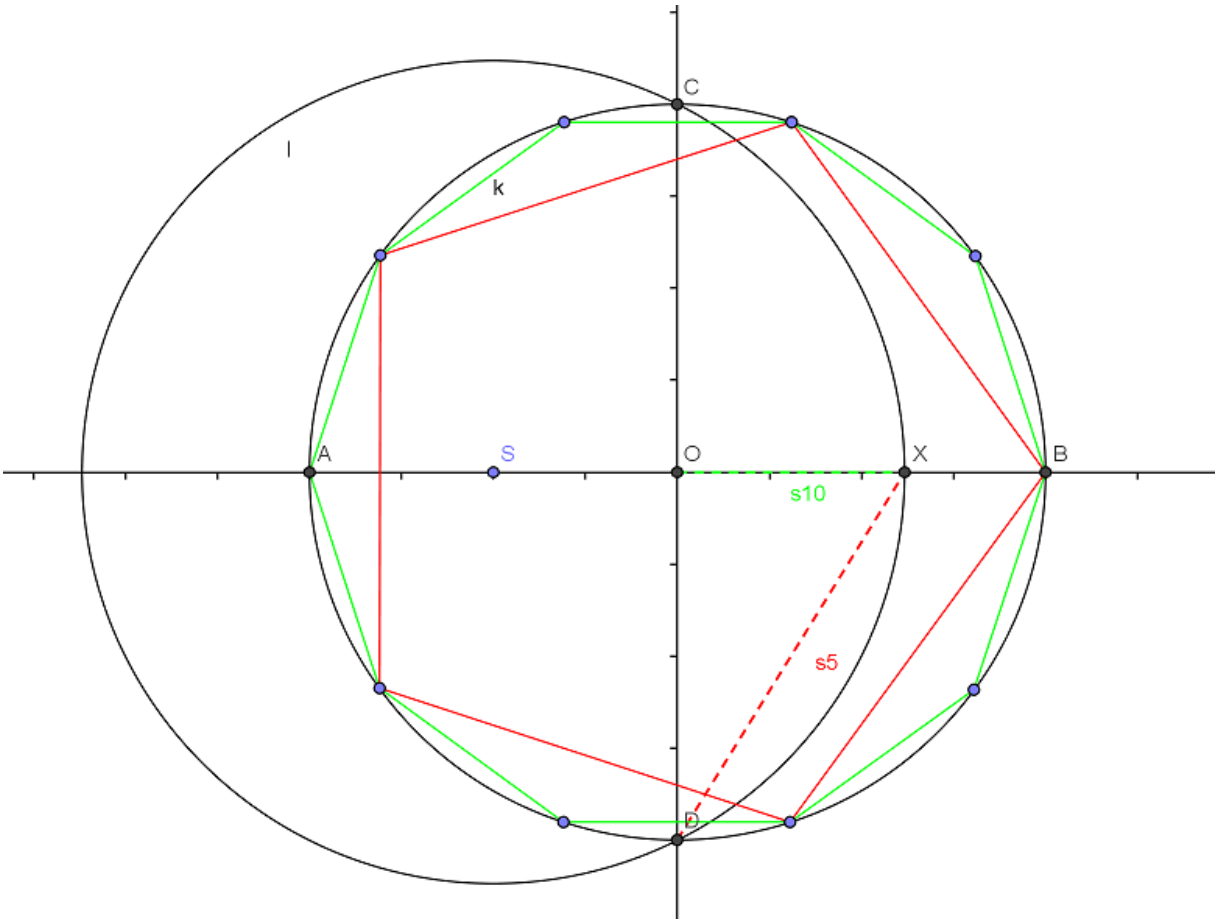
Díky tvrzení výše víme, že pravidelný pětiúhelník lze sestrojit pomocí eukleidovské konstrukce. Ověřme tedy teorii.

Číslo $n = 5$ je opět Fermatovým prvočíslem. Podle věty o eukleidovsky konstruovatelných pravidelných mnohoúhelnících lze sestrojit pravidelný pětiúhelník pouze s pomocí pravítka a kružítka:

Uvažujme kartézskou soustavu souřadnic s počátkem v bodě $O = [0; 0]$.

1) k: $k(O; r)$
2) A, B, C, D: body vzniknou jako průsečíky kružnice k se souřadnicovými osami x, y
3) S: $|AS| = |SO|$
4) l: $l(S; SD)$
5) X: $X = l \cap OB$

Délka strany pravidelného pětiúhelníku je pak $s_5 = |DX|$, zároveň délka strany pravidelného desetiúhelníku je rovna $s_{10} = |OX|$. Zde vidíme, že pravidelný desetiúhelník lze tedy také zkonstruovat za využití pravítka a kružítka a to proto, že číslo $n = 10$ lze vyjádřit ve tvaru součinu mocniny čísla 2 a nějakého Fermatova prvočísla, tj. $10 = 2.5$.



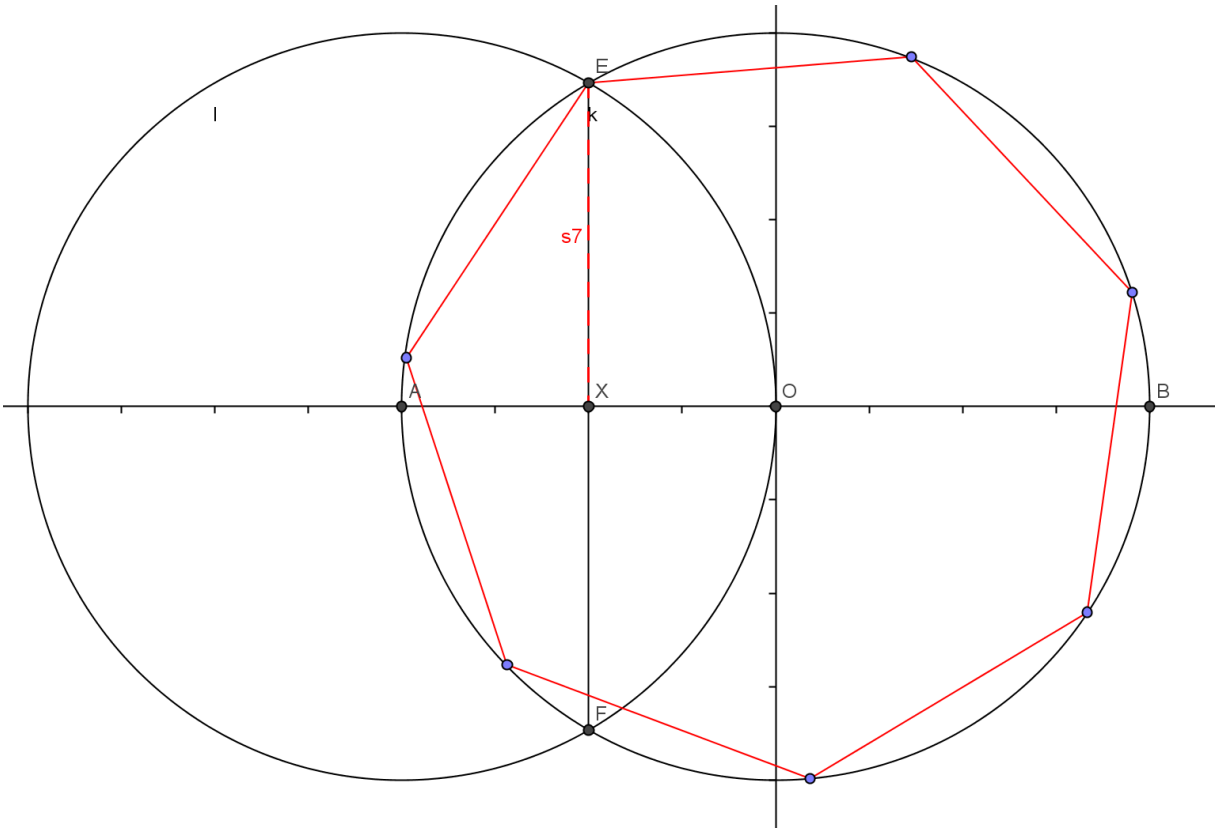
Obrázek 5: Sestrojení pravidelného pětiúhelníku a desetiúhelníku

Pravidelný sedmiúhelník patří mezi mnohoúhelníky, které nelze sestrojit pomocí pravítka a kružítka přesně. U takových mnohoúhelníků ovšem existují přibližné konstrukce:

Uvažujme kartézskou soustavu souřadnic s počátkem v bodě $O = [0; 0]$.

1. $k(O; r)$
2. A, B: body A, B vzniknou jako průniky kružnice k s osou x
3. $l(A; AO)$
4. E, F: $\{E, F\} = l \cap k$
5. X: $X = \overleftrightarrow{EF} \cap \overleftrightarrow{AO}$

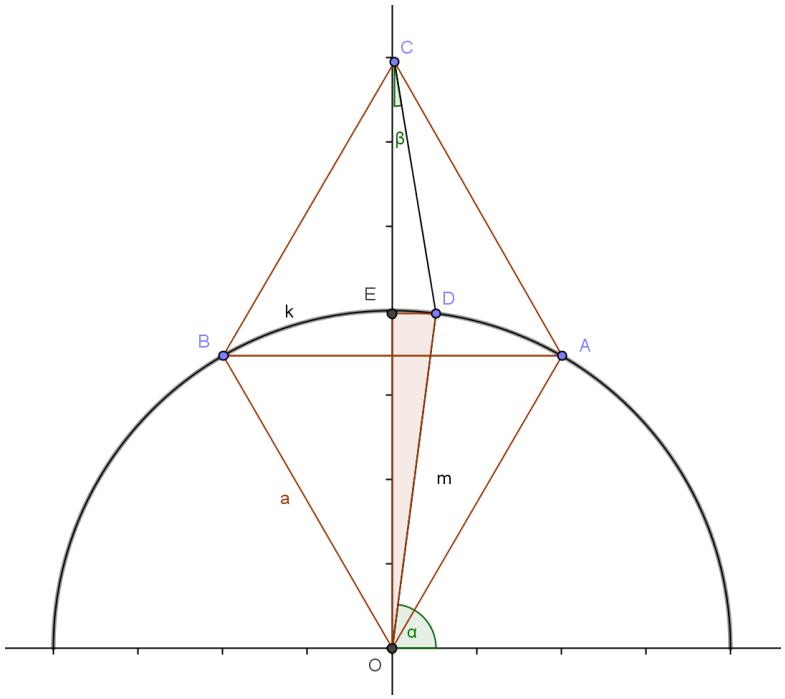
Přibližná délka strany pravidelného sedmiúhelníku je pak rovna délce $s_7 = |EX| = |FX|$.



Obrázek 6: Sestrojení pravidelného sedmiúhelníku

2.2.2 Přibližná konstrukce úhlu 10° pravítkem a kružítkem

Návod na přibližnou konstrukci úhlu 10° pomocí pravítka a kružítka pochází z časopisu Rozhledy matematicko-fyzikální a autorem je Ing. Nedbal.



Obrázek 7: Přibližná konstrukce úhlu 10°

V kartézské soustavě souřadnic narýsujeme kružnici k se středem v bodě O a poloměrem a. Dále narýsujeme shodné rovnostranné trojúhelníky OAB a ABC o straně a tak, že jejich společná výška OC leží v ose y. Kružnice k má rovnici $x^2 + y^2 = a^2$. Dále sestrojíme bod D tak, aby úhel, který svírá přímka $m = OD$ s osou x, byl roven úhlu $\alpha = 82°30'$. Tento úhel sestrojíme tak, že od $90°$ odečteme $\frac{1}{4}.30°$. Přímka m má rovnici $y = x.\operatorname{tg}\alpha$. Nyní řešme soustavu těchto dvou rovnic:

$$x^2 + y^2 = a^2$$
$$y = x.\operatorname{tg}\alpha$$
$$---------$$
$$x^2 + x^2.\operatorname{tg}^2\alpha = a^2$$
$$x^2(1 + \operatorname{tg}^2\alpha) = a^2$$
$$x^2.\frac{1}{\cos^2\alpha} = a^2$$
$$---------$$
$$x_0 = a.\cos\alpha$$
$$y_0 = a.\sin\alpha$$

Výsledkem jsou souřadnice x_0, y_0 průsečíku D přímky m s kružnicí k.

Nyní zjistíme délku výšky v jednoho z trojúhelníků a souřadnice bodu C. Použijeme k tomu libovolný pravoúhlý trojúhelník:

$$\sin 60° = \frac{v}{a}$$
$$v = \frac{a\sqrt{3}}{2}.$$

Bod C má tedy souřadnice $\left[0, a\sqrt{3}\right]$. Nyní nás zajímá délka úsečky ED. Opět pomocí pravoúhlého trojúhelníka, tj. trojúhelníka EOD, počítáme $\cos\alpha = \frac{ED}{a}$ a z toho vyplývá, že délka $ED = a.\cos\alpha$. Dále délku úsečky EC spočteme jako rozdíl délek $OC - OE$. Délka $OE = a.\sin\alpha$. Tedy $EC = OC - OE = a\sqrt{3} - a.\sin\alpha = a(\sqrt{3} - \sin\alpha)$. Jelikož známe délky ED, EC, můžeme přistoupit ke zjištění velikosti úhlu β:

$$\operatorname{tg}\beta = \frac{ED}{EC} = \frac{a.\cos\alpha}{a(\sqrt{3} - \sin\alpha)} = \frac{\cos\alpha}{\sqrt{3} - \sin\alpha}.$$

Dosadíme-li úhel $\alpha = 82°30'$, dostaneme $\operatorname{tg}\beta = \frac{0{,}13053}{0{,}74061}$, z čehož získáme

$$\beta = 9°59'44''.$$

Relativní chyba je tedy rovna $\frac{16''}{10°} = \frac{16''}{36000''} = 0{,}044\%$.

Máme tedy přibližnou, avšak dá se říct velmi přesnou, konstrukci úhlu 10°, kterou můžeme využít například při přibližné konstrukci pravidelného devítiúhelníku, neboť středový úhel devítiúhelníku je roven $\frac{360°}{9} = 40°$, tedy čtyřnásobku námi sestrojeného úhlu.

[14]

Věta 2.2.3

Lze-li kružnici rozdělit pomocí pravítka a kružítka na a a b dílů, jsou-li a, b nesoudělná čísla, pak lze rozdělit kružnici i na ab dílů, a to pomocí součtů a rozdílů oblouků.

[4]

Příklad: Platnost věty ověříme na příkladu. Vezměme například pravidelný dvanáctiúhelník.

$$n = 12 = 3.4, \qquad D(3,4) = 1.$$

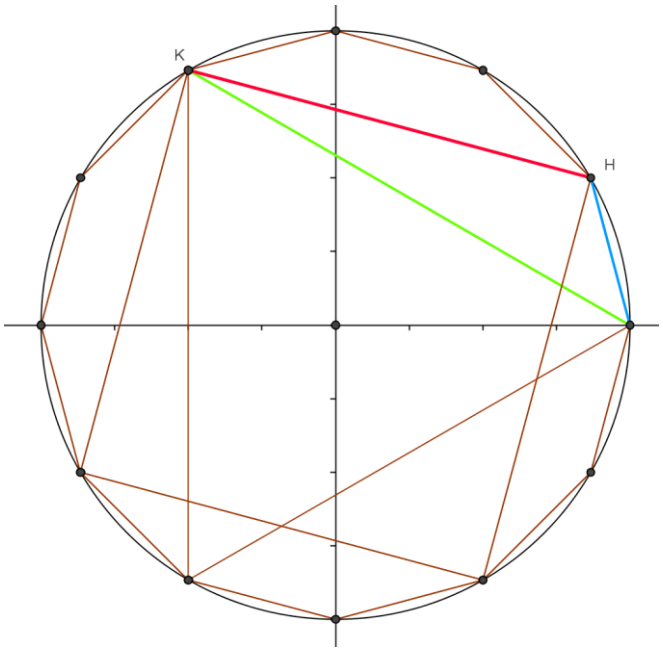
Chceme sestrojit $\frac{1}{n}$-tý díl kružnice. Pro rovnici $n = ab$ po úpravě platí $\frac{1}{n} = \frac{u}{a} + \frac{v}{b}$. Pro sestrojení $\frac{1}{n}$-tého dílu kružnice je třeba vzít $u$krát $\frac{1}{a}$-tý díl kružnice a přičíst k němu $v$krát $\frac{1}{b}$-tý díl kružnice.

Pro dvanáctiúhelník platí:

$$1 = (-1).3 + 1.4,$$

$$\frac{1}{12} = \frac{1}{3} - \frac{1}{4},$$

stačí tedy vzít třetinu kružnice a od ní odečíst čtvrtinu kružnice. Tím získáme požadovanou dvanáctinu kružnice.



Obrázek 8: Vytvoření strany dvanáctiúhelníku pomocí trojúhelníka a čtverce

Jak je vidět z obrázku, narýsovali jsme rovnostranný trojúhelník. Třetina kružnice odpovídá bodu K, myšleno z počátečního bodu všech mnohoúhelníků $[1,0]$. Z bodu K jsme pak tedy narýsovali čtverec. Odečtením čtvrtiny oblouku kružnice od třetiny oblouku kružnice jsme získali bod H, který odpovídá druhému vrcholu pravidelného dvanáctiúhelníku. Postupným nanášením této délky jsme pak získali zbylé vrcholy.

2.3 Johann Friedrich Carl Gauss a pravidelný sedmnáctiúhelník

Významný německý fyzik a matematik se narodil 30. dubna 1777 v Braunschweigu a zemřel 23. února 1855 v Göttingenu. Už v jeho mládí bylo vidět, že je velmi nadaný. Číst se naučil ještě před nástupem do školy. Výborně zvládal aritmetiku a také počítání zpaměti. Říká se, že v pouhých třech letech upozornil svého otce na chybu při výpočtu mzdy (a to díky tomu, že ho při výpočtech vždy pozoroval). V sedmi letech začal Gauss chodit do obecné školy, kde po dvou letech postoupil do aritmetické třídy. Již v té době Gauss vynikal svým nadáním. Při úloze vypočítat součet všech přirozených čísel od jedné do sta překvapil učitele svou rychlou odpovědí. Dovedl si totiž odvodit formuli pro součet aritmetické řady. Ten spočetl tak, že vytvořil dvojice čísel, jejichž součty byly vždy rovny číslu 101, tedy $(1+100)+(2+99)+(3+98)+\cdots+(50+51)$. Takových párů je v řadě padesát. Celkovým součtem tedy pak je součin těchto dvou čísel, $5\,050$. Ve 14 letech se seznámil s vévodou z Brunšviku, díky kterému mohl začít studovat na Collegium Carolinum, zde studoval čtyři roky antické jazyky.

Své objevy si Gauss zaznamenával do deníku. V něm byly zmínky například o zákonu chyb, distribuci prvočísel, trojúhelníkových číslech, nebo třeba o komplexních číslech a konstrukci pravidelných mnohoúhelníků. Teprve devatenáctiletý Gauss dokázal, že pravidelný sedmnáctiúhelník lze sestrojit pouze pomocí pravítka a kružítka, tedy že je eukleidovsky konstruovatelný. Od dob starých Řeků se předpokládalo, že takto lze sestrojit takové mnohoúhelníky, které mají počet stran roven číslu 2^m, kde $m = 2, 3, \ldots$ a dále ty, kde je počet vrcholů roven $2^m.3$, $2^m.5$, $2^m.3.5$, kde $m = 0, 1, \ldots$ Poté Gauss přišel se souvislostí sestrojitelnosti pravidelných mnohoúhelníků s Fermatovými prvočísly. Pro $n = 2^{2^m} + 1$, kde $m = 0, 1$ je konstrukce známá a jednoduchá (konstrukci pravidelného trojúhelníku a pětiúhelníku jsem ukázala v předchozím příkladě). Pro $m = 2$ ovšem dostáváme $n = 17$, tedy jedná se o pravidelný sedmnáctiúhelník.

[7]

Dne 30. března 1796 devatenáctiletý Gauss zjistil, že je možné zkonstruovat pravidelný sedmnáctiúhelník. Tento objev ho údajně přesvědčil věnovat se matematice místo filologii. Prvního června 1796 jeho výsledky zveřejnil v německém časopisu Intellegenzblatt der allgemeinen Litteraturzeitung A. W. Zimmermann, který byl profesorem na Collegium Carolinum a brzy se stal i Gaussovým mentorem. Poté to samé Gauss prezentoval na konci své knihy Disquistiones Arithmeticae, ve které dokazuje sestrojitelnost pro každý mnohoúhelník s počtem vrcholů $n = 2^{2^m} + 1$, tedy rovným Fermatovým prvočíslům.

[8]

2.3.1 Konstrukce pravidelného sedmnáctiúhelníku na základě Gaussových period

Gaussovy periody jsou uskupení kořenů na základě jejich charakteristického uspořádání. Tento postup se provádí pro binomické rovnice, u kterých je $n = p$, p je prvočíslo. V našem případě je $n = 17$, číslo 17 je prvočíslo. Jejich vytváření spočívá v tom, že se jako první vytvoří dvě periody o $\frac{p-1}{2}$ sčítancích. Vytvoříme tedy periody y_1, y_2 o $\frac{17-1}{2} = 8$ sčítancích. Platí v nich, že každý následující sčítanec je druhou mocninou předcházejícího. Dále platí, že periody y_1, y_2 jsou kořeny kvadratické rovnice s celistvými koeficienty. Poté se provede vytvoření dalších period, které budou nyní $\frac{p-1}{4}$-členné, tj. periody z_1 až z_4 o $\frac{17-1}{4} = 4$ sčítancích. V nich platí, že každý sčítanec je čtvrtou mocninou předcházejícího a opět věta, že každá dvojice period z_1 až z_4 vyhovuje kvadratické rovnici, jejíž koeficienty jsou racionální funkce předcházejících period y_1, y_2. V našem příkladě jsme ještě dělili na periody o $\frac{p-1}{8}$ sčítancích, tím jsme vytvořili periody u_1 až u_8 o $\frac{17-1}{8} = 2$ sčítancích. Ty jsou kořeny kvadratické rovnice, jejíž koeficienty jsou racionálně závislé na předcházejících čtyřčlenných periodách. Obecně protože $p - 1 = 2^m$, kde m je samo mocninou čísla 2, po $m - 1$ děleních dostaneme konečně dvoučlenné periody, kde každá z nich je kořenem kvadratické rovnice s koeficienty racionálně závislými na přecházejících (čtyřčlenných) periodách.

Tímto postupem tedy zjišťujeme, že primitivní kořen, označme ho např. ε, a tedy i všechny ostatní primitivní kořeny dané binomické rovnice $x^p - 1 = 0$, lze nalézt postupným řešením řetězce kvadratických rovnic, a tedy vyjádřit pomocí druhých odmocnin. Z toho vyplývá, že mohou být sestrojeny pomocí kružítka a pravítka.

[4]

Kořeny binomické rovnice $x^n - 1 = 0$ lze vyjádřit podle Moivreovy věty jako

$$x = \cos k\alpha + i \sin k\alpha,\ \alpha = \frac{2\pi}{n},\ k = 0, 1, \dots, n-1.$$

Uvažujeme-li pravidelný sedmnáctiúhelník, pak rovnici $x^{17} - 1 = 0$ můžeme vydělit výrazem $x - 1$. Obdržíme polynom

$$x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 +$$
$$+x^7 + +x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

který je již nad celými čísly nerozložitelný, a zároveň stupeň tohoto polynomu, $16 = 2^4$, je mocninou čísla 2, což je podle Gausse nutná podmínka pro to, aby mohla být rovnice (položíme-li tento polynom rovný nule) řešitelná pomocí druhých odmocnin, tedy šla převést na řetězec kvadratických rovnic. Tato rovnice má kořeny $x_1, x_2, \dots, x_{16}$, které lze vyjádřit výrazem $x_k = \cos k\alpha + \ i \sin k\alpha$, kde $\alpha = \frac{2\pi}{17} = 21°10´35{,}3´´$ a $k = 1, 2, 3, \dots, 16$. Při tom platí $x_k = x_1^k$ pro $k = 1, 2, \dots, 16$ a zároveň pro všechna k platí $x_k^{17} = 1$. Jak je vidět, tak koeficienty kořenů mají zároveň význam mocnitelů.

Dále platí (dle Gausse), že číslo 3 je primitivním kořenem čísla 17, to znamená, že mocniny čísla 3 dělené číslem 17 dávají všechny zbytky od 1 do 16, tedy udávají úplnou soustavu zbytků $modulo$ 17:

$$3^0 \equiv 1 = x_1$$
$$3^1 \equiv 3 = x_3$$
$$3^2 \equiv 9 = x_9$$
$$3^3 \equiv 10 = x_{10}$$
$$\vdots$$
$$3^{14} \equiv 2 = x_2$$
$$3^{15} \equiv 6 = x_6$$

Tyto kořeny tedy popořadě jsou:

$$x_1, x_3, x_9, x_{10}, x_{13}, x_5, x_{15}, x_{11}, x_{16}, x_{14}, x_8, x_7, x_4, x_{12}, x_2, x_6$$

Těchto šestnáct kořenů nyní uspořádáme do Gaussových period:

$$y_1 = x_1 + x_9 + x_{13} + x_{15} + x_{16} + x_8 + x_4 + x_2 = 3^0 + 3^2 + \cdots + 3^{14}$$
$$y_2 = x_3 + x_{10} + x_5 + x_{11} + x_{14} + x_7 + x_{12} + x_6 = 3^1 + 3^3 + \cdots + 3^{15}$$
$$z_1 = x_1 + x_{13} + x_{16} + x_4 = 3^0 + 3^4 + 3^8 + 3^{12}$$
$$z_2 = x_9 + x_{15} + x_8 + x_2 = 3^2 + 3^6 + 3^{10} + 3^{14}$$
$$z_3 = x_{10} + x_{11} + x_7 + x_6 = 3^3 + 3^7 + 3^{11} + 3^{15}$$
$$z_4 = x_3 + x_5 + x_{14} + x_{12} = 3^1 + 3^5 + 3^9 + 3^{13}$$

$$u_1 = x_1 + x_{16} = 3^0 + 3^8, u_2 = x_{13} + x_4 = 3^4 + 3^{12}$$
$$u_3 = x_{15} + x_2 = 3^6 + 3^{14}, u_4 = x_9 + x_8 = 3^2 + 3^{10}$$
$$u_5 = x_{11} + x_6 = 3^7 + 3^{15}, u_6 = x_{10} + x_7 = 3^3 + 3^{11}$$
$$u_7 = x_5 + x_{12} = 3^5 + 3^{13}, u_8 = x_3 + x_{14} = 3^1 + 3^9$$

Z rovnice

$$x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 +$$
$$+x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$$

vyplývá, že

$$y_1 + y_2 = x_1 + x_2 + x_3 + \cdots + x_{16} = -1.$$

Dále zjistíme součin $y_1 y_2$. Postupným roznásobení získáme celkem 64 členů, vzhledem k $x^{17} = 1$ upravujeme mocnitele na menší než 17 ($modulo$ 17). Získáme

$$y_1 y_2 = 4(x_1 + x_2 + \cdots + x_{16}) = 4.(-1) = -4.$$

Z tohoto vyplývá, že y_1, y_2 jsou kořeny kvadratické rovnice $y^2 + y - 4 = 0$.

Podobně získáme $z_1 + z_2 = y_1$, $z_1 z_2 = -1$, tedy z_1, z_2 jsou kořeny kvadratické rovnice $z^2 - y_1 z - 1 = 0$. Dále $z_3 + z_4 = y_2, z_3 z_4 = -1$, tedy z_3, z_4 jsou kořeny kvadratické rovnice $z^2 - y_2 z - 1 = 0$. Také všechny kořeny u lze stejným způsobem určit. Postupnými výpočty a dosazováním bychom vypočetli samotné hodnoty jednotlivých kořenů.

Všechny periody u mají tvar podle vzorce $u = x_k + x_{17-k} = 2\cos k\alpha$, kde $\alpha = \frac{2\pi}{17}$.

Hodnoty period jsou pak $u_1 = 2\cos\alpha, u_2 = 2\cos 4\alpha, u_3 = 2\cos 2\alpha, u_4 = 2\cos 8\alpha$, ...

Jen pro ukázku uvedeme, jak takový kořen pravidelného sedmnáctiúhelníku vypadá:

$$\cos\frac{2\pi}{17} = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}}$$
$$+\frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

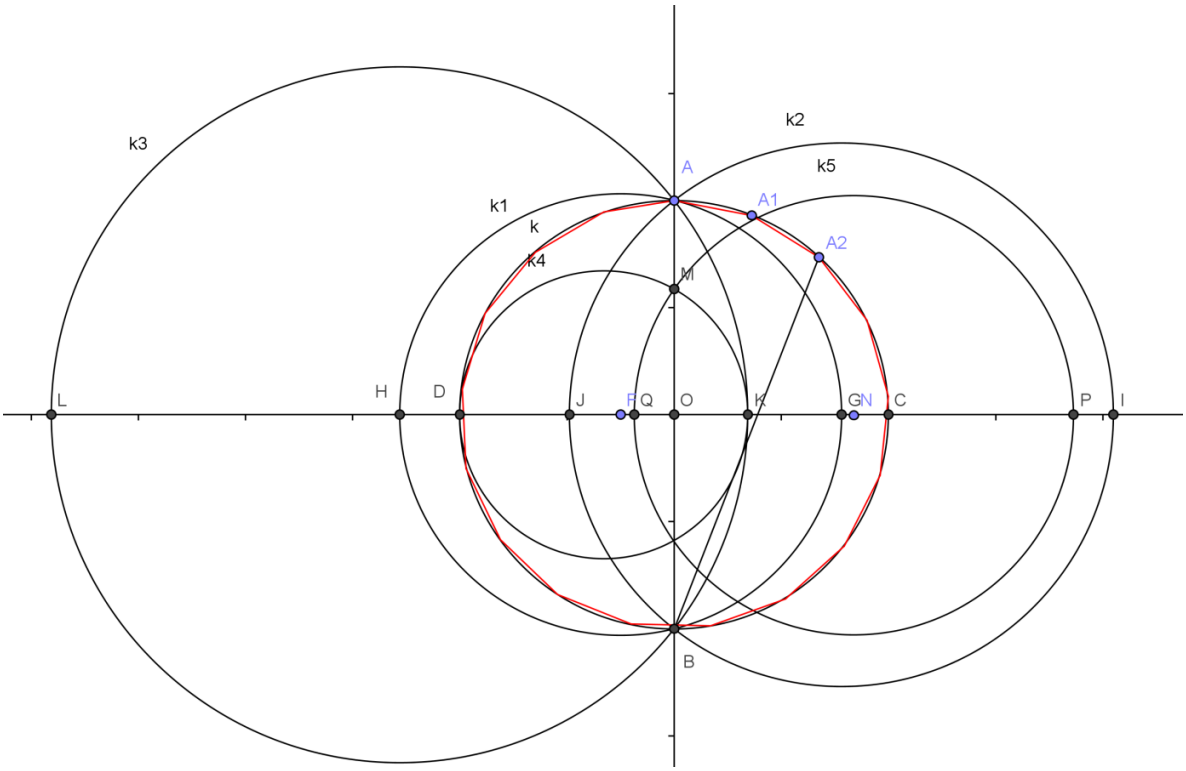
Toto číslo udává x-ovou souřadnici prvního kořene. Kdybychom jím vedli kolmici na osu x, protnula by se s jednotkovou kružnicí, čímž by vytvořila vrchol pravidelného sedmnáctiúhelníku.

Samotná konstrukce je potom následující:

Sestrojme kružnici k se středem v počátku kartézské soustavy $O = [0; 0]$ a poloměrem $r = 1$. Body A, B, C, D jsou průsečíky kružnice k s osami x, y. Nalezněme bod F ležící

na úsečce OD tak, aby $|OF| = \frac{1}{4}$. Dále sestrojíme kružnici k_1 se středem v bodě F a poloměrem $r = |AF| = \frac{1}{4}\sqrt{17}$, tato kružnice protíná osu x v bodech G a H tak, že $|OG| = \frac{\sqrt{17}-1}{2} = \frac{y_1}{2}$ a $|OH| = \frac{-\sqrt{17}-1}{4} = \frac{y_2}{2}$. Sestrojme kružnici k_2 se středem v bodě G a poloměr $r = |AG|$. Kružnice protíná osu x v bodech I a J, kde $|OI| = \frac{y_1}{2} + \sqrt{\frac{y_1^2}{4} + 1} = z_1$ a $|OJ| = \frac{y_1}{2} - \sqrt{\frac{y_1^2}{4} + 1} = z_2$. Další kružnice k_3 má střed v bodě H a poloměr $r = |AH|$ a protíná osu x v bodech K a L, kde $|OK| = \frac{y_2}{2} + \sqrt{\frac{y_2^2}{4} + 1} = z_4$ a $|OL| = \frac{y_2}{2} - \sqrt{\frac{y_2^2}{4} + 1} = z_3$. Nyní sestrojíme kružnici k_4, která prochází body D, K, se středem na úsečce OD a protíná osu y v kladné části v bodě M. Velikost $|OM| = \sqrt{z_4}$. Potom určeme bod N tak, že $|MN| = \frac{1}{2}|OI| = \frac{z_1}{2}, |ON| = \sqrt{\frac{z_1^2}{4} - z_4}$. Poslední kružnice k_5 se středem v bodě N a poloměrem $r = |MN|$ protíná osu x v bodech P a Q tak, že $|OP| = \frac{z_1}{2} + \sqrt{\frac{z_1^2}{4} - z_4} = u_1$ a $|OQ| = \frac{z_1}{2} - \sqrt{\frac{z_1^2}{4} - z_4} = -u_2$. Nyní sestrojme tětivu kružnice k z bodu B o délce $|OP| = u_1$. Tato tětiva spojuje bod B s bodem A_2. Pokud rozdělíme oblouk AA_2 na dva stejně dlouhé oblouky, dostaneme bod A_1. Získali jsme tedy tři po sobě následující vrcholy pravidelného sedmnáctiúhelníku A, A_1, A_2. Postupným nanášením délky strany sedmnáctiúhelníku získáme i zbylé vrcholy.

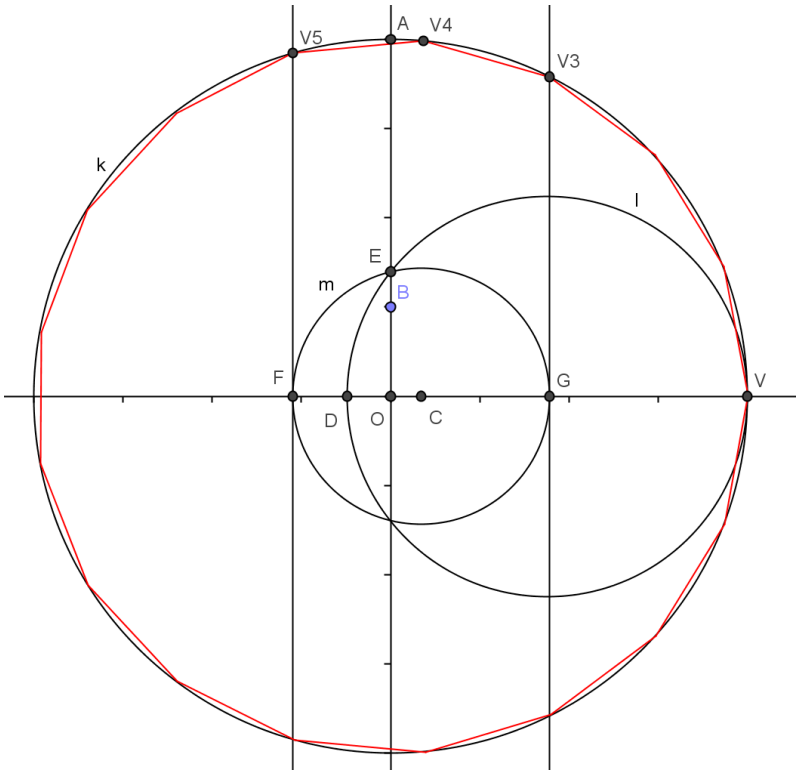
[9]



Obrázek 9: Konstrukce sedmnáctiúhelníku na základě Gaussových period

2.3.2 Richmondova konstrukce pravidelného sedmnáctiúhelníku

Jedna z možných konstrukcí pravidelného sedmnáctiúhelníku je také Richmondova konstrukce (1893). Základem je narýsování kružnice k se středem v bodě O a libovolně vybraný bod V, ležící na této kružnici. Dále se sestrojí bod A takový, že přímka OA je kolmá na přímku OV. Dále se určí bod B, který leží na úsečce OA tak, že délka úsečky OB je rovna čtvrtině délky úsečky OA. Bod C leží na úsečce OV a zároveň velikost úhlu OBC je roven čtvrtině velikosti úhlu OBV. Potom bod D leží na přímce OV tak, aby velikost úhlu DBC byla rovna polovině pravého úhlu, tedy 45°. Nechť dále bod E je bod, kde kružnice l určená body D,V, se středem na úsečce OV, protíná úsečku AO. Nyní narýsujeme kružnici m se středem v bodě C, která prochází bodem E. Nechť body F a G označují průsečíky této kružnice m a přímky OV. Potom body V_3 a V_5 jsou průsečíky kolmic vedených body F a G s kružnicí k.



Obrázek 10: Richmondova konstrukce pravidelného sedmnáctiúhelníku

Body V, V_3 a V_5 jsou nultý, třetí a pátý vrchol pravidelného sedmnáctiúhelníku. Půlením úhlu $V_3\mathrm{O}V_5$ najdeme vrchol V_4, čímž získáme velikost strany s_{17}. Celý sedmnáctiúhelník pak snadno získáme postupným nanášením této délky po kružnici k.

[8]

2.4 Řešitelnost binomické rovnice $x^n - 1 = 0$ pomocí druhých odmocnin

Řešení binomické rovnice $x^n - 1 = 0$, tj. nalezení všech n-tých odmocnin z jedné, to znamená odmocňování, je ekvivalentní úloze dělení kružnice na n stejných dílů, tj. sestrojování pravidelných mnohoúhelníků. Kdy je tato konstrukce řešitelná pouze pomocí pravítka a kružítka, tedy kdy je možné sestrojit kořeny binomické rovnice pouze kružítkem a pravítkem? Pomocí pravítka a kružítka jsme schopni sestrojit součet dvou úseček $a + b$, rozdíl dvou úseček $a - b$, libovolný celočíselný násobek dané úsečky $ka, k \in Z$, podíl dvou úseček $\frac{a}{b}$ a konečně druhou odmocninu $\sqrt{a}$.

Pomocí pravítka a kružítka lze sestrojit libovolnou funkci daných veličin (úseček), je-li k jejímu vytvoření třeba vykonat operace součet, rozdíl, násobení, dělení a druhé odmocňování těchto veličin v konečném počtu.

Aby kořeny rovnice $f(x) = 0$ mohly být sestrojeny pomocí pravítka a kružítka, je nutnou a zároveň postačující podmínkou, aby byla rovnice řešitelná pomocí druhých odmocnin.

Sestrojení pravidelného mnohoúhelníku tedy vede k řešení binomické rovnice pomocí druhých odmocnin. Podle Gausse je každá obecná rovnice typu $x^n - 1 = 0$ algebraicky řešitelná, avšak k tomu, aby bylo její kořeny možné vyjádřit pomocí druhých odmocnin, je nutné, aby číslo n bylo součinem mocniny $2^m . p_1 . p_2 \dots p_k$, kde p_i jsou Fermatova prvočísla, tedy $p_i = 2^{2^m} + 1$, a každé toto prvočíslo se může vyskytovat pouze jednou, a to pouze v první mocnině, $m = 0$ nebo je kladné celé číslo. Tato podmínka je nutná a zároveň postačující. Samozřejmě mnohoúhelníky, u nichž $n = 2^m$, lze jednoduše konstruovat pomocí pravítka a kružítka pouze dělením úhlu.

Je-li možné řešit cyklotomický polynom pomocí druhých odmocnin, pak je možné řešit pomocí druhých odmocnin i příslušnou binomickou rovnici. Naopak nelze-li cyklotomický polynom řešit pomocí druhých odmocnin, pak nelze takto řešit ani příslušnou binomickou rovnici, protože její primitivní kořeny není možné vyjádřit pomocí druhých odmocnin.

Každý cyklotomický polynom je ireducibilní (význam bude vysvětlen v další kapitole). Pro ireducibilní rovnici $f(x) = 0$ platí, že je řešitelná pomocí druhých odmocnin, jestliže je její stupeň mocninou dvojky. Podmínka je nutná, nikoliv postačující.

Metoda Gaussových period uvedená v předchozím textu je postupem, při kterém se řešení složité rovnice převádí na řešení řetězce kvadratických rovnic. Kořeny je tedy možné vyjádřit pomocí druhých odmocnin.

[4][12]

Věta 2.4.1 (Reciproká rovnice)

Rovnici ve tvaru $a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-2} x^2 + a_{n-1} x + a_n = 0$ nazveme rovnicí reciprokou

a) prvního druhu, jestliže pro její koeficienty platí

$$a_0 = a_n, a_1 = a_{n-1}, a_2 = a_{n-2}, \dots,$$

b) druhého druhu, jestliže pro její koeficienty platí

$$a_0 = -a_n, a_1 = -a_{n-1}, a_2 = -a_{n-2}, \dots$$

Dále platí, má-li reciproká rovnice kořen α, pak je jejím kořenem také číslo $\frac{1}{\alpha}$.

[12]

Příklad: Mějme binomickou rovnici pro dělení kruhu $x^5 - 1 = 0$.

Kořenem této rovnice bude jistě $x_1 = 1$. Můžeme tedy napsat rozklad této rovnice $(x-1)(x^4 + x^3 + x^2 + x + 1)$. Polynom $x^4 + x^3 + x^2 + x + 1 = 0$ je pátý cyklotomický polynom a právě cyklotomické polynomy vedou k reciprokým rovnicím. Vydělme tento polynom x^2, dostaneme $x^2 + \frac{1}{x^2} + x + \frac{1}{x} + 1 = 0$. Nyní zavedeme novou neznámou $x + \frac{1}{x} = y$, umocněním této neznámé na druhou získáme $x^2 + \frac{1}{x^2} = y^2 - 2$, a dosadíme do rovnice:

$$y^2 - 2 + y + 1 = y^2 + y - 1 = 0.$$

Kořeny této kvadratické rovnice jsou rovny $y_{1,2} = \frac{-1 \pm \sqrt{5}}{2}$. Nyní dosadíme zpět do neznámé:

$$x + \frac{1}{x} = y,$$
$$x^2 + 1 = xy.$$

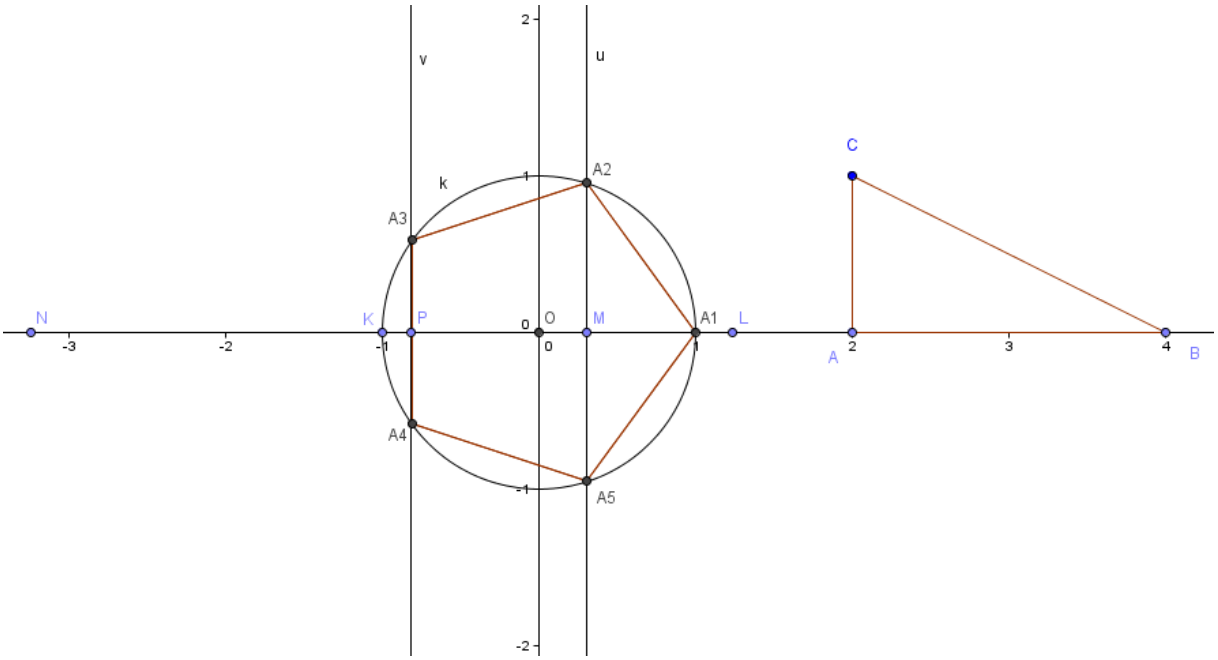
Pro kořen $y_1 = \frac{-1+\sqrt{5}}{2}$ dostaneme kvadratickou rovnici $x^2 + \frac{1-\sqrt{5}}{2}x + 1 = 0$. Její diskriminant je roven $D = \frac{-10-2\sqrt{5}}{4} < 0$.

$$x_{2,3} = \frac{\frac{-1+\sqrt{5}}{2} \pm \sqrt{\frac{-10-2\sqrt{5}}{4}}}{2} = \frac{-1+\sqrt{5}}{4} \pm \frac{\sqrt{-10-2\sqrt{5}}}{4}\, i$$
$$= \frac{1}{4}\left(-1 + \sqrt{5} \pm \sqrt{-10-2\sqrt{5}}\, i\right).$$

Pro kořen $y_2 = \frac{-1-\sqrt{5}}{2}$ dostaneme kvadratickou rovnici $x^2 + \frac{1+\sqrt{5}}{2}x + 1 = 0$. Její diskriminant je roven $D = \frac{-10+2\sqrt{5}}{4} < 0$.

$$x_{4,5} = \frac{\frac{-1-\sqrt{5}}{2} \pm \sqrt{\frac{-10+2\sqrt{5}}{4}}}{2} = \frac{-1-\sqrt{5}}{4} \pm \frac{\sqrt{-10+2\sqrt{5}}}{4}\, i$$
$$= \frac{1}{4}\left(-1 - \sqrt{5} \pm \sqrt{-10+2\sqrt{5}}\, i\right).$$

[12]



Obrázek 11: Konstrukce pravidelného pětiúhelníku na základě algebraických výrazů

Předchozí konstrukce byly jednoduché a známé. Vymysleli je geometři, kteří se snažili konstrukce zjednodušit a popsat je v několika málo krocích. Z pohledu algebraika jsou některé konstrukce také jednoduché. Například výše uvedený pětiúhelník. Díky vypočítaným kořenům pomocí reciproké rovnice můžeme konstruovat pravidelný pětiúhelník takto:

První vrchol A_1 je zřejmý z kořene x_1 a má souřadnice $[1,0]$. Vrcholům A_2, A_5 odpovídají kořeny x_2, x_3. Tyto kořeny lze zakreslit do Gaussovy roviny jako body, které mají shodné x-ové souřadnice a jejich y-ové souřadnice se liší pouze znaménkem. To znamená, že tyto dva vrcholy jsou osově souměrné podle osy x. Vezměme tedy x-ovou souřadnici těchto bodů rovnou $\frac{-1+\sqrt{5}}{4}$. Délku $\sqrt{5}$ získáme jako délku přepony a pravoúhlého trojúhelníka s délkami stran $b = 1$ a $c = 2$. Z bodu $K = [-1,0]$ udělejme půlkružnici o poloměru $\sqrt{5}$ v kladném směru osy, protože tuto hodnotu ve výrazu přičítáme. Tímto vytvoříme bod L, který má souřadnici $x = -1 + \sqrt{5}$. My ovšem potřebujeme pouze čtvrtinu úsečky OL, které odpovídá úsečka OM. Nyní z bodu M sestrojíme kolmici u k ose x. Jelikož víme, že vrcholy pravidelného pětiúhelníku musí ležet na kružnici, tak body, které vznikly protnutím kolmice u s jednotkovou kružnicí k, jsou shodné právě s dvěma jeho vrcholy. Stejným způsobem sestrojíme i zbylé dva vrcholy A_3, A_4, kterým odpovídají kořeny x_4, x_5 zakreslené opět do Gaussovy roviny jako body. Z bodu K opět sestrojíme půlkružnici o poloměru $\sqrt{5}$ v záporném směru osy, protože tuto hodnotu odečítáme. Tím vznikne bod N. Stejně tak potřebujeme znát pouze čtvrtinu úsečky NO, které odpovídá úsečka PO. Bodem

P vedeme kolmici v k ose x. Průsečíky této kolmice a kružnice k odpovídají zbývajícím vrcholům pravidelného pětiúhelníku.

Na střední škole jsme počítali tabulkové hodnoty goniometrických funkcí pro úhly $30°, 45°, 60°$. Když se podíváme na kořeny zadané binomické rovnice, vypočetli jsme vlastně také hodnoty některých goniometrických funkcí. Vezměme v úvahu vrchol A_2, který jsme získali pomocí kořene $x_2 = \frac{1}{4}\left(-1 + \sqrt{5} + \sqrt{10 + 2\sqrt{5}}\, i\right)$, tedy:

$$A_2 = \left[\frac{-1+\sqrt{5}}{4}, \frac{\sqrt{10+2\sqrt{5}}}{4}\right].$$

Uvážíme-li pravoúhlý trojúhelník OA_2M, který má délku přepony OA_2 rovnou poloměru kružnice, tj. 1, pak úhel ležící u vrcholu O je roven $\frac{360°}{5} = 72°$. Vypočtením kořenu jsme získali hodnoty

$$\sin 72° = \frac{\sqrt{10+2\sqrt{5}}}{4},$$

$$\cos 72° = \frac{-1+\sqrt{5}}{4}.$$

Stejně bychom určili hodnoty funkcí pro úhel $144°$ ze souřadnic vrcholu A_3:

$$\sin 144° = \frac{\sqrt{10-2\sqrt{5}}}{4},$$

$$\cos 144° = \frac{-1-\sqrt{5}}{4}.$$

Dále pro úhel $216°$ ze souřadnic vrcholu A_4 a pro úhel $288°$ ze souřadnic vrcholu A_5.

3. IREDUCIBILITA POLYNOMŮ PRO DĚLENÍ KRUHU A JEJÍ DŮKAZY

3.1 Primitivní polynom

Polynom $f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$ s celočíselnými koeficienty $a_i, i = 0, 1, 2, \ldots, n$ nazýváme primitivním polynomem právě tehdy, když jsou jeho koeficienty nesoudělné, to znamená, že největším společným dělitelem čísel a_i je číslo jedna. Dále platí, že pokud jsou dva polynomy $g(x)$ a $h(x)$ primitivními polynomy, pak polynom $gh(x)$ vzniklý jejich součinem je opět primitivní polynom.

[4]

Příklad:

Primitivním polynomem je například polynom $f(x) = 5x^4 - 4x^3 - 3x^2 + x - 3$, u kterého největším společným dělitelem koeficientů $D(5, -4, -3, 1, -3)$ je číslo jedna. Naopak primitivním polynomem není polynom $f(x) = 6x^3 - 8x^2 - 2x + 4$, u kterého je největším společným dělitelem jeho koeficientů číslo dva, tedy $D(6, -8, -2, 4) = 2$. Tento polynom je tedy teprve dvojnásobkem primitivního polynomu, tedy

$$f(x) = 2(3x^3 - 4x^2 - x + 2).$$

Z polynomu s racionálními koeficienty můžeme také dostat primitivní polynom. Například u polynomu $f(x) = \frac{x^2}{3} + \frac{x}{4} + \frac{3}{2}$ převedeme zlomky na stejného jmenovatele, tj. $f(x) = \frac{4x^2+3x+18}{12}$, a vytkneme $f(x) = \frac{1}{12}(4x^2 + 3x + 18)$, kde největší společný dělitel koeficientů $D(4, 3, 18) = 1$. Polynom v závorce je tedy primitivní.

3.2 Reducibilní polynom

Reducibilní polynom je polynom s celočíselnými koeficienty, který lze rozložit na součin dvou polynomů opět s celočíselnými koeficienty, tj.

$$f(x) = g(x)h(x),$$

kde žádný z polynomů $g(x)$ a $h(x)$ nemá stupeň rovný nule.

Dokažme nyní, že koeficienty polynomů jsou celočíselné.

Uvažujme, že polynomy $g(x)$ a $h(x)$ mají racionální koeficienty. Vytvořme z těchto polynomů polynomy primitivní. To znamená, že racionální koeficienty převedeme na společného jmenovatele a před každý polynom poté vytkneme největšího společného dělitele těchto koeficientů. Tímto dostaneme, že $g(x) = \frac{D_1}{s} g_1(x)$ a $h(x) = \frac{D_2}{t} h_1(x)$, kde čísla D_1, D_2 jsou vytknutí největší společní dělitelé a čísla s, t jsou jmenovatelé zlomků. Polynomy $g_1(x)$ a $h_1(x)$ jsou primitivní polynomy. Nyní dosaďme získané polynomy zpět do základní rovnice:

$$f(x) = g(x)h(x) = \left[\frac{D_1}{s} g_1(x)\right]\left[\frac{D_2}{t} h_1(x)\right] = \frac{D_1 D_2}{st} g_1(x)h_1(x).$$

Nyní vezměme zlomek $\frac{D_1 D_2}{st} = \frac{p}{q}$, kde čísla p a q jsou nesoudělná. Máme tedy polynom

$$f(x) = \frac{p}{q} g_1(x)h_1(x).$$

Jelikož polynom na levé straně výrazu podle uvedené věty musí mít celočíselné koeficienty stejně jako polynom $f(x)$, a protože čísla p, q jsou nesoudělná, potom všechny koeficienty

musí být dělitelné číslem q. Polynom $g_1(x)h_1(x)$ ovšem musí být primitivní, protože je vytvořen jako součin dvou primitivních polynomů. Proto nezbývá nic jiného, že položit $q = 1$, čímž získáme $f(x) = p.g_1(x)h_1(x)$. Z toho vyplývá rozklad polynomu $f(x)$ na součin dvou polynomů s celočíselnými koeficienty.

[4]

Příklad:

Příklady reducibilních polynomů nad celými čísly s jejich rozkladem:

- $x^3 - x = x(x^2 - 1) = x(x - 1)(x + 1)$
- $x^2 - 4 = (x - 2)(x + 2)$
- $x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1)$
- $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$
- $x^5 + x^4 + 3x^3 + 3x^2 + 2x + 2 = (x - 1)^2(x - 5)(x + 3)$
- $3x^2 - 3 = 3(x^2 - 1) = 3(x - 1)(x + 1)$

Příklad reducibilního polynomu nad komplexními čísly s jeho rozkladem:

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

Věta 3.2.1 (Rozklad reducibilních polynomů pomocí Hornerova schématu)

Algoritmus pojmenovaný po Williamu Georgi Hornerovi slouží k rozkladu polynomů na lineární a kvadratické členy a k jejich vyhodnocování. Postup algoritmu je takový, že se do záhlaví opíší koeficienty polynomu a odhadne se jeho libovolný kořen nebo se zapíše kořen, který máme vyšetřit. U prvního koeficientu se číslo opíše do třetí řádky, toto opsané číslo se pak vynásobí kořenem a výsledek se zapíše pod následující kořen do druhé řádky. Tato dvě čísla, spolu v jednom sloupečku, se sečtou a výsledek se zapíše do stejného sloupečku do třetího řádku. Poté se postupuje stejně od vynásobení kořenem. Jestli jsme kořen odhadli správně, neboli vyšetřované číslo je nulovým bodem zadaného polynomu, zjistíme po dokončení třetího sloupečku, kde se v posledním řádku vyskytne nula. Zároveň čísla nacházející se v tomto řádku nám dávají koeficienty zbytkového polynomu.

Příklad: Pomocí Hornerova schématu rozložte polynom
$f(x) = x^5 - 4x^4 + 2x^3 + 2x^2 + x + 6$ na součin kořenových činitelů.

	1	−4	2	2	1	6
−1		−1	5	−7	5	−6
	1	−5	7	−5	6	0

$x = 1$ je tedy kořen polynomu a získáváme rozklad:

$$f(x) = (x + 1)(x^4 - 5x^3 + 7x^2 - 5x + 6).$$

Rozkládáme dále.

	1	−5	7	−5	6
3		3	−6	3	−6
	1	−2	1	−2	0

$$f(x) = (x + 1)(x - 3)(x^3 - 2x^2 + x - 2).$$

	1	−2	1	−2
2		2	0	2
	1	0	1	0

Získáme konečný rozklad:

$$f(x) = (x + 1)(x - 3)(x - 2)(x^2 + 1).$$

[15]

3.3 Normovaný polynom

Normovaným polynomem nazýváme polynom, který má u nejvyšší mocniny koeficient roven jedné. Je-li v rozkladu $f(x) = g(x)h(x)$ normovaného polynomu $f(x)$ s celočíselnými koeficienty na činitele $g(x)$ a $h(x)$ s racionálními koeficienty koeficient u nejvyšší mocniny funkce $g(x)$ roven jedné, stejně tak u funkce $h(x)$, pak je tento rozklad rozkladem na polynomy s celočíselnými polynomy.

[4]

3.4 Ireducibilní polynom

Opakem reducibilního polynomu je polynom ireducibilní. Jde o takový polynom, který nelze rozložit na součin dvou polynomů s celočíselnými koeficienty. Uvažujeme-li, že $f(x) = g(x)h(x)$ a zároveň polynom $f(x)$ je ireducibilní, pak jeden z polynomů, $g(x)$ nebo $h(x)$, musí mít stupeň roven nule, tedy polynom je roven pouze konstantě.

Příklad: Nad reálnými čísly jsou ireducibilními polynomy všechny lineární polynomy, například $x - 9, x + 3, \ldots$, a všechny kvadratické polynomy, u kterých je hodnota diskriminantu záporná. Nad komplexními čísly jsou to pak všechny lineární polynomy.

Konkrétně mějme polynom $x^2 + 1$, který je nad reálnými čísly ireducibilní, nelze ho rozložit na součin polynomů nižšího stupně, kdežto nad komplexními čísly jej lze rozložit jako $x^2 + 1 = (x - i)(x + i)$. Stejně tak polynom $2x^2 + 2$, který lze zapsat jako $2(x^2 + 1)$ je stále ireducibilní nad reálnými čísly.

Věta 3.4.1 (Vlastnosti ireducibilních polynomů)

1. Je-li $f(x)$ ireducibilní polynom a $g(x)$ libovolný polynom, potom je buď polynom $g(x)$ dělitelný polynomem $f(x)$ nebo jsou polynomy nesoudělné, neboť největším společným dělitelem těchto polynomů je buď konstanta, nebo přímo ireducibilní polynom $f(x)$.
2. Má-li rovnice $g(x) = 0$ nějaký společný kořen s ireducibilní rovnicí $f(x) = 0$, potom všechny kořeny rovnice $f(x) = 0$ jsou zároveň i kořeny rovnice $g(x) = 0$ a polynom $g(x)$ je dělitelný polynomem $f(x)$. Společný kořen je totiž kořenem jejich největšího společného dělitele, který tedy není roven konstantě, tedy tyto dvě funkce nejsou nesoudělné a podle předchozího bodu je tedy $g(x)$ dělitelné $f(x)$. Pokud by žádný kořen ireducibilní rovnice $f(x) = 0$ nebyl zároveň kořenem rovnice $g(x) = 0$, pak by byly tyto funkce nesoudělné.
3. Ireducibilní rovnice $f(x) = 0$ nemůže mít žádný společný kořen s rovnicí $g(x) = 0$, která je nižšího stupně než rovnice $f(x) = 0$. Polynom $g(x)$ by podle předchozího bodu totiž musel být dělitelný polynomem $f(x)$, což vzhledem ke stupňům polynomů není možné.
4. Dvě ireducibilní rovnice $f(x) = 0$ a $g(x) = 0$ nemohou mít žádný společný kořen, neboť pokud by tomu tak bylo, musela by být rovnice $f(x) = 0$ dělitelná rovnicí $g(x) = 0$ nebo naopak, ovšem dané rovnice jsou obě ireducibilní, proto to není možné.

[4]

Věta 3.4.2

Pro všechna $n \in N$ jsou cyklotomické polynomy ireducibilní nad racionálními čísly, a tedy i nad celými čísly.

[11]

3.5 Důkaz ireducibility cyklotomických polynomů podle Leopolda Kroneckera

Jelikož důkaz ireducibility cyklotomických polynomů $\phi_n(x)$ v obecném případě, pro libovolné n, je poměrně složitý, je tento důkaz zaměřen na cyklotomické polynomy, kde $n = p^\alpha$.

Tyto polynomy jsou tvaru

$$\phi_{p^\alpha}(x) = x^{p^{\alpha-1}(p-1)} + x^{p^{\alpha-1}(p-2)} + \cdots + x^{p^{\alpha-1}2} + x^{p^{\alpha-1}} + 1\,.$$

Důkaz provedeme sporem, tedy předpokládejme, že polynom $\phi_{p^\alpha}(x)$ lze rozložit na součin dvou polynomů s celočíselnými koeficienty:

$$\phi_{p^\alpha}(x) = f(x)g(x).$$

Protože koeficient u nejvyšší mocniny polynomu je roven jedné, musí být i koeficienty u nejvyšší mocniny funkcí $f(x)$ a $g(x)$ rovny jedné, podle věty o normovaném polynomu. Nyní dosadíme-li do této rovnice $x = 1$ a víme-li, že $\phi_{p^\alpha}(1) = p$, potom dostaneme:

$$p = f(1)g(1).$$

Jelikož p je prvočíslo, musí být jeden z činitelů roven ± 1 a druhý $\pm p$. Předpokládejme například, že $f(1) = \pm 1$. Nyní označme β jako kořen rovnice $\phi_{p^\alpha}(x) = 0$, zároveň je tento kořen kořenem polynomu $f(x) = 0$, tedy $f(\beta) = 0$.

Nechť je ε libovolným kořenem rovnice $\phi_{p^\alpha}(x)$, to znamená, že je jedním z primitivních kořenů binomické rovnice $x^{p^\alpha} - 1 = 0$. Všechny primitivní kořeny tedy můžeme označit:

$$\varepsilon, \varepsilon^a, \varepsilon^b, \varepsilon^c, \dots, \varepsilon^k,$$

kde $a, b, c, \dots, k$ nejsou dělitelné číslem p a tedy jsou nesoudělná s p^α. Nyní uvažujme jejich součin:

$$f(\varepsilon)f(\varepsilon^a)f(\varepsilon^b)f(\varepsilon^c) \dots f(\varepsilon^k).$$

Díky tomu, že se mezi kořeny $\varepsilon, \varepsilon^a, \varepsilon^b, \varepsilon^c, \dots, \varepsilon^k$, které představují všechny kořeny rovnice $\phi_{p^\alpha}(x) = 0$, určitě nachází i kořen rovný β a $f(\beta) = 0$, je celý tento součin roven nule.

Označme funkci

$$F(x) = f(x)f(x^a)f(x^b)f(x^c) \dots f(x^k)\,.$$

Kořenem funkce $F(x)$ je $x = \varepsilon$, kde ε je libovolný z kořenů rovnice $\phi_{p^\alpha}(x) = 0$. Funkce $F(x)$ má tedy za své kořeny všechny kořeny funkce $\phi_{p^\alpha}(x) = 0$, z čehož plyne, že $F(x)$ je dělitelná $\phi_{p^\alpha}(x)$. Tedy:

$$F(x) = \phi_{p^\alpha}(x)h(x),$$

přičemž $h(x)$ musí mít celočíselné koeficienty, protože koeficienty u nejvyšších mocnin $F(x)$ a $\phi_{p^\alpha}(x)$ jsou rovny jedné.

Dosadíme-li $x = 1$ do $F(x) = f(x)f(x^a)f(x^b)f(x^c) \dots f(x^k)$ a vzhledem k podmínce $f(1) = \pm 1$ je $F(1) = f(1)f(1)f(1)f(1) \dots f(1) = \pm 1$. Dále je $\phi_{p^\alpha}(1) = p$. Z toho dostáváme, že:

$$\pm 1 = p.h(1).$$

Ovšem součin dvou celých čísel p a $h(1)$ nemůže být nikdy roven ± 1. Z toho plyne nesprávnost předpokladu, že $\phi_{p^\alpha}(x)$ je rozložitelný na součin dvou jednodušších polynomů s celočíselnými koeficienty. A z důkazu toho, že $\phi_{p^\alpha}(x)$ není reducibilní vyplývá jeho ireducibilita.

[4]

4. PŘÍKLAD CYKLOTOMICKÉHO POLYNOMU S „NEČEKANÝM“ KOEFICIENTEM

4.1 Koeficienty cyklotomických polynomů

Cyklotomický polynom je polynom, který nabývá tvaru

$$\phi_n(x) = \sum_{i=0}^{n-1} a_i x^i = a_0 x^0 + a_1 x^1 + a_2 x^2 + a_3 x^3 + \dots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1},$$

kde čísla $a_0, a_1, a_2, \dots, a_{n-1}$ se nazývají koeficienty polynomu. Stupeň cyklotomického polynomu může být roven nejvýše $n - 1$.

Vypišme si například prvních patnáct cyklotomických polynomů:

- $\phi_1(x) = x - 1$
- $\phi_2(x) = x + 1$
- $\phi_3(x) = x^2 + x + 1$
- $\phi_4(x) = x^2 + 1$
- $\phi_5(x) = x^4 + x^3 + x^2 + x + 1$
- $\phi_6(x) = x^2 - x + 1$
- $\phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
- $\phi_8(x) = x^4 + 1$
- $\phi_9(x) = x^6 + x^3 + 1$
- $\phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$
- $\phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

- $\phi_{12}(x) = x^4 - x^2 + 1$
- $\phi_{13}(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
- $\phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$
- $\phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$

Cyklotomické polynomy $\phi_2(x), \phi_3(x), \phi_5(x), \phi_7(x), \phi_{11}(x), \phi_{13}(x)$ jsme našli podle vzorce, kde n je prvočíslo. Polynomy $\phi_4(x), \phi_8(x), \phi_9(x)$ podle vzorce, kde n je mocnina nějakého prvočísla. Ostatní cyklotomické polynomy buď nalezneme pomocí obecného vzorce, nebo podle vzorců pro n dvojnásobek a čtyřnásobek nějakého prvočísla.

Na první pohled by se mohlo zdát, že koeficienty cyklotomického polynomu budou vždy rovné ± 1 nebo nule. Ovšem není tomu tak, neboť kdybychom ve výpisu pokračovali dále, došli bychom k cyklotomickému polynomu $\phi_{105}(x)$, u kterého se poprvé objevuje koeficient rovný -2, a to právě u x^7 a x^{41}. Dále se koeficient rovný ± 2 objevuje například u polynomů $\phi_{165}(x), \phi_{455}(x), \phi_{715}(x), \ldots$ Stejně tak koeficient rovný ± 3 se poprvé vyskytuje v polynomu $\phi_{385}(x)$, koeficient rovný ± 4 poprvé u polynomu $\phi_{1365}(x)$, koeficient rovný ± 5 poprvé najdeme u polynomu $\phi_{1785}(x)$, koeficient ± 6 u polynomu $\phi_{2805}(x)$, koeficient ± 7 u polynomu $\phi_{3135}(x)$. Takto bychom mohli pokračovat stále dál.

Tyto koeficienty se objevují pouze u takových cyklotomických polynomů, kde číslo n lze napsat jako součin alespoň tří lichých prvočísel. Právě pro $\phi_{105}(x)$ platí, že číslo 105 je první a zároveň nejmenší číslo, které je dělitelné právě třemi odlišnými nejmenšími lichými prvočísly, tj. $105 = 3.5.7$. Dále jsou

$$385 = 5.7.11,$$
$$1\,365 = 3.5.7.13,$$
$$1\,785 = 3.5.7.17,$$
$$2\,805 = 3.5.11.17,$$
$$\text{a } 3\,135 = 3.5.11.19.$$

[10]

Věta 4.1.1 (Zjišťování koeficientů cyklotomického polynomu metodou T. Y. Lama a K. H. Leunga)

Tato metoda je užívána u cyklotomických polynomů $\phi_n(x)$, kde $n = pq$ a čísla p, q jsou dvě různá prvočísla a $\phi_{pq}(x) = \sum_{k=0}^{(p-1)(q-1)} a_k x^k$. Potom zapišme hodnotu $\varphi(pq)$ Eulerovy funkce jako

$$\varphi(pq) = (p-1)(q-1) = rp + sq.$$

Dále nechť k je stupeň a zároveň platí $0 \leq k \leq (p-1)(q-1)$. Potom

1. $a_k = 1$ právě tehdy, když $k = ip + jq$ pro $i \in \langle 0; r\rangle$ a $j \in \langle 0; s\rangle$,
2. $a_k = -1$ právě tehdy, když $k + pq = ip + jq$ pro $i \in \langle r+1; q-1\rangle$ a $j \in \langle s+1; p-1\rangle$,
3. jinak $a_k = 0$.

Navíc platí, pokud $p > q$, že prostřední koeficient polynomu je roven $(-1)^r$.

[10]

Příklad: Určete koeficienty cyklotomického polynomu $\phi_6(x)$.

Nejprve ověříme podmínku o součinu prvočísel: $6 = 2.3$.

Dále vypočtěme hodnotu Eulerovy funkce: $\varphi(6) = (2-1)(3-1) = 2 = 1.2 + 0.3$.

Vypišme si tedy: $p = 2$,
$q = 3$,
$r = 1$,
$s = 0$.

a) $k = 0$

1. $a_0 = 1$ právě tehdy, když $0 = 0.2 + 0.3$ a zároveň $0 \in \langle 0; 1\rangle$ a $0 \in \langle 0; 0\rangle$… platí
2. $a_0 = -1$ právě tehdy, když $0 + 6 = 1.2 + 1.3$ a zároveň $1 \in \langle 2; 2\rangle$ a $1 \in \langle 1; 1\rangle$… neplatí
3. jinak $a_0 = 0$… neplatí, neboť platí první podmínka

Stejným způsobem zjistíme ostatní koeficienty.

b) $k = 1$

1. $a_1 = 1$ právě tehdy, když $1 = -1.2 + 1.3$ a zároveň $-1 \in \langle 0; 1\rangle$ a $1 \in \langle 0; 0\rangle$… neplatí
2. $a_1 = -1$ právě tehdy, když $1 + 6 = 2.2 + 1.3$ a zároveň $2 \in \langle 2; 2\rangle$ a $1 \in \langle 1; 1\rangle$… platí
3. jinak $a_1 = 0$… neplatí

c) $k = 2$

1. $a_2 = 1$ právě tehdy, když $2 = 1.2 + 0.3$ a zároveň $1 \in \langle 0; 1\rangle$ a $0 \in \langle 0; 0\rangle$… platí
2. $a_2 = -1$ právě tehdy, když $2 + 6 = 1.2 + 2.3$ a zároveň $1 \in \langle 2; 2\rangle$ a $2 \in \langle 1; 1\rangle$… neplatí
3. jinak $a_2 = 0$… neplatí

Koeficienty a_2 až a_0 se tedy rovnají popořadě $1, -1, 1$. Cyklotomický polynom má tedy tvar $\phi_6(x) = x^2 - x + 1$. Pro kontrolu, prostřední koeficient polynomu je opravdu roven $(-1)^1 = -1$.

Věta 4.1.2 (Koeficienty cyklotomického polynomu $\phi_n(x)$, kde n je prvočíslo nebo jeho mocnina)

Pro všechny koeficienty cyklotomického polynomu $\phi_n(x)$, kde n je libovolné prvočíslo nebo je mocninou prvočísla, platí, že jsou rovné jedné.

Příklad: Určete koeficienty cyklotomického polynomu $\phi_{11}(x)$.

Cyklotomický polynom $\phi_n(x)$, kde číslo n je prvočíslo, získáme, když binomickou rovnici $x^n - 1$ vydělíme výrazem $x - 1$. Číslo 11 je prvočíslo. V našem případě tedy budeme dělit binomickou rovnici $x^{11} - 1$ výrazem $x - 1$:

$$\phi_{11}(x) = \frac{x^{11} - 1}{x - 1} = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

Jak je vidět, všechny koeficienty cyklotomického polynomu $\phi_{11}(x)$ jsou rovné číslu 1, což souhlasí s předchozí větou.

Příklad: Určete koeficienty cyklotomického polynomu $\phi_9(x)$.

Cyklotomický polynom $\phi_9(x)$ je polynom, kde číslo n je mocninou prvočísla. Konkrétně máme číslo 9, které je druhou mocninou prvočísla 3. Tvar cyklotomického polynomu tedy dostaneme podle vzorce:

$$\phi_{p^\alpha}(x) = \frac{x^{p^\alpha} - 1}{x^{p^{\alpha-1}} - 1}.$$

Dělíme tedy:

$$\phi_9(x) = \phi_{3^2}(x) = \frac{x^{3^2} - 1}{x^{3^{2-1}} - 1} = \frac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1.$$

Opět můžeme vidět, že všechny koeficienty cyklotomického polynomu $\phi_9(x)$ jsou rovné číslu 1, což souhlasí s předchozí větou.

Věta 4.1.3 (Koeficienty cyklotomického polynomu $\phi_n(x)$, kde n je dvojnásobkem nebo čtyřnásobkem lichého prvočísla)

Pro koeficienty cyklotomického polynomu $\phi_n(x)$, kde n je dvojnásobkem libovolného lichého prvočísla, platí

$$\phi_{2p}(x) = \frac{x^{2p}-1}{x^p-1}.\frac{x-1}{x^2-1} = x^{p-1} - x^{p-2} + x^{p-3} - \ \ldots - x + 1,$$

tedy koeficienty jsou rovné ± 1 a zároveň znaménka se pravidelně střídají.

[10]

Příklad: Tento vzorec lze využít například při zjišťování koeficientů u cyklotomického polynomu $\phi_n(x)$, kde $n = 6, 10, 14, 22, 26, 38, \ldots$ Vypočtěte cyklotomický polynom $\phi_{10}(x)$.

$$\phi_{10}(x) = \frac{x^{10}-1}{x^5-1}.\frac{x-1}{x^2-1} = \frac{x^{11}-x^{10}-x+1}{x^7-x^5-x^2+1} = x^4 - x^3 + x^2 - x + 1.$$

Pro koeficienty cyklotomického polynomu $\phi_n(x)$, kde n je čtyřnásobkem libovolného lichého prvočísla, platí

$$\phi_{4p}(x) = \frac{x^{4p}-1}{x^{2p}-1}.\frac{x^2-1}{x^4-1} = x^{2p-2} - x^{2p-4} + x^{2p-6} - \ \ldots - x^2 + 1,$$

tedy koeficienty jsou rovné ± 1 a zároveň se pravidelně střídají.

[10]

Příklad: Tento vzorec lze využít například při zjišťování koeficientů u cyklotomického polynomu $\phi_n(x)$, $n = 12, 20, 28, 42, 44, 68, 76, \ldots$ Vypočtěte cyklotomický polynom $\phi_{12}(x)$.

$$\phi_{12}(x) = \frac{x^{12}-1}{x^6-1}.\frac{x^2-1}{x^4-1} = \frac{x^{14}-x^{12}-x^2+1}{x^{10}-x^6-x^4+1} = x^4 - x^2 + 1.$$

Závěr

Cílem této bakalářské práce s názvem „Polynomy pro dělení kruhu“ bylo podat ucelený výklad o souvislosti mezi binomickými rovnicemi, cyklotomickými polynomy a sestrojitelnosti pravidelných mnohoúhelníků. Práce je rozčleněna do čtyř kapitol a je doplněna množstvím vypočtených ilustračních příkladů, které slouží k lepšímu pochopení vykládaného tématu nebo mají za úkol dokázat pravdivost tvrzení.

V první kapitole jsme se zabývali binomickými rovnicemi a n-tými odmocninami. Začali jsme binomickými rovnicemi obecně a vysvětlili si, proč se binomické rovnice také označují jako rovnice pro dělení kruhu. Poté jsme uvažovali takové binomické rovnice, které by dělili jednotkovou kružnici. Vysvětlili jsme si pojem primitivní kořeny a jejich vlastnosti, zde jsme uvedli názorný příklad.

V druhé kapitole jsme se zabývali polynomy pro dělení kruhu neboli cyklotomickými polynomy. Vysvětlili jsme si, jak se z binomických rovnic dostaneme k cyklotomických polynomům a jejich vytvoření jsme si ukázali také na příkladech. V této kapitole jsme se pak zabývali otázkou sestrojitelnosti pravidelných mnohoúhelníků, a to pomocí pravítka a kružítka. Obsáhlou ukázku tvoří konstrukce pravidelného sedmnáctiúhelníku na základě Gaussových period. Dále jsme probrali řešitelnost binomických rovnic pomocí druhých odmocnin a uvedli některé důsledky.

Ve třetí kapitole jsme se zabývali ireducibilitou cyklotomických polynomů. Vysvětlili jsme si některé důležité pojmy. Dále jsme uvedli metodu rozkladu polynomů pomocí Hornerova schématu, kterou jsme ilustrovali na jednoduchém příkladu. Poté jsme určili vlastnosti ireducibilních polynomů a podali důkaz ireducibility podle Leopolda Kroneckera.

V poslední kapitole jsme se zabývali koeficienty cyklotomických polynomů, určili jsme, jak tyto koeficienty v některých příkladech vypadají. Na závěr jsme se naučili metodu jejich určování, kterou jsme si názorně ukázali na příkladě.

Resumé

The aim of this bachelor´s thesis with the title „Polynomials for division of the circle“ was to put a compact interpretation on the connection between the binomial equations, cyclotomic polynomials and the construction of the regular polygons. The thesis is divided into four chapters. These chapters are supplemented by a number of solved exercises for illustration, which should help to the better comprehension of the given topic or which should prove the veracity of the statements. The work begins with the solution of the binomial equations which is logically followed by the theory of polynomials for division of the circle that is also called cyclotomic polynomials. The author of this work tried to deal widely with the question of the construction of the regular polygons only with the aid of a ruler and a pair of compasses. The significant part of this work is dedicated to the question of the construction of the regular heptadecagon, which Johann Carl Friedrich Gauss worked on. In this thesis there is also mentioned and solved the irreducibility of the cyclotomic polynomials and their other characteristics. In the end of this work the author looks into the coefficients of the cyclotomic polynomials.

Seznam použité literatury a internetových zdrojů

[1] ŠILAROVÁ, Lenka. *Komplexní čísla ve výuce matematiky na střední škole s využitím internetu* [online]. Praha [cit. 2014-02-10]. Dostupné z: http://www.karlin.mff.cuni.cz/~robova/stranky/silarova/. Diplomová práce. Univerzita Karlova v Praze, Matematicko-fyzikální fakulta, Katedra didaktiky matematiky. Vedoucí práce RNDr. Jarmila Robová, CSc.

[2] *Binomická rovnice* [online]. [cit. 2014-02-13]. Dostupné z: http://mozartak.ic.cz/vyuka/sma/Komplexni01.pdf

[3] *Mnohoúhelník* [online]. [cit. 2014-02-13]. Dostupné z: http://www.google.cz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCwQFjAA&url=http%3A%2F%2Fwww.1zstrebon.cz%2Fdownload.php%3Fid%3D580&ei=pCEsU7mqLcOPtQaD_oDQAQ&usg=AFQjCNEks1_WtrJe5V7MkwrWTP_vHlm-MA&sig2=gQVfu4FRLATesjF_C1usQg&bvm=bv.62922401,d.Yms

[4] ŠKOLNIK, Adolf Grigorjevič a Alfons BAŠTA. *Dělení kruhu*. 1. vydání. Praha: Československé akademie věd, 1953.

[5] *Eukleidovská konstrukce* [online]. [cit. 2014-05-15]. Dostupné z: http://www.kmt.zcu.cz/subjects/geom/Uctexty/wKontsr.pdf

[6] Fuchs, Eduard. *Fermatova prvočísla* [online]. [cit. 2014-05-15]. Dostupné z: http://bart.math.muni.cz/~fuchs/Efuchs/historie_pdf/6ferm.pdf

[7] KOUTNÝ, F. *Carl Friedrich Gauss*. [online]. [cit. 2014-03-18]. Dostupné z: http://www.zas.cz/download/gauss.pdf

[8] *MathPages: Constructing the Heptadecagon* [online]. [cit. 2014-03-23]. Dostupné z: http://mathpages.com/home/kmath487.htm

[9] *Časopis pro pěstování mathematiky a fysiky: O pravidelném sedmnáctiúhelníku* [online]. V Praze: Nákladem Jednoty českých mathematiků, 1872- [cit. 2014-03-28]. Dostupné z: http://dml.cz/bitstream/handle/10338.dmlcz/123514/CasPestMatFys_033-1904-5_6.pdf

[10] *Wolfram MathWorld: The Web's Most Extensive Mathematics Resource: Cyclotomic Polynomial* [online]. [cit. 2014-05-21]. Dostupné z: http://mathworld.wolfram.com/CyclotomicPolynomial.html

[11] PROCHÁZKA, Ladislav a kol. *Algebra*. 1. vydání. Praha: Academia, 1990, 560 s. ISBN 80-200-0301-0.

[12] SCHWARZ, Štefan. *O rovnicích*. 2. vydání. Praha: Jednota československých matematiků a fysiků, 1947. Cesta k vědění.

[13] SCHWARZ, Štefan. *Základy náuky o riešení rovníc*. 2. vydání. Bratislava: SAV, 1968.

[14] *Rozhledy matematicko-fyzikální: časopis pro studující středních škol a zájemce o matematiku, fyziku a informatiku*. Praha: Jednota českých matematiků a fyziků, 1921-, roč. 1972/73, str. 76-77.

[15] HONZÍK, Lukáš. *Elementární algebra* [přednáška]. Plzeň: ZČU, 2012.

[16] *Matematika: Goniometrický tvar komplexního čísla* [online]. [cit. 2014-02-13]. Dostupné z: http://www.matematika.cz/komplexni-goniometricky-tvar

Seznam obrázků