Komplexní čísla I

Komplexní čísla jsou důležitým rozšířením reálných čísel. Poprvé, spíše náhodou na ně narazil Gerolamo Cardano, když se snažil najít jeho známé vzorce pro řešení kubických rovnic. Dnes víme, že komplexní čísla nám mohou dopomoci k řadě zkratek a novým tvrzením z reálných čísel. Některé takové aplikace si ukážeme v tomto seriálu.

Pokud budeme chtít k objevení komplexních čísel přistupovat trochu systematičtěji, tak vznikají právě z toho, že bychom chtěli v reálných číslech umět odmocňovat záporná čísla. V tom nám zabraňuje to, že pro každé reálné číslo platí $x^2 \geq 0$. Na podobný problém narazíme, i když budeme řešit kvadratické rovnice.

Bylo by velmi pěkné, kdyby každá kvadratická rovnice měla dva kořeny (nebo jeden dvojnásobný). Ovšem víme, že rovnice se záporným diskriminantem nemají v reálných číslech žádné kořeny. K tomu by nám opět jen stačilo umět odmocnit záporný diskriminant.

Oba tyto problémy jsou spolu úzce svázány, dokonce by nám stačilo i odmocnit jediné číslo, třeba -1, nebo vyřešit jediný kvadratický polynom se záporným diskriminantem, třeba x^2+1, a byli bychom za vodou. Proto přidáváme k reálným číslům imaginární jednotku i, která je právě $\sqrt{-1}$, stejně jako kořen x^2+1.

Vzniknou nám tím komplexní čísla, která jsou mnohem homogennější a zároveň i zajímavější než čísla reálná. Ukážou nám souvislosti mezi exponenciálou a goniometrickými funkcemi, každý polynom tu bude mít právě tolik kořenů, kolik bychom čekali. A kromě toho ještě mnohem více užitečných nebo zajímavých vlastností.

Představení komplexních čísel

V této kapitole zavedeme komplexní čísla. K tomu existuje více různých přístupů a žádný z nich není lepší nebo horší. Tady pro zajímavost uvádíme tři různé postupy, pokud se ti některý nelíbí, klidně ho přeskoč. Stačit ti bude jeden a někdy ani to ne, protože budeme pracovat převážně s jejich vlastnostmi a ne jejich definicemi.

Reálně dvojicové

Komplexní čísla můžeme definovat přímo, pomocí reálných čísel. Každé komplexní číslo z lze napsat jako $a+bi$ pro a, b reálná. Definujeme je tedy tímto předpisem. *Komplexní číslo* z je dvojice čísel reálných (z_0, z_1) (představuj si pod touto dvojicí zápis $z = z_0 + z_1 i$). Na komplexních číslech pak definujeme operace sčítání a násobení následujícím způsobem

$$z + w = (z_0, z_1) + (w_0, w_1) = (z_0 + w_0, z_1 + w_1),$$
$$zw = (z_0 w_0 - z_1 w_1, z_0 w_1 + z_1 w_0).$$

Označíme si $i = (0, 1)$ a čísla tvaru $(a, 0)$ ztotožněme s reálnými čísly, budeme tedy psát a místo $(a, 0)$. Všimni si, že opravdu $i^2 = -1$, to jsme přesně chtěli.

Maticové

Jedno z nejjednodušších zavedení komplexních čísel je pomocí znalostí z maticového počtu.[1]

[1] Pokud neumíš počítat s maticemi, můžeš se podívat třeba do prasečí knihovny na příspěvek Matice od Káti Fišerové (*http://mks.mff.cuni.cz/library/MaticeKF/MaticeKF.pdf*).

Řekneme, že komplexní čísla jsou právě čtvercové matice 2×2, tvaru

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Podívejme se, jestli opravdu dostáváme pořád to samé. Kam se nám tentokráte schovalo i a kde jsou reálná čísla? Prvně se poohlídneme po jedničce, jednička je číslo, které je neutrální vůči násobení. Tedy vynásobíme-li jedničku číslem z, vyjde nám opět jenom z. Tuto vlastnost má matice

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

Reálná čísla pak snadno najdeme jako násobky jedničky, tedy pro $a \in \mathbb{R}$

$$a = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

Dále i bude „ta druhá“ matice než jednička, tj. $i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Zkusme si toto i umocnit na druhou.

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 \cdot (-1) & 0 \\ 0 & (-1) \cdot 1 \end{pmatrix} = -1$$

Opravdu je to to, co jsme hledali. Všimni si, že i z matice lze snadno vidět rozklad na reálnou a imaginární část, platí

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + bi.$$

Cvičení. Vynásob si dvě komplexní čísla zapsaná ve tvaru matic a ověř si, že formule pro násobení z prvního způsobu zavedení komplexních čísel funguje i tady.

Tady můžeme definovat absolutní hodnotu trochu jiným způsobem než obvykle, totiž pomocí determinantu matice: $|z| = \sqrt{\det z}$. Vyjde nám opravdu to samé jako při obvyklé definici, kterou najdeš v další kapitole.

Dále si všimneme, že determinant je vždycky nezáporný a nulový jen pro nulovou matici, takže každá z těchto matic má matici inverzní (kromě nuly), to nám říká že každým komplexním číslem různým od nuly můžeme dělit.

Cvičení. Najdi vzoreček pro $1/z$, je-li $z = a + ib$ nenulové komplexní číslo, pomocí inverzní matice.

Mnohočlenné

Myšlenka této konstrukce je vskutku jednoduchá. Rozhodneme se, že chceme přidat jeden prvek k reálným číslům, totiž číslo i, že $i^2 = -1$, tj. kořen kvadratického polynomu $x^2 + 1$. V tomto odstavci se budeme snažit to udělat o kousek korektněji, než že prostě řekneme, že $i = \sqrt{-1}$. Tímto symbol $\sqrt{\ }$ maličko ztrácí smysl, neboť komplexní odmocniny jsou vždycky dvě.[2]

Abychom to mohli udělat poctivě, budeme potřebovat kousíček teorie. Která však není složitá, funguje naprosto stejně jako teorie kolem celých čísel. Můžeš si porovnávat a představovat všechno, co bude následovat, na celých číslech.

[2] Můžeš namítat, že odmocnina z nuly je jen jedna, ale ve skutečnosti je jedna dvakrát. ;-)

První věc je dělení mnohočlenů se zbytkem. Určitě víš, že mnohočleny se dají dělit se zbytkem stejně jako celá čísla. Tedy mám-li dané $f(x), g(x)$ mnohočleny s reálnými koeficienty (třeba), umím najít jejich celomnohočlenový podíl $q(x)$ a zbytek $r(x)$, že

$$f(x) = q(x) \cdot g(x) + r(x)$$

a přitom $r(x)$ je „menší“ než $g(x)$. Menší tady pro nás znamená, že má menší stupeň.

Můžeme teď definovat na všech možných zbytcích po dělení nějakým daným mnohočlenem $g(x)$ operace sčítání a násobení. Jednoduše tak, že zbytky nejdříve sečteme, resp. vynásobíme a pak najdeme zbytek součtu, resp. součinu. Tj. když to zapíšeme symbolicky,

$$r_1(x) +_g r_2(x) = (r_1(x) + r_2(x)) \bmod g(x),$$
$$r_1(x) \cdot_g r_2(x) = (r_1(x) \cdot r_2(x)) \bmod g(x).$$

Množinu všech zbytků po dělení mnohočlenem $f(x)$ s těmito operacemi budeme značit[3] $\mathbb{R}[x]/f(x)$. Všimni si, že počítání v tomto oboru není nic jiného než s počítání s x-em, které splňuje rovnost $f(x) = 0$, ke které sáhneme vždycky, když máme moc vysoký exponent u x. Také si představ, jak vypadají všechny zbytky modulo $f(x)$, jsou to právě polynomy tvaru

$$a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0,$$

kde $a_0, a_1, \ldots, a_{n-1}$ jsou reálná čísla a n je stupeň $f(x)$.

Zajímat nás budou mnohočleny, které jsou nerozložitelné. Ty mají mezi polynomy stejný význam jako prvočísla mezi celými čísly. Mnohočlen $f(x)$ nazveme *nerozložitelný*, pokud se nedá netriviálně rozložit na součin dvou jiných, tj. kdykoliv $f(x) = g(x) \cdot h(x)$, pak buď $g(x)$ nebo $h(x)$ je konstantní.

V reálných číslech jsou nerozložitelné právě kvadratické mnohočleny se záporným diskriminantem.[4] Kdyby se kvadratický mnohočlen měl rozložit na dva nekonstantní, tak oba mají stupeň 1, tedy jsou lineární. U lineárních mnohočlenů snadno najdeme jejich kořen, který bude kořenem i původního kvadratického. Jeden z nerozložitelných polynomů tedy je $x^2 + 1$, to je přesně ten, který nás bude zajímat.

Proč nás zajímají právě nerozložitelné? Z jednoduchého důvodu, abychom mohli dělit. Kdybychom počítali modulo $f(x)$ a $f(x)$ by se nám rozkládal na $g(x)h(x)$, tak by platilo $g(x) \cdot_f h(x) = 0$ a už z principu bychom nemohli dělit zbytkem $g(x)$, protože bychom dostali, že

$$0 = \frac{0}{g(x)} = \frac{g(x) \cdot_f h(x)}{g(x)} = h(x),$$

což vůbec nedává smysl. Pokud $f(x)$ ale bude nerozložitelný, tak dělit můžeme. I to se dá zdůvodnit, není to příliš těžké, ale zbytečně dlouhé, takže nám to na tomto místě raději uvěř.

Takže například vezmeme-li si mnohočleny s racionálními koeficienty a vybereme-li polynom $f(x) = x^3 + 2x^2 - 2$, který je nerozložitelný,[5] tak můžeme počítat například:

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

---

[3] Množinu všech mnohočlenů s reálnými koeficienty značíme $\mathbb{R}[x]$.

[4] Dokázat to, že v reálných číslech žádné jiné nejsou nerozložitelné, je relativně složité a použijí se při tom netriviální vlastnosti komplexních čísel, na to se podíváme trochu důkladněji ještě později.

[5] To se dá snadno dokázat Eisensteinovým kritériem.

Tedy platí $(1-x)^{-1} = x^2 + 3x + 3$ a převrácená hodnota se dá spočítat i pro každý jiný zbytek modulo $f(x)$, ačkoliv to není úplně snadné.

Nyní už konečně můžeme korektně definovat komplexní čísla krásně a elegantně. Polynom, který nás zajímá, je $x^2 + 1$. Při přeznačení proměnné jako i, pak definujme

$$\mathbb{C} = \mathbb{R}[i]/(i^2 + 1).$$

Důležitá vlastnost, ta o kterou jsme usilovali, je, že teď už mnohočlen $x^2 + 1$ má kořen, a totiž původní neznámou i. Když dosadíme do $x^2 + 1$ za x číslo i, dostaneme $i^2 + 1$, což dá po vydělení mnohočlenem $i^2 + 1$ zbytek 0. Podobná věc platí i v obecnějším případě; když máme libovolné $\mathbb{R}[\alpha]/f(\alpha)$, polynom $f(x)$ má vždycky kořen α. Takže podobným způsobem můžeme zkonstruovat třeba i těleso, které bychom mohli nazvat *Eisensteinovými čísly*.[6]

$$\mathbb{E} = \mathbb{R}[\omega]/(\omega^2 + \omega + 1)$$

Ovšem žádnou takovou konstrukcí nedostaneme nic jiného než komplexní čísla. Tedy v každém z těchto oborů najdeme i, že $i^2 = -1$, a naopak v $\mathbb{C}$ umíme hledat kořeny polynomu $x^2 + x + 1$.

Cvičení. Najdi v $\mathbb{E}$ kořeny polynomu $x^2 + 1$.

Cvičení. Je-li $f(x) = x^2 + bx + c$ nerozložitelný kvadratický polynom, najdi v $\mathbb{R}[\alpha]/f(\alpha)$ kořeny polynomu $x^2 + 1$.

Vlastnosti komplexních čísel

V předchozí kapitole jsme se dozvěděli, jak se komplexní čísla dají zkonstruovat, ale to nám neřekne, jaké mají vlastnosti.

S komplexními čísly budeme pracovat jednoduše jako s dvojicemi reálných čísel (a, b), psáno $z = a + ib$, kde „imaginární jednotka“ i má vlastnost $i^2 = -1$. Samostatná čísla a a b mají taktéž neodmyslitelnou funkci, proto definujeme pomocné funkce *reálná část* a *imaginární část* (čistě proto, že někdy nebudeme mít komplexní čísla napsaná v tomto hezkém tvaru) komplexního čísla $a + bi$ vztahy

$$\Re(a + bi) = a, \qquad \Im(a + bi) = b.$$

Když se chvíli zamyslíš nad vlastnostmi čísla $-i$, uvidíš, že jsou mnohdy stejné jako vlastnosti čísla i, neboť také platí $(-i)^2 = -1$. Když tedy v některých našich tvrzeních zaměníme i a $-i$, jejich platnost se nezmění. Proto je přirozené definovat pojem *číslo komplexně sdružené* k číslu $a + bi$. To se značí poněkud netradičně pruhem nahoře a definuje následovně.

$$\overline{a + bi} = a - bi$$

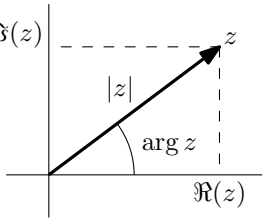
Další velmi použitelná funkce je *absolutní hodnota* komplexního čísla, někdy též zvaná *modul*. Je dána vzorečkem

$$|a + bi| = \sqrt{a^2 + b^2}.$$

Vyjadřuje něco jako „velikost“ komplexního čísla. Komplexní čísla nejde nějak rozumně lineárně uspořádat, jako například čísla reálná. Pokud budeme chtít mluvit o nějakém komplexním číslu jako o „větším“, většinou budeme porovnávat absolutní hodnoty.

[6] V třetím díle seriálu se budeme se zabývat použitím komplexních čísel v teorii čísel, tam se setkáme s Eisensteinovými celými čísly.

A jak si vlastně komplexní čísla představit? Jednoduše. Zakreslíme si číslo $a + bi$ do roviny jako bod se souřadnicemi $[a, b]$. Jeho modul bude udávat vzdálenost od bodu $[0, 0]$ a komplexně sdružené komplexní číslo bude vzor bodu $[a, b]$ v osové souměrnosti s osou x.



Sčítání, odčítání i násobení komplexních čísel je jednoduché. Pokud však dvě komplexní čísla budeme chtít vydělit, budeme potřebovat nějak upravit jejich podíl. Za tímto účelem se používá tzv. metoda rozšíření číslem komplexně sdruženým se jmenovatelem. Tedy chceme-li spočítat podíl $\frac{a+bi}{c+di}$ dvou komplexních čísel, postupujeme následovně

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd+i(bc-ad)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + i\frac{bc-ad}{c^2+d^2}.$$

A jelikož a, b, c i d byla čísla reálná, pak podíly $\frac{ac-bd}{c^2+d^2}$ a $\frac{bc-ad}{c^2+d^2}$ budou reálné. Všimni si, že ve jmenovateli se vyskytuje právě druhá mocnina absolutní hodnoty dělitele $c + di$, kdyby nás zajímalo jen kolik je $1/z$, tak snadno stejným způsobem odvodíme vzoreček $1/z = \overline{z}/|z|^2$, který je jen úpravou vztahu $z\overline{z} = |z|^2$.

Všechna komplexní čísla z, pro která bude platit $|z| = 1$, budu nazývat *komplexní jednotky*. Množina všech komplexních jednotek je jednotková kružnice se středem v počátku. Pěkná vlastnost těchto čísel je, že když je mezi sebou násobíme, dostáváme jen další komplexní jednotky. Kromě toho pro tato čísla se dobře počítají inverze, platí totiž $z^{-1} = \overline{z}$.

Cvičení. Ověřte, že výše definované funkce mají následující vlastnosti:

(i) $z + \overline{z} = 2\Re(z)$, $z - \overline{z} = 2\Im(z)$,
(ii) $|\overline{z}| = |z|$,
(iii) $|z_1 z_2| = |z_1|\,|z_2|$,
(iv) $|z_1| - |z_2| \leq |z_1 + z_2| \leq |z_1| + |z_2|$.

Řešení kvadratické rovnice

Všechno, pro co zavádíme komplexní čísla, byla neschopnost najít kořeny kvadratických polynomů se záporným diskriminantem. Podívejme se tedy, jak jsme si pomohli. K tomu prvně budeme muset umět komplexní čísla odmocňovat, tj. pro dané z řešit rovnici $x^2 = z$.

Odmocňování komplexních čísel

Odmocňování kladných reálných čísel je jednoduché. Díky výše uvedenému arzenálu však už umíme odmocňovat i čísla záporná, neboť pro $a \geq 0$ platí $\sqrt{-a} = \sqrt{-1}\sqrt{a} = \pm i\sqrt{a}$. Obecněji se komplexní číslo $a + bi$ odmocní následujícím způsobem. Nejprve předpokládejme, že odmnocniny z komplexních čísel jsou opět komplexní čísla a označme $c + di = \sqrt{a + bi}$., Pak umocněním

máme $c^2 + 2cdi - d^2 = (c + di)^2 = a + bi$. Porovnáním reálných a komplexních částí dostáváme soustavu

$$c^2 - d^2 = a, \quad 2cd = b.$$

Dosazením druhé rovnosti do první dostaneme rovnici $4c^4 - 4ac^2 - b^2 = 0$. Tato rovnice však má vždy řešení, neboť

$$c_{1,2}^2 = \frac{4a \pm 4\sqrt{a^2 + b^2}}{8} = \frac{a}{2} \pm \frac{\sqrt{a^2 + b^2}}{2}$$

a jedna z těchto druhých mocnin kořenů je nekladná, druhá nezáporná. Proto vždy bude druhá odmocnina z komplexního čísla existovat. Na první pohled by se mohlo zdát, že druhá odmocnina z komplexního čísla je jednoznačná, a to odmocnina z předchozího nazáporného kořenu. Avšak podíváme-li se pořádně, je jasné, že obě dvě nalezené dvojice (c, d) se liší o znaménko.

Odvození řešení kvadratické rovnice

Nyní se zaměřme na řešení rovnice $x^2 + px + q = 0$,[7] kde $p, q \in \mathbb{R}$. Úpravou (doplněním na čtverec) dostaneme

$$x^2 + px + q = \left(x + \frac{1}{2}p\right)^2 - \frac{1}{4}p^2 + q = 0$$

a převedením konstant na druhou stranu a odmocněním dostaneme výsledek

$$x_{1,2} = -\frac{p}{2} \pm \frac{\sqrt{p^2 - 4q}}{2}.$$

Pro $p^2 - 4q \geq 0$ je tento vztah ve skutečnosti vzoreček pro hledání kořenů kvadratické rovnice. Pokud však $p^2 - 4q < 0$, pak budou obě řešení kvadratické rovnice čísla komplexní. Navíc porovnáme-li jejich komplexní a reálné části, zjistíme, že oba kořeny jsou komplexně sdružená čísla. To je velmi užitečný nástroj, protože nyní už při řešení kvadratické rovnice s reálnými koeficienty nemusíme vždy pracně hledat oba kořeny. Když nám totiž první kořen vyjde komplexní, druhý už nutně musí být komplexně sdružený s prvním.

Kdybychom však řešili obecnější rovnici $x^2+px+q = 0$, kde $p, q \in \mathbb{C}$, tak též nemáme problém, neboť stačí aplikovat předchozí poznatek o odmocnině z komplexního čísla. Zde však už nebudou nutně oba kořeny komplexně sdružená čísla. Bude tomu tak pouze tehdy, když koeficient p bude reálné číslo. Rozšířili jsme tedy středoškolský vzoreček do komplexních čísel a umíme najít kořeny libovolné kvadratické rovnice.

Cvičení.

(i) Najděte druhé odmocniny z komplexního čísla $3 - 4i$.
(ii) Vyřešte v komplexních číslech rovnice $z^2 - 3 + 2i = 0$, $z^4 + 2z^2 + 5 = 0$ a $z^2 - \overline{z} = 0$.

Goniometrický tvar komplexních čísel

Nejen zápisem $z = a + bi$ můžeme popsat komplexní číslo. V některých zápisech se lépe sčítá, v jiných se zase jednodušeji násobí. Druhý způsob, který si ukážeme, je tzv. *goniometrický tvar komplexního čísla*

$$z = r(\cos\phi + i\sin\phi),$$

[7] Koeficientu u x^2 se jednoduše zbavíme vydělením celé rovnice.

kde $r = |z|$ je modul a ϕ, nazýváno *argument* komplexního čísla a značeno $\arg(z)$, je určeno reálnou a imaginární částí z rovnicemi

$$\cos\phi = \frac{\Re(z)}{|z|}, \quad \sin\phi = \frac{\Im(z)}{|z|}.$$

Číslo ϕ proto není určeno jednoznačně, dokud se neomezíme na interval $[0, 2\pi)$, neboť řešením uvedené soustavy je každé číslo tvaru $\phi = \phi_0 + 2k\pi$, kde $k \in \mathbb{Z}$ a $\phi_0 \in [0, 2\pi)$ řeší tutéž soustavu.

Pokud si zadefinované pojmy chcete geometricky představit, pak r udává vzdálenost z od počátku a ϕ značí kladný[8] úhel, který svírá kladná polopřímka reálných čísel se spojnicí počátku s bodem z.

Nyní k tomu, proč se nám tento zápis hodí. Zkusme si jím napsat „neintuitivní“ operaci násobení. Máme-li dvě komplexní čísla

$$z_1 = r_1(\cos\phi_1 + i\sin\phi_1), \quad z_2 = r_2(\cos\phi_2 + i\sin\phi_2),$$

pak snadným použitím součtových vzorců dospějeme k rovnosti

$$z_1 z_2 = r_1 r_2(\cos(\phi_1 + \phi_2) + i\sin(\phi_1 + \phi_2)).$$

Tohle je už je ale mnohem intuitivnější zápis násobení. Říká nám, že násobek dvou komplexních čísel bude mít od počátku vzdálenost rovnou součinu vzdáleností obou činitelů. Navíc chceme-li získat úhel udávající součin dvou komplexních čísel, stačí sečíst úhly udávající jednotlivé činitele. Obdobně podle goniometrických vzorců by se ověřil i podíl dvou komplexních čísel, akorát zde budu druhým modulem dělit a druhý argument odčítat

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}\big(\cos(\phi_1 - \phi_2) + i\sin(\phi_1 - \phi_2)\big).$$

Jelikož nám násobení a dělení šlo v goniometrickém tvaru neuvěřitelně jednoduše, zkusme rovnou mocnění. To nám usnadňuje následující věta.

Věta. (Moivreova[9] věta) *Uvažujeme-li komplexní číslo z v goniometrickém tvaru $z = r(\cos\phi + i\sin\phi)$, pak pro libovolné $n \in \mathbb{Z}$ platí*

$$z^n = r^n\big(\cos(n\phi) + i\sin(n\phi)\big).$$

Důkaz. Je-li n přirozené číslo, pak se vzorec snadno ověří matematickou indukcí. Buď tedy $z = r(\cos\phi + i\sin\phi)$, pro $n = 1$ vzoreček zřejmě platí, nechť tedy platí pro n a počítejme

$$\begin{aligned} z^{n+1} &= z^n z = r^n(\cos n\phi + i\sin n\phi)\cdot r(\cos\phi + \sin\phi) \\ &= r^{n+1}\big(\cos(n+1)\phi + i\sin(n+1)\phi\big). \end{aligned}$$

V poslední rovnosti jsme použili vztah pro součin komplexních čísel v goniometrickém tvaru.

Budeme-li uvažovat n záporné, pak snadno odvodíme

$$z^n = \frac{1}{z^{-n}} = \frac{1}{r^{-n}}(\cos(n\phi) - i\sin(n\phi))^{-1} = r^n(\cos(n\phi) + i\sin(n\phi))$$

[8] Bráno proti směru hodinových ručiček.

[9] Moivre de Abraham, francouzský matematik 1667–1754

díky tomu, že $(\cos n\phi - i\sin n\phi)$ je komplexní jednotka, a tedy pro ni platí $z^{-1} = \overline{z}$. $\square$

Cvičení.

(i) Napište komplexní čísla $1 - i\sqrt{3}$ a $\sqrt{2} + i\sqrt{2}$ v goniometrickém tvaru.

(ii) Pokuste se spočítat $\left(\frac{1+i}{1-i}\right)^{42}$.

Pokusíme-li se na levou stranu Moivreovy věty dosadit za z komplexní jednotku v goniometrickém tvaru a následně umocnit podle binomické věty, dostaneme

$$\cos(n\phi) + i\sin(n\phi) = (\cos\phi + i\sin\phi)^n = \sum_{k=1}^{n} \binom{n}{k} \cos^{n-k}\phi i^k \sin^k\phi.$$

Využijeme-li toho, že $i^2 = -1$, $i^3 = -i$ a $i^4 = 1$, pak porovnáním reálných a imaginárních částí dostáváme zajímavé identity

$$\begin{aligned}\cos(n\phi) &= \binom{n}{0}\cos^n\phi - \binom{n}{2}\cos^{n-2}\phi\sin^2\phi + \dots,\\ \sin(n\phi) &= \binom{n}{1}\cos^{n-1}\phi\sin\phi - \binom{n}{3}\cos^{n-3}\phi\sin^3\phi + \dots,\end{aligned}$$

které nám pomůžou pro zapamatování vzorců pro goniometrické funkce.

Exponenciální tvar komplexních čísel

Komplexní exponenciální funkce

Budeme chtít najít obdobu reálné exponenciální funkce $\exp(x) = e^x$ v komplexních číslech. Číslo e je tady pro nás *Eulerovo číslo*, neboli základ přirozeného logaritmu. Je to takové reálné číslo, že $e^x \geq 1 + x$ pro vsechna $x \in \mathbb{R}$.

Nejdůležitější vlastnost reálné exponenciály je

$$\exp(x + y) = \exp(x)\exp(y).$$

Budeme tedy hledat funkci $\exp\colon \mathbb{C} \to \mathbb{C}$, která toto splňuje pro každé $x, y \in \mathbb{C}$. Navíc budeme chtít, aby v nějakém dobrém smyslu rozšiřovala reálnou exponenciálu, tedy aby $\exp(x) = e^x$ pro každé $x \in \mathbb{R}$.

Prvně zkusme dosadit do rovnice za x reálné číslo a a za y imaginární číslo ib, $b \in \mathbb{R}$.

$$\exp(a + ib) = \exp(a)\exp(ib) = e^a\exp(ib).$$

Tedy bude nás zajímat hlavně funkce $\exp(ix)\colon \mathbb{R} \to \mathbb{C}$. Označme si

$$c(x) = \Re(\exp(ix)) \text{ a } s(x) = \Im(\exp(ix)).$$

Pak $c, s\colon \mathbb{R} \to \mathbb{R}$ jsou reálné funkce, které jednoznačně určují $\exp(ix) = c(x) + is(x)$. Zkusme do rovnice dosadit ix za x a iy za y, dostaneme

$$\begin{aligned}\exp(ix + iy) &= c(x + y) + is(x + y),\\ \exp(ix)\exp(iy) &= \big(c(x) + is(x)\big)\big(c(y) + is(y)\big) = \big(c(x)c(y) - s(x)s(y)\big) + i\big(s(x)c(y) + c(x)s(y)\big).\end{aligned}$$

Porovnáním reálných a imaginárních částí tedy dostaneme

$$c(x+y) = c(x)c(y) - s(x)s(y),$$
$$s(x+y) = s(x)c(y) + c(x)s(y),$$

což vypadá přesně jako součtové vzorce pro goniometrické funkce cos a sin. Vidíme, že jedno z řešení je tedy $\exp(ix) = \cos(x) + i\sin(x)$. Ostatní řešení nás zajímat nebudou, přestože tato rovnice jich má víc. Třeba všechny funkce $f(ix) = \cos(kx) + i\sin(kx)$ pro $k \in \mathbb{R}$ dané. Naše řešení je ale nejvýznačnější.[10]

Konečně definujme *komplexní exponenciální funkci* vztahem

$$e^z = e^{a+bi} = \exp(a+ib) = e^a(\cos b + i\sin b).$$

Při detailnějším prozkoumání zjistíme, že exponenciála nám převádí komplexní čísla na komplexní čísla, a to tak, že $|e^{a+ib}| = e^a$ a argument e^{a+ib} je roven b.

Stejně jako goniometrický tvar komplexních čísel nebyl jednoznačný, dostáváme i zde periodičnost v proměnné b s periodou 2π,[11] neboť je-li $z = a + ib$, tak platí

$$e^{z+2\pi i} = e^{a+(b+2\pi)i} = e^a(\cos(b+2\pi) + i\sin(b+2\pi)) = e^a(\cos b + i\sin b) = e^z.$$

Exponenciální tvar komplexních čísel

Definice komplexní exponenciály nám silně připomíná goniometrický tvar komplexního čísla. Pojďme si proto zkusit zavést exponenciální tvar komplexního čísla $z = r(\cos\phi + i\sin\phi)$ vztahem

$$z = re^{i\phi},$$

kde $r = |z|$ a ϕ je argument z. Na tento tvar můžeme nahlížet jen jako na zkratku goniometrického tvaru, prostě místo $\cos\phi + i\sin\phi$ píšeme jen $e^{i\phi}$.

Hlavní výhodou tohoto zápisu jsou dobře zapamatovatelná pravidla pro násobení, dělení a umocňování, jelikož platí

$$r_1e^{i\phi_1}r_2e^{i\phi_2} = r_1r_2e^{i(\phi_1+\phi_2)},$$
$$\frac{r_1e^{i\phi_1}}{r_2e^{i\phi_2}} = \frac{r_1}{r_2}e^{i(\phi_1-\phi_2)},$$
$$(re^{i\phi})^n = r^ne^{in\phi},\ n \in \mathbb{Z}.$$

Cvičení.

(i) Nalezněte goniometrický a exponenciální tvar komplexních čísel $1+i$ a $-\sqrt{3}-i$.
(ii) Vypočítejte hodnoty $e^{2\pi i}, 3e^{-\frac{\pi}{2}i}$.

---

[10] Je to zhruba z toho důvodu, že pro takovouto exponenciálu bude platit $\exp'(z) = \exp(x)$ (kde $\exp'$ značí derivaci funkce exp), což je podmínka obdobná tomu, že $e^x \geq 1 + x$ pro reálnou exponenciálu.

[11] Tu můžeme vnímat jako periodičnost celé funkce e^x s periodou $2\pi i$. Trochu to odporuje tomu, že periodická funkce je ta, která se pořád opakuje, protože tahle funkce se opakuje jen v jednom směru.

Ještě než se přesuneme dál, uvedeme si pár důležitých vztahů kolem komplexní exponenciály. První z nich je souvislost pěti nejdůležitějších matematických konstant, tj. čísel 0, 1, e, π a i, to kdybys náhodou někdy zapomněl hodnotu π a chtěl si ji vypočítat nebo nedej bože kdybys zapomněl, kolik je 0. ;-)

$$e^{\pi i} + 1 = 0.$$

Další se zajímavých vztahů je vztah exponenciály a goniometrických funkcí. Ve skutečnosti vlastně jde jen o definici komplexní exponenciály. Snadno si za cvičení odvodíš vztahy

$$2i\sin(x) = e^{ix} - e^{-ix}, \quad 2\cos(x) = e^{ix} + e^{-ix}, \quad i\,\mathrm{tg}(x) = \frac{e^{ix} - e^{-ix}}{e^{ix} + e^{-ix}}.$$

Komplexní logaritmus

Podívejme se na komplexní logaritmus. Logaritmus je inverzní funkce k exponenciále. Budou nás tedy zajímat řešení rovnice

$$a = e^x,$$

pro $a \in \mathbb{C}$ nenulové. Snadno nahlédneš, že tato rovnice má nekonečně mnoho řešení, neboť je-li x řešení, tak i $x + 2\pi i$ je řešení. Opravdu, zapíšeme-li $x = x_1 + ix_2$, pak naše rovnice má tvar

$$a = e^{x_1}(\cos x_2 + i \sin x_2),$$

a uvidíme, že řešení jsou právě všechna čísla tvaru $x + 2k\pi i$ pro k celé a x nějaké jedno řešení. A to díky tomu, že reálná exponenciála je prostá a funkce sin a cos jsou právě 2π-periodické.

Nyní můžeme zavést nejednoznačnou[12] funkci ln, která komplexnímu číslu a přiřadí všechny jeho možné logaritmy, tj.

$$\ln(a) = \{x : e^x = a\}.$$

Budeme-li trochu opatrnější, podaří se nám zadefinovat i jednoznačný komplexní logaritmus. Prozkoumejme trochu podrobněji exponenciální funkci. Označme $f(z) = e^z$. Pak $f\colon \mathbb{C} \to \mathbb{C} - \{0\}$, ovšem abychom dostali jednoznačnost ve smyslu, že pro libovolné $z_1 \neq z_2 \in \mathbb{C}$ platí $f(z_1) \neq f(z_2)$, budeme muset omezit definiční obor f na „pás“[13]

$$D = \{z \in \mathbb{C} : -\pi \leq \Im(z) < \pi\}.$$

Máme tedy novou funkci $g\colon D \to \mathbb{C} - \{0\}$ takovou, že $f = g$ na D.

Nyní už je g prostá, neboť $r_1 e^{i\phi_1} = r_2 e^{i\phi_2}$ implikuje $r_1 = r_2$ a $\phi_1 = \phi_2$, a proto se můžeme bavit o inverzní funkci k g. Označme tedy hledanou inverzní funkci $\mathrm{Ln} : \mathbb{C} - \{0\} \to D$ a hovořme o ní jako o *komplexní logaritmické funkci*, zkráceně logaritmu.

Jak ale bude vypadat reálná a imaginární část g? Označíme-li si je hodnotami x_1 a x_2, pak z rovnosti $\mathrm{Ln}(z) = x_1 + ix_2$ plyne

$$z = e^{x_1 + ix_2} = e^{x_1}(\cos x_2 + i \sin x_2),$$

[12] Nejednoznačné komplexní funkce jsou docela zajímavé, dokonce kolem nich existuje i nějaká docela složitá teorie.

[13] Tento pás jsme si mohli zvolit, někteří autoři raději volí pás ohraničen hodnotami 0 a 2π.

což podle zápisu komplexního čísla v goniometrickém tvaru dává $|z| = e^{x_1}$ a $\arg(z) = x_2$. Tím máme jednoznačně dané hodnoty x_1 a x_2 a můžeme tedy pro $z = r(\cos\phi + i\sin\phi)$ psát

$$\mathrm{Ln}(z) = \log|z| + i\arg(z),$$

kde $\log(t)$ značí reálný (přirozený) logaritmus čísla t.

Vidíme tedy, že komplexní logaritmus je jednoznačný, pokud bereme jeho imaginární část modulo 2π.

Ještě nezapomeňme na jednu velmi důležitou poznámku. Pro počítání s komplexním logaritmem neplatí stejné pravidla jako pro reálné logaritmy. Konkrétněji $\mathrm{Ln}(t^s) \neq s\,\mathrm{Ln}(t)$, protože

$$2\,\mathrm{Ln}(i) = 2\frac{\pi i}{2} = \pi i \neq -\pi i = \mathrm{Ln}(-1) = \mathrm{Ln}(i^2).$$

Tyto rovnosti budou platit jen modulo $2\pi i$, tj. $\mathrm{Ln}(ab) = \mathrm{Ln}(a) + \mathrm{Ln}(b) + 2\pi i k$ pro nějaké k celé.

Cvičení. Spočtěte následující komplexní logaritmy: $\mathrm{Ln}(-2), \mathrm{Ln}(i), \mathrm{Ln}(1+i)$.

Umocňování a odmocňování komplexních čísel

V této kapitolce si ukážeme, jak by šlo pěkně definovat umocňování na komplexní číslo, tedy naučíme se počítat takové hodnoty jako i^i. Využijeme toho také pro snadné umocňování a odmocňování.

Zatím umíme umocňovat na libovolné komplexní číslo jen konstantu e. Jak toho ale využít pro umocnění nějakého jiného čísla? Stačí si uvědomit, že

$$b = e^{\ln b}.$$

V tomto vztahu používáme nejednoznačný komplexní logaritmus. Chceme tím vyjádřit to, že ať si vezmeme libovolné číslo z množiny $\ln b$, tak bude výše uvedený vztah splněn.

Dobře, můžeme ho tedy použít k počítání b^a? Co kdyby

$$b^a = \left(e^{\ln b}\right)^a = e^{a\ln b}?$$

Ve skutečnosti takto definujeme umocňování libovolného čísla, tedy vztah $b^a = e^{a\ln b}$ pro nás bude vlastně definice.

Budeme-li chtít spočítat třeba $b^{1/2}$, budeme počítat $e^{(\ln b)/2}$, tj. je-li $b = re^{i\phi}$, pak dostaneme

$$\begin{aligned}\ln b &= \{\ln r + i(\phi + 2\pi k) : k \in \mathbb{Z}\},\\ \frac{\ln b}{2} &= \left\{\frac{\ln r}{2} + i\left(\frac{\phi}{2} + \pi k\right) : k \in \mathbb{Z}\right\},\end{aligned}$$

a nakonec

$$b^{1/2} = \{\sqrt{r}e^{i\phi/2}, \sqrt{r}e^{i(\phi/2+\pi)}\} = \pm\sqrt{r}e^{i\phi/2}.$$

Vidíš, že jsme dostali obě druhé odmocniny z b. Podobně můžeme spočítat i třetí, čtvrté, nebo π-té odmocniny. Také se tímto dobře počítají mocniny komplexních čísel, ale to nejde o nic jiného než o převlečenou Moivreovu větu.

Dobře, ale jak to bude vypadat u počítání takových kvantit jako i^i? Ukážeme to na konkrétním případě, z něho si snadno odvodíš, jak to bude vypadat obecně. Spočtěme tedy hodnoty $i^i = e^{i \ln i}$. Prvně $\ln i = \{\pi i/2 + 2k\pi i : k \in \mathbb{Z}\}$, tedy $i \ln i = \{-\pi/2 - 2k\pi : k \in \mathbb{Z}\}$. Tedy máme řešení

$$i^i = e^{-\pi/2 - 2k\pi}, \quad k \in \mathbb{Z}.$$

Všimni si, že nám vyšlo nekonečně mnoho hodnot. Podobně to dopadne třeba i pro 4^i nebo pro obecný případ s nenulovou imaginární částí exponentu.

Cvičení. Spočti 4^i, $\sqrt[7]{-i}$ a $2^{\sqrt{i}}$.

Zatím jsme pracovali s nejednoznačným logaritmem, totéž můžeme dělat i s jednoznačným logaritmem, čímž dostaneme jednoznačné hodnoty b^a, ale pokud by si někdo zvolil na začátku jiný pás než my, tak mu teď budou vycházet jiné hodnoty. Pro nás by tedy například platilo $\sqrt{i} = (\sqrt{2}/2 + i\sqrt{2}/2)$ a $i^i = e^{-\pi/2}$.

Jak sčítat komplexně

Goniometrický tvar komplexních čísel lze dobře využít i pro sčítání některých řad. Jeden z typických příkladů je následující:

Příklad. Je-li n přirozené a α reálné, spočtěte součet

$$\sin\alpha + \sin 2\alpha + \cdots + \sin n\alpha.$$

Řešení. Označme hledaný součet S. Použijeme goniometrický tvar komplexních čísel, asi nás bude zajímat číslo $z = \cos\alpha + i\sin\alpha$. Tedy náš součet bude imaginární část nějakého součtu komplexních čísel. Doplníme ke každému sinu ještě kosinus, uvažujme tedy součet

$$T = 1 + (\cos\alpha + i\sin\alpha) + (\cos 2\alpha + i\sin 2\alpha) + \cdots + (\cos n\alpha + i\sin n\alpha).$$

Všimni si, že $S = \Im(T)$. Dále si všimneme, že členy tohoto součtu jsou právě mocniny čísla z z Moivreovy věty. Dostáváme

$$T = 1 + z + z^2 + \cdots + z^n.$$

Známým trikem ale umíme T krásně sečíst. Platí totiž $1 + zT = T + z^{n+1}$, takže

$$\begin{aligned} T &= \frac{z^{n+1} - 1}{z - 1} = \frac{\cos(n+1)\alpha + i\sin(n+1)\alpha - 1}{\cos\alpha + i\sin\alpha - 1} \\ &= \frac{(\cos(n+1)\alpha + i\sin(n+1)\alpha - 1)(\cos\alpha - i\sin\alpha - 1)}{2(1 - \cos\alpha)}. \end{aligned}$$

Dále nás bude zajímat jen imaginární část

$$\begin{aligned} S = \Im(T) &= \frac{\sin((n+1)\alpha)(\cos\alpha - 1) - \sin\alpha(\cos(n+1)\alpha - 1)}{2(1 - \cos\alpha)} \\ &= \frac{\sin n\alpha - \sin(n+1)\alpha + \sin\alpha}{2(1 - \cos\alpha)} = \frac{2\cos\frac{n\alpha}{2}\sin\frac{n\alpha}{2} - 2\cos\frac{(n+2)\alpha}{2}\sin\frac{n\alpha}{2}}{4\sin^2\frac{\alpha}{2}} \\ &= \left(\cos\frac{n\alpha}{2} - \cos\frac{(n+2)\alpha}{2}\right)\frac{\sin\frac{n\alpha}{2}}{2\sin^2\frac{\alpha}{2}} = \sin\frac{(n+1)\alpha}{2}\sin\frac{n\alpha}{2} \Big/ \sin\frac{\alpha}{2}. \end{aligned}$$

□

Komplexní kombinatorika

Určitě jsi někdy počítal součet všech sudých kombinačních čísel[14]

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \cdots = 2^{n-1}.$$

V rychlosti ukážeme, jak se to dělá, abychom mohli spočítat trošku složitější součty. Tento součet se dokazuje jednoduše tak, že sečteme dvě binomické věty.

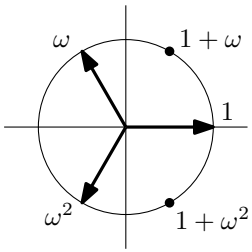
$$\begin{aligned}
(1+1)^n &= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \dots \\
(1-1)^n &= \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \dots \\
2^n + 0^n &= 2\binom{n}{0} + 0\binom{n}{1} + 2\binom{n}{2} + 0\binom{n}{3} + \dots
\end{aligned}$$

Zbyde nám jen poslední rovnost podělit dvěma a dostaneme, co jsme chtěli. Z toho se pak odvodí i součet lichých kombinačních čísel. □

Ale co bychom dělali, kdybychom chtěli sečíst třeba každé třetí kombinační číslo?

$$\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \dots$$

Otázka zní, co bylo zajímavé na číslech 1 a -1 pro předchozí případ. Jestli hádáš, že to, že jsou to druhé odmocniny z jedné, tak máš pravdu. Pro tento součet třetích kombinačních čísel tedy budeme potřebovat třetí odmocniny z jedné. To jsou čísla 1, $\omega = e^{2\pi i/3}$ a $\omega^2 = e^{-2\pi i/3}$, přitom $\omega^2 + \omega + 1 = 0$, což si snadno představíš, pokud si tato čísla nakreslíš do Gaussovy roviny.



Platí tedy

$$\begin{aligned}
(1+1)^n &= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \dots, \\
(1+\omega)^n &= \binom{n}{0} + \omega\binom{n}{1} + \omega^2\binom{n}{2} + \binom{n}{3} + \omega\binom{n}{4} + \dots, \\
(1+\omega^2)^n &= \binom{n}{0} + \omega^2\binom{n}{1} + \omega\binom{n}{2} + \binom{n}{3} + \omega^2\binom{n}{4} + \dots.
\end{aligned}$$

[14] V této kapitole budeme některé součty ukončovat třemi tečkami, přestože jsou všechny konečné. Je to z prostého důvodu, že se nebudeme dlouze zamýšlet, který člen je poslední. Vše by však mělo být intuitivně jasné.

Nyní nám zbývá už jen tyto rovnosti sečíst, dostaneme

$$2^n + (1+\omega)^n + (1+\omega^2)^n = 3\binom{n}{0} + 3\binom{n}{3} + 3\binom{n}{6} + \dots.$$

Přitom ještě umíme elegantně spočítat $(1+\omega)^n$, protože $1+\omega$ je právě $e^{\pi i/3}$ a podobně $1+\omega^2$ je $e^{-\pi i/3}$. Z Moivreovy věty tedy máme

$$\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \dots = \frac{2^n}{3} + \frac{2}{3}\cos\frac{n\pi}{3}.$$

Všimni si, že není na první pohled vidět, že pravá strana je vůbec celočíselná. Na druhý pohled je to už trochu zřetelnější, neboť $\cos\frac{n\pi}{3}$ je vždy ± 1 nebo $\pm\frac{1}{2}$, tedy alespoň čitatel je celočíselný. To, že je vždy dělitelný třemi, si rozmysli sám. □

Cvičení. Spočtěte součty:

(i) $\binom{n}{1} + \binom{n}{4} + \binom{n}{7} + \binom{n}{10} + \dots$ (ii) $\binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \dots$

Rozklady mnohočlenů

V předchozí kapitole ses naučil, jak najít kořeny libovolného kvadratického mnohočlenu s komplexními koeficienty. Takže víme, že každý takový mnohočlen se rozkládá na kořenové činitele. Ale jak je to s mnohočleny vyšších stupňů? O tom mluví základní věta algebry, kterou není úplně snadné dokázat, ovšem všechny známé důkazy jsou zajímavé tím, že docela jednoduše vyplývají z nějaké složité teorie (například jeden z nich používá komplexní analýzu, teorii kolem vlastností komplexních funkcí, které mají derivaci).

Věta. (Základní věta algebry) *Každý mnohočlen s koeficienty v komplexních číslech má kořen.*

Důsledek. *Je-li $f(x) \in \mathbb{C}[x]$ mnohočlen s komplexními koeficienty stupně n, pak $f(x)$ má právě n kořenů, počítáme-li je s násobností, tj. existují $x_1, x_2, \dots, x_n$, že*

$$f(x) = a(x-x_1)(x-x_2)\cdots(x-x_n).$$

Důkaz. Budeme dokazovat matematickou indukcí podle stupně mnohočlenu $f(x)$. Pro konstantní (nenulové) mnohočleny tvrzení triviálně platí. Předpokládejme nyní, že platí pro mnohočleny stupně n a buď $f(x)$ stupně $n+1$.

Dle základní věty algebry má $f(x)$ kořen x_0, pak ale $f(x) = (x-x_0)g(x)$ pro nějaké $g(x) \in \mathbb{C}[x]$. Přitom $g(x)$ má stupeň n, tedy pro něj můžeme použít indukční předpoklad a víme, že se rozkládá na lineární faktory – nechť

$$g(x) = a(x-x_1)(x-x_2)\cdots(x-x_n).$$

Pak ale

$$f(x) = a(x-x_0)(x-x_1)\cdots(x-x_n).$$ □

Základní věta algebry má také dobré důsledky v reálných číslech, konkrétněji zjednodušuje práci s reálnými polynomy. K tomu se nám bude hodit jednoduchý náhled. Máme-li $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$ mnohočlen s reálnými koeficienty a z jeho komplexní kořen, pak $\overline{z}$

je určitě kořenem polynomu $\overline{f}(x) = \overline{a_n}x^n + \cdots + \overline{a_0}$. Přitom ale koeficienty a_i jsou reálné, takže s nimi komplexní sdružení nic neudělají. Dokázali jsme tedy tvrzení:

Tvrzení. *Je-li $f(x) \in \mathbb{R}[x]$ a $z \in \mathbb{C}$ jeho komplexní kořen, pak i $\overline{z}$ je kořen $f(x)$.*

Podívejme se ještě na kvadratický trojčlen $f(x)$, jehož kořeny jsou z a $\overline{z}$. Ten z Viétových vztahů má tvar

$$f(x) = x^2 - (z + \overline{z})x + z\overline{z} = x^2 - 2\Re(z)x + |z|^2,$$

tedy má reálné koeficienty. Navíc pokud z má nenulovou imaginární část, tak tento trojčlen je nerozložitelný. Totiž

$$x^2 + 2\Re(z)x + |z|^2 = (x^2 + \Re(z))^2 + \Im(z)^2,$$

odkud už lze vidět, že se nerozkládá. Diskriminant této rovnice je $-4\Im(z)^2$. Nyní už snadno odvodíme následující variantu základní věty algebry v reálných číslech.

Věta. *Je-li $f(x) \in \mathbb{R}[x]$ polynom s reálnými koeficienty. Pak $f(x)$ se v $\mathbb{R}$ rozkládá na lineární a nerozložitelné kvadratické mnohočleny.*

Důkaz. Nejdříve rozložíme $f(x)$ na lineární činitele v $\mathbb{C}$ pomocí základní věty algebry. Pak rozdělíme kořeny do dvou množin, na reálné a ty ostatní, s nenulovou imaginární částí. Ty ryze komplexní se nám díky předchozímu tvrzení popárují. Tedy máme rozklad

$$f(x) = a(x - a_1)\cdots(x - a_k)\cdot(x - z_1)(x - \overline{z}_1)\cdots(x - z_l)(x - \overline{z}_l),$$

kde a_i jsou reálné a z_i jsou ryze komplexní. Přitom a je vedoucí koeficient $f(x)$, tedy je reálný. Navíc součiny $(x - z_i)(x - \overline{z}_i)$ mají reálné koeficienty z předchozí poznámky a přitom jsou nerozložitelné v $\mathbb{R}$, tedy tímto opravdu dostáváme kýžený rozklad. $\square$

A k čemu to je? Můžeme tímto způsobem rozkládat reálné mnohočleny, které bychom jinak uměli rozložit pouze v komplexních číslech. Podívej se na následující dva příklady.

Příklad. Rozložte mnohočlen $x^4 + 4$ v reálných číslech.

Řešení. Rozložme zadaný mnohočlen nejdříve v komplexních číslech. Jeho kořeny jsou právě všechny čtvrté odmocniny z -4. Tj. čísla

$$z_0 = \sqrt{2}e^{\frac{\pi i}{4}}, z_1 = \sqrt{2}e^{\frac{3\pi i}{4}}, z_2 = \sqrt{2}e^{\frac{-3\pi i}{4}}, z_3 = \sqrt{2}e^{\frac{-\pi i}{4}}.$$

Nyní je popárujme podle komplexního sdružení, tedy z_0 s z_3 a z_1 s z_2. Spočteme trojčleny, které mají tyto dvojice kořenů:

$$x^2 - (z_0 + z_3)x + z_0z_3 = x^2 - 2x + 2,$$
$$x^2 - (z_1 + z_2)x + z_1z_2 = x^2 + 2x + 2.$$

Nakonec jsme tedy odvodili krásný rozklad $x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$, který je dokonce nad celými čísly.

Příklad. Rozložte mnohočlen $x^8 - 1$ v celých číslech.

Řešení. Obdobně jako v předchozím případě, ho nejdříve rozložíme v komplexních číslech, jeho kořeny jsou osmé odmocniny z jedné, tj. čísla

$$e^{\frac{\pi}{4}i}, i, e^{\frac{3\pi}{4}i}, -1, e^{-\frac{3\pi}{4}i}, -i, e^{-\frac{\pi}{4}i}, 1.$$

Opět je spárujeme a spočteme kvadratické mnohočleny kromě ± 1, které nám zůstanou na ocet a dají v rozkladu lineární faktory $(x-1)$ a $(x+1)$. Hledané kvadratické mnohočleny pak jsou

$$x^2+\sqrt{2}x+1,\ x^2+1,\ x^2-\sqrt{2}x+1.$$

Odtud je vidět, že nejlepší rozklad, který můžeme dostat v celých číslech, je

$$x^8-1=(x^4+1)(x^2+1)(x+1)(x-1),$$

kde člen x^4+1 je součinem kvadratických činitelů $x^2\pm\sqrt{2}x+1$, tedy se v celých číslech nerozkládá, protože takový rozklad by musel být i rozkladem v reálných číslech.

Seriál II. – Komplexní geometrie

V druhé části seriálu si povíme něco o geometrii v komplexních číslech i o komplexních číslech v geometrii. Souvislost komplexních čísel s planimetrií přichází přirozeně z představy Gaussovy roviny. Každému komplexnímu číslu je tak přiřazen právě jeden bod roviny a naopak. Některé geometrické pojmy pak snadno souvisí s pojmy komplexními. My si tady tyto souvislosti vyložíme a naučíme se je využívat při řešení geometrických úloh. Nezapomeň, že někdy lze naopak použít geometrii při řešení úloh s komplexními čísly.

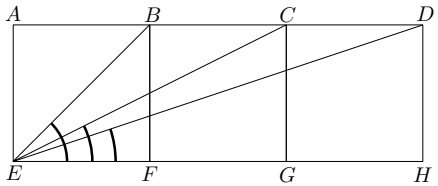
Naším cílem nebude spolehlivě vyřešit jakoukoli geometrickou úlohu, ale především si ukážeme úlohy, které se pomocí komplexních čísel řeší jednodušeji a u kterých již od začátku řešení víme, že tímto způsobem úlohu vyřešíme, což u ryze geometrického přístupu prostě nejde. Je však mnoho geometrických úloh, které pomocí komplexních čísel řešit nedoporučujeme. Například pokud se v úloze vyskytují dvě nebo více kružnic, pak většinou komplexní čísla efektivně použít nepůjdou. Naopak u mnohých úloh se použití přímo nabízí, třeba skoro libovolná úloha s rovnostrannými trojúhelníky se může zjednodušit.

Tento text by tedy měl čtenáři přinést především jiný úhel pohledu na geometrické úlohy, aby věnoval třeba jen pár vteřin myšlence, zdali tato úloha nejde vyřešit za pomoci komplexních čísel. I při tak krátké době je totiž možné zjistit, jestli je zadaná úloha vhodná na to, abychom ji vyřešili pomocí komplexních čísel, neboť jejich využití je spíš technicky, ne myšlenkově náročné.

Motivace

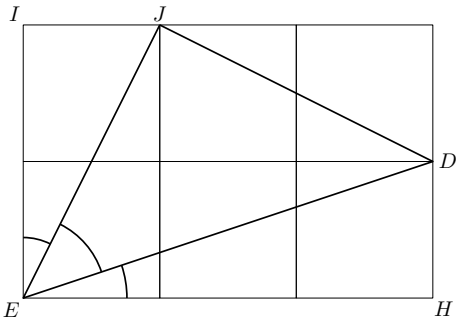
Podívejme se nejdříve na jeden jednoduchý příklad, jak lze použít komplexní čísla v geometrii. U tohoto příkladu pro srovnání uvádíme i syntetické (geometrické) řešení.

Příklad. (Motivační) Máme vedle sebe tři čtverce $ABFE$, $BCGF$ a $CDHG$ jako na obrázku.



Spočtěte součet úhlů $|\sphericalangle BEH| + |\sphericalangle CEH| + |\sphericalangle DEH|$.

Syntetické řešení. Uvažme následující obrázek složený ze čtverců.

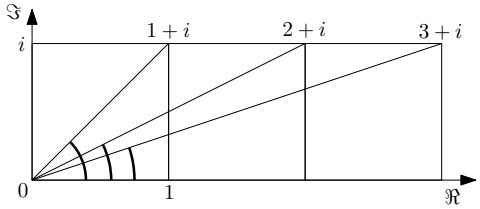


Pak zřejmě $|\sphericalangle JEI| = |\sphericalangle CEH|$, stejně tak úhel DEH je dokonce totožný s původním úhlem DEH. Dále snadno nahlédneme, že $\triangle DEJ$ je podobný s $\triangle BEF$ neboť jsou oba rovnoramenné pravoúhlé s pravým úhlem u vrcholu J, respektive F.

Platí tedy, že hledaný součet je součtem vyznačených úhlů u vrcholu E.

$$|\sphericalangle BEH| + |\sphericalangle CEH| + |\sphericalangle DEH| = |\sphericalangle JED| + |\sphericalangle IEJ| + |\sphericalangle DEH| = \frac{\pi}{2}. \qquad \square$$

Komplexní řešení. Položme si situaci do komplexní roviny, tak aby $E = 0$, $F = 1$ a $A = i$.



Pak můžeme hledaný součet úhlů spočítat jako argument součinu čísel $1+i$, $2+i$ a $3+i$, neboť při násobení se argumenty sčítají a zadané tři úhly jsou právě argumenty těchto tří čísel. Hledaný součet je tedy

$$\arg(1+i)(2+i)(3+i) = \arg(1+3i)(3+i) = \arg i(3-i)(3+i) = \arg 10i = \frac{\pi}{2}. \qquad \square$$

Všimni si, že ani jedno z těchto řešení nijak nevyčnívá, obě jsou zhruba stejně dlouhá, zhruba stejně elegantní a také zhruba stejně triková, ačkoliv v druhém je největší trik v tom, použít komplexní čísla. Tak to většinou bývá, komplexní čísla ti nemohou výrazně zjednodušit cestu, ale mohou ti pomoci docela elegantní cestu najít.

Podívejme se nyní trochu hlouběji na teorii, kterou budeme používat.

Tři body na přímce

Nejprve si ujednoťme značení. Pokud budeme psát bod $Z(z)$, bude to znamenat, že máme v rovině bod Z, kterému přísluší komplexní číslo z. Jak bylo řečeno v první části seriálu, každému komplexnímu číslu z odpovídá bod v Gaussově rovině, který má souřadnice $[\Re(z), \Im(z)]$. Pokud zapíšeme $z = a + bi$, pak bod Z má souřadnice $[a, b]$.

Pokusme se teď najít několik způsobů, jak říci, že tři body roviny, označme je $A(a)$, $B(b)$ a $Z(z)$ leží na přímce (častěji budeme říkat, že jsou kolineární).

Jednoduše to půjde z trojúhelníkové nerovnosti, ve které musí nastat rovnost. Body A, Z, B leží na přímce v daném pořadí, právě když platí

$$|a - b| = |a - z| + |b - z|.$$

Druhá možnost, jak zapsat, že bod Z leží na přímce AB je konvexní kombinace. Tj.

$$Z \in AB \quad \Leftrightarrow \quad z = ua + (1-u)b,\ u \in \mathbb{R}.$$

Pokud bychom chtěli, aby bod Z ležel na úsečce AB, stačí se omezit pouze na $u \in [0, 1]$. Všimněme si, že jak se parametr u pohybuje od 0 k 1, tak bod z se pohybuje od b k a. Když povolíme hodnoty u mimo interval $[0, 1]$, pak bod Z leží na přímce AB.

Třetí a poslední možnost, kterou si zde uvedeme, je vektorový zápis. Ten nám říká, že $Z \in AB$ právě tehdy, když vektory $a - z$ a $a - b$ jsou až na násobek stejné, neboli

$$Z \in AB \quad \Leftrightarrow \quad \frac{a-z}{a-b} = k \ \in \mathbb{R}.$$

Je-li navíc číslo k z intervalu $(0, 1)$, pak jsou tyto body v pořadí A, Z, B, neboli Z leží na úsečce AB.

Z konvexního zápisu je dokonce vidět vzorec pro bod Z na úsečce AB, který ji dělí v poměru $|AZ| : |ZB| = m : n$. Musíme akorát vhodně zvolit hodnotu t. Vztah pro bod Z je tedy

$$z = \frac{n}{m+n}a + \frac{m}{m+n}b.$$

Uveďme si jedno zobecnění. Pokud bychom chtěli popsat množinu bodů Z, které leží uvnitř trojúhelníku daného vrcholy $A(a)$, $B(b)$, $C(c)$, pak použijeme konvexní kombinaci dvakrát za sebou. Nejprve zvolíme bod $D(d)$ na úsečce AB a pak zvolíme bod Z na úsečce DC. Celkem tedy máme pro $s, t \in [0, 1]$ vztah pro z

$$z = sc + (1-s)d = sc + (1-s)(ta + (1-t)b) = sc + t(1-s)a + (1-s)(1-t)b,$$

což lze jednodušeji napsat jako

$$z = ua + vb + wc, \quad u, v, w \in [0, 1], \ u + v + w = 1.$$

Příklad 1. Mějme trojúhelník ABC. V závislosti na vrcholech najděte polohu těžiště $T(t)$.

Řešení. Označme $D(d)$ střed strany AB, pak $d = \frac{a+b}{2}$. Jelikož těžiště T dělí CD v poměru $2 : 1$, máme

$$t = \frac{1}{3}c + \frac{2}{3}d = \frac{1}{3}(a + b + c).$$

Příklad 2. V pravidelném šestiúhelníku $ABCDEF$ jsou na diagonálách AC a CE dány body M a N tak, že

$$\frac{|AM|}{|AC|} = \frac{|CN|}{|CE|} = \ r \in \mathbb{R}.$$

Určete hodnotu r, pokud víte, že body B, M, N jsou kolineární. (IMO 1982 – 5. příklad)

Řešení. Uvažujme komplexní rovinu s počátkem ve středu šestiúhelníku $ABCDEF$, který je natočen tak, že body A, B, C, D, E a F mají souřadnice 1, ϵ, ϵ^2, ϵ^3, ϵ^4 a ϵ^5, kde

$$\epsilon = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

Z definice hodnoty r máme

$$m = rc + (1-r)a = r\epsilon^2 + (1-r) = r(\epsilon^2 - 1) + 1,$$
$$n = re + (1-r)c = r\epsilon^4 + (1-r)\epsilon^2 = r(\epsilon^4 - \epsilon^2) + \epsilon^2,$$

Body B, M, N jsou kolineární právě tehdy, když podíl

$$\frac{m-b}{n-b} = \frac{m-\epsilon}{n-\epsilon} \in \mathbb{R}.$$

Tento podíl je však závislý pouze na r. Stačí tedy zjistit jeho imaginární část a položit ji rovnou nule. Úprava tohoto podílu je jen technické cvičení na několik řádků, uvedeme pouze výsledek.

$$\Im\left(\frac{m-\epsilon}{n-\epsilon}\right) = \Im\left(\frac{r(\epsilon^2-1)+1-\epsilon}{r(\epsilon^4-\epsilon^2)+\epsilon^2-\epsilon}\right) = \cdots = -\frac{\sqrt{3}(3r^2-1)}{2(3r^2+1)}.$$

Jelikož $r \in [0,1]$, jediná reálná hodnota r, pro kterou leží body B, M, N na přímce, je $r = \frac{\sqrt{3}}{3}$.

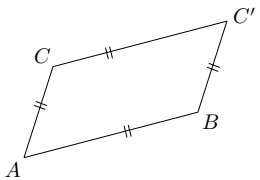
Výhoda komplexního přístupu ke geometrickým úlohám je ta, že už od začátku je vidět, že se dá úloha tímto způsobem vyřešit. U předchozí úlohy jsme už od začátku věděli, že dostaneme podíl komplexních čísel závislých na r a půjde jen o to spočítat jeho imaginární část, což je docela jednoduché. Otázkou při rozhodování, zda chceme zadanou úlohu řešit pomocí komplexních čísel, je, zdali tento způsob bude technicky náročný, nebo ne. Odpověď se může u každého z nás lišit, proto necháváme na čtenáři, nakolik bude výše uvedené metody používat. V každém případě ale doporučujeme jejich použití zvážit.

Geometrická zobrazení v Gaussově rovině

V této kapitole se budeme věnovat geometrickým zobrazením v rovině. Určitě většinu z nich znáš a mnohé z nich umíš elegantně použít v úlohách. Nás bude zajímat, jak se pomocí komplexních čísel dají snadněji počítat obrazy bodů v různých zobrazeních. Některá zobrazení, jako například stejnolehlost a otočení, jsou v komplexních číslech velmi přirozená, jiná, jako třeba osová souměrnost, už tolik ne. Přesto si uvedeme vzorce pro všechna základní známá zobrazení.

Posunutí

Nejjednodušší zobrazení, které nás bude zajímat, je posunutí, konkrétněji posunutí o vektor (orientovanou úsečku) AB. Pro zopakování, v geometrii je to zobrazení takové, že bod C zobrazí na bod C' tak, že $ABC'C$ je rovnoběžník (popř. zdegenerovaný rovnoběžník, obecně tedy $|AB| = |CC'|$, $|AC| = |BC'|$ a přitom $CC' \parallel AB$).



V Gaussově rovině toto zobrazení vypadá velmi jednoduše. Pokud označíme a, b, c a c' odpovídající komplexní čísla bodům A, B, C a C', tak

$$c' = c + (b - a).$$

Tedy posunutí je dáno jediným komplexním číslem $b-a$. Obecněji *posunutí o číslo* c je zobrazení $t_c\colon \mathbb{C} \to \mathbb{C}$, které je dáno předpisem

$$t_c(x) = x + c.$$

Podíváme-li se na to z druhé strany, uvědomíme si, že jsme právě popsali, jak geometricky vypadá sčítání komplexních čísel. To se nám bude hodit při popisu dalších geometrických zobrazení.

Podívejme se třeba rovnou na stejnolehlost. Nejdříve nás bude zajímat stejnolehlost se středem v počátku a pak pomocí ní popíšeme všechny ostatní stejnolehlosti tak, že nejprve posuneme střed stejnolehlosti do počátku, provedeme stejnolehlost a pak posunutí vrátíme zpátky. Tedy je-li $h_S\colon \mathbb{C} \to \mathbb{C}$ stejnolehlost se středem $S(s)$ a nějakým daným koeficientem, h_0 stejnolehlost se stejným koeficientem, ale se středem v počátku, pak

$$h_S(x) = h_0(x - s) + s.$$

Stejnolehlost a otočení

Pro zopakování, *stejnolehlost* v rovině je zobrazení $h_{S,k}$, kde S je střed a $k \in \mathbb{R}$ koeficient stejnolehlosti, které zobrazí bod X na bod X' takový, že body S, X a X' leží na přímce a $|k| \cdot |SX| = |SX'|$. Znaménko koeficientu k se na situaci promítne tak, že pokud $k > 0$, leží X' na polopřímce SX, jinak leží na polopřímce opačné. Stejnolehlost je podobné zobrazení (tím myslíme, že zobrazí každý trojúhelník na jemu podobný, a dokonce koeficient podobnosti bude k).

A jak tedy vypadá v Gaussově rovině stejnolehlost se středem v počátku (koeficient máme stále k)? Jednoduše, jako násobení reálným číslem k. Všimni si totiž, že zobrazení

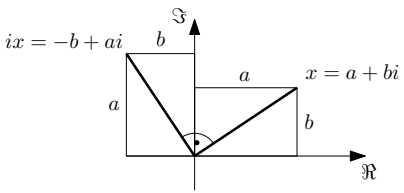
$$h_{0,k}(x) = kx$$

opravdu splňuje naše požadavky na stejnolehlost, neboť body 0, x a kx leží na přímce, $|kx| = |k| \cdot |x|$ a bod kx leží na správné straně od počátku.

Pomocí výše popsaného obratu si napíšeme vzorec pro stejnolehlost $h_{S,k}$ se středem S a koeficientem k. Doporučujeme ti ale, aby sis, budeš-li chtít v úloze použít jedinou stejnolehlost, zvolil souřadnice tak, abys měl střed v počátku, zjednoduší ti to výpočty.

$$h_{S,k}(x) = k(x - s) + s = kx + (1 - k)s$$

Tímto jsme zjistili, jak v komplexní rovině vypadá násobení reálným číslem – jde o stejnolehlost se středem v počátku. Jistě tě napadá přirozená otázka, jak to bude vypadat při násobení libovolným komplexním číslem. Začněme s násobením imaginární jednotkou i. Je-li $x = a + bi$, pak $ix = -b + ai$. Když si tato dvě čísla nakreslíme do Gaussovy roviny, můžeme si všimnout, že jejich spojnice s počátkem jsou na sebe kolmé, neboť celý obdélník, ve kterém se x schovává, je otočený kolem počátku o $90°$.[15]



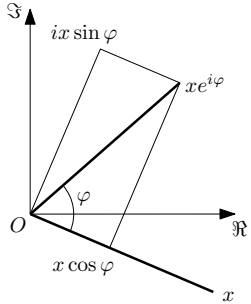
Dále se podíváme na násobení komplexní jednotkou, tj. číslem z, že $|z| = 1$. Budeme ho zapisovat v exponenciálním tvaru $z = e^{i\phi}$.

[15] Teď bys měl říct, že toto není korektní důkaz, protože jsme tvrzení dokázali jen pro x v prvním kvadrantu. Ve všech ostatních se to ale dokáže podobně.

Uvažme tedy zobrazení $r_\phi\colon \mathbb{C} \to \mathbb{C}$, které je dané předpisem

$$r_\phi(x) = xe^{i\phi} = x(\cos\phi + i\sin\phi) = x\cos\phi + ix\sin\phi.$$

Násobení číslem i i reálnými čísly $\cos\phi$ a $\sin\phi$ si už umíme geometricky představit, nakresleme si obrázek.



Všimni si, že $xe^{i\phi}$ je úhlopříčkou v obdélníku se stranami délky $|x\cos\phi|$ a $|x\sin\phi|$, tedy podle Pythagorovy věty $|xe^{i\phi}|^2 = |x|^2\cos^2\phi + |x|^2\sin^2\phi = |x|^2$, proto $xe^{i\phi}$ je stejně dlouhé jako x. Navíc z definice funkcí sin a cos můžeme vidět, že svírá s x úhel právě ϕ. Tudíž násobení číslem $e^{i\phi}$ není nic jiného než otočení o úhel ϕ.

Ještě jednou zopakujeme vzoreček pro rotaci a posuneme ho do bodu S. Rotace kolem bodu $S(s)$ o úhel ϕ má v komplexních číslech vzorec

$$r_{S,\phi}(x) = (x - s)e^{i\phi} + s.$$

A jak to tedy vypadá úplně obecně? Každé komplexní číslo si můžeme napsat v goniometrickém tvaru $z = r(\cos\phi + i\sin\phi)$. Násobení číslem z pak bude složení rotace o úhel ϕ a stejnolehlosti s koeficientem r, vše se středem v počátku.[16]

Všimni si zajímavé souvislosti: budeme-li chtít vědět, jak vypadá vzorec pro středovou souměrnost s_S se středem v $S(s)$, máme dvě možnosti náhledu. Středová souměrnost je stejnolehlost s koeficientem -1, čímž bychom dostali vzorec $s_S(x) = -(x-s)+s$, nebo je středová souměrnost také otočení o π, tj. $s_S(x) = (x-s)e^{i\pi} + s = -(x-s) + s$. V obou případech dostáváme stejný vzorec

$$s_S(x) = -(x - s) + s = 2s - x.$$

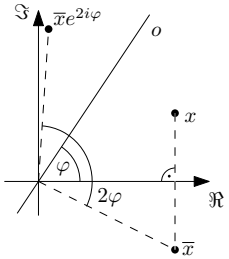
Osová souměrnost

Na vzoreček pro osovou souměrnost můžeme přijít docela snadno. Stačí se zamyslet nad komplexním sdružením. To totiž není nic jiného než osová souměrnost podle reálné osy. Zbývá nám pak zjistit, jak otočit a posunout osu tam, kam chceme. Osová souměrnost podle osy procházející počátkem a svírající s reálnou osou úhel ϕ bude tedy[17]

$$o_\phi(x) = \overline{xe^{-i\phi}} \cdot e^{i\phi} = \overline{x}e^{i\phi}e^{i\phi} = \overline{x}e^{2i\phi}.$$

[16] Mohli bychom o takových zobrazeních mluvit jako o „komplexní stejnolehlosti“, ale to jen pro představu. Ve skutečnosti se toto geometrické zobrazení jmenuje *spirální podobnost*.

[17] Zkus si rozmyslet, proč je tato osová souměrnost složením osové souměrnosti podle reálné osy a otočení o 2ϕ.



Budeme-li mít osu danou dvěma body $A(a)$ a $B(b)$, pak osovou souměrnost podle osy AB dostaneme tak, že nejdříve posuneme střed do bodu A a pak vynásobíme číslem $b-a$, které nám zařídí rotaci o požadovaný úhel.

$$o_{AB}(x) = \overline{(x-a)}\frac{b-a}{\overline{b-a}} + a$$

Tento vzorec však uvádíme jen pro ukázku. V konkrétních případech ti doporučujeme si ho odvodit zvlášť, nebo si raději posunout počátek do bodu na ose a použít předchozí úvahy.

Podívejme se nyní na několik příkladů, jak lze elegantně použít zobrazení v úlohách.

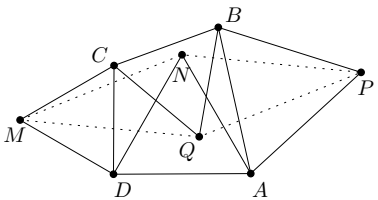
Příklad 3. Na stranách konvexního čtyřúhelníku $ABCD$ jsou připsány rovnostranné trojúhelníky tak, že na stranách BC a DA jsou tyto trojúhelníky připsány dovnitř, zatímco na stranách AB a CD jsou připsány ven. Označme vzniklé vrcholy nad stranami AB, BC, CD a DA postupně P, Q, M a N. Popište čtyřúhelník $PQMN$. (IMO 1982 – Shortlist)

Řešení. Označíme

$$\epsilon = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \frac{\sqrt{3}}{2} + \frac{1}{2}i,$$

což geometricky interpretuje otočení o 60°. Pak

$$p = b + \epsilon(a-b), \quad q = b + \epsilon(c-b),$$
$$m = d + \epsilon(c-d), \quad n = d + \epsilon(a-d).$$

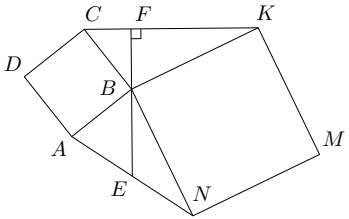


Celkem tedy máme

$$p + m = b + d + \epsilon(a - b + c - d) = q + n.$$

To je ale jen jinak řečeno, že $PQMN$ je rovnoběžník.

Příklad 4. Mějme dva čtverce $ABCD$ a $BNMK$, které se neprotínají a označme E střed AN a F patu kolmice z B v trojúhelníku CBK. Dokažte, že body F, B a E leží v přímce.



Řešení. Zaveďme si souřadný systém se středem v bodě $F(f)$ tak, aby body $C(c)$ a $K(k)$ ležely na reálné ose a bod $B(b)$ na imaginární ose. Máme tedy $c, k \in \mathbb{R}$ a $b = b_0 i$, kde $b_0 \in \mathbb{R}$. Rotace se středem v bodě B a úhlem $\pi/2$ nám převede bod C na bod A, proto

$$a = b + i(c - b) = b(1 - i) + ci.$$

Obdobně rotace se středem v B o $-\pi/2$ nám převede bod K na bod $N(n)$, tedy

$$n = b - i(k - b) = b(1 + i) - ki.$$

Bod $E(e)$ je střed AN, tudíž

$$e = \frac{a + n}{2} = \frac{b(1 - i) + ci + b(1 + i) - ki}{2} = b + \frac{c - k}{2} i$$

a stačí nám ověřit kolinearitu podle třetího kritéria, tedy vyšetřit podíl

$$\frac{e - b}{b - f} = \frac{b + \frac{c-k}{2} i - b}{b} = \frac{c - k}{2b} i = \frac{c - k}{2b_0} \in \mathbb{R}.$$

Proto body F, B a E jsou kolineární.

Úhly a kolmost

Obecně nás bude zajímat, jaký úhel svírají úsečky AB a CD v komplexní rovině, máme-li dány body $A(a)$, $B(b)$, $C(c)$ a $D(d)$. Předpokládejme, že $A \neq B$ a $C \neq D$. Je jasné, že si obě úsečky můžeme posunout do počátku. Budeme pak tedy zjišťovat, jaký úhel svírají vektory čísel $a - b$ a $c - d$. Uvědomíme-li si, jak se dělí čísla v goniometrickém tvaru, vidíme, že úhel, který nás zajímá, je vlastně $\arg \frac{a-b}{c-d}$.

Mohou nastat dva speciální případy. Pokud $(a-b)/(c-d) \in \mathbb{R}$, tedy $\Im\big((a-b)/(c-d)\big) = 0$, pak jsou obě úsečky rovnoběžné, neboť svírají orientovaný úhel 0 nebo π. Naopak také může nastat, že $(a - b)/(c - d)$ je reálným násobkem čísla i (ryze imaginární), tedy $\Re\big((a - b)/(c - d)\big) = 0$, pak úsečky AB a CD svírají pravý úhel.

Všimni si, že pokud zjišťujeme, zda jsou vektory (a, b) a (c, d) na sebe kolmé, zajímá nás jen reálná část podílu

$$\frac{a + ib}{c + id} = \frac{(a + ib)(c - id)}{c^2 + d^2}.$$

Především tedy jestli je nulová, nebo ne. Proto nás zajímá jen nulovost reálné části součinu

$$\Re\big((a+ib)(c-id)\big) = ac + bd.$$

To ti možná připomene tzv. *skalární součin*. Opravdu, dva vektory jsou na sebe kolmé, právě když $ac + bd = 0$.

Ukážeme si to na následující zajímavé větě, ve které po dlouhém zamyšlení můžeš nalézt právě větu o Thaletově kružnici.

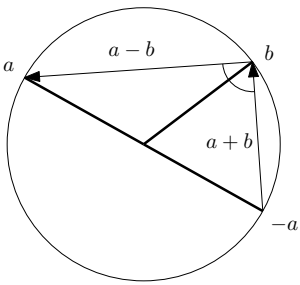
Věta. (Thaletova) *Nechť $a, b \in \mathbb{C}$, $a \neq \pm b$, jsou komplexní čísla na kružnici se středem v počátku. Pak pro nějaké $r \in \mathbb{R} \setminus \{0\}$ platí*

$$\frac{a+b}{a-b} = ir.$$

Důkaz. Zapišme si čísla a i b v goniometrickém tvaru, $a = p(\cos\alpha + i\sin\alpha)$ a $b = p(\cos\beta + i\sin\beta)$, a dosaďme do levé strany. Zlomek můžeme rovnou pokrátit číslem p a pak za pomoci vzorců pro součet goniometrických funkcí dostaneme

$$\begin{aligned}\frac{a+b}{a-b} &= \frac{(\cos\alpha + \cos\beta) + i(\sin\alpha + \sin\beta)}{(\cos\alpha - \cos\beta) + i(\sin\alpha - \sin\beta)} = \frac{2\cos\sigma\cos\delta + 2i\sin\sigma\cos\delta}{-2\sin\sigma\sin\delta + 2i\cos\sigma\sin\delta} \\ &= \frac{(\cos\sigma + i\sin\sigma)\cos\delta}{i(\cos\sigma + i\sin\sigma)\sin\delta} = -i\operatorname{cotg}\delta,\end{aligned}$$

kde $\sigma = \frac{1}{2}(\alpha+\beta)$ a $\delta = \frac{1}{2}(\alpha-\beta)$. Tvrzení tedy platí pro $r = -\operatorname{cotg}\delta$. Všimni si, že díky tomu, že $\alpha \neq \pi + \beta$, je $\operatorname{cotg}\delta$ nenulový. $\square$



Alternativní důkaz. Použijeme pomocného tvrzení, že pro čísla a, b se stejnou absolutní hodnotou platí $\arg(a+b) = (\arg a + \arg b)/2$, které vyplývá z toho, že čísla 0, a, b a $a+b$ tvoří kosočtverec v Gaussově rovině. Označme ještě $\arg a = \alpha$ a $\arg b = \beta$. Pak platí

$$\arg\frac{a+b}{a-b} = \arg(a+b) - \arg(a-b) = \frac{\alpha+\beta}{2} - \frac{\alpha+\beta+\pi}{2} = -\frac{\pi}{2},$$

a tedy $\Re\left(\frac{a+b}{a-b}\right) = r\cos(-\pi/2) = r \cdot 0 = 0$. $\square$

Příklad 5. Mějme konvexní pětiúhelník $ABCDE$. Označme postupně M, N, P, Q, X a Y středy úseček BC, CD, DE, EA, QN a PM. Dokažte, že $XY \parallel AB$.

Řešení. Ať malá písmena udávají souřadnice příslušných velkých bodů. Pak souřadnice středů stran jsou

$$m = \frac{1}{2}(b+c), \quad n = \frac{1}{2}(c+d), \quad p = \frac{1}{2}(d+e), \quad q = \frac{1}{2}(e+a).$$

Dále máme

$$x = \frac{1}{4}(c+d+e+a), \quad y = \frac{1}{4}(b+c+d+e).$$

Aby $XY \parallel AB$, musí být podíl $(x-y)/(a-b)$ reálné číslo. Tedy protože

$$\frac{x-y}{a-b} = \frac{a-b}{4(a-b)} = \frac{1}{4},$$

je $XY \parallel AB$.

Komplexní geometrie trojúhelníka

Nechť je v rovině dán trojúhelník ABC. Zvolme vhodně souřadnicový systém s počátkem ve středu kružnice opsané trojúhelníku ABC. To proto, že pak budou mít body $A(a)$, $B(b)$ a $C(c)$ od počátku stejnou vzdálenost. Dále můžeme ještě zvolit velikost trojúhelníka. Tu volme tak, aby $|a| = |b| = |c| = 1$. Pro další použití ještě označme

$$s_1 = a + b + c,$$
$$s_2 = ab + ac + bc,$$
$$s_3 = abc.$$

Nyní se budeme zabývat různými speciálními případy.

Typy trojúhelníků

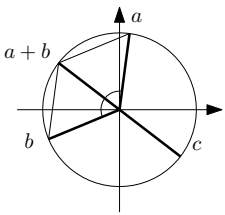
Pokusme se nyní komplexně popsat rovnostranný a pravoúhlý trojúhelník. Nezapomeňme však, že stále uvažujeme počátek ve středu kružnice opsané ABC.

Věta 6. *Trojúhelník ABC je rovnostranný právě tehdy, když $s_1 = 0$.*

Důkaz. Označme $\omega = e^{2\pi i/3}$ a BÚNO předpokládejme, že trojúhelník je značen proti směru hodinových ručiček. Pak jelikož počátek je střed kružnice opsané, tak ABC je rovnostranný, právě když $b = \omega a$, $c = \omega^2 a$. Protože platí, že $1 + \omega + \omega^2 = 0$, máme

$$s_1 = a + b + c = a(1 + \omega + \omega^2) = 0.$$

Obráceně, bez újmy na obecnosti předpokládejme, že a, b a c jsou na jednotkové kružnici uspořádány proti směru hodinových ručiček. Pokud $s_1 = 0$, pak $a+b = -c$, a tedy $|a+b| = |c| = 1$. Přitom ale stále platí $|a| = |b| = 1$. Body $a, b, a+b, 0$ tedy vytvoří kosočtverec, jehož úhlopříčka je stejně dlouhá jako jeho strana.



Tedy vektory čísel a a b musí svírat úhel $2 \cdot \frac{\pi}{3}$, a proto $b = \omega a$. Podobně také $c = \omega b$, z čehož dostaneme $c = \omega^2 a$. $\square$

Věta 7. *Trojúhelník ABC je pravoúhlý právě tehdy, když $s_1 s_2 = s_3$.*

Důkaz. Trojúhelník je pravoúhlý, právě když střed kružnice opsané leží na některé straně, tj. dvě komplexní čísla reprezentující vrcholy jsou opačná. Vezměme BÚNO $a = -b$. Pak ale $s_1 = c$, a proto

$$\frac{s_1 s_2}{s_3} = \frac{c(ab + ac + bc)}{abc} = \frac{ab + bc + ca}{ab} = 1 + \frac{c}{a} + \frac{c}{b} = 1 + \frac{c}{a} - \frac{c}{a} = 1.$$

Naopak $s_1 s_2 = s_3$ implikuje

$$(a + b)(b + c)(c + a) = (a + b + c)(ab + ac + bc) - abc = s_1 s_2 - s_3 = 0,$$

tedy některá dvě komplexní čísla z a, b, c jsou opačná a jsme hotovi. $\square$

Eulerova přímka

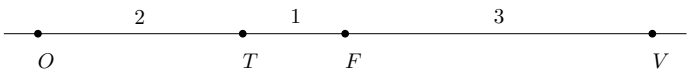
Jak už bylo řečeno, těžiště $T(t)$ trojúhelníku ABC se dá vyjádřit vztahem

$$t = \frac{a + b + c}{3}.$$

Nyní připomeňme Eulerovu přímku[18]. Je to taková přímka, na které postupně leží body O, T a V, postupně značící střed opsané kružnice, těžiště a průsečík výšek. A nejen to. Střed úsečky OV je znám též pod pojmem střed Feuerbachovy kružnice[19], někdy též zvané kružnice devíti bodů. Ne proto, že na ní leží pouze devět bodů, ale proto, že na ní leží devět význačných bodů. Jsou to středy stran a paty výšek trojúhelníku ABC a dále středy úseček AV, BV a CV. Všechny potřebné poměry vzdáleností bodů O, T, F a V jsou

$$\frac{|OT|}{|TV|} = \frac{1}{2}, \quad \frac{|TF|}{|OT|} = \frac{1}{2}.$$

Nejlépe je to vidět na následujícím obrázku.



Zpátky k našemu popisu význačných bodů trojúhelníku. Známe souřadnice bodů O a T, proto umíme zapsat i souřadnice bodů $F(f)$ a $V(v)$, protože

$$t = \frac{1}{3}o + \frac{2}{3}f \quad \Rightarrow \quad f = \frac{3}{2}t - \frac{1}{2}o = \frac{a + b + c}{2},$$
$$t = \frac{2}{3}o + \frac{1}{3}v \quad \Rightarrow \quad v = 3t - 2o = a + b + c.$$

To, že průsečík výšek V se dá zapsat jako $a + b + c$, je velice užitečné zjištění.

[18] Leonhard Euler, 1707 – 1783

[19] Karl Wilhelm Feuerbach, 1800 – 1834

Jen jako zkoušku ověříme, že opravdu bodem V prochází všechny výšky. Ze symetrie stačí dokázat, že $AV \perp BC$. K tomu nám bude stačit ukázat, že podíl $(v-a)/(b-c)$ je ryze imaginární. Když si dosadíme za $v = a+b+c$, dostaneme $(b+c)/(b-c)$, což je podíl, o kterém nám hovoří Thaletova věta, a tedy je ryze imaginární.

Máme tedy v rukou docela silný aparát. Pojďme si ho vyzkoušet na příkladu.

Příklad 8. Na kružnici opsané trojúhelníku ABC je dán bod M. Označme F_A, F_B a F_C středy Feuerbachových kružnic trojúhelníků MBC, MCA a MAB. Dokažte, že trojúhelníky ABC a $F_AF_BF_C$ jsou podobné.

Řešení. Buď střed souřadnicového systému ve středu kružnice opsané O. Pak O je též středem kružnic opsaných trojúhelníkům MBC, MCA a MAB, tedy středy Feuerbachových kružnic těchto trojúhelníků spočítáme jako

$$f_A = \frac{m+b+c}{2}, \quad f_B = \frac{m+a+c}{2}, \quad f_C = \frac{m+a+b}{2}.$$

Nyní už stačí dát příslušné strany do poměru a zjistíme, že

$$\frac{F_AF_B}{AB} = \frac{f_B - f_A}{b-a} = -\frac{1}{2}.$$

Ze symetrie tedy máme, že trojúhelníky ABC a $F_AF_BF_C$ jsou si podobné v poměru $2:1$.

Seriál III. – Komplexní teorie čísel

V posledním soutěžním díle seriálu se budeme zabývat tím, jak lze komplexní čísla využít v teorii čísel. Na začátku si uvedeme malý trik s rozkládáním polynomů v komplexních číslech. V celém zbytku budeme budovat jakousi obdobu dělitelnosti, kterou známe z celých čísel, v číslech komplexních. Speciálně nás budou zajímat obory Gaussových celých čísel a Eisensteinových celých čísel, něco o nich se dočteš dále.

Tento díl je relativně náročný, co se týče znalostí z teorie čísel, některé potřebné věci si vyložíme, některé alespoň připomeneme. Kdybys i přesto měl s něčím problém, můžeš zkusit zapátrat v následujících doporučených zdrojích. Prvním z nich je předloňský seriál o teorii čísel, který najdeš na PraSečích stránkách,[20] druhým je kniha Metody řešení matematických úloh I. Znalosti, které z teorie čísel předpokládáme, jsou však docela elementární a jistě s nimi potíže mít nebudeš.

Užití rozkladů v teorii čísel

V této kapitolce si ukážeme, jak lze využít umění rozkládání polynomů pomocí koplexních čísel v některých úlohách z teorie čísel. Není to světoborná metoda a dá se obejít, pokud potřebný rozklad známe. Výhodou však je, že s její pomocí umíme rozklad najít, i když ho neznáme, a tedy je tato metoda univerzálnější.

Příklad. Najděte všechna prvočísla tvaru $n^4 + 4^n$, kde n je přirozené číslo.

Řešení. Dosadíme-li $n = 1$, dostaneme $1^4 + 4 = 5$, takže jedno řešení je 5. Když budeme ještě chvíli zkoušet, zjistíme, že už mnoho nových řešení nedostaneme, a tedy bychom chtěli dokázat, že je-li $n > 1$, pak $n^4 + 4^n$ je složené.

Nejprve nahlédneme, že pro sudé n je číslo $n^4 + 4^n$ sudé (a různé od 2), buď tedy $n = 2k + 1$, k celé. Chceme dokázat, že

$$p = n^4 + 4 \cdot 4^{2k} = n^4 + 4 \cdot 2^{4k}$$

je číslo složené. Nejlepší by bylo nalézt přímo rozklad $x^4 + 4y^4$. Rozložme si tedy polynom $x^4 + 4$ v reálných číslech metodou z prvního dílu seriálu:

$$x^4 + 4 = (x - 1 + i)(x - 1 - i)(x + 1 + i)(x + 1 - i) = (x^2 - 2x + 2)(x^2 + 2x + 2).$$

Tedy platí

$$\begin{aligned} x^4 + 4y^4 &= y^4 \left(\left(\frac{x}{y} \right)^4 + 4 \right) = y^2 \left(\left(\frac{x}{y} \right)^2 - 2 \left(\frac{x}{y} \right) + 2 \right) \cdot y^2 \left(\left(\frac{x}{y} \right)^2 + 2 \left(\frac{x}{y} \right) + 2 \right) \\ &= \left(x^2 - 2xy + 2y^2 \right) \left(x^2 + 2xy + 2y^2 \right). \end{aligned}$$

V našem speciálním případě dostaneme rozklad

$$p = \left(n^2 - 2^{k+1} n + 2^{2k+1} \right) \left(n^2 + 2^{k+1} n + 2^{2k+1} \right),$$

přičemž druhá závorka je určitě ostře větší než 1, tedy p může být prvočíslo jedině tehdy, když první závorka je ± 1. Platí ale nerovnost

$$n^2 + 2^{2k+1} \geq n^2 + 2^{2k} + 1 \geq 2 \cdot 2^k n + 1, \qquad (\star)$$

[20] *http://mks.mff.cuni.cz/archive/28/9.pdf*

(její druhá část je důsledkem AG-nerovnosti $a^2 + b^2 \geq 2ab$), tedy

$$n^2 - 2^{k+1}n + 2^{2k+1} \geq 1.$$

Rovnost nastane, právě když nastane rovnost v obou nerovnostech z $(\star)$, tj. $2^k = 1$ a $n = 2^k$, což odpovídá $k = 0$, $n = 2k + 1 = 1$ a $p = n^4 + 4^n = 5$. Jediné prvočíslo tohoto tvaru je tedy 5.

Příklad. Dokažte, že součin dvou čísel tvaru $x^2 + xy + y^2$, kde x, y jsou celá čísla, je také tvaru $x^2 + xy + y^2$.

Řešení. Označme si $\omega = e^{(2\pi/3)i}$ kořen polynomu $x^2 + x + 1$. Platí

$$x^2 + xy + y^2 = (x - \omega y)(x - \overline{\omega} y).$$

Jsou-li tedy $a = x_1^2 + x_1 y_1 + y_1^2$ a $b = x_2^2 + x_2 y_2 + y_2^2$, pak použitím vztahu $\omega^2 = -1 - \omega$ odvodíme, že

$$\begin{aligned} ab &= \big((x_1 - \omega y_1)(x_2 - \omega y_2)\big)\big((x_1 - \overline{\omega} y_1)(x_2 - \overline{\omega} y_2)\big) \\ &= \big(x_1 x_2 - y_1 y_2 + (x_1 y_2 + x_2 y_1 - y_1 y_2)\omega\big) \cdot \big(x_1 x_2 - y_1 y_2 + (x_1 y_2 + x_2 y_1 - y_1 y_2)\overline{\omega}\big). \end{aligned}$$

Přitom druhý součin jsme ani nemuseli počítat, neboť je komplexně sdružený s prvním. Z posledního řádku už je vidět, že vhodná x a y taková, že $ab = x^2 + xy + y^2$, jsou právě koeficienty u 1 a u ω z prvního součinu, tedy jsou to čísla

$$\begin{aligned} x &= x_1 x_2 - y_1 y_2, \\ y &= x_1 y_2 + x_2 y_1 - y_1 y_2. \end{aligned}$$

Cvičení 1. Najděte všechna prvočísla tvaru $a^4 + a^2 + 1$.

Úloha 2. Je-li n přirozené a $4^n + 2^n + 1$ je prvočíslo, pak je n mocninou 3. Dokažte.

Úloha 3. Dokažte, že $2^{2^{2011}} + 2^{2^{2010}} + 1$ má alespoň 2011 prvočíselných dělitelů.

Teorie čísel není jenom dělitelnost celých čísel, ale i dělitelnost a rozložitelnost mnohočlenů s celočíselnými koeficienty. Podívejme se tedy na pár souvisejících úloh.

Připomeňme si, že pokud polynom $f(x)$ *dělí* polynom $g(x)$, znamená to, že existuje polynom $h(x)$ takový, že $f(x) = g(x)h(x)$. Neřekneme-li jinak, předpokládáme, že všechny koeficienty polynomů jsou reálná čísla.

Občas nás budou zajímat i polynomy s celočíselnými koeficienty. Pak budeme při dělitelnosti chtít, aby i polynom $h(x)$ měl celočíselné koeficienty.

Příklad. Buďte m, n přirozená. Dokažte, že $x^n - 1$ dělí polynom $x^m - 1$, právě když $n \mid m$.

Řešení. Nejprve si vzpomeneme na několik vlastností mnohočlenů. Ani jeden ze zadaných mnohočlenů nemá vícenásobný kořen, neboť kořeny jsou n-té (resp. m-té) odmocniny z jedné, které v Gaussově rovině tvoří vrcholy pravidelného n-úhelníku (resp. m-úhelníku) s jedním vrcholem v bodě 1, vepsaného do jednotkové kružnice. Proto platí, že $x^n - 1 \mid x^m - 1$, pokud všechny kořeny $x^n - 1$ jsou zároveň kořeny $x^m - 1$.[21]

[21] Platí totiž $x^n - 1 = (x - k_1)(x - k_2) \cdots (x - k_n)$, kde k_i jsou právě kořeny $x^n - 1$. Přitom kořenoví činitelé jsou navzájem nesoudělní.

Nejdříve dokážeme opačnou implikaci. Označme $\varepsilon_n = e^{(2\pi/n)i}$ n-tou odmocninu z jedné, která je na jednotkovém kruhu následující po 1 v kladném smyslu. Zřejmě $\varepsilon_n^n = 1$, tedy ε_n je kořenem polynomu $x^n - 1$. Přitom ale $\varepsilon_n^m = e^{(2\pi m/n)i}$, a to může být rovno 1, jen pokud je exponent násobkem $2\pi i$, tj. $m/n \in \mathbb{Z}$ a $n \mid m$.

Naopak nechť $m = kn$ a buď α kořen mnohočlenu $x^n - 1$. Pak

$$\alpha^m - 1 = \alpha^{kn} - 1 = (\alpha^n)^k - 1 = 1^k - 1 = 0,$$

a tedy α je kořenem polynomu $x^m - 1$.

Budeš-li s kořeny obou polynomů (které jsou odmocninami z jedné) nakládat trochu opatrněji, určitě snadno vyřešíš následující cvičení. Zkus si jej poté vyřešit i bez komplexních čísel. Poradíme ti, že je výhodné použít Euklidův algoritmus.

Cvičení 4. Nalezněte největšího společného dělitele[22] mnohočlenů $x^m - 1$ a $x^n - 1$ v závislosti na přirozených číslech n a m.

Cvičení 5. S využitím poznatků z posledního uvedeného příkladu ukažte, že $2^n - 1$ dělí $2^m - 1$, právě když $n \mid m$.

Na závěr si uvedeme jednu úlohu k zamyšlení. Při jejím řešení zkus použít vlastnosti n-tých odmocnin z jedné a zkus přijít na to, jak tato úloha souvisí s předchozími dvěma úlohami.

Úloha 6. Číslo $\varphi \in \mathbb{C}$ nazveme *primitivní* n-tou odmocninou z jedné, pokud $\varphi^n = 1$ a pro žádné přirozené d, $d \mid n$ a $d \neq n$, neplatí, že $\varphi^d = 1$.

Nechť čísla $\varphi_1, \varphi_2, \ldots, \varphi_k$ jsou všechny primitivní n-té odmocniny z jedné.[23] Dokažte, že mnohočlen

$$c_n(x) = (x - \varphi_1)(x - \varphi_2) \cdots (x - \varphi_k)$$

má racionální koeficienty.

Tři klíčové věty z dělitelnosti

V tomto díle seriálu budeme definovat něco, co bychom intuitivně nazvali komplexní celá čísla. Rozumné přístupy jsou dva, Gaussova a Eisensteinova čísla. Než se do nich pustíme, shrneme si klíčové vlastnosti dělitelnosti na celých číslech. Pokud víš, jak se pracuje s dělitelností polynomů, všimni si, že následující tři tvrzení platí nejen pro celá čísla, ale rovněž pro polynomy.

Řekneme, že číslo[24] *a dělí* číslo b, pokud existuje číslo c takové, že $ac = b$. Píšeme $a \mid b$. Číslo a nazýváme *dělitelem* čísla b a číslo b *násobkem* čísla a. Pokud $a \mid b$ a zároveň $b \mid a$, budeme říkat, že čísla a a b jsou *asociovaná*, a budeme psát $a \parallel b$. Čísla asociovaná s jedničkou nazveme *invertibilní*. Invertibilními čísly jsou právě ta čísla a, pro něž je $1/a$ celé, tedy v celých číslech se jedná o ± 1.[25]

Důležitou vlastností celých čísel je dělení se zbytkem, formálně to popíšeme v následující větě.

---

[22] *Největším společným dělitelem* mnohočlenů $f(x)$ a $g(x)$ nazveme takový mnohočlen $d(x)$, pro který platí $d(x) \mid f(x)$ a $d(x) \mid g(x)$, a zároveň pro každý jiný polynom $c(x)$, který dělí jak $f(x)$, tak $g(x)$, platí $c(x) \mid d(x)$. Jinými slovy, $d(x)$ je společný dělitel a každý jiný společný dělitel ho dělí – tím zaručíme, že $d(x)$ je mezi všemi společnými děliteli ten o „největší“.

[23] Jestlipak víš, čemu je rovno k? K řešení úlohy to ovšem není potřeba.

[24] Nebo taky mnohočlen, chceš-li.

[25] V polynomech nad reálnými čísly jsou to všechny konstantní nenulové polynomy.

Věta. (dělení se zbytkem) *Jsou-li a, b libovolná celá čísla, pak existuje jediné $r \geq 0$, $|r| < |b|$, a jediné $q \in \mathbb{Z}$ takové, že*

$$a = qb + r.$$

Číslo q nazveme celočíselným podílem $a : b$ a číslo r zbytkem a po dělení b.

Dělení se zbytkem je velmi užitečné, neboť nám zaručuje, že každá dvě čísla mají největšího společného dělitele. *Společným dělitelem* čísel a, b nazveme každé c, pro které platí, že $c \mid a$ a současně $c \mid b$ (česky řečeno, c je společným dělitelem čísel a a b), *největším společným dělitelem* pak nazveme takového společného dělitele, který je „největší“ ve smyslu dělitelnosti. Tedy d je největší společný dělitel a a b, pokud ho dělí každý společný dělitel a a b. Největšího společného dělitele a a b budeme značit (a, b). Pokud nastane případ $(a, b) = 1$, řekneme, že čísla a a b jsou *nesoudělná*.

Všimni si, že tato definice největšího společného dělitele není jednoznačná, neboť je-li $d = (a, b)$, pak i $-d = (a, b)$. Z toho si ale nebudeme dělat hlavu, protože platí $d \parallel -d$, tedy tato čísla mají z pohledu dělitelnosti stejné vlastnosti. Obecně platí, že společný dělitel je určen jednoznačně až na přenásobení invertibilním prvkem. Měli bychom tedy správně psát $(a, b) \parallel d$ místo $(a, b) = d$, ale to dělat nebudeme. Rovností $(a, b) = d$ budeme mít vždy na mysli asociovanost $(a, b) \parallel d$.

Jak vlastně využijeme dělení se zbytkem k výpočtu největšího společného dělitele? Běžně se používá Euklidův algoritmus, jehož výhodou je, že funguje i v obecnějších případech. Chceš-li se o jeho možnostech dozvědět podrobněji, podívej se do prvního dílu předloňského seriálu o teorii čísel.

Uvažme množinu

$$I = \{ka + lb : k, l \in \mathbb{Z}\}.$$

Předně si všimni, že všechna $i \in I$ jsou násobky libovolného společného dělitele c ($c \mid a$ a $c \mid b$, tedy i $c \mid ka$, lb a $c \mid ka + lb = i$). Všimni si také, že tato vlastnost charakterizuje společného dělitele a a b, neboť pokud c dělí každý prvek I, pak speciálně dělí i a, i b.

Nyní si vezmeme nejmenší kladný prvek d množiny I a dokážeme, že všechna čísla v I jsou násobky d. Nechť tedy pro spor $na + mb \in I$ není násobek d. Pak $na + mb$ vydělíme se zbytkem číslem d:

$$na + mb = qd + r.$$

Protože $d \nmid n$, dostáváme, že $r \neq 0$. Přitom $r = na + mb - qd$ a $d = ka + lb$, tedy $r = (n - kq)a + (m - ql)b$, neboli $r \in I$. To je ale spor s volbou d, protože zřejmě $r < d$.

Ukázali jsme tedy, že d je společným dělitelem a a b a současně násobkem libovolného jiného společného dělitele, neboť je to prvek I, tj. $(a, b) = d$.

Jedním pěkným důsledkem tohoto postupu je další důležité tvrzení. Všimni si však, že celé to zatím visí jen na dělení se zbytkem a mohli bychom sem dospět stejně tak Euklidovým algoritmem.

Věta. (Bézoutova) *Jsou-li a, b celá čísla, pak existují $k, l \in \mathbb{Z}$, že platí*

$$ka + lb = (a, b).$$

Cvičení 7. Pomocí Bézoutovy věty dokažte, že platí $(a, bc) \mid (a, b) \cdot (a, c)$.

Cvičení 8. Jsou-li b a c nesoudělná, ukažte, že platí dokonce $(a, bc) = (a, b) \cdot (a, c)$.

Podívejme se dále, a to na prvočísla. Číslo p nazveme *prvočíslem*, jestliže není invertibilní[26] a platí, že kdykoliv $p \mid ab$, pak $p \mid a$ nebo $p \mid b$.[27] Kdybychom se tě zeptali, co je to prvočíslo, odpověděl bys možná, že je to číslo, které nemá žádné vlastní dělitele, tedy každý dělitel je asociovaný s 1 nebo s p. Tyto dvě definice jsou v celých číslech ekvivalentní, ale není to úplně zřejmé.

Čísla, která nemají netriviální rozklad na součin, nazveme *ireducibilní*. Tedy r je ireducibilní, jestliže není invertibilní, a kdykoliv $r = ab$, je a nebo b invertibilní.

Dokažme nejdříve, že každé prvočíslo je ireducibilní. Kdyby $p = ab$, muselo by platit $p \mid a$ nebo $p \mid b$. Bez újmy na obecnosti můžeme předpokládat, že $p \mid a$, ale zároveň $a \mid p$, neboť $ab = p$, tedy $p \parallel a$. Tedy $ba = p = ja$, kde j je invertibilní, tj. $j = b$ a b je invertibilní.

Důkaz opačné implikace je trochu složitější a potřebujeme k němu Bézoutovu větu. Nechť tedy r je ireducibilní a $r \mid ab$. Platí

$$r = (r, ab) \mid (r, a) \cdot (r, b),$$

přičemž (r, x) může nabývat pouze hodnot 1 a r (až na přenásobení invertibilním prvkem). Přitom nemůže nastat případ $(r, a) = (r, b) = 1$, neboť pak by $r \mid 1$. Tedy buď $(r, a) = r$, nebo $(r, b) = r$, v prvním případě $r \mid a$, v druhém $r \mid b$. $\square$

Věta. (o jednoznačném rozkladu) *Je-li n celé číslo, tak existuje jednoznačný rozklad čísla n na prvočísla (až na pořadí a přenásobení invertibilními prvky).*

Důkaz. Pouze naznačíme základní myšlenku, exaktní důkaz je zbytečně technicky náročný. Nejprve budeme chtít dokázat, že se číslo n rozkládá. Budeme postupovat indukcí podle $|n|$. Invertibilní čísla ± 1 se rozkládají triviálně jako prázdný součin se znaménkem.[28] Buď tedy n celé a předpokládejme, že tvrzení platí pro všechna čísla s menší absolutní hodnotou.

Mohou nastat dvě možnosti. Buď n je ireducibilní, pak n je prvočíslo a $n = n$ je roklad na prvočinitele, nebo je n rozložitelné, tedy existují a a b, že $n = ab$, $|a| < n$ a $|b| < n$, neboť jde o netriviální rozklad. Pro a a b použijeme indukční předpoklad a dostaneme rozklad n na prvočinitele.

K důkazu jednoznačnosti využijeme poznatku, že prvočísla jsou ireducibilní prvky. Stačí dokázat, že kdykoliv $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ pro prvočísla p_i a q_i, pak $k = l$ a při vhodném očíslování $p_1 \parallel q_1$, $p_2 \parallel q_2$ atd. Platí totiž, že $p_1 \mid q_1 q_2 \cdots q_l$, tedy p_1 dělí jedno z čísel q_i, označme ho q_1. Přitom q_1 je nerozložitelné, takže $p_1 \parallel q_1$. Dále postupujeme analogicky. $\square$

K čemu se nám hodí jednoznačný roklad na prvočinitele? Například k vyslovení následujícího tvrzení, které nám pomůže řešit některé diofantické rovnice.

Tvrzení. (o mocninách) *Je-li n přirozené a a, b jsou celá nesoudělná čísla taková, že $ab = c^n$ pro nějaké celé c, potom jak a, tak b jsou n-té mocniny (až na přenásobení invertibilním prvkem). Tedy existují x a y taková, že $a = \pm x^n$ a $b = \pm y^n$.*

Důkaz. Důkaz je docela jednoduchý a my ho zde pouze naznačíme, detaily si rozmysli sám. Klíčovým krokem je rozložit a, b i c na prvočinitele a porovnat rozklady čísel ab a c^n. Pak už

---

[26] Jedničku za prvočíslo nepovažujeme.

[27] V celých číslech navíc požadujeme, aby byla prvočísla kladná. Dělá se to proto, abychom se zbavili nejednoznačností typu $4 = 2^2 = (-2)^2$. V jiných oborech by tato podmínka byla příliš složitá, a proto ji raději vypouštíme.

[28] Vynásobíme-li nula čísel, dostaneme jedničku – ze stejného důvodu je $0! = 1$.

si stačí jen uvědomit, že tvrzení „a a b jsou nesoudělná“ vlastně znamená, že se v prvočíselném rozkladu čísla a nevyskytuje žádné prvočíslo, které je obsaženo v prvočíselném rozkladu b, a naopak. V neposlední řadě to, že číslo je n-tou mocninou, znamená, že všechna prvočísla v jeho rozkladu se vyskytují v mocnině, která je násobkem n. $\square$

U tohoto tvrzení si musíme dát velký pozor, abychom nezapomněli na znaménka u a a b. Může totiž platit $ab = 6^2 = 36$, ale $a = -4$ a $b = -9$, což jsou nesoudělná čísla, ale ani jedno z nich není čtverec.

Příklad. Nalezněte všechny dvojice celých čísel x, y, pro něž platí

$$x = (y + x)(y - x).$$

Řešení. Upravme si rovnici do tvaru

$$(x + 1)x = y^2.$$

Čísla $x + 1$ a x jsou po sobě jdoucí, a tudíž nesoudělná. Každý jejich společný dělitel musí dělit i jejich rozdíl, který je 1. Musí tedy existovat čísla a a b taková, že $\pm a^2 = x$ a $\pm b^2 = x + 1$, obě se stejným znaménkem.

Nejprve se podíváme na případ, kdy jsou x a $x + 1$ nezáporná. Platí

$$1 = (x + 1) - x = b^2 - a^2 = (b - a)(b + a).$$

Víme tedy, že $b - a = b + a = \pm 1$. Můžeme vyjádřit $2b = \pm 2$, tj. $b = \pm 1$, $a = 0$ a $x = 0$. Dosadíme-li do původní rovnice, dostaneme $y = 0$.

Jsou-li x a $x + 1$ nekladná, pak podobně dostaneme

$$1 = (x + 1) - x = a^2 - b^2 = (a - b)(a + b).$$

Jestliže budeme stejným způsobem postupovat dále, dostaneme řešení $x + 1 = 0$, tj. $x = -1$ a $y = 0$.

Úloha má tedy dvě řešení, jimiž jsou dvojice $(x, y) = (0, 0)$ a $(-1, 0)$.

Tento postup funguje, umíme-li rovnici upravit do pěkného tvaru. Co bychom ale dělali například s rovnicí $x^2 + 1 = y^3$? Jediný rozumný tvar, do něhož jsme schopni ji upravit, je $(x + i)(x - i) = y^3$. Potom ale potřebujeme nějakou teorii a větu o rozkladu na prvočinitele v komplexních číslech. Na to se podíváme v několika následujících kapitolách. Nejdříve však musíme vybudovat nějakou teorii.

Něco málo o kvadratických zbytcích

K tomu, abychom si odvodili některé poznatky z teorie čísel v komplexním oboru, se nám bude hodit vědět něco málo o kvadratických zbytcích. Podíváme na celá čísla a na jejich zbytky po dělení prvočíslem p a položíme si otázku, které zbytky mohou být druhou mocninou nějakého (celého) čísla.

Připomeňme si nejdříve definici kongruence. Říkáme, že čísla a a b jsou *kongruentní* modulo n, jestliže $n \mid a - b$, píšeme $a \equiv b \pmod{n}$. Znamená to, že čísla a a b dávají stejný zbytek modulo n. Často budeme mluvit jen o zbytcích modulo n, pod tím si můžeš představit nějakou

množinu reprezentantů zbytků, obvykle množinu $\{0, 1, \ldots, n-1\}$ nebo pro $n = 2k+1$ množinu $\{-k, -k+1, \ldots, k\}$.

Pokud řekneme, že x je jednoznačné modulo n, myslíme tím, že existuje číslo b takové, že x je vždy kongruentní s b modulo n, tedy dvě různé hodnoty x se liší jen o násobek čísla n. Například kongruence $x \equiv 3$ má modulo 5 jednoznačné řešení, přestože má nekonečně mnoho řešení tvaru $5k+3$, kde k je celé číslo.

Konečně tedy přistupme k definici kvadratického zbytku pro číslo n. Řekneme, že $a \in \mathbb{Z}$ je *kvadratický zbytek*, pokud existuje b takové, že b^2 dává po dělení číslem n stejný zbytek jako a, tj. $n \mid b^2 - a$. V jazyce kongruencí, a je kvadratický zbytek modulo n právě tehdy, když má kongruence $x^2 \equiv a \pmod{n}$ řešení.

Kvadratické zbytky se hodí při řešení některých diofantických rovnic. Velmi užitečné je znát kvadratické zbytky malých modulů. Například kvadratické zbytky modulo 3 jsou 0 a 1, modulo 4 rovněž 0 a 1, modulo 8 jsou to 0, 1 a 4.

Na ostatní kvadratické zbytky snadno přijdeš, když si vypíšeš všechny zbytky modulo n a spočítáš jejich druhé mocniny. Ukážeme si to pro modul 4: $0^1 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 0$ a $3^2 = 9 \equiv 1 \pmod{4}$. Skutečně, kvadratické zbytky modulo 4 jsou právě 0 a 1. Toto pozorování využijeme v následující úloze.

Příklad. Najděte všechna celá čísla x, y a k, která řeší rovnici

$$x^2 + y^2 = 4k + 3.$$

Řešení. Podíváme se na rovnici modulo 4. Platí

$$x^2 + y^2 \equiv 3 \pmod{4},$$

ale možné kvadratické zbytky modulo 4 jsou jen 0 a 1. Tedy ať sečteme jakoukoli dvojici čtverců, nemůžeme nikdy dostat zbytek 3. Úloha proto nemá v celých číslech žádné řešení.

Příklad. Najděte všechna celá čísla x, y a k, která řeší rovnici

$$x^2 + xy + y^2 = 3k + 2.$$

Řešení. V tomto příkladu použijeme kvadratické zbytky modulo 3. Levou stranu vynásobíme čtyřmi a počítáme modulo 3:

$$4(x^2 + xy + y^2) = (2x+y)^2 + 3y^2 \equiv (2x+y)^2.$$

Protože $4 \equiv 1 \pmod{3}$, zbytek pravé strany po dělení třemi se při násobení čtyřmi nezmění. Musí tedy platit kongruence

$$(2x+y)^2 \equiv 2 \pmod{3}.$$

Číslo 2 však není kvadratický zbytek modulo 3, rovnice proto nemá řešení.

Do konce této kapitoly se budeme zabývat už jen kvadratickými zbytky modulo lichá prvočísla, které pro nás budou užitečné. Speciálně se pak zaměříme na zbytky -1 a -3.

Následující lemma, které budeme dále používat, je spíše technické. Jeho důkaz není příliš zajímavý, uvádíme ho jen pro úplnost.

Lemma. *Je-li p prvočíslo a $f(x)$ polynom stupně n s celočíselnými koeficienty takový, že p nedělí alespoň jeden z koeficientů $f(x)$, pak existuje nejvýše n řešení kongruence $f(x) \equiv 0$ modulo p.*

Tedy existuje nejvýše n čísel $0 \le a_1 < a_2 < \cdots < a_k < p$, že $f(a_i) \equiv 0 \pmod p$ pro všechna $i = 1, 2, \ldots, k$. Navíc každé b takové, že $f(b) \equiv 0 \pmod p$, je kongruentní s jedním z čísel a_1, $a_2, \ldots, a_k$.

Důkaz. V tomto důkazu bude modul u všech kongruencí p. Tvrzení dokážeme indukcí. Začněme polynomem stupně 0, tedy konstantním polynomem $f(x) = k$. Přitom $p \nmid k$, tedy kongruence $k = f(x) \equiv 0$ neplatí a nemá žádné řešení x.

Nechť je tvrzení splněno pro všechny polynomy stupně nejvýše $n - 1$. Buď $f(x)$ polynom stupně n, který má alespoň jeden kořen modulo n (nemá-li žádný kořen, tvrzení zřejmě platí), označme ho a_0 (tj. $f(a_0) \equiv 0$). Z dělení polynomů se zbytkem víme, že existuje polynom $g(x)$ s celočíselnými koeficienty a existuje celé číslo r, že

$$f(x) = (x - a_0)g(x) + r.$$

Zbytek r je navíc roven $f(a_0)$, neboť po dosazení a_0 musí nastat rovnost. Dále víme, že $p \mid f(a_0) = r$. Pro každé a tedy platí

$$f(a) \equiv f(a) - r = (a - a_0)g(a) \pmod p.$$

Buďte $a_1, a_2, \ldots, a_k$ kořeny $g(x)$ modulo p z indukčního předpokladu. Přidáme-li k nim a_0, dostaneme kořeny $a_0, a_1, \ldots, a_k$ polynomu $f(x)$ modulo p. Číslo a_0 můžeme vypustit, pokud se už nachází mezi ostatními čísly. Všech čísel je dohromady nejvýše $k + 1$, což určitě není více než n, protože $k \le n - 1$ podle indukčního předpokladu.

Nyní ukážeme, že kongruence $f(x) \equiv 0$ nemá žádné další řešení. Je-li b takové, že $f(b) \equiv 0$, pak

$$p \mid f(b) \equiv f(b) - r = (b - a_0)g(b),$$

a protože p je prvočíslo, víme, že buď $p \mid b - a_0$, nebo $p \mid g(b)$. Nechť jsou $a_1, a_2, \ldots, a_k$ čísla z indukčního předpokladu pro $g(x)$. Pak první možnost říká, že $b \equiv a_0$, druhá, že b je kongruentní s jedním z $a_1, a_2, \ldots, a_k$.

Dohromady dostáváme, že b je kongruentní s jedním z čísel a_i pro $i = 0, 1, \ldots, k$. $\square$

V tomto lemmatu je potřeba, aby bylo p prvočíslo, neboť například pro $n = 6$ má kongruence $x(x-1) \equiv 0 \pmod 6$ řešení 0, 1, 3 a 4. Všimni si, že podobné tvrzení platí pro kořeny mnohočlenů v reálných nebo komplexních číslech.

Tvrzení. *Je-li $p > 2$ prvočíslo, pak existuje právě $(p - 1)/2$ navzájem nekongruentních nenulových kvadratických zbytků modulo p.*

Důkaz. Je-li a kvadratický zbytek, tj. $a \equiv b^2$, pak kongruence $x^2 \equiv a \pmod p$ má právě dvě řešení, a to b a $-b$.

Navíc každé b^2 dává nějaký zbytek, tedy kvadratické zbytky jsou právě zbytky

$$1^2 = (-1)^2, 2^2 = (-2)^2, \ldots, \left(\frac{p-1}{2}\right)^2 = \left(\frac{p+1}{2}\right)^2,$$

které jsou po dvou různé. $\square$

Tvrzení. *Je-li $p = 4k + 1$ kladné prvočíslo, pak -1 je kvadratický zbytek modulo p.*

Důkaz. Tvrzení odvodíme z tzv. Wilsonovy věty. Ta říká, že $(p-1)! \equiv -1 \pmod{p}$ pro každé prvočíslo p. Vyjádřeme si tedy $(p-1)!$ trochu jinak:

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdots (p-1) \equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdots (-2) \cdot (-1) \\ &= \left(1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\right)^2 (-1)^{\frac{p-1}{2}} = a^2,\end{aligned}$$

kde $a = \left(\frac{p-1}{2}\right)!$, protože $(p-1)/2 = 4k/2 = 2k$ je sudé. Tedy $a^2 \equiv -1$ podle Wilsonovy věty. $\square$

Tvrzení. *Je-li $p = 3k+1$ kladné prvočíslo, pak -3 je kvadratický zbytek modulo p.*

Důkaz. Nejprve ukážeme, že kongruence $x^2 + x + 1 \equiv 0$ má řešení modulo p. Pokud $x^2 + x + 1$ vynásobíme $x - 1$, dostaneme kongruenci

$$x^3 \equiv 1 \pmod{p},$$

která má určitě řešení $x = 1$. My potřebujeme najít jiné řešení. Z malé Fermatovy věty víme, že $a^{p-1} \equiv 1 \pmod{p}$ pro každé prvočíslo p a a nesoudělné s p, zde speciálně $a^{3k} \equiv 1$, tedy každé a^k, $p \nmid a$, je řešením naší kongruence.

Co kdyby ovšem $a^k \equiv 1$ pro každé takové a? To podle lemmatu z této kapitoly může nastat pro nejvýše k hodnot a. My však máme k disposici celkem $3k$ navzájem nekongruentních čísel $1, 2, \ldots, p-1$, tedy pro alespoň jedno a musí platit $a^k \not\equiv 1$. Našli jsme tedy řešení $b = a^k$ kongruence $x^3 - 1 \equiv 0$, které není kongruentní s 1 modulo p.

Platí $p \mid (b-1)(b^2+b+1)$, přičemž $b = a^k \not\equiv 1$, a tedy $p \mid b^2+b+1$, neboť p je prvočíslo, a b je kořenem x^2+x+1 modulo p.

Nyní upravíme kongruenci. Všimneme si, že $p \neq 2$, takže násobení čtyřmi je ekvivalentní úpravou.

$$\begin{aligned}x^2 + x + 1 &\equiv 0 \pmod{p} \\ 4x^2 + 4x + 4 &\equiv 0 \\ (2x+1)^2 &\equiv -3\end{aligned}$$

Tedy $(2b+1)^2 \equiv -3$, což dokazuje, že -3 je kvadratický zbytek modulo p. $\square$

Gaussova celá čísla

Prvním z oborů, kterými se zde budeme zabývat, jsou Gaussova celá čísla.[29] *Gaussovým celým číslem* rozumíme komplexní číslo tvaru $a + ib$, kde $a, b \in \mathbb{Z}$ jsou celá čísla. Tam, kde nemůže dojít k záměně s Eisensteinovými čísly nebo jinými obory, budeme občas nazývat Gaussova celá čísla zkráceně *celistvá čísla*. Množinu všech Gaussových celých čísel budeme značit $\mathbb{Z}[i]$.[30] Gaussova čísla jsou vlastně jakési mřížové body v Gaussově rovině.

Na Gaussových číslech definujeme dělitelnost stejně jako na celých číslech. Číslo a dělí číslo b, pokud existuje celistvé číslo c, že $ac = b$. Tedy například číslo 2 dělí číslo $2+2i$, číslo $1+i$ dělí 2, neboť $(1+i)(1-i) = 2$, číslo $1+2i$ dělí $5-5i$, neboť $(1+2i)(-1-3i) = 5-5i$, atd.

---

[29] angl. Gaussian integers

[30] Toto značení znamená, že k celým číslům přidáme komplexní jednotku i a všechny součty a součiny. Až budeme mít Eisensteinova celá čísla, budeme je značit $\mathbb{Z}[\omega]$. Možná už zvládneš uhodnout, jak budou vypadat.

Invertibilní prvky, tj. dělitelé jedničky, jsou na Gaussových číslech právě čtyři, a to ± 1 a $\pm i$. Takže budeme-li zkoumat dělitelnost, nebude nás zajímat přenásobení některým z těchto prvků, podobně jako nás v celých číslech nezajímalo znaménko.

Všimni si, že některá prvočísla z celých čísel se v Gaussových číslech rozkládají, například $2 = -i(1+i)^2$ a $5 = (1+2i)(1-2i)$.

Cvičení 9. Rozhodněte, zda pro celé číslo a platí, že $1 + i \mid a$ právě tehdy, když a je sudé. Podle čeho lze poznat, jestli je číslo $a + ib$ dělitelné $1 + i$?

Nyní se podíváme se na dělení se zbytkem. Zformulujeme tvrzení, které pro nás bude v Gaussových číslech jedním z klíčových, přestože je vlastně jednoduché a naprosto stejné, jako v číslech celých.

Začneme Gaussovou normou, neboli velikostí Gaussova čísla. Definujeme *(Gaussovu) normu* Gaussova čísla $a + ib$ jako

$$N_i(a + ib) = (a + ib)(a - ib) = a^2 + b^2.$$

Nejprve si všimni, že norma je vždy nezáporné celé číslo, přičemž nulová je pouze pro nulu. Srovnáme-li definici s obyčejnou normou komplexních čísel, máme $N_i(x) = |x|^2$ (druhá mocnina zajišťuje, že bude norma vždy kladná, a tedy přes ni můžeme dokazovat matematickou indukcí). Pokud nebude hrozit, že by došlo k záměně, budeme často normu x značit jen $N(x)$.

Cvičení 10. Ukažte, že norma součinu je součinem norem, tedy že pro libovolné a a $b \in \mathbb{Z}[i]$ platí $N(ab) = N(a)N(b)$. Z této rovnosti odvoďte, že pokud $a \mid b$, pak $N(a) \mid N(b)$.

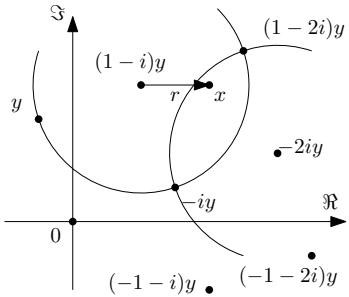
Všimni si, že platí-li $x \mid y$ a $y \neq 0$, pak $N_i(x) \leq N_i(y)$, což je obdoba tvrzení v celých číslech, které říká, že $x \mid y$ implikuje $|x| \leq |y|$. Platí-li totiž $xc = y$, pak $N(x)N(c) = N(xc) = N(y)$, a navíc pokud $y \neq 0$, pak $c \neq 0$ a $N(c) \geq 1$. Z definice normy je vidět také to, že pro každé Gaussovo číslo $a + ib$ platí $a + ib \mid N(a + ib)$.

Tedy už tě jistě napadne, jak bude vypadat tvrzení o dělení se zbytkem, ve kterém se vyskytuje velikost čísla.

Věta. (dělení se zbytkem) *Jsou-li $x, y \in \mathbb{Z}[i]$, pak existují čísla $q, r \in \mathbb{Z}[i]$, $N(r) < N(y)$, že*

$$x = qy + r.$$

Důkaz. Zkusme si situaci přestavit v Gaussově rovině. Vezmeme všechny násobky čísla y (tj. všechna čísla tvaru $(a + ib)y = ay + b(iy)$, kde $a, b \in \mathbb{Z}$), ty tvoří zvětšenou a otočenou mřížku.



Chceme dokázat, že každé číslo x má k nějakému mřížovému bodu blíž než $|y|$. Pak bude totiž platit $qy - x = r$, kde qy je onen nejbližší mřížový bod a čísla q a r jsou právě ta, která hledáme, neboť

$$N(r) = |r|^2 = |qy - x|^2 < |y|^2 = N(y).$$

Zbývá ještě zdůvodnit, proč vnitřky kruhů o poloměru $|y|$ a středech v mřížových bodech ky ($k \in \mathbb{Z}[i]$) pokrývají celou Gaussovu rovinu. To je ale jasné z geometrické představy a z toho, že kruhy se středem ve vrcholech čtverce a poloměrem délky jeho strany tento čtverec pokrývají. $\square$

V přechozím tvrzení jsme nevyslovili jednoznačnost zbytku po dělení, což sice není úplně šťastné, nicméně nám to vlastně vůbec nevadí, protože používáme především existenci. Pokud bychom chtěli jednoznačné zbytky, stačí si vybrat vhodnější reprezentanty, například čísla tvaru $a + ib$, kde $0 \leq a < \Re(y)$ a $0 \leq b < \Im(y)$.

Vzpomeňme si na Euklidův algoritmus, ten bude v Gaussových číslech fungovat velmi podobně jako v číslech celých. Je založen na tom, že jsou-li a, b celistvá, pak $(a, b) = (a, b - ka)$ pro libovolné k. Většinou se používá tak, že za k zvolíme celočíselný podíl a a b. Nám ale bude bohatě stačit, když $N(b - ka) < N(b)$. Díky tomu budeme mít zaručeno, že normy obou čísel nám postupně klesají. Protože jsou to přirozená čísla, po konečném počtu kroků se dostaneme k nule a získáme $(a, b) = (d, 0) = d$.

Ukážeme si tento postup třeba na dvojici čísel $8 + i$ a 13. Všimni si, že normy se opravdu postupně zmenšují.

$$\begin{aligned} 13 &= (8 + i) + (5 - i) \\ 8 + i &= (5 - i) + (3 + 2i) \\ 5 - i &= (1 - i)(3 + 2i) + 0 \end{aligned}$$

Tedy $(8 + i, 13) = 3 + 2i$.

Obráceným postupem umíme najít řešení Bézoutovy rovnice $xa + yb = (a, b)$, což už bude probíhat naprosto stejně jako v celých číslech. Například pro předchozí dvojici

$$3 + 2i = (8 + i) - (5 - i) = (8 + i) - (13 - (8 + i)) = 2(8 + i) - 13.$$

Věta. (Bézoutova) *Jsou-li a, b libovolná Gaussova celá čísla, pak existují $x, y \in \mathbb{Z}[i]$ taková, že platí*

$$ax + by = (a, b).$$

Cvičení 11. Najděte největšího společného dělitele a řešení Bézoutovy rovnice pro čísla $3 + 5i$ a $4 + 2i$.

Gaussova prvočísla

Gaussovým prvočíslem nazveme takové celistvé číslo $p = a + bi$, že kdykoliv $p \mid xy$, pak $p \mid x$ nebo $p \mid y$. Díky Bézoutově větě je toto ekvivalentní s tím, že kdykoliv $p = xy$, pak x nebo y je invertibilní, což se dokáže naprosto stejně jako v celých číslech. Podívej se do předcházející kapitoly a přesvědč se o tom sám.

Otázkou je, jak vypadají Gaussova prvočísla. Některá prvočísla z celých čísel se totiž v Gaussových číslech rozkládají, např. $2 = -i(1 + i)^2$ nebo $5 = (1 + 2i)(1 - 2i)$.

Cvičení 12. Najděte rozklad prvočísla 17 v Gaussových číslech.

Cvičení 13. Dokažte, že číslo 3 se v Gaussových celých číslech nerozkládá, a jde tedy o Gaussovo prvočíslo.

Máme před sebou obtížný úkol charakterizovat Gaussova prvočísla, popsat, která běžná prvočísla se rozkládají a jak, a která naopak zůstávají nerozložitelná. Ještě než se do toho pustíme, podíváme se na jednoznačnost rozkladu. Podobně jako v celých číslech i tady platí věta o jednoznačnosti rozkladu na prvočísla.

Věta. (o jednoznačnosti rozkladu na prvočísla) *Každé Gaussovo celé číslo lze jednoznačně (až na pořadí a přenásobení jednotlivých činitelů invertibilním prvkem) rozložit na součin Gaussových prvočísel.*

Důkaz je stejný jako v případě celých čísel, jen indukce se provádí podle Gaussovy normy.

Cvičení 14. Proč není rovnost $5 = (1+2i)(1-2i) = (2+i)(2-i)$ ve sporu s jednoznačným rozkladem na prvočísla?

Zamysleme se nad tím, jak můžou vypadat Gaussova prvočísla. Budou zjevně dvou typů – první z nich jsou obyčejná prvočísla, která se nerozkládají v Gaussových číslech (např. 3, 7 nebo 31), druhá budou prvočísla tvaru $a+bi$, kde jak a, tak b je nenulové. Podívejme se nyní blíže na prvočísla druhého typu a na jejich normu. Více řekne následující tvrzení:

Tvrzení. *Je-li $p = a+ib$, kde $a, b \in \mathbb{Z}$ jsou nenulová a p je Gaussovo prvočíslo, pak $N(p)$ je prvočíslo.*

Důkaz. Dokážeme tvrzení přímo. Definice říká, že kdykoliv máme x, y celá čísla taková, že $N(p) \mid xy$, pak $N(p) \mid x$ nebo $N(p) \mid y$.

V Gaussových číslech platí

$$p \mid N(p) \mid xy,$$

tedy z toho, že p je Gaussovo prvočíslo, víme, že $p \mid x$ nebo $p \mid y$. Nechť tedy BÚNO $p \mid x$. Protože x má nulovou imaginární část, platí $\overline{p} \mid \overline{x} = x$ a číslo $\overline{p}$ musí být také Gaussovo prvočíslo, neboť má stejné algebraické vlastnosti jako p.

Často nastane situace, že p a $\overline{p}$ jsou nesoudělná. Spočteme-li jejich největší společný dělitel, dostaneme $(a+ib, a-ib) = (a+ib, 2b)$.

Rozeberme dva případy. Když p je nesoudělné s 2, pak $(a+ib, 2b) = (a+ib, b) = (a, b)$, což je celé číslo, které dělí p, s normou ostře menší, než je norma p. Jediné takové číslo je 1. Vzhledem k tomu, že p a $\overline{p}$ jsou nesoudělná a obě dělí x, platí $N(p) = p \cdot \overline{p} \mid x$.

Zbývá dokázat tvrzení pro p soudělná s $2 = -i(1+i)^2$. Takové je ale pouze prvočíslo $p = 1+i$, pro které je tvrzení zřejmé, neboť $N(1+i) = 2$. $\square$

O něco snažší je popsat běžná prvočísla, která se nerozkládají v Gaussových číslech. Mějme nějaké takové kladné prvočíslo p. Víme, že p se nerozkládá v $\mathbb{Z}$. Předpokládejme, že p se je dělitelné nějakým Gaussovým prvočíslem $a+bi$, které není asociované s p. Pak ale $N(a+bi) \mid N(p) = p^2$ a $N(a+bi)$ je také kladné prvočíslo, tedy jedině $N(a+bi) = p$. Řešíme rovnici

$$a^2 + b^2 = p$$

s neznámými a, b v celých číslech. Podíváme-li se na situaci modulo 4, vidíme, že a^2 i b^2 mohou dávat zbytek 0 nebo 1, tedy možné zbytky pravé strany jsou 0, 1 a 2. Tedy pro prvočísla tvaru $4k+3$ nemá rovnice řešení, a tudíž jsou prvočísla tohoto tvaru Gaussovými prvočísly. O těch ostatních zatím rozhodnout neumíme, ale za chvilku dokážeme, že se všechna rozkládají. K tomu se nám bude hodit následující tvrzení.

Věta. *Je-li p prvočíslo v celých číslech a existuje-li $a \in \mathbb{Z}$ takové, že $p \mid a^2+1$, tedy kongruence $x^2+1 \equiv 0$ má řešení a, pak se prvočíslo p rozkládá v Gaussově oboru jako*

$$p = (p, a+i) \cdot (p, a-i),$$

přičemž $(p, a+i)$ a $(p, a-i)$ jsou Gaussova prvočísla.

Důkaz. Nejprve ukážeme, že platí rovnost $p = (p, a+i) \cdot (p, a-i)$. Tu snadno odvodíme ze vztahu

$$p = (p, a^2+1) = (p, (a+i) \cdot (a-i)) \mid (p, a+i)(p, a-i).$$

Čísla $a+i$ a $a-i$ se liší právě o $2i$, tedy jejich společný dělitel je rozhodně dělitelem dvojky. Díky tomu pro $p \neq 2$ víme, že dokonce $(p, a+i)(p, a-i) = (p, (a+i)(a-i)) = p$.

Pro $p = 2$ zdůvodníme situaci zvlášť. Řešeními kongruence $x^2+1 \equiv 0 \pmod 2$ jsou právě lichá čísla a. Chceme ukázat, že pro lichá a je $2 = (2, a+i)(2, a-i)$.

Platí $(2, a+i) = (2, a-i)$. Protože a je liché, je $(2, a+i) = (2, 1+i) = 1+i$. Přitom $(1+i)^2 = 2i$, tedy rovnost $2 = (2, a+i)^2 = (2, a+i)(2, a-i)$ opravdu platí (až na přenásobení invertibilním prvkem).

Dokážeme, že $(p, a-i)$ je Gaussovo prvočíslo. Nejprve spočteme $N((p, a-i))$. Zřejmě jsou čísla $(p, a-i)$ a $(p, a+i)$ komplexně sdružená, neboť p je celé a $\overline{a-i} = a+i$. Tedy

$$N((p, a-i)) = N((p, a+i)) = (p, a-i)(p, a+i) = p.$$

Nechť $x \mid (p, a-i)$, tedy $N(x) \mid N((p, a-i)) = p$, a norma x je 1 nebo p, neboť p je prvočíslo. V prvním případě je x invertibilní a v druhém platí $N(x) = N((p, a-i))$, tedy vzhledem k tomu, že $x \mid (p, a-i)$, víme, že $x \parallel (p, a-i)$. Dokázali jsme, že pokud $x \mid (p, a-i)$ a x není invertibilní, pak $x \parallel (p, a-i)$. Tedy $(p, a-i)$ je ireducibilní a je to prvočíslo. $\square$

Všimni si, že přechozí věta nám dává i návod, jak spočítat rozklad nějakého prvočísla (pokud existuje). Například prvočíslo 5 se rozkládá, neboť $2^2+1 \equiv 0 \pmod 5$, a jeho rozklad je

$$5 = (5, 2+i)(5, 2-i) = (2+i)(2-i).$$

Podobně třeba prvočíslo 13 se rozkládá, neboť $5^2+1 \equiv 0 \pmod{13}$. Jeden z činitelů v rozkladu je pak

$$(13, 5+i) = (3-2i, 5+i) = 3-2i,$$

druhý je s ním komplexně sdružený, tedy $13 = (3-2i)(3+2i)$.

Cvičení 15. Najděte rozklady prvočísel 29 a 401 v Gaussových celých číslech.

Zbývá nám poslední krok v charakterizaci Gaussových prvočísel, a sice jak poznat, že kongruence $x^2+1 \equiv 0 \pmod p$ má řešení. Totéž pro celá čísla jsme zkoumali v sekci o kvadratických zbytcích.

Kongruence má řešení pro všechna prvočísla tvaru $4k+1$, tedy tato prvočísla se rozkládají v Gaussově oboru. Prvočísla tvaru $4k+3$ se nerozkládají, to jsme dokázali samostatně na začátku. Osamoceně stojí prvočíslo 2, které se rozkládá jako $(1+i)^2$.

Uvedeme ještě jednu finální větu, která shrne naše poznatky.

Věta. *Gaussova prvočísla jsou právě jednoho z tvarů*

(1) *$a+ib$, kde $a^2+b^2 = p$ je 2 nebo prvočíslo tvaru $4k+1$,*
(2) *up, kde u je invertibilní a p je přirozené prvočíslo tvaru $4k+3$.*

Cvičení 16. Čísla tvaru $4k+3$ nikdy nejsou součtem dvou čtverců, to jsme dokázali současně s tím, že prvočísla tvaru $4k+3$ se nerozkládají. Může ale existovat číslo tvaru $4k+1$, které nelze zapsat jako součet dvou čtverců?

Cvičení 17. Rozložte číslo $8-6i$ na Gaussova prvočísla.

Úloha. Najděte všechna přirozená čísla x a y, která řeší rovnici

$$x^2+y^2=2009.$$

Řešení. Rozklad pravé strany na prvočísla je $2009=7^2\cdot 41$, chtěli bychom ji rozložit na Gaussova prvočísla. V případě prvočísla 7 je to snadné, 7 je tvaru $4k+3$, tedy je to Gaussovo prvočíslo. Avšak prvočíslo 41 je tvaru $4k+1$, takže se bude rozkládat.

Platí $41 \mid 9^2+1=82$. Tedy 41 se rozkládá na $(41,9+i)\cdot(41,9-i)$. Spočteme jeden z těchto největších společných dělitelů

$$(41,9+i)=(5-4i,9+i)=(4+5i,9+i)=(4+5i,5-4i)=4+5i$$

Tedy $41=(4+5i)(4-5i)$.

Upravme konečně rovnici do tvaru

$$(x+iy)(x-iy)=7^2(4+5i)(4-5i).$$

Máme-li rozklad součinu $(x+iy)(x-iy)$ na Gaussova prvočísla, zbývá si uvědomit, že čísla $x+iy$ a $x-iy$ jsou komplexně sdružená, což nám velmi omezí možnost volby. Když nezapomeneme na invertibilní prvky, dostaneme pro $x+iy$ celkem osm možností

$$\pm 7(4+5i),\ \pm 7i(4+5i),\ \pm 7(4-5i) \text{ a } \pm 7i(4-5i).$$

Úloha má tedy osm řešení, jimiž jsou dvojice

$$(x,y)=(\pm 35,\pm 28) \text{ a } (\pm 28,\pm 35).$$

Úloha 18. (MO 56, domácí kolo A) Najděte všechny dvojice (x,y) přirozených čísel, pro něž platí

$$x^2+y^2=2005(x-y).$$

Při řešení některých úloh pomocí Gaussových celých čísel se nám bude hodit tvrzení o mocninách, jak je uvedeno v kapitole o dělitelnosti v celých číslech. Zopakujme si ho ještě jednou v Gaussových celých číslech, tentokrát již bez důkazu. Důkaz je stejný jako u celých čísel.

Tvrzení. (o mocninách) *Buď n přirozené, $a,b\in\mathbb{Z}[i]$ nesoudělná a $c\in\mathbb{Z}[i]$ libovolné a nechť platí $ab=c^n$. Pak a i b jsou n-té mocniny až na přenásobení invertibilním prvkem. Tedy existují x, y a $k\in\{0,1,2,3\}$, že $a=i^kx^n$ a $b=i^{-k}y^n$.*

Úloha. Nalezněte všechna celá čísla x,y, která splňují rovnici

$$x^2+1=y^3.$$

Řešení. Nejdříve si rozložíme levou stranu rovnice:

$$(x+i)(x-i)=y^3.$$

V tuto chvíli bychom chtěli použít tvrzení, bohužel ale nevíme, jestli jsou $x+i$ a $x-i$ nesoudělná. Rozhodně však platí $(x+i, x-i) = (x+i, 2i) \mid 2i = (1+i)^2$, tedy máme celkem tři možnosti pro největšího společného dělitele.

Je-li $(x+i, x-i) = 1$, můžeme použít tvrzení. Než to uděláme, uvědomíme si, že každý invertibilní prvek můžeme napsat jako třetí mocninu ($i = (-i)^3$, $-1 = (-1)^3$, atd.), tedy se nemusíme zabývat invertibilními prvky a víme, že

$$(x+i) = (a+bi)^3 = a^3 + ia^2b - ab^2 - ib^3 = (a^3 - ab^2) + i(a^2b - b^3)$$

pro nějaká celá a, b. Srovnáním imaginárních částí dostaneme

$$a^2b - b^3 = (a-b)(a+b)b = 1.$$

Všichni činitelé jsou celočíselní dělitelé čísla 1, tedy musí být rovni ± 1. Speciálně $b = \pm 1$. Čísla $a-b$ a $a+b$ se liší o 2 a obě jsou ± 1, což znamená, že jedno z nich je 1 a druhé -1, každopádně však $a = 0$. Rovnice tak můžeme upravit do tvaru $-b^3 = 1$, odkud už je vidět, že $b = -1$. Máme tedy $x + i = (0 - 1i)^3 = (-i)^3 = i$ a $x = 0$, z čehož vyplývá, že $y^3 = 1$ a $y = 1$.

Zbývá nám ověřit, jestli může nastat $(x+i, x-i) > 1$, tedy $1+i \mid x+i$ i $x-i$. Pak ale $-i(1+i)^2 = 2 \mid (x+i)(x-i) = y^3$, tedy dokonce $8 \mid y^3 = x^2 + 1$. To ale v celých číslech nastat nemůže, neboť pak by x muselo být liché a x^2 by po dělení 8 dávalo zbytek 1.

Dohromady máme jediné, triviální řešení $x = 0$ a $y = 1$.

Úloha 19. Najděte všechny dvojice celých čísel x, y takové, že x je liché a platí

$$x^2 + 4 = y^3.$$

Úloha 20. S využitím Gaussových čísel najděte všechny pythagorejské trojice celých čísel x, y a y. Tedy vyřešte diofantickou rovnici

$$x^2 + y^2 = z^2.$$

Eisensteinova celá čísla

Druhý způsob, jak definovat celá čísla v číslech komplexních, nám dávají Eisensteinova čísla. Podobně jako Gaussova čísla byla vlastně mřížovými body ve čtvercové mřížce v Gaussově rovině, Eisensteinova celá čísla jsou mřížové body v trojúhelníkové mřížce. Trojúhelníková mřížka přichází jak se spoustou zajímavých vlastností, které postupně objevíme, tak i s několika zákeřnostmi, o kterých si povíme.

Začněme definicí. Označme si ω jednu ze třetích odmocnin z jedné, a to

$$\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2} i.$$

Každé číslo tvaru $a + \omega b$, kde $a, b \in \mathbb{Z}$, nazveme *Eisensteinovým celým číslem*[31]. Množinu všech Eisensteinových čísel označíme $\mathbb{Z}[\omega]$.

Nejtěžší věc, na kterou si budeš muset zvyknout, je způsob, jakým se s těmito čísly počítá. Platí totiž $\omega^2 = -\omega - 1$ (trochu horší vztah, než $i^2 = -1$, že?), tedy součin dvou Eisensteinových čísel je

$$(a + b\omega)(c + d\omega) = (ab - bd) + (bc + ad - bd)\omega.$$

[31] angl. Eisenstein integer

Velmi často budeme užívat také vztahů $\omega^3 = 1$ a $\omega^2 + \omega = -1$. Ještě se podívejme na komplexní sdružení, které můžeme vyjádřit jako

$$\overline{a + b\omega} = a + b\omega^2 = (a - b) - b\omega.$$

Podobně jako v Gaussových číslech definujeme *Eisensteinovu normu* čísla $a + b\omega$ jako

$$N_\omega(a + b\omega) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2.$$

Také zde platí, že $N_\omega(x) = x \cdot \overline{x} = |x|^2$, tedy norma je vždy nezáporná, přičemž nulová je pouze pro $x = 0$. Ještě připomeneme, že pokud $x \mid y$ v Eisensteinových číslech, pak $N_\omega(x) \mid N_\omega(y)$, zejména je-li $y \neq 0$, pak $N_\omega(x) \leq N_\omega(y)$.

Tam, kde nebude hrozit, že by došlo k záměně, budeme psát pouze $N(x)$ místo $N_\omega(x)$.

Invertibilních prvků v Eisensteinových celých číslech je ještě více než v Gaussových číslech. Jsou to všechna Eisensteinova čísla s normou 1, tedy k jejich nalezení vyřešíme rovnici

$$a^2 - ab + b^2 = 1.$$

Mohou nastat dvě možnosti. Buď mají a a b stejné znaménko, nebo mají opačné znaménko. V prvním případě můžeme navíc předpokládat, že jsou obě nenulová. Rovnici upravíme do tvaru

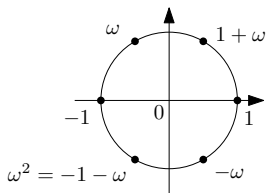
$$(a - b)^2 + ab = 1,$$

odkud vidíme, že všechny členy na levé straně jsou nezáporné a $ab > 0$, tedy jediná možnost je $ab = 1$ a $a = b$. Máme tak invertibilní čísla $1 + \omega$ a $1 - \omega$.

V druhém případě si rovnici upravíme do tvaru

$$(a + b)^2 - 3ab = 1.$$

Přitom $1 \geq -3ab \geq 0$, tedy $-3ab = 0$, a víme, že jeden z koeficientů musí být nulový. Ze vztahu $(a + b)^2 = 1$ odvodíme, že druhý koeficient je ± 1. Čísla ± 1 a $\pm\omega$ jsou tedy také invertibilní. Máme celkem šest invertibilních prvků v $\mathbb{Z}[\omega]$, které si můžeme znázornit na jednotkové kružnici. Jsou to právě všechny šesté odmocniny z jedné.



Věta. (dělení se zbytkem) *Jsou-li x, y Eisensteinova celá čísla, pak existují $q, r \in \mathbb{Z}[\omega]$, $N(r) < N(y)$, taková, že*

$$x = qy + r.$$

Důkaz pouze naznačíme. Postup je obdobný jako u Gaussových čísel, ale tentokrát tvoří násobky čísla y trojúhelníkovou mřížku a naším cílem je pokrýt rovnostranný trojúhelník kruhy se středy ve vrcholech a poloměry rovnými délce strany.

Euklidův algoritmus tu vypadá stejně jako v Gaussových číslech, stačí nám zaručit, že normy budou postupně klesat. Spočtěme tedy na ukázku největšího společného dělitele čísel 13 a $6+8\omega$.

$$\begin{aligned} 13 &= -\omega(6+8\omega) + (5-2\omega) \\ 6+8\omega &= \omega(5-2\omega) + (4+\omega) \\ 5-2\omega &= (1-\omega)(4+\omega) + 0 \end{aligned}$$

Platí $(13, 6+8\omega) = 4+\omega$.

Cvičení 21. Najděte největšího společného dělitele $(7+14\omega, 4-2\omega)$.

Konečně zde máme opět větu o dělení se zbytkem a všechny její důsledky, Bézoutovu větu a větu o jednoznačném rozkladu na prvočinitele. Důkazy jsou velmi podobné těm již provedeným, a tedy je už nebudeme opakovat.

Věta. (Bézoutova) *Jsou-li $a, b \in \mathbb{Z}[\omega]$, pak existují Eisensteinova celá čísla x, y, že platí*

$$ax + by = (a, b).$$

Eisensteinovým prvočíslem nazveme Eisensteinovo celé číslo p, které není invertibilní, a kdykoliv $p \mid ab$ (a, $b \in \mathbb{Z}[\omega]$), pak $p \mid a$ nebo $p \mid b$. Stejně jako v Gaussově oboru lze ekvivalentně říct, že p je ireducibilní.

Věta. (o rozkladu na prvočinitele) *Každé Eisensteinovo celé číslo a se rozkládá jednoznačně (až na pořadí a invertibilní prvky) na součin Eisensteinových prvočísel. Tedy existují Eisensteinova prvočísla $p_1, p_2, \ldots, p_k$, že $a = p_1 p_2 \cdots p_k$, a kdykoliv $a = q_1 q_2 \cdots q_l$ pro Eisensteinova prvočísla q_i, $0 < i \leq l$, pak $l = k$ a při vhodném očíslování $p_i \parallel q_i$ pro každé i.*

Dále nás bude zajímat, jak poznat Eisensteinovo prvočíslo. Situace je zde velmi podobná jako v Gaussových číslech. Některá běžná prvočísla se budou rozkládat, některá ne a na výjimečné pozici prvočísla 2 bude tentokrát prvočíslo 3, protože v Eisensteinově oboru můžeme odmocnit číslo -3, vskutku

$$(1+2\omega)^2 = 1 + 4\omega + 4\omega^2 = 1 - 4 = -3.$$

Tedy prvočíslo 3 se rozloží jako $3 = -(1+2\omega)^2$. Všimni si, že $1+2\omega$ je Eisensteinovo prvočíslo, neboť žádné neinvertibilní číslo s menší normou ho nedělí (žádné takové ani není).

Tvrzení. *Je-li $p = a + b\omega$ Eisensteinovo prvočíslo, pak buď p je asociované s nějakým běžným prvočíslem, nebo $N(p)$ je prvočíslo.*

Důkaz. Předpokládejme, že $p = a + b\omega$ je Eisensteinovo prvočíslo, které není asociované s běžným prvočíslem. Platí, že $\overline{p} = (a-b) - b\omega$ je také Eisensteinovo prvočíslo, neboť kdykoliv $\overline{p} \mid xy$, pak po komplexním sdružení dostaneme, že $p \mid \overline{x} \cdot \overline{y}$, tedy $p \mid \overline{x}$ nebo $p \mid \overline{y}$. Dalším komplexním sdružením dostaneme $\overline{p} \mid x$ nebo $\overline{p} \mid y$.

Platí $N(p) = p \cdot \overline{p}$. Předpokládejme navíc, že neplatí $p \parallel \overline{p}$ a dokažme, že $N(p)$ je prvočíslo. Nechť $N(p) \mid ab$ pro nějaká celá a, b. Pak

$$p \mid N(p) \mid ab$$

a p je Eisensteinovo prvočíslo, tedy $p \mid a$ nebo $p \mid b$. BÚNO $p \mid a$. Přitom a je celé, tedy $\overline{p} \mid \overline{a} = a$. Protože p a $\overline{p}$ jsou dvě neasociovaná, a tudíž nesoudělná prvočísla, dostáváme nakonec $N(p) = p \cdot \overline{p} \mid a$.

Zbývá vyšetřit, co se stane, když $p \parallel \overline{p}$, což nastane tehdy a jen tehdy, když $(p, \overline{p}) = p$. Počítejme:

$$(a + b\omega, (a - b) - b\omega) = (a + b\omega, -b - 2b\omega) = (a + b\omega, b(1 + 2\omega)).$$

Platí $(a + b\omega, b) = (a, b) = 1$, neboť (a, b) je celé číslo, které dělí p. Tedy

$$(p, \overline{p}) = (p, 1 + 2\omega).$$

Jediná možnost tedy je, že $p \parallel 1 + 2\omega$, a proto $N(p) = N(1 + 2\omega) = 1 - 2 + 4 = 3$, což je běžné prvočíslo. $\square$

Tvrzení. *Je-li p nezáporné prvočíslo tvaru $3k + 2$, pak p je také Eisensteinovo prvočíslo.*

Důkaz. Dokážeme, že takové p je v Eisensteinově oboru ireducibilní. Nechť tedy $a + b\omega$ je Eisensteinovo prvočíslo, které dělí p a není asociované s p. Pak nutně platí, že $N(a + b\omega) = a^2 - ab + b^2 = p$, neboť norma je nezáporné prvočíslo v $\mathbb{Z}$, které dělí prvočíslo p.

Ovšem rovnice $a^2 - ab + b^2 = 3k + 2$ nemá v celých číslech řešení, neboť vynásobíme-li ji čtyřmi a upravíme modulo 3, dostaneme

$$(2a - b)^2 + 3b^2 = 4a^2 - 4ab + 4b^2 \equiv 2 \pmod 3,$$

tedy $(2a - b)^2 \equiv -1 \pmod 3$, ale -1 není kvadratickým zbytkem modulo 3. $\square$

Už tedy víme, že prvočísla tvaru $3k + 2$ se nerozkládají. Nyní dokážeme, že prvočísla tvaru $3k + 1$ se rozkládají, o čemž svědčí například rozklad $7 = (1 - 2\omega)(3 + 2\omega)$. To bude trochu obtížnější, zato však velmi podobné důkazu tvrzení, že prvočísla tvaru $4k + 1$ se rozkládají v Gaussových číslech.

Věta. *Je-li p prvočíslo takové, že kongruence $x^2 + x + 1 \equiv 0$ má řešení a modulo p, pak se p rozkládá v Eisensteinových číslech jako*

$$p = (p, a - \omega)(p, \overline{a - \omega})$$

a obě čísla $(p, a - \omega)$ a $(p, \overline{a - \omega})$ jsou Eisensteinova prvočísla.

Důkaz. Důkaz této věty pouze naznačíme. Provede se podobně jako důkaz obdobné věty z Gaussových čísel.

Nejdříve ukážeme, že platí rovnost $p = (p, a - \omega)(p, \overline{a - \omega})$. Rozebereme dvě možnosti. V první řadě vezmeme prvočísla, která nejsou dělitelná $1 + 2\omega$, což jsou všechna prvočísla p kromě 3. V tomto případě jsou oba činitelé nesoudělní. Pro druhou možnost, $p = 3$, se rovnost dokáže přímo. Nakonec zbyde ověřit, že $(p, a - \omega)$ je prvočíslo s normou p.

Detaily důkazu si můžeš rozmyslet jako (poněkud obtížné) cvičení.

Například budeme-li chtít rozložit prvočíslo 13, můžeme postupovat tak, že budeme hledat řešení kongruence $x^2 + x + 1 \equiv 0 \pmod{13}$. Zkusíme několik malých zbytků. Zbytky 1 ani 2 rozhodně řešením nejsou, ale už $3^2 + 3 + 1$ dává součet 13, takže 3 řešením je. Víme tedy, že $13 = (13, 3 - \omega)(13, 4 + \omega)$. Přitom platí

$$(3 - \omega)(4 + \omega) = 12 - \omega - \omega^2 = 13,$$

tedy musí být $(13, 3 - \omega) = 3 - \omega$ a máme rozklad $13 = (3 - \omega)(4 + \omega)$.

Je užitečné si uvědomit, že k rozkladu prvočísla na Eisensteinova prvočísla nám stačí spočítat jen jednoho činitele, neboť ten druhý bude k němu komplexně sdružený. Opravdu platí $\overline{3-\omega} = 4+\omega$.

Cvičení 22. Rozložte prvočísla 19, 31 a 421 na Eisensteinova prvočísla.

K dokončení charakterizace Eisensteinových prvočísel už nám chybí jen dokázat, že kongruence $x^2+x+1 \equiv 0$ má řešení modulo p pro nezáporné prvočíslo $p = 3k+1$. Z kapitoly o kvadratických zbytcích víme, že pro taková čísla je -3 kvadratický zbytek (připomínáme, že -3 se dá v Eisensteinových číslech odmocnit).

Upravujme tedy zadanou kongruenci, všechny úpravy budou ekvivalentní.

$$\begin{aligned} x^2+x+1 &\equiv 0 \pmod{p} \\ 4x^2+4x+4 &\equiv 0 \pmod{p} \\ (2x+1)^2 &\equiv -3 \pmod{p} \end{aligned}$$

Je-li $b^2 \equiv -3$, řešíme rovnici $2x+1 \equiv b \pmod{p}$. Upravíme ji přenásobením $(p+1)/2$:

$$\begin{aligned} x+\frac{p+1}{2} &\equiv \frac{p+1}{2}b \pmod{p} \\ x &\equiv \frac{p+1}{2}(b-1) \end{aligned}$$

Našli jsme tedy řešení x, čímž jsme dokázali, že prvočísla tvaru $3k+1$ se rozkládají na součin dvou Eisensteinových prvočísel. Konečně můžeme zformulovat závěrečnou větu.

Věta. *Eisensteinova prvočísla jsou právě jednoho z tvarů*

(1) $a+\omega b$, *kde* $a^2-ab+b^2 = p$ *je* 3 *nebo prvočíslo tvaru* $3k+1$,
(2) up, *kde* u *je invertibilní a* p *je kladné prvočíslo tvaru* $3k+2$.

Cvičení 23. Rozložte Eisensteinovo číslo $9-15\omega$ na Eisensteinova prvočísla.

Úloha. Najděte všechny dvojice celých čísel x, y splňujících rovnici

$$(x+y)^2 = xy + 2011.$$

Řešení. Upravíme si rovnici do tvaru

$$x^2+xy+y^2 = 2011$$

a rozložíme

$$(x-\omega y)(x+(1+\omega)y) = 2011.$$

Zbývá rozložit pravou stranu na Eisensteinova prvočísla. Číslo 2011 je prvočíslo a po dělení třemi dává zbytek 1, tedy se rozkládá na součin dvou Eisensteinových prvočísel. Nyní potřebujeme nalézt aspoň jedno řešení kongruence

$$x^2+x+1 \equiv 0 \pmod{2011}.$$

K tomu můžeme použít třeba počítač. Zjistíme, že nejmenší celočíselné řešení je 205, a tedy platí, že prvočíslo v rozkladu 2011 je

$$(2011, 205-\omega) = (-39+10\omega, 205-\omega).$$

Přitom $N(-39+10\omega) = 39^2 + 39\cdot 10 + 10^2 = 2011$. Tedy roklad 2011 je

$$2011 = (-39+10\omega)(-49-10\omega).$$

Může nastat celkem 12 možností, prvních šest je $x - \omega y = \varepsilon(-39+10\omega)$, dalších šest pak $x - \omega y = \varepsilon(-49-10\omega)$, kde ε je jeden ze šesti invertibilních prvků. Uvědomíme-li si, že můžeme prohodit x a y a u obou čísel změnit znaménko, stačí nám vlastně spočítat jen tři možnosti:

$$\begin{aligned} x - y\omega &= -39+10\omega, \\ x - y\omega &= (1+\omega)(-39+10\omega) = -49-39\omega, \\ x - y\omega &= \omega(-39+10\omega) = -10-49\omega, \end{aligned}$$

Úloha má celkem dvanáct řešení. Zapíšeme-li je jako neuspořádané dvojice, budou to $\{x,y\} = \{39,10\}$, $\{-39,-10\}$, $\{49,-39\}$, $\{-49,39\}$, $\{49,-10\}$ a $\{-49,10\}$.

Úloha. Dokažte, že je-li $p = 3k+1$ prvočíslo, pak existuje jednoznačný zápis $p = a^2 + 3b^2$, kde a a b jsou nezáporná celá čísla.

Řešení. Víme, že prvočíslo $p = 3k+1$ se rozkládá v Eisensteinově oboru na součin dvou prvočísel, tj.

$$p = (x - \omega y)(x + y + \omega y).$$

Stejně tak se rozkládá i výraz

$$a^2 + 3b^2 = (a - (1+2\omega)b)(a + (1+2\omega)b) = (a - b - 2b\omega)(a + b + 2b\omega).$$

Je-li y kladné a sudé, z předchozího vztahu dostáváme $y = 2b$, $a - b = x$ a $a + b = x + y$. Vyřešíme soustavu tří rovnic o dvou neznámých a a b, řešením je $b = y/2$ a $a = x + y/2$, pokud $x > -y/2$, jinak $a = -x - y/2$.

Pro ostatní případy musíme najít lepší rozklad prvočísla p. Víme ovšem, že rozklad je jednoznačný až na asociovanost činitelů, tedy můžeme pouze přenásobovat závorky jedním z šesti invertibilních prvků v $\mathbb{Z}[\omega]$. Všimni si, že všechny invertibilní prvky jsou mocninami $1+\omega$, např. $\omega = (1+\omega)^2$. Podívejme se tedy, co se stane s činitelem $x - y\omega$ po přenásobení $(1+\omega)$:

$$(x - y\omega)(1+\omega) = (x+y) + x\omega \qquad (\star\star)$$

Pokud je x kladné a sudé, máme také řešení. Stačí položit $b = x/2$ a a dopočítat jako v předchozím případě.

Zbývá nejnepříjemnější situace, kdy jsou obě čísla x a y lichá. Pak se ale ještě jednou podívejme na vzoreček $(\star\star)$. Číslo $x+y$ je sudé, zvolíme tedy $x' = x+y$ a $y' = x$, čímž převedeme situaci na již rozebraný případ. Přenásobením $1+\omega$ pak dostaneme opět koeficient u ω sudý.

Jediný problém bychom mohli mít se znaménky, ten se ale snadno vyřeší přenásobíme $x - y\omega$ číslem -1.

Zatím jsme dokázali, že úloha má alespoň jedno řešení, které ovšem ještě zdaleka nemusí být jednoznačné. Dokažme tedy jednoznačnost. Buďte a a b kladná čísla taková, aby platilo $a^2 + 3b^2 = p$. Opět zvolme rozklad $p = (x - y\omega)(x + y + y\omega)$. Vzhledem k jednoznačnosti rozkladu musí platit jedna z dvanácti rovností

$$\begin{aligned} (a + b + 2\omega b) &= (x - y\omega)(1+\omega)^k, \\ (a + b + 2\omega b) &= (x + y + y\omega)(1+\omega)^k, \end{aligned}$$

kde $k = 0, 1, \ldots 5$. Ukážeme, že nejvýše jedna z těchto rovností může být splněna. Připomeňme, že obě čísla a i b jsou kladná (ani jedno nemůže být nulové, neboť pak by p nebylo prvočíslo). Napišme si tedy pravé strany těchto rovností:

$$\pm(x - y\omega),\ \pm((x + y) + x\omega),\ \pm(y + (x + y)\omega),$$
$$\pm((x + y) + y\omega),\ \pm(x + (x + y)\omega),\ \pm(-y + x\omega).$$

Dokažme, že právě jedno z čísel x, y a $x + y$ je sudé. Rozhodně nemohou být sudá obě čísla x a y, protože pak by $p = x^2 + xy + y^2$ bylo sudé prvočíslo tvaru $3k + 1$, a takové neexistuje. Zbývá tedy ukázat, že je-li jedno z čísel x a y sudé a druhé liché, pak $x + y$ je liché, a že jsou-li obě čísla x a y lichá, pak $x + y$ je sudé, což je zřejmé.

Zbydou nám pouze čtyři pravé strany, a to ty, které mají u ω sudý koeficient. Například je-li y sudé, pak možné pravé strany jsou

$$(x - y\omega),\ (-x + y\omega),\ ((x + y) + y\omega) \text{ a } (-(x + y) - y\omega).$$

Navíc víme, že b musí být kladné, což nám vyloučí ještě další dvě závorky se záporným koeficientem. Je-li například y záporné a sudé, zbydou závorky

$$(x - y\omega) \quad \text{a} \quad (-(x + y) - y\omega).$$

Dopočítejme a, pokud nastane rovnost v prvním či druhém případě:

$$a = \begin{cases} x + y/2, & \text{když } (a + b + 2b\omega) = (x - y\omega), \\ -(x + y) + y/2 = -x - y/2, & \text{když } (a + b + 2b\omega) = ((x + y) - y\omega). \end{cases}$$

všimni si, že tyto dvě hodnoty mají stejnou velikost a opačné znaménko, tedy jen jedna z nich může být kladná. Stejná situace nastane i u všech (šesti) ostatních případů, a to proto, že $a^2 + 3b^2 = (-a)^2 + 3b^2$. veškeré podmínky, které jsme zatím použili jsme použili kvůli b, takže nutně i výraz

$$(-a + b) + 2\omega b$$

musí nabývat jedné ze dvou zatím nevyloučených hodnot. Rozhodně platí $(a + b) + 2\omega \neq (-a + b) + 2\omega$, tedy jsme vyloučili poslední závorku a zbyla nám už jen jediná, což jsme chtěli dokázat.

Úloha 24. Najděte všechny trojice celých čísel (x, y, z) splňujících

$$x^2 - xy + y^2 = 2^z.$$

… a další imaginární teorie

V poslední krátké kapitole si ukážeme, jak lze v teorii čísel využít kvaterniony. Kvaterniony jsou taková „komplexní čísla na druhou“, mají tři imaginární jednotky a velmi nepříjemnou vlastnost, že *nejsou komutativní*, tj. neplatí $ab = ba$ pro každé a a b.

Nejprve si definujme imaginární jednotky v kvaterninonech. Buďte i, j a k formální symboly pro imaginární jednotky. Definujeme operaci $\cdot$ na množině $\{\pm 1, \pm i, \pm j, \pm k\}$ tak, aby splňovala

$$i^2 = j^2 = k^2 = ijk = -1,$$

přičemž 1 a -1 se chovají obvykle, tedy $1 \cdot a = a$ pro každé a a $(-1)^2 = 1$, $-1 \cdot i = i \cdot -1 = -i$, $-1 \cdot j = -j$, atd. Z těchto vztahů si můžeš odvodit všechny součiny.

Pro jistotu uvádíme tabulku pro násobení, tedy vlastně jen její část, neboť zbytek se odvodí snadno. Pokud násobíme dvě čísla s různými znaménky, musíme v tabulce znaménko změnit, pokud se stejnými, necháváme stejné znaménko součinu.

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Všimni si, že pro imaginární jednotky platí $ij = -ji$, $ik = -ki$ a $jk = -kj$.

Cvičení 25. Spočtěte jik.

Nyní umíme násobit komplexní jednotky. To už je prakticky všechno, co potřebujeme k tomu, abychom mohli definovat kvaterniony.

Kvaternionem rozumíme čtyřčlen $a_1 + a_2 i + a_3 j + a_4 k$. Sčítání kvaternionů definujeme jako

$$(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k) = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k$$

a násobení kvaternionů jako násobení polynomů s proměnnými i, j a k za použití tabulky uvedené výše, tj.

$$\begin{aligned}(a_1 + a_2 i + a_3 j + a_4 k) \cdot (b_1 + b_2 i + b_3 j + b_4 k) = \\ = (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) + (a_1 b_2 + a_2 b_1 + a_4 b_3 - a_3 b_4)i + \\ + (a_1 b_3 + a_3 b_1 + a_4 b_2 - a_2 b_4)j + (a_1 b_4 + a_4 b_1 + a_2 b_3 - a_3 b_2)k.\end{aligned}$$

Množina všech kvaternionů se obvykle značí $\mathbb{H}$.[32]

K čemu se taková věc hodí? Podobně jako jsme definovali Gaussova celá čísla, můžeme definovat kvaterniony s celočíselnými koeficienty – *Lipshitzova celá čísla* jsou kvaterniony tvaru $a + bi + cj + dk$, kde a, b, c a d jsou celá čísla. Množinu všech takových čísel budeme značit $\mathbb{Z}[i, j, k]$.

Definujeme si i jejich normu jako

$$N_L(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2.$$

Všimni si, že i pro tuto normu je $N(xy) = N(x)N(y)$ pro každé $x, y \in \mathbb{Z}[i, j, k]$, což se snadno odvodí ze vztahu

$$N(a + bi + cj + dk) = N(a - bi - cj - dk) = (a + bi + cj + dk)(a - bi - cj - dk).$$

Už jen z této úvahy umíme dokázat následující lemmátko.

Lemma. *Jsou-li a a b celá čísla, která lze napsat jako součet čtyř čtverců celých čísel, pak i číslo ab lze napsat jako součet čtyř čtverců celých čísel.*

[32] Objevil je a poprvé popsal irský matematik William Rowan Hamilton.

Důkaz. Stačí si uvědomit, že číslo a lze zapsat jako součet čtverců čísel a_1, a_2, a_3 a a_4, právě když je normou Lipschitzova celého čísla $q_a = a_1 + a_2 i + a_3 j + a_4 k$. Podobně označme q_b Lipshitzovo celé číslo, že $N(q_b) = b$. Pak zřejmě $N(q_a q_b) = ab$, a tedy celá čísla, která hledáme, jsou právě koeficienty Lipschitzova čísla $q_a q_b$. $\square$

Toto lemmátko je užitečné například pro důkaz slavné Lagrangeovy věty o čtyřech čtvercích, díky němu se totiž můžeme omezit jen prvočísla x.

Věta. (Lagrangeova věta o čtyřech čtvercích) *Je-li x libovolné přirozené číslo, pak existují celá čísla a, b, c a d taková, že*

$$x = a^2 + b^2 + c^2 + d^2.$$

Důkaz je složitý a vynecháme ho.

Všimni si však, že o prvočíslech tvaru $4k + 1$ umíme na základě teorie o Gaussových číslech dokázat, že jsou součtem dokonce dvou čtverců, a o prvočíslech tvaru $3k + 1$ umíme z teorie o Eisensteinových číslech dokázat, že jsou tvaru $a^2 + 3b^2$, a tedy jsou součtem čtyř čtverců (z nichž tři jsou stejné). Lagrangeovu větu tedy neumíme dokázat pouze pro prvočísla tvaru $12k + 11$.

Například platí

$$2 = 1^2 + 1^2 + 0^2 + 0^2, \quad 5 = 1^2 + 2^2 \quad \text{a} \quad 7 = 2^2 + 3 \cdot 1^2.$$

Cvičení 26. Dokažte, že čísla tvaru $4^{m-1}(8k + 7)$ pro k a m přirozená nelze napsat jako součet pouze tří čtverců celých čísel (tedy že čtyři je opravdu nejmenší možný počet čtverců, který potřebujeme).

Problémové úlohy

V poslední kapitole ti přinášíme problémové (těžké) úlohy k zamyšlení. Jsou to úlohy, ke kterým se může hodit znát něco z teorie, kterou jsme vyložili v tomto díle seriálu, avšak někdy ani to nebude stačit (jako v případě předposlední a poslední úlohy) a budeš se muset zamyslet nad vlastní teorií nebo vymyslet jiný trikový způsob.

Úloha 27. Dokažte, že následující dvě rovnice nemají žádné netriviální celočíselné řešení (x, y, z). Netriviálním řešením se myslí takové trojice, že všechna tři čísla jsou nenulová.

$$x^3 + y^3 = z^3$$
$$x^4 + y^4 = z^2$$

Úloha 28. Je-li p prvočíslo, řešte rovnici

$$y^2 + 1 = x^p$$

v celých číslech.

Úloha 29. Najděte všechna celá čísla x, y splňující

$$y^6 = x^5 + 1.$$

Úloha 30. Řešte v celých číslech rovnici

$$3x^2 + 1 = y^2.$$

Úloha 31. Najděte všechny dvojice celých čísel (x, y), která splňují

$$x^2 = y^3 + 1.$$

Úloha 32. Najděte všechny dvojice (x, y) celých čísel splňujících

$$x^2 + 3 = y^5.$$

Úloha 33. Řešte v celých číslech

$$x^2 + 2 = y^3.$$

Úloha 34. Dokažte, že neexistují taková celá čísla x a y, že

$$x^2 + 5 = y^3.$$

Seriál IV. – Závěr

V prvních třech dílech seriálu jsme se věnovali několika kapitolám o komplexních číslech, ovšem ani obsah těchto pár témat jsme zdaleka nevyčerpali, komplexní čísla jsou hlubokou a zajímavou tematikou, na kterou jistě budeš při studiu matematiky znova a znova narážet. Doufáme, že jsme Ti je v tomto seriálu přiblížili natolik, že se k nim budeš uchylovat i v případě, kdy se nevyskytují v zadání problému, protože vybočením z krabice (oboru reálných čísel) si často umíme cestu zkrátit nebo alespoň zjednodušit.

Dnes na závěr si na malém prostoru řekneme něco o ještě imaginárnějších oborech, než jsou komplexní čísla, a uvedeme si seznam užitečné literatury, kde můžeš najít něco více o komplexních číslech a použitých metodách.

Další imaginární teorie ...

V předchozím díle seriálu jsme si zadefinovali kvaterniony, tedy jakási čtyřrozměrná komplexní čísla se třemi imaginárními jednotkami. Zopakujeme ještě jejich definici

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\},$$

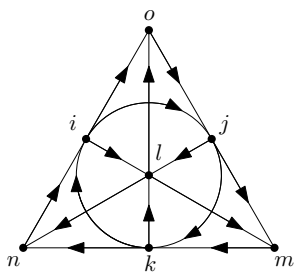
přitom i, j a k jsou komplexní jednotky, které splňují $i^2 = j^2 = k^2 = ijk = -1$. Pokud si vzpomínáš, kvaterniony nejsou komutativní, například $ij = k = -ji$.

Dá se však pokročit ještě dál, to se dostaneme k tzv. *oktonionům*. Oktoniony mají komplexních jednotek sedm: i, j, k, l, m, n, o. Jsou to tedy čísla tvaru

$$a + bi + cj + dk + el + fm + gn + ho,$$

kde a, b, ... , h jsou reálná čísla. Jejich násobení už je ale hodně ošklivá operace a nesplňuje ani asociativitu, tj. obecně neplatí, že $x(yz) = (xy)z$.

Jak se ale takové obludy násobí? Čísla i, j, ... jsou komplexní jednotky, tedy platí $i^2 = j^2 = \cdots = h^2 = -1$. To, jak se násobí mezi sebou, nám prozradí následující obrázek:



Chceme-li vynásobit dvě jednotky, najdeme si je na obrázku a najdeme čáru (kružnici nebo přímku), která je spojuje. Výsledkem je třetí jednotka na této čáře se znaménkem $+$, pokud vede šipka od prvního činitele k druhému, a se znaménkem $-$, pokud jsme šli proti směru šipky. Např. $ij = k$, $nk = -m$ a $on = i$.

Cvičení. Vynásob $(i + 2j - m) \cdot (k + 3o)$.

Řešení. $2i - 4j - 6m + 2n$.

Cvičení. Ukaž, že násobení není asociativní, tj. najdi oktoniony x, y a z, že $(xy)z \neq x(yz)$.

Na tomto místě by bylo záhodno říct, že dále se už postoupit nedá. Neexistuje žádné rozumné rozšíření oktonionů. Formálně o tom mluví Hurwitzova věta. Formulujeme si ji trochu neformálně:

Věta. (Hurwitz) *Reálná čísla, komplexní čísla, kvaterniony a oktoniony jsou jediná čtyři rozšíření reálných čísel, ve kterých umíme sčítat, odčítat, násobit, dělit a měřit normu (absolutní hodnotu).*

Literatura

Nakonec uvádíme seznam literatury, na kterou jsme v seriálu odkazovali a z které jsme během psaní seriálu čerpali. Asi nejdůležitější inspirací pro nás byla kniha [AA], z níž vychází hlavně druhý díl seriálu, je psaná v angličtině, obsahuje mnohem širší obzory než to, co se vešlo do seriálu, a vřele ji doporučujeme ke studiu. Slabší českou obdobou této knihy je [R]. Třetí díl seriálu vycházel z práce [O_1] a hodně ji rozšířil.

[AA] Andreescu T., Andrica D., *Complex numbers A to ... Z*, Boston, 2006.

[KaOR] Kala V., Opršal J., Rolínek M., *Teorie čísel (seriál)*, Prase, Praha, 2009, *http://mks.mff.cuni.cz/archive/28/9.pdf.*

[Kl] Klazar M., *Introduction to Number Theory (lecture notes)*, 2006.

[KuHŠ] Kučera R., Herman J., Šimša J., *Metody řešení matematických úloh I.*, Masarykova Univerzita, Brno, 2001.

[O_1] Opršal J., Gaussovská prvočísla, Brno, 2006, *http://atrey.karlin.mff.cuni.cz/~snek/pub/matika/gaussovska_prvocisla.pdf.*

[O_2] Opršal J., Kvadratické zbytky, Sborník Rapotín (2007), 32–34, *http://mks.mff.cuni.cz/library/KvadratickeZbytkyJO/KvadratickeZbytkyJO.pdf.*

[R] Ráb M., *Komplexní čísla v elementární matematice*, Masarykova Univerzita, Brno, 1996.