ROZHLEDY
MATEMATICKO-PŘÍRODOVĚDECKÉ.

ROČNÍK 12 (1932/33). ČÍSLO 4.

Čísla Gaussova.

Vl. Knichal.

(Dokončení.)

Věta 2. Každé číslo Gaussovo α, pro něž $N(\alpha) > 1$, dá se rozložiti v součin Gaussových prvočísel, t. j. platí $\alpha = \pi_1 . \pi_2 \ldots \pi_n$, kde π_i je Gaussovo prvočíslo ($i = 1, 2, \ldots, n$, $n \geqq 1$, celé).

Důkaz provedeme úplnou indukcí vzhledem k $N(\alpha)$. Uvědomme si napřed: je-li α Gaussovo prvočíslo, naše věta je správná, není-li α Gaussovo prvočíslo, existují dvě Gaussova čísla α_1, α_2 taková, že platí

$$\alpha = \alpha_1\alpha_2, \quad N(\alpha_1) > 1, \quad N(\alpha_2) > 1;$$

tedy

$$1 < N(\alpha_1) < N(\alpha), \quad 1 < N(\alpha_2) < N(\alpha).$$

1. Buď $N(\alpha) = 2$. Pak je α Gaussovo prvočíslo; jinak by bylo $\alpha = \alpha_1\alpha_2$, kde α_1, α_2 by byla Gaussova čísla, pro něž $1 < N(\alpha_1) < < N(\alpha) = 2$, což je vyloučeno.

2. Buď $n \geqq 2$, celé. Předpokládejme, že máme naši větu již dokázánu pro všechna uvažovaná α, pro něž $N(\alpha) \leqq n$. Pak platí také, jestliže $N(\alpha) = n + 1$.

Buďto je totiž α Gaussovo prvočíslo, anebo platí $\alpha = \alpha_1\alpha_2$, kde α_1, α_2 jsou Gaussova čísla, pro něž $1 < N(\alpha_1) < N(\alpha) = n + 1$, $1 < N(\alpha_2) < N(\alpha) = n + 1$. Tedy můžeme psáti ($r \geqq 1$, celé, $s \geqq 1$, celé)

$$\alpha_1 = \pi_1\pi_2 \ldots \pi_r, \quad \alpha_2 = \pi'_1\pi'_2 \ldots \pi'_s,$$

kde $\pi_1, \pi_2, \ldots, \pi_r, \pi'_1, \pi'_2, \ldots, \pi'_s$ jsou Gaussova prvočísla. Pak

$$\alpha = \pi_1\pi_2 \ldots \pi_r\pi'_1\pi'_2 \ldots \pi'_s.$$

Věta 3. Buďte $r \geqq 1$, $s \geqq 1$, celá čísla. Nechť $\pi_1, \pi_2, \ldots, \pi_r$, $\pi'_1, \pi'_2, \ldots, \pi'_s$ jsou Gaussova prvočísla a nechť platí

$$\pi_1\pi_2 \ldots \pi_r = \pi'_1\pi'_2 \ldots \pi'_s.$$

Pak $r = s$ a systém čísel $\pi_1, \pi_2, \ldots, \pi_r$ je totožný až na pořadí a na jednotkové faktory (t. zn. Gaussovy jednotky) se systémem

$\pi'_1, \pi'_2, \ldots, \pi'_s$. (T. zn. při vhodném označení dolních indexů lze psáti $\pi_i = \varepsilon_i \pi'_i$, $i = 1, 2, \ldots, r$, kde $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ jsou Gaussovy jednotky.)

Důkaz provedeme úplnou indukcí vzhledem k r.*)

1. Buď $r = 1$. Nechť

$$\pi_1 = \pi'_1 \pi'_2 \ldots \pi'_s.$$

Kdyby $s \geqq 2$, dalo by se π_1 rozložiti v součin Gaussových čísel o normách větších než 1, což je vyloučeno. Tedy je $s = 1$ a $\pi_1 = \pi'_1$.

2. Buď $n \geqq 1$, celé. Předpokládejme, že naše věta platí pro všechna uvažovaná $r \leqq n$. Dokážeme si, že platí i pro $r = n + 1$. Nechť tedy

$$\pi_1 \pi_2 \ldots \pi_{n+1} = \pi'_1 \pi'_2 \ldots \pi'_s. \tag{6}$$

Postupným užitím věty 1. (součin $\pi'_1 \pi'_2 \ldots \pi'_s$ je dělitelný π_{n+1}) se přesvědčíme, že jedno z čísel $\pi'_1, \pi'_2, \ldots, \pi'_s$ je dělitelno π_{n+1}. Vhodným označením indexů docílíme toho, že je to právě π'_s. Tedy $\pi'_s = \varepsilon \pi_{n+1}$, kde ε je Gaussova jednotka. Po vykrácení obdržíme tudíž z (6)

$$\pi_1 \pi_2 \ldots \pi_n = (\varepsilon \pi'_1) \,.\, \pi'_2 \ldots \pi'_{s-1}.$$

Poněvadž naše věta je správná (podle předpokladu) pro $r = n$, je[5]) $s = n + 1$ a vhodným označením indexů lze docíliti toho, že

$$\pi_1 = \varepsilon'_1 (\varepsilon \pi'_1) = \varepsilon_1 \pi'_1, \ \pi_2 = \varepsilon_2 \pi'_2, \ldots, \pi_n = \varepsilon_n \pi_n,$$

při čemž $\varepsilon'_1, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ jsou Gaussovy jednotky.[6])

Důsledek. Z věty 2. a 3. plyne ihned důsledek, že každé číslo Gaussovo α, pro něž $\mathrm{N}(\alpha) > 1$, dá se až na jednotkové faktory (Gaussovy jednotky) jediným způsobem rozložiti v součin Gaussových prvočísel.

Dalším naším úkolem bude rozhodnouti, zda dané Gaussovo číslo α je Gaussovým prvočíslem, nebo ne. Nežli však odvodíme hledané kriterium, dokážeme si dvě pomocné věty.

Věta 4. Buď p liché prvočíslo. V této a následující větě bude S značiti systém čísel $1, -1, 2, -2, 3, -3, \ldots, \frac{1}{2}(p-1), -\frac{1}{2}(p-1)$.

Ke každému číslu a z S lze nalézti jediné číslo a' rovněž z S takové, že[7]) $aa' \equiv 1 \pmod{p}$.

Důkaz. Nejdříve je patrno, že každé celé číslo b nesoudělné s p je kongruentní s nějakým číslem z ze systému S podle modulu p.

---

[5]) $\varepsilon \pi'_1$ je rovněž Gaussovo prvočíslo.

[6]) $\pi_{n+1} = \varepsilon_{n+1} \pi'_s$, kde $\varepsilon_{n+1} = 1/\varepsilon$ platí již podle hořejšího.

[7]) Jsou-li a, b, p $(p \neq 0)$ celá čísla, znamená $a \equiv b \pmod{p}$ (čti a je kongruentní s b podle modulu p) totéž, co $p/(a-b)$. Snadno se přesvědčíme, že $a \equiv a$, je-li $a \equiv b$, je $b \equiv a$, je-li $a \equiv b$ a $b \equiv c$, je $a \equiv c$ a konečně je-li $a \equiv b$ a $c \equiv d$, je $a + c \equiv b + d$, $a - c \equiv b - d$, $ac \equiv bd$, vše podle téhož modulu p.

*) Bez újmy obecnosti lze předpokládati, že $r \leqq s$.

Určeme totiž celé číslo c tak, aby $|\,b - cp\,|$ bylo nejmenší. Klaďme $z = b - cp$. Pak je předně $z \equiv b \pmod{p}$, $z \neq 0$ (neboť jinak by p/b). Poněvadž $|\,b - cp\,|$ je minimální, je $|\,z\,| \leqq |\,z \pm p\,|$, tedy $z^2 \leqq (z \pm p)^2 = z^2 \pm 2zp + p^2$. Tudíž je $\mp 2zp \leqq p^2$ čili $|\,z\,| \leqq \frac{1}{2}p$ a z patří tedy do S.

Každé číslo ze systému R: $a, a^2, a^3, \ldots, a^p$ je kongruentní s jedním číslem ze systému S. Tento systém obsahuje však pouze $p - 1$ čísel. Tudíž existují dvě čísla a^r, a^s ($1 \leqq r < s \leqq p$; r, s celé) ze systému R taková, že

$$a^r \equiv a^s \pmod{p},$$

t. zn., že $p/a^r\,(1 - a^{s-r})$. Poněvadž $(a, p) = 1$, je $p/(1 - a^{s-r})$, t. zn. $a^{s-r} \equiv 1 \pmod{p}$ $(s - r \geqq 1)$. Buď a' ze systému S takové, že $a^{s-r-1} \equiv a' \pmod{p}$. Je tudíž $aa' \equiv 1 \pmod{p}$.

Kdyby kromě a' existovalo v S ještě číslo a'' takové, že $aa'' \equiv$ $\equiv 1 \pmod{p}$, bylo by $a\,(a' - a'') \equiv 0 \pmod{p}$ čili [ježto $(a, p) = 1$] $p/(a' - a'')$. Je však $|\,a'\,| < \frac{1}{2}p$, $|\,a''\,| < \frac{1}{2}p$ a tedy

$$|\,a' - a''\,| < \tfrac{1}{2}p + \tfrac{1}{2}p = p.$$

Tudíž $$a' = a''.$$

Věta 5. Buď p liché prvočíslo. Pak platí

$$[1 \,.\, 2 \,.\, 3 \ldots \tfrac{1}{2}(p - 1)]^2 \equiv (-1)^{\frac{1}{2}(p+1)} \pmod{p}.$$

Důkaz. Předpokládejme $p > 3$ (pro $p = 3$ věta je zřejmě správná). Buď a číslo z S, $|\,a\,| \neq 1$. Určeme a' z S tak, aby $aa' \equiv$ $\equiv 1 \pmod{p}$ (viz větu 4.). Pak $|\,a'\,| \neq 1$ (jinak by $|\,a\,| = 1$). Dále je $a \neq a'$, neboť jinak by $a^2 - 1$ bylo dělitelno p, čili buďto by bylo $a \equiv 1$, anebo $a \equiv -1 \pmod{p}$, t. j. bylo by $a = \pm 1$.

Do systému A zařaďme právě všechna čísla a z S, pro něž $|\,a\,| \neq 1$ a pro něž $a < a'$, kde a' je číslo svrchu určené. Nechť A sestává z těchto čísel (mezi sebou různých):

$$a_1, a_2, a_3, \ldots, a_r.$$

Buď a'_i $(i = 1, 2, \ldots, r)$ takové číslo z S, pro něž $a_i a'_i \equiv$ $\equiv 1 \pmod{p}$. Jsou tedy podle věty 4. čísla $a'_1, a'_2, a'_3, \ldots, a'_r$ vesměs mezi sebou různá. Označme tento systém A'. Žádné číslo a_i ze systému A není rovné žádnému číslu a'_j ze systému A'. Kdyby $a_i = a'_j$, bylo by $1 \equiv a_j a'_j \equiv a_j a_i \pmod{p}$, tedy $a_j = a'_i$. Podle definice systému A je $a_i < a'_i = a_j < a'_j$, tedy by bylo $a_i < a'_j$ proti předpokladu.

Žádná dvě čísla ze systému S':

$$+1, -1, a_1, a_2, \ldots, a_r, a'_1, a'_2, \ldots, a'_r$$

nejsou si tedy rovna. Každé číslo a z S je však v S' obsaženo: Můžeme předpokládati, že $|\,a\,| \neq 1$. Najděme a' z S tak, aby

$aa' \equiv 1 \pmod p$. Buď je nyní $a < a'$ a pak je a v A, anebo je $a > a'$ a pak je a' v A a tedy a v A'. Systémy S a S' se tedy až na pořadí shodují a je $2r + 2 = p - 1$ čili $r = \frac{1}{2}(p-1) - 1$.

Tedy

$$1 \,.\, 2 \,.\, 3 \ldots \tfrac{1}{2}(p-1) \,.\, (-1)(-2) \ldots [-\tfrac{1}{2}(p-1)] \equiv$$
$$\equiv -(a_1a'_1)(a_2a'_2) \ldots (a_ra'_r) \equiv -1 \pmod p,$$

tedy $$[1 \,.\, 2 \,.\, 3 \ldots \tfrac{1}{2}(p-1)]^2 \equiv (-1)^{\frac{1}{2}(p+1)} \pmod p.$$

Důsledek z věty 5. Buď p liché prvočíslo a nechť $\frac{1}{2}(p-1)$ je sudé (t. j. p je tvaru $4n + 1$, kde n je celé). Pak existuje celé číslo z takové, že $z^2 \equiv -1 \pmod p$ [stačí klásti $z = 1 \,.\, 2 \,.\, 3 \ldots \frac{1}{2}(p-1)$].

Věta 6. Buď p prvočíslo tvaru $4n + 1$ (n celé). Pak p není Gaussovo prvočíslo.

Důkaz. Podle důsledku z věty 5. existuje celé číslo z takové, že $z^2 + 1$ je dělitelno p, tedy součin $(z + i)(z - i)$ je dělitelný p. Kdyby p bylo Gaussovo prvočíslo, pak by podle věty 1. jeden z činitelů $z + i$, $z - i$ musel býti dělitelný p, t. j. muselo by existovati Gaussovo číslo $a + bi$ takové, že

$$ap + bpi = z \pm i$$

(platí buďto znaménko $+$ anebo $-$). Tedy by muselo býti $bp = \pm 1$ pro nějaké celé b, což je vyloučeno.

Věta 7. 2 není Gaussovo prvočíslo a platí $2 = (1 + i)(1 - i)$. (Zřejmé.)

Věta 8. Buď $\alpha = a + bi$ Gaussovo číslo. α je Gaussovým prvočíslem tenkráte a jenom tenkráte, jestliže

1. buďto α je asociované číslo ku prvočíslu tvaru $4n + 3$ (n celé),

2. anebo $\mathrm{N}(\alpha)$ je buďto prvočíslo tvaru $4n + 1$ neb $\mathrm{N}(\alpha) = 2$.

Důkaz. I. Buď α Gaussovo prvočíslo. Klaďme $\bar{\alpha} = a - bi$. (Vždy je $\mathrm{N}(\alpha) \geqq 2$.)

1. $\mathrm{N}(\alpha)$ je prvočíslo; je-li to sudé prvočíslo, je $\mathrm{N}(\alpha) = 2$, je-li to liché prvočíslo je $\mathrm{N}(\alpha)$ tvaru $4n + 1$, neboť součet celých kvadrátů $\mathrm{N}(\alpha) = a^2 + b^2$ nemůže nikdy býti tvaru $4n + 3$ (čtverec celého čísla je vždy buď tvaru $4n$ anebo tvaru $4n + 1$).

2. $\mathrm{N}(\alpha)$ není prvočíslo, tedy nechť $\mathrm{N}(\alpha) = r \,.\, s$, kde $r \geqq 2$, $s \geqq 2$ jsou celá čísla. $\mathrm{N}(\alpha) = \alpha \,.\, \bar{\alpha}$ je dělitelno α a tudíž podle věty 1. je buď r anebo s dělitelno α. Nechť je to r, t. j. nechť platí $r = \alpha\beta$, kde β je Gaussovo číslo. Z rovnice $\alpha\bar{\alpha} = rs$ plyne pak $\bar{\alpha} = \beta s$ čili[8]) $\alpha = \bar{\beta}s$. Poněvadž α je Gaussovo prvočíslo, musí (ježto $s \geqq 2$) $\bar{\beta} = \varepsilon$ býti Gaussova jednotka a s musí býti prvo-

[8]) $\bar{\beta}$ je číslo konjugované ku β.