Časopis pro pěstování mathematiky a fysiky

Karel Rychlík

O kvadratických tělesech číselných [II.]

Časopis pro pěstování mathematiky a fysiky, Vol. 50 (1921), No. 2-3, 177--190

Persistent URL: http://dml.cz/dmlcz/109176

Příloha k Časopisu pro pěstování mathematiky a fysiky.

O kvadratických tělesech číselných

Dr. Karel Rychlík.

(Dokončení.)

§ 8. Číslo celé, dělitelnost jednotky a číslo associované vzhledem k p v tělese čísel racionálných

Každé číslo racionálné a lze psáti ve tvaru $a = \frac{a'}{a''} p^r$, kdež p je racionálné prvočíslo, a', a'' jsou čísla celá nedělitelná p, r číslo celé; r nazývá se *řádem* čísla a vzhledem k p; položíme $| a |_p = p^r$.*) Je li $r \geqq 0$, nazývá se *číslo a celé vzhledem k p*; pak $| a |_p \geqq 1$. Ihned pak je patrna platnost věty: Z racionálných čísel $a, 1/a$ $(a \neq 0)$ jest aspoň jedno celé (p). Věta tato pro celistvost v obyčejném slova smyslu neplatí. Číslo celé (p) lze psáti ve tvaru $a = \bar{a}/a''$, kdež $\bar{a}$, a'' jsou čísla celá (v obyč. slova smyslu) a'' není dělitelno p. I lze ihned dokázati, že *součet, rozdíl a součin dvou čísel celých* (p) $a_1 = \bar{a}_1/a_1''$, $a_2 = \bar{a}_2/a_2''$ *je zase číslo celé* p. Jest totiž

$$a_1 \pm a_2 = \frac{\bar{a}_1 a_2'' \pm a_1'' \bar{a}_2}{a_1'' a_2''}, \qquad a_1 a_2 = \frac{\bar{a}_1 \bar{a}_2}{a_1'' a_2''},$$

při čemž čitatelé jsou čísla celá, jmenovatelé čísla celá nedělitelná p.

Je-li ve znázornění čísla $a = \frac{a'}{a''} p^r$, $r = 0$, t. j. $| a |_p = 1$, dostáváme čísla celá (p), jichž převratná hodnota je zase číslo celé (p): ta nazveme *jednotkami* (p). Součin a podíl dvou jednotek (p) je zase jednotka (p). I lze vyjádřiti každé číslo racionálné a ve tvaru $a = p^r e$, kdež e je jednotkou (p).

*) Místo »vzhledem k p« budeme psáti krátce »(p)«.

Zavedeme nyní pojem *dělitelnosti* (p) pro čísla celá (p) a, $b \neq 0$; a je dělitelno (p) b, je-li a/b číslo celé (p). Tu pak platí věty: *Je-li číslo a celé (p) dělitelno (p) číslem $b \neq 0$ celým (p), b dělitelno (p) číslem c celým (p), je a dělitelno (p) c. Jsou-li čísla celá (p) a, b dělitelna (p) číslem d celým (p), je $a \pm b$ dělitelno (p) číslem d. Každé číslo celé (p) je patrně dělitelno (p) všemi jednotkami.*

Dvě čísla racionálná a, b, jichž podíl je jednotka (p), nazveme spolu *associovanými* (p), což označíme $a \sim b$ (p). I platí vztahy: $a \sim a$ (p); *z* $a \sim b$ (p) *plyne* $b \sim a$ (p); *z* $a \sim b$ (p), $b \sim c$ (p) *plyne* $a \sim c$ (p); $a_1 \sim b_1$ (p), $a_2 \sim b_2$ (p) *plyne* $a_1 a_2 \sim b_1 b_2$ (p) $a_1/a_2 \sim b_1/b_2$ (p).

Číslo celé (v obyčejném slova smyslu) je celé vzhledem ku všem prvočíslům a též opak platí.

§ 9. Čísla celá, dělitelnost, jednotky, čísla associovaná vzhledem k p v tělese kvadrarickém.

Číslo α z tělesa kradratického $R(\sqrt{m})$ je *celé* (p), je-li kořenem rovnice druhého stupně $x^2 + a_1 x + c_2 = 0$, kdež a_1, a_2 jsou čísla racionálná celá (p). Je tedy α též kořenem rovnice tvaru $b_0 x^2 + b_1 x + b_2 = 0$, kdež b_0, b_1, b_2 jsou čísla celá racionálná, b_0 nedělitelné p. Tuto rovnici lze uvésti ve tvar $(b_0 x)^2 + b_0 b_1 (b_0 x) + b_0^2 b_2 = 0$, z čehož plyne, že $b_0 \alpha = \beta$ je číslo celé z kvadratického tělesa (v obyč. slova smyslu). *Lze tedy číslo celé (p) z $R(\sqrt{m})$ vyjádřiti jako podíl čísla celého z $R(\sqrt{m})$ a racionálného čísla celého nedělitelného p.* Též opak platí: *Podíl čísla celého z $R(\sqrt{m})$ a čísla racionálného celého nedělitelného p, je číslo celé (p).*

Každé číslo γ z $R(\sqrt{m})$ lze vyjádřiti jako podíl dvou čísel celých (p), dokonce lze pak za jmenovatele zvoliti mocnost p. Vyjádříme-li totiž γ jako podíl čísla celého β a celého racionálného b, $\gamma = \beta/b$, $b = p^r e$, kdež e není dělitelno p, je $\gamma = \alpha/p^r$, při čemž $\alpha = \beta/e$ je číslo celé (p).

Číslo celé z $R(\sqrt{m})$ v obyčejném slova smyslu je celé vzhledem ke všem prvočíslům a naopak, je-li číslo z $R(\sqrt{m})$ celé vzhledem ke všem prvočíslům, je to celé číslo z $R(\sqrt{m})$ v obyč. slova smyslu.

Zase platí věta: *Číslo α celé (p) z kvadratického tělesa, které je racionálné, je racionálné číslo celé (p).* Položme $\alpha = \beta/b$, kdež β je celé číslo v obyčejném slova smyslu z $R(\sqrt{m})$ a b racionálné celé číslo nedělitelné p. Ježto α je racionálné je též $\beta = b\alpha$ racionálné. Je tedy β, jakožto číslo racionálné a zároveň celé z $R(\sqrt{m})$ v obyč. slova smyslu, racionálné celé číslo a $\alpha = \beta/b$ pak skutečně celé (p).

Součet, rozdíl a součin dvou čísel α_1, α_2 celých (p) z $R(\sqrt{m})$ je zase číslo celé (p).

Vyjádřeme $\alpha_1 = \beta_1/b_1$, $\alpha_2 = \beta_2/b_2$, kdež β_1, β_2 jsou čísla celá z $R(\sqrt{m})$ a b_1, b_2 čísla celá racionálná nedělitelná p. I bude $\alpha_1 \pm \alpha_2 = \frac{\beta_1 b_2 \pm \beta_2 b_1}{b_1 b_2}$, $\alpha_1 \alpha_2 = \frac{\beta_1 \beta_2}{b_1 b_2}$, z čehož tvrzení ihned vyplývá.

Číslo α celé (p) je *dělitelno* (p) číslem $\beta \neq 0$ celým (p), je-li α/β číslo celé (p). Pro dělitelnost (p) platí věty obdobné jako pro dělitelnost v obyčejném slova smyslu (str. 56).

Podobně bude ε *jednotkou* (p) číslo z tělesa kvadratického, je-li $1/\varepsilon$ číslo celé (p), Platí věty obdobné s oněmi pro jednotky v obyč. slova smyslu (str. 56).

Číslo celé (p) z tělesa $R(\sqrt{m})$ je jednotkou (p) tehdy a jen tehdy, je-li jeho norma jednotkou (p). Důkaz obdobný jako pro jednotky v obyčejném slova smyslu (str. 56, 57).

Zase nazveme dvě čísla α, β z $R(\sqrt{m})$, jichž podíl je jednotka (p) spolu *associovanými* (p), $\alpha \sim \beta\,(p)$, je-li jich podíl jednotka (p); platí věty obdobné s oněmi na str. 57, 58).

§ 10. Base tělesa kvadratického vzhledem k p.

Basí (p) nazveme dvojici čísel lineárně neodvislých ω_1, ω_2, která má tu vlastnost, že čísla celá (p) dají se znázorniti ve tvaru $a\omega_2 + b\omega_2$ s koeficienty a, b reacionálnými celými (p). Lze snadno dokázati větu:

Base tělesa $R(\sqrt{m})$ v obyčejném slova smyslu je také basí (p).

Je-li ω_1, ω_2 basí $R(\sqrt{m})$ v obyčejném slova smyslu, jsou jistě čísla tvaru $a\omega_1 + b\omega_2$, kdež a, b jsou čísla racionálná

celá (p), čísla z $R(\sqrt{m})$ celá (p). Je-li pak α číslo celé (p), lze je znázorniti ve tvaru α/c, kdež α je celé z $R(\sqrt{m})$ a c racionálné celé (obě v obyč. slova smyslu) nedělitelné p. α lze znázorniti ve tvaru $\alpha = a\omega_1 + b\omega_2$, kdež a, b jsou čísla racionálná celá, tak že $\alpha = a\omega_1 + b\omega_2$, kdež $a = a/c$, $b = b/c$ jsou čísla racionálná jistě celá (p).

Známe-li jednu basi (p), ω_1, ω_2, *lze každou jinou* $\bar{\omega}_1$, $\bar{\omega}_2$ *vyjádřiti pomocí jí ve tvaru 1.)* $\bar{\omega}_1 = c_{11}\omega_1 + c_{12}\omega_2$, $\bar{\omega}_2 = c_{21}\omega_1 + c_{22}\omega_2$, *kdež koeficienty jsou čísla racionálná celá* (p) *a determinant* $C = \begin{vmatrix} c_{11} & c_{12} \\ c_{21} & c_{23} \end{vmatrix}$ *je jednotka* (p).

Ježto ω_1, ω_2 je base (p), je $D(\omega_1, \omega_2) \neq 0$. Má-li býti $\bar{\omega}_1$, $\bar{\omega}_2$ též base, musí býti rovněž $D(\bar{\omega}_1, \bar{\omega}_2) \neq 0$ a musí býti možno vyjádření $\omega_1 = c_{11}\bar{\omega}_1 + c_{12}\bar{\omega}_2$, $\omega_1 = c_{21}\bar{\omega}_1 + c_{22}\bar{\omega}_2$, kdež koeficienty jsou celé (p). Jich determinant označme $\bar{C}$. I bude $D(\omega_1, \omega_2) = \bar{C}^2 D(\bar{\omega}_1, \bar{\omega}_2)$, $D(\bar{\omega}_1, \bar{\omega}_2) = C^2 D(\omega_1, \omega_2)$ a odtud $C^2\bar{C}^2 = 1$, $C\bar{C} = \pm 1$ a ježto C, $\bar{C}$ jsou čísla celá (p), musí býti C jednotkou (p). Podmínka ta je také dostačující. Z 1.) plyne $C\omega_1 = c_{22}\bar{\omega}_1 - c_{12}\bar{\omega}_2$, $C\omega_2 = -c_{21}\omega_1 + c_{11}\bar{\omega}_2$, při čemž C je jednotka (p), tak že ω_1, ω_2 je vyjádřeno pomocí $\bar{\omega}_1$, $\bar{\omega}_2$ zase s koeficienty celými (p).

Z té okolnosti, že determinant C je jednotka (p), plyne, že pro všechny base (p) má diskriminant týž řád (p).

Za basi (p) lze dle věty na předešlé stránce zvoliti čísla 1, ω tvořící basi v obyčejném slova smyslu.

Lze však snadno nahlédnouti, že v případě $m \equiv 1 \pmod 4$, p liché, je basí též $1, \sqrt{m}$, poněvadž mezi dvojicí $1, \sqrt{m}$ a $1, \omega$ jsou vztahy $1 = 1$, $\omega = \frac{1}{2} + \frac{1}{2}\sqrt{m}$; $1 = 1$, $\sqrt{m} = -2 + 2\omega$, kdež koeficienty pro p liché jsou celé (p). Je tedy base (p) vždy $1, \sqrt{m}$ vyjma případ $m \equiv 1 \pmod 4$ $p = 2$, kdy je basí (p) $1, \frac{1}{2}(1 + \sqrt{m})$.

§ 11. Největší společná míra dvou čísel celých vzhledem k p v tělese kvadratickém.

Není-li α *dělitelno* β *ani* β *dělitelno* α *vzhledem k* p, *je* α *i* β *dělitelno* $\alpha + \beta$ *vzhledem k* p.

Uvažujme podíl α/β. Ani podíl ten ani jeho převratná hodnota není číslo celé (p). Z toho plyne, že to není číslo racio-

nálné. (Viz str. 177.) Nechť je α/β kořenem rovnice kvadratické s racionálnými koeficienty $ax^2 + bx + c = 0$. O číslech a, b, c lze předpokládati, že jsou to čísla celá nesoudělná. Ježto α/β není celé (p), je koeficient a dělitelný p. β/α je kořenem rovnice kvadratické $cx^2 + bx + a = 0$ a ježto to není celé číslo vzhledem k p, je nutně c dělitelno p. b pak nesmí býti dělitelno p: jest to jednotka (p). ježto a i c jsou dělitelny p, b není dělitelno p, není $a - b + c$ dělitelno p: je to jednotka (p). Uvažujme podíl $\frac{\alpha}{\alpha+\beta} = \frac{\frac{\alpha}{\beta}}{\frac{\alpha}{\beta}+1}$. Rovnici, jíž vyhovuje, dostaneme z rovnice $ax^2 + bx + c = 0$ pro α/β, klademe-li $x / (x + 1) = u$, tedy $x = u / (1 - u)$. Rovnice ta tedy je $au^2 + b(1 - u)u + c(1 - u)^2 = (a - b + c)u^2 + (b - 2c)u + c = 0$. Ježto $a - b + c$ je jednotka (p), je $\alpha / (\alpha + \beta)$ celé (p). Podíl $\frac{\beta}{\alpha+\beta} = \frac{1}{\frac{\alpha}{\beta}+1}$ je kořenem rovnice, kterou z rovnice pro α/β dostaneme, klademe-li $1 / (x + 1) = v$, t. j. $x = (1 - v) / v$. Rovnice ta je $a(1 - v)^2 + b(1 - v)v + cv^2 = (a - b + c)v^2 + (b - 2a)v + a = 0$ a z ní je zase patrno, že $\beta / (\alpha + \beta)$ je číslo celé (p).

Jsou-li dána dvě čísla α, β celá (p) z $R(\sqrt{m})$, nazývá se jejich *největší společnou měrou* (p) číslo celé (p), které má tyto vlastnosti: 1. je společným dělitelem (p) čísel α, β, 2 každý společný dělitel (p) x čísel α, β je dělitelem δ vzhledem k p.

Taková *největší spol. míra* (p) *v tělese* $R(\sqrt{m})$ *vždy eksistuje a je určena v podstatě jednoznačně*, t. j. *všechna čísla celá o vlastnostech 1. a 2. jsou spolu associována* (p).

Je-li α dělitelno (p) β, je největší společnou měrou (p) čísel α, β číslo β a podobně, je-li β dělitelno (p) α, je jí α. Není-li α dělitelno (p) β, ani β dělitelno α, je jich největší společnou měrou (p) $\alpha + \beta$. Vlastnost 1. je dle věty předešlé splněna, vlastnost 2. je ihned patrná. Že největší společná míra (p) je určena v podstatě jednoznačně plyne ze 2. Dejme tomu, že bychom měli dvě čísla splňující 2., δ_1 a δ_2. Dle 2. musí

pak býti δ_1 dělitelno (p) δ_2 a též naopak, t. j. čísla δ_1 a δ_2 musí býti pak associována (p).

§ 12. Rozklad čísel z kvadratického tělesa v prvočinitele vzhledem k p.

Nazveme *číslem nerozložitelným* (p) číslo π celé (p), které není jednotkou (p), a je dělitelno (p) pouze samo sebou a jednotkami (p). Každé číslo celé (p) buď je s π nesoudělné (p) nebo je π dělitelno.

Dokážeme si, že, uvažujeme-li v tělese kvadratickém dělitelnost (p), *má číslo nerozložitelné* (p) π *vlastnost prvočísla. Je-li součin dvou čísel* α, β *celých* (p) *dělitelný* (p) π, *je aspoň jeden z činitelů* α, β *dělitelný* (p) π.

Dejme tomu, že není α dělitelno (p) π. Pak jsou čísla α, π nesoudělná (p). π může býti dělitelno (p) α jen je-li α jednotkou (p). Pak plyne z toho, že $\alpha\beta$ je dělitelno (p) π, že též β je dělitelno (p) π. Není-li α jednotka (p), není ani α dělitelno (p) π, ani π dělitelno (p) α, je tedy $\alpha + \pi$ největší společnou měrou (p) čísel α, π; ježto jsou to čísla nesoudělná (p). je $\alpha + \pi = \varepsilon$ jednotka (p). I bude $\alpha\beta + \beta\pi = \varepsilon\beta$ a ježto $\alpha\beta$ je dělitelno (p) π, plyne z toho, že β je dělitelno (p) π. Z toho je platnost věty vyslovené ihned patrna. Dále je jasno, že platí věta: *Je-li součin prvočísel* (p) $\pi_1, \pi_2 \ldots \pi_k$ *dělitelný* (p) *prvočíslem* (p) π, *je* π *associováno* (p) *aspoň s jedním z činitelů* $\pi_1, \pi_2, \ldots \pi_k$.

Každé číslo celé (p) *z* $R(\sqrt{m})$ *je buď jednotka* (p) *neb prvočíslo* (p) *neb součin konečného počtu prvočísel* (p).

Čísla celá o normě jednotkové (p) (řádu 0 vzhledem k p) jsou patrně jednotky (p). Aby byla věta dokázána, stačí tedy důkaz, že z platnosti její pro číslo celé (p) s normou řádu $< m$ vzhledem k p, plyne platnost pro číslo α celé (p) s normou řádu m vzhledem k p. Je-li α nerozložitelné (p), je to dokázáno. Je-li α rozložitelné, $\alpha = \beta\gamma$, $|N\beta|_p > 1$ $|N\beta|_p > 1$, pak $N\alpha = N\beta N\gamma$, $|N\beta|_p < |N\alpha|_p$, $|N\gamma|_p < |N\alpha|_p$. Mají tedy β i γ normy řádu $< m$ vzhledem k p, i platí o nich dle předpokladu věta vyslovená. Tím pak platnost její dokázána obecně.

Rozklad čísla celého (p) v prvočinitele (p) lze provésti v podstatě jednoznačně, pokládáme-li takové dva rozklady za v podstatě stejné, u nichž 1. změněn jen pořádek činitelů, 2. činitelé nahraženi čísly s nimi associovanými (p).

Dejme tomu, že bychom pro číslo celé α měli dva rozklady v prvočinitele (p) $\alpha = \pi_1\pi_2 \ldots \pi_k = \varrho_1\varrho_2 \ldots \varrho_l$. Součin prvočísel (p) $\pi_1\pi_2 \ldots \pi_k$ je dělitelný ϱ_1, je tedy aspoň jeden z prvočinitelů $\pi_1, \pi_2 \ldots \pi_k$ associován (p) s ϱ_1. Nechť je na př. $\pi_1 \sim \varrho_1$ (p). Pak $\pi_2\pi_3 \ldots \pi_k \sim \varrho_2\varrho_3 \ldots \varrho_l$ (p). Podobnou úvahou bychom seznali, že ϱ_2 je associováno (p) aspoň s jedním z prvočinitelů $\pi_2 \ldots \pi_k$, na př. s π_2, tak že by pak $\pi_3\pi_4 \ldots \pi_k \sim \varrho_3\varrho_4 \ldots \varrho_l$ a t. d.

Norma každého prvočísla (p) z $R(\sqrt{m})$ je číslo celé (p) dělitelné p. Z toho plyne, že *prvočísla (p) z $R(\sqrt{m})$ jsou dělitelé (p) racionálného prvočísla p.* Je-li rozklad p v $R(\sqrt{m})$ v prvočinitele (p) $p = \pi_1\pi_2 \ldots \pi_k$, musí býti pro normy $p^2 = |N\pi_1|_p\,|N\pi_2|_p \ldots |N\pi_1|_p$ a je-li $|N\pi_1|_p = p^{f_1}, \ldots |N\pi_k|_p = p^{f_k}$, musí býti $f_1 + f_2 + \ldots + f_k = 2$. Čísla celá kladná $f_1, f_2, \ldots f_k$ jsou *stupně* prvočísel resp. $\pi_1, \pi_2 \ldots \pi_k$. I musí býti buď $f_1 = 1$, $f_2 = 1$ neb $f_1 = 2$.

V případě $f_1 = 2$ zůstává p v $R(\sqrt{m})$ prvočíslem (p).

V případě $f_1 = 1$, $f_2 = 1$ rozpadá se p v $R(\sqrt{m})$ v součin dvou prvočinitelů (p) $\pi_1\pi_2$. Je-li π libovolné prvočíslo (p) z $R(\sqrt{m})$ (takže $\pi \sim \pi_1$ neb π_2 (p)), je také číslo sdružené π prvočíslo (p) a ježto $|N\pi|_p = p$ je $\pi\pi' \sim p\,(p)$, takže π je associováno (p) s jedním z prvočísel (p) π_1, π_2, π' s druhým. Jsou dvě možnosti: buď jsou v tělese dvě prvočísla (p) spolu neassociovaná (p), za něž pak lze zvoliti prvočísla (p) spolu sdružená π, π', neb jsou všechna prvočísla (p) spolu associována (p), takže $\pi' \sim \pi$.

Mohou tedy celkem nastati tři případy:

1. V tělese $R(\sqrt{m})$ jsou dvě prvočísla (p) spolu associovaná (p) o normě řádu 1, za něž lze zvoliti čísla spolu sdružená π, π', $p \sim \pi\pi'\,(p)$, $N\pi = N\pi' \sim p\,(p)$. Každé číslo celé (p) z $R(\sqrt{m})$ lze psáti ve tvaru $\varepsilon\pi^k\pi'^{k'}$, kdež ε je jednotka (p), k, k' jsou racionálná celá čísla ≥ 0. Ježto každé číslo z $R(\sqrt{m})$ je podílem dvou čísel celých (p), jsou všechna čísla z $R(\sqrt{m})$

dána ve tvaru $\varepsilon\pi^k\pi'^{k'}$, kdež k, k' jsou čísla racionálná celá. Z věty o podstatně jednoznačné rozložitelnosti plyne, že pomocí jiného prvočísla $\bar{\pi} \sim \pi\ (p)$ by bylo totéž číslo znázorněno v tvaru $\bar{\varepsilon}\bar{\pi}^k\bar{\pi}'^{k'}$, kdež $\bar{\varepsilon}$ je zase jednotka.

2. V tělese $R(\sqrt{m})$ jsou všechna prvočísla (p) spolu associována (p), norma jich má řád 1, $p \sim \pi^2\ (p)$, $\pi' \sim \pi\ (p)$, $N\pi \sim p\ (p)$. Čísla z $R(\sqrt{m})$ lze znázorniti ve tvaru $\varepsilon\pi^k$, kdež ε je jednotka (p) a k racionálné celé číslo. Pro číslo celé je $k \geqq 0$

3. Prvočíslo racionálné p zůstává v $R(\sqrt{m})$ prvočíslem (p), každé prvočíslo (p) z $R(\sqrt{m})$ je s ním associováno (p), normy jich mají řád 2. Čísla z $R(\sqrt{m})$ lze psáti ve tvaru εp^k, kdež ε je jednotka (p), k celé číslo racionálné, pro čísla celá pak $k \geqq 0$.

V případě 1. a 3. je racionálné prvočíslo p dělitelno (p) první mocninou prvočísla (p) z $R(\sqrt{m})$, v případě 2. druhou mocninou. Proto v případě 1. a 3. nazývá se *prvočíslo* (p) z $R(\sqrt{m})$ prvočíslem *prvého řádu*, v případě 2. *druhého řádu*.

Konečně lze snadno nahlédnouti, že za prvočíslo (p) π, které je číslo celé (p) z $R(\sqrt{m})$, lze voliti číslo celé z $R(\sqrt{m})$ v obyčejném slova smyslu. Dle § 9. str. 178 lze položiti $\pi = \bar{\pi}/e$, kdež $\bar{\pi}$ je celé číslo z $R(\sqrt{m})$, e racionálné celé číslo nedělitelné p. Ježto e je jednotka (p), je $\bar{\pi} = \pi e$ prvočíslo (p), a je to nad to číslo celé z $R(\sqrt{m})$ (v obyč. slova smyslu).

Pro p liché lze prvočíslo (p) z $R(\sqrt{m})$ voliti v tvaru $x + y\sqrt{m}$, kdež x, y jsou čísla racionálná celá. Při $m \equiv 2, 3 \pmod 4$ plyne to z předešlého, při $m \equiv 1 \pmod 4$, ježto base (p) je $1, \sqrt{m}$, bude prvočíslo (p) tvaru $\bar{x} + \bar{y}\sqrt{m}$, kdež $\bar{x}$, $\bar{y}$ sou čísla celá (p). I bude $\bar{x} + \bar{y}\sqrt{m} = \dfrac{x + y\sqrt{m}}{e}$, kdež x, y jsou čísla racionálná celá, e číslo celé nedělitelné p, tedy jednotka p. Pak bude $x + y\sqrt{m}$ také prvočíslem (p) z $R(\sqrt{m})$.

§ 13. Stanovení prvočísel (p) v tělese kvadratickém.

Budeme se nejprve zabývati prvočísly racionálnými p lichými. Basí (p) tělesa je 1, $\sqrt{m}$. Zjistíme nejprve, kdy v $R(\sqrt{m})$ je $p \sim \pi^2\ (p)$ (případ 2.), při čemž $\pi = x + y\sqrt{m}$ (x, y, čísla celá). Ze vztahu $\pi^2 = x^2 + my^2 + 2xy\sqrt{m} \sim p\ (p)$ je patrno, že musí

býti $x^2 + my^2$ i $2xy$ dělitelno p. Aby bylo $2xy$ dělitelno p, musí býti buď x neb y dělitelno p. Kdyby bylo y dělitelno p, pak by z té okolnosti, že $x^2 + my^2$ má býti dělitelno p plynulo, že též x je dělitelno p. Bylo by tedy π dělitelno p a nemohlo by býti $\pi^2 \sim p$.

Uvažujme případ, že y není dělitelno p, je však x dělitelno p. Aby bylo $x^2 + my^2$ děliteluo p, musí býti m dělitelno π. Naopak, je-li m dělitelno p, je $\pi = \sqrt{m}$ prvočíslem (p) v $R(\sqrt{m})$ a je skutečně $\pi^2 = m \sim p$, $N\pi = m \sim p\,(p)$. Tedy *liché prvočíslo racionálné p rozpadá se v $R(\sqrt{m})$ vzhledem k p v čtverec prvočísla (p) (je druhého řádu) tehdy a jen tehdy, je-li dělitelem m.*

Nechť tedy dále p není obsaženo v m a ptejme se, kdy p se rozpadne v součin dvou různých prvočísel (p), $p \sim \pi\,\pi'$ (p), $\pi = x + y\sqrt{m}$, (x, y čísla celá, $y \neq 0$). Ze vztahu $\pi\,\pi' = x^2 - y^2 m \sim p$ (p) je viděti, že musí býti $x^2 - my^2 \equiv 0 \pmod{p}$, $\left(\frac{x}{y}\right)^2 - m \equiv 0 \pmod{p}$ t. j. musí býti řešitelna kongruence $z^2 - m \equiv 0 \pmod{p}$. Naopak, je-li tato kongruence řešitelná, existuje kořen r takový, že $r^2 - m \equiv 0 \pmod{p^2}$. Je-li totiž s kořen té kongruence takový, že $s^2 - m \equiv 0 \pmod{p^2}$, bude, položíme-li $r = s + s'p$, $s = r - s'p$, $r^2 - m - 2s'p, \equiv 0 \pmod{p^2}$, tedy jistě $r^2 - m \equiv 0 \pmod{p}$, zvolíme-li však s' nedělitelné p, nebude $r^2 - m$ dělitelno p^2. Klademe-li pak $\pi = r + \sqrt{m}$, $\pi' = r - \sqrt{m}$, bude $\pi\,\pi' = r^2 - m \equiv 0 \pmod{p}$ $\not\equiv 0 \pmod{p^2}$, tedy skutečně $\pi\,\pi' \sim p$ (p).

Prvočíslo racionálné p neobsažené v m rozpadá se v $R(\sqrt{m})$ v součin dvou neassociovaných prvočísel (p), tehdy a jen tehdy, je-li řešitelná kongruence $z^2 \equiv m \pmod{p}$, t. j. je-li m kvadratickým zbytkem $(\mathrm{mod}\ p)$. Zůstane tedy p prvočíslem (p) v tělese $R(\sqrt{m})$, není-li kongruence ta řešitelná, t. j. je-li m kvadratickým nezbytkem.

Obraťme se nyní k prvočíslu 2. Je-li $m \equiv 2$ neb $3 \pmod{4}$, je basí (p) tělesa $R(\sqrt{m})$ zase $1, \sqrt{m}$. *Pro* $m \equiv 2 \pmod{4}$ je $2 \sim \pi^2$ (2), $\pi = \sqrt{m}$, $\pi' = -\sqrt{m} \sim \pi$. *Pro* $m \equiv 3 \pmod{4}$ je $2 \sim \pi^2$ (2), $\pi = 1 + \sqrt{m}$. Jest totiž $\pi\,\pi' = 1 - m \sim 2$ (2), $\frac{\pi}{\pi'} = \frac{1+\sqrt{m}}{1-\sqrt{m}} = 1 + \frac{2\sqrt{m}}{1-\sqrt{m}} = 2 + \frac{2}{\pi'}\sqrt{m}$. Ježto $2/\pi' \sim \pi$

(2) je celé číslo, je π/π' celé číslo, jehož norma je jednotka (2) a tedy $\pi \sim \pi'$ (2).

Je li $m \equiv 1 \pmod 4$ je base (2) dána čísly 1, $\frac{1}{2}(1+\sqrt{m})$ Rozeznávejme dva případy $m \equiv 1$ a $5 \pmod 8$. *Pro* $m \equiv 1 \pmod 8$, t. j. $m = 1 + 8m'$ *je* 2 *associováno se součinem dvou prvočísel* (2) *neasociovaných spolu* (2). *Lze zvoliti* $\pi = \frac{1}{2}(5+\sqrt{m})$, $\pi' = \frac{1}{2}(5-\sqrt{m})$. Pak je $\pi\pi' = \frac{1}{4}(25-m) = 6 - 2m' = 2[1-2(m'-1)] \sim 2$ (2), $\frac{\pi}{\pi'} = \frac{5+\sqrt{m}}{5-\sqrt{m}} = 1 + \frac{2\sqrt{m}}{5-\sqrt{m}} = 1 + \frac{\sqrt{m}}{\pi'}$. Ježto $\sqrt{m}$ je jednotka (2) (norma $\sqrt{m}$ je totiž jednotka (2)), není π/π' celé číslo (2), takže jistě není $\pi \sim \pi'$ (2).

Pro $m \equiv 5 \pmod 8$, $m = 5 + 8m'$ *zůstává v* $R(\sqrt{m})$ 2 *prvočíslem* (2). Pro prvočíslo π vzhledem k 2, $\pi = x + \frac{1}{2}(1+\sqrt{m})\,y$ musí býti $N\pi = (x+\frac{1}{2}y)^2 - \frac{1}{4}my^2$ dělitelno 2, $x^2 + xy = \frac{1-m}{4}\,y^2 \equiv 0 \pmod 2$ t. j. $x^2 + xy - y^2 \equiv 0 \pmod 2$. Té rovnici lze vyhověti jen tak, že $x \equiv 0$, $y \equiv 0 \pmod 2$. Musí tedy býti π dělitelno 2(2), z čehož ihned plyne, že 2 zůstane v $R(\sqrt{m})$ prvočíslem (2). Celkem vidíme, že *prvočísla druhého řádu jsou dělitelé diskriminantu* d *tělesa.*

§ 14. Divisory v tělese kvadratickém.

Abychom mohli vyjádřiti pohodlně pravidla dělitelnosti v kvadratickém tělese $R(\sqrt{m})$, zavedeme pojem divisorů. Všem prvočíslům spolu associovaným (p) přiřadíme jeden a týž *prvodivisor*. Stupeň a řád onoho prvočísla (p) bude též *stupněm* resp. *řádem prvodivisoru*. Tak dostaneme pro každé prvočíslo racionálné jeden nebo dva prvodivisory. Budeme pak uvažovati *divisory*, výrazy to z konečného počtu prvodivisorů $\mathfrak{p}, \mathfrak{q}, \ldots \mathfrak{r}$ utvořené $\mathfrak{d} = \mathfrak{p}^k \mathfrak{q}^l \ldots \mathfrak{r}^n$, kdež $k, l, \ldots n$ jsou racionálná celá čísla. Pro divisory budeme definovati *rovnost*, *součin* a *podíl* Zavedeme nejprve divisor jednotkový $\mathfrak{j}$, pro který platí $\mathfrak{d}\mathfrak{j} = \mathfrak{j}\mathfrak{d} = \mathfrak{d}$, $\mathfrak{d}/\mathfrak{j} = \mathfrak{d}$; $\mathfrak{p}^0 = \mathfrak{q}^0 = \ldots = \mathfrak{r}^0 = \mathfrak{j}$. Je-li $\mathfrak{d} = \mathfrak{p}^k \mathfrak{q}^l$

$\ldots \mathfrak{r}^m$ můžeme psáti též $\mathfrak{d} = \mathfrak{p}^k\ \mathfrak{q}^l \ldots \mathfrak{r}^m\ \mathfrak{s}^o \ldots \mathfrak{t}^o$, kdež $\mathfrak{s}^o, \ldots \mathfrak{t}^s$ jsou prvodivisory. Tak lze dosíci, že ve výrazech pro několik divisorů vyskytují se tytéž prvodivisory. Dva divisory $\mathfrak{d}_1 = \mathfrak{p}_1^{k_1}\ \mathfrak{q}_1^{l_1} \ldots \mathfrak{r}_1^{n_1}$ a $\mathfrak{d}_2 = \mathfrak{p}_2^{k_2}\ \mathfrak{q}_2^{l_2} \ldots \mathfrak{r}_2^{n_2}$ budou rovny, bude-li $k_1 = k_2$, $l_1 = l_2, \ldots n_1 = n_2$. Součin a podíl budou definovány $\mathfrak{d}_1\,\mathfrak{d}_2 = \mathfrak{p}^{k_1 + k_2}\ \mathfrak{q}^{l_1 + l_2} \ldots \mathfrak{r}^{n_1 + n_2}$, $\mathfrak{d}_1/\mathfrak{d}_2 = \mathfrak{p}^{k_1 - k_2}\ \mathfrak{q}^{l_1 - l_2} \ldots \mathfrak{r}^{n_1 - n_2}$.

Pro všechna prvočísla $\pi\,(p)$ spolu associovaná (p) má $(N\pi)_p$ tutéž hodnotu p^f, kdež f je stupeň prvočísla $(p)\pi$. Nazveme $(N\pi)_p$ *normou* příslušného prvodivisoru $\mathfrak{p}$, $N\mathfrak{p} = p^f$. Je-li pak divisor $\mathfrak{d} = \mathfrak{p}^k\ \mathfrak{q}^l \ldots \mathfrak{r}^n$, položíme $N\mathfrak{d} = (N\mathfrak{p})^k\ (N\mathfrak{q})^l \ldots (N\mathfrak{r})^m$. I bude $N\mathfrak{d}_1\,\mathfrak{d}_2 = N\mathfrak{d}_1\,N\mathfrak{d}_2$, $N\mathfrak{d}_1/\mathfrak{d}_2 = N\mathfrak{d}_1/N\mathfrak{d}_2$.

Divisor $\mathfrak{d} = \mathfrak{p}^k\ \mathfrak{q}^l \ldots \mathfrak{r}^n$ je *celý*, je-li $k \geqq 0$, $l \geqq 0, \ldots$ $n \geqq 0$. Divisor $\mathfrak{d}_1 = \mathfrak{p}^{k_1}\ \mathfrak{q}^{l_1} \ldots \mathfrak{r}^{n_1}$ je *dělitelný* divisorem $\mathfrak{d}_2 = \mathfrak{p}^{k_2}\ \mathfrak{q}^{l_2} \ldots \mathfrak{r}^{n_2}$, je-li $\mathfrak{d}_1/\mathfrak{d}_2$ divisor celý. K tomu nutno a postačí, aby $k_1 \geqq k_2$, $l_1 \geqq l_2, \ldots n_1 \geqq n_2$. Jsou-li dány divisory celé $\mathfrak{d}_1 = \mathfrak{p}^{k_1}\ \mathfrak{q}^{l_1} \ldots \mathfrak{r}^{n_1}$, $\mathfrak{d}_2 = \mathfrak{p}^{k_2}\ \mathfrak{q}^{l_2} \ldots \mathfrak{r}^{n_2}$ utvořme divisor $\mathfrak{d} = \mathfrak{p}^k\ \mathfrak{q}^l \ldots \mathfrak{r}^n$, kdež $k = Min\ (k_1, k_2)$, $l = Min\ (l_1, l_2) \ldots$ $n = Min\ (n_1, n_2)$.*) Oba divisory $\mathfrak{d}_1$, $\mathfrak{d}_2$ jsou $\mathfrak{d}$ dělitelny a každý divisor obsažený v $\mathfrak{d}_1$ a $\mathfrak{d}_2$ je v $\mathfrak{d}$ obsažen. Žádný jiný divisor nemá těchto vlastností. Dejme tomu, že divisor $\overline{\mathfrak{d}}$ má je též. Ježto každý divisor obsažený v $\mathfrak{d}_1$ a $\mathfrak{d}_2$ je obsažen v $\mathfrak{d}$, bylo by $\mathfrak{d}$ dělitelno $\overline{\mathfrak{d}}$ a naopak, ježto také každý divisor obsažený v $\mathfrak{d}_1$ a $\mathfrak{d}_2$ je obsažen $\overline{\mathfrak{d}}$, bylo by $\overline{\mathfrak{d}}$ dělitelno $\mathfrak{d}$. Platily by tedy rovnice $\mathfrak{d} = \overline{\mathfrak{d}}\mathfrak{e}$, $\overline{\mathfrak{d}} = \mathfrak{d}\mathfrak{f}$, kdež $\mathfrak{e}$, $\mathfrak{f}$ jsou celé divisory. Z nich by plynulo $\mathfrak{e}\mathfrak{f} = \mathfrak{j}$, čemuž nelze vyhověti jinak než že $\mathfrak{e} = \mathfrak{f} = \mathfrak{j}$. Divisor $\mathfrak{d}$ nazývá se *největší společnou měrou divisorů* $\mathfrak{d}_1$, $\mathfrak{d}_2$. Je-li to divisor jednotkový, nazývají se divisory $\mathfrak{d}_1$, $\mathfrak{d}_2$ *nesoudělné*. Podobně by to bylo pro více divisorů.

Budiž α číslo z tělesa $R\ (\sqrt{m})$ Je-li α a číslo s ním sdružené kořenem rovnice $a_0\,x^2 + a_1\,x + a_2 = 0$, kdež a_0, a_1, a_2 jsou racionálná čísla celá nesoudělná, může býti číslo nejednotkou pouze vzhledem ku konečnému počtu racionálných prvočísel $p, q, \ldots r$, totiž vzhledem k prvočinitelům čísel a_0 a a_2. Je-li α celé číslo z $R\ (\sqrt{m})$, je nejednotkou vzhledem k racio-

*) *Min* (a, b) je menší z obou čísel a, b neb společná jich hodnota, jsou-li si čísla a, b rovna.

nálným prvočíslům obsaženým v normě α. Prvočíslo p nechť se na př rozpadá v $R(\sqrt{m})$ v součin dvou prvočísel (p) neassociovaných (p), $p \sim \pi\,\pi'$ (p), jimž přiřadíme prvodivisory $\mathfrak{p}$, $\mathfrak{p}'$; q nechť je associováno se čtvercem prvočísla (q) $q \sim \varkappa^2$ (q) a $\varkappa$ přiřadíme prvodivisor $\mathfrak{q}$; r nechť zůstane v $R(\sqrt{m})$ prvočíslem a přiřadíme mu prvodivisor $\mathfrak{r}$. Je-li pak $\alpha \sim \pi^k\,\pi'^{k'}$ (p), $\alpha \sim \varkappa^l$ $(q), \ldots$ $\alpha \sim r^n$ $(\mathfrak{r})$, přiřadíme číslu α divisor $\mathfrak{p}^k\,\mathfrak{p}'^{k'}\,\mathfrak{q}^l \ldots \mathfrak{r}^n$, který označíme též (α). Divisory přiřaděné k číslům tělesa nazveme *divisory hlavními*. (Shledáme v násl. §, že eksistují tělesa, v nichž nejsou všechny divisory hlavními.) Pak bude patrně $(1) = \mathfrak{j}$ a též $(\eta) = \mathfrak{j}$, značí-li η libovolnou jednotku z $R(\sqrt{m})$. Pro prvočísla racionálná bude $(p) = \mathfrak{p}\mathfrak{p}'$ $(q) = \mathfrak{q}^2$, $\ldots$ $(r) = \mathfrak{r}$. *Číslo α bude celé tehdy a jen tehdy, je-li divisor mu odpovídající (α) celý*, což plyne ihned z toho, že podmínkou nutnou a postačující pro celistvost α je, aby bylo celé vzhledem ke všem prvočíslům racionálným. Snadno lze dokázati, že $(\alpha_1\,\alpha_2) = (\alpha_1)\,(\alpha_2)$, $(\alpha_1/\alpha_2) = (\alpha_1)/(\alpha_2)$. Aby celé číslo α_1 bylo dělitelno celým číslem α_2 je nutno a stačí, aby bylo α_1/α_2 celé, tedy i divisor (α_1/α_2) celý, t. j. divisor (α_1) dělitelný (α_2).

Podmínka nutná a postačující pro dělitelnost dvou čísel je dělitelnost příslušných divisorů. Pro associovanost čísel α_1 a α_2 dostáváme pak nutnou a postačující podmínku, aby divisory (α_1) a (α_2) byly si rovny.

Zavedeme dále dělitelnost mezi divisory a čísly, nahradivše při tom vždy číslo příslušným divisorem. Pak platí věty:

Je-li celé číslo α dělitelno celým divisorem $\mathfrak{d}$, pak je $\alpha\,\lambda$ též dělitelna $\mathfrak{d}$, ať je λ jakékoliv celé číslo.

Jsou-li celá čísla α_1, α_2 dělitelna celým divisorem $\mathfrak{d}$, je též $\alpha_1 + \alpha_2$ dělitelno $\mathfrak{d}$. Nechť je $\mathfrak{d} = \mathfrak{p}^k\,\mathfrak{p}'^{k'}\,\mathfrak{q}^l \ldots \mathfrak{r}^n$. Ježto α_1 i α_2 je dělitelno $\mathfrak{d}$, je α_1 i α_2 dělitelno (p) $\pi^k\,\pi'^{k'}$ tedy též $\alpha_1 + \alpha_2$ dělitelno $\pi^k\,\pi'^{k'}$ (p). Podobně je $\alpha_1 + \alpha_2$ dělitelno $\varkappa^l$ $(q) \ldots$ r^n (r). Z toho je ihned patrno, že $\alpha_1 + \alpha_2$ je dělitelno $\mathfrak{d}$.

Největší společná míra čísel celých α_1, α_2 bude největší společná míra divisorů (α_1), (α_2). Bude to divisor, jen vyjímečně divisor hlavní, jemuž odpovídá číslo celé z tělesa. Bude li to divisor jednotkový, nazveme čísla α_1, α_2 *nesoudělná*

Při označení jako svrchu odpovídají prvodivisory $\mathfrak{p}$, $\mathfrak{p}'$ prvočíslům (p) spolu sdruženým; nazveme je *prvodivisory* spolu

sdruženými; z téhož důvodu položíme $\mathfrak{q}' = \mathfrak{q}$, $\mathfrak{r}' = \mathfrak{r} = (r)$. Je tedy $\mathfrak{p}\mathfrak{p}' = (p) = (N\mathfrak{p}) = (N\mathfrak{p}')$. $\mathfrak{q}\,\mathfrak{q}' = \mathfrak{q}^2 = (q) = (N\mathfrak{q}) = (N\mathfrak{q}')$. . . . $\mathfrak{r}\,\mathfrak{r}' = (r^2) = (N\mathfrak{r}) = (N\mathfrak{r}')$. *Divisor* $\mathfrak{d}'$ *sdružený* s daným divisorem $\mathfrak{d}$ budeme definovati jako divisor, který z $\mathfrak{d}$ dostaneme, nahradíme-li každý prvodivisor prvodivisorem sdruženým. I je patrně $\mathfrak{d}\,\mathfrak{d}' = (N\mathfrak{d}) = (N\mathfrak{d}')$. Pro divisor hlavní (α) je divisor přidružený, jak lze snadnou úvahou zjistiti, (α'). Poněvadž $(\alpha)\,(\alpha') = (\alpha\alpha') = (N\alpha)$ a též $(\alpha)\,\alpha') = (N(\alpha)) = (N(\alpha'))$ jsou racionálná čísla $N\alpha$ a $N(\alpha)$*) spolu associována, a ježto $N(\alpha)$ je dle definice kladné, je $N(\alpha) = (N\alpha)$.

§ 15. Příklad: Těleso $R(\sqrt{-5})$.

Všímněme si nyní tělesa $R(\sqrt{-5})$. Base jeho je $1, \sqrt{-5}$ a to je též base vzhledem ke všem prvočíslům. Diskriminant je -20, jediná prvočísla druhého řádu jsou prvočinitelé tohoto čísla 2, 5. Dle § 13. je $2 \sim (1 + \sqrt{-5})^2$ (2), kdež $\varkappa_1 = 1 + \sqrt{-5}$ je prvočíslo (2) z $R(\sqrt{-5})$. Přiřaďme mu prvodivisor $\mathfrak{q}_1$. I bude $(2) = \mathfrak{q}_1^2$. Dále je $\varkappa_2 = \sqrt{-5}$ prvočíslem (5), takže $5 = -\varkappa_2^2$. Přiřaďme $\sqrt{-5}$ prvodivisor $\mathfrak{q}_2$, takže $(5) = \mathfrak{q}_2^2$. Abychom rozhodli o 3, uvažujme kongruenci $z^2 \equiv -5 \pmod 3$. Má kořen $r = 1$ a není $1 \equiv -5 \pmod{3^2}$, takže $3 \sim (1 + \sqrt{-5})\,(1 - \sqrt{-5})$ (3) a prvočísla (3) $\pi_1 = 1 + \sqrt{-5}$. $\pi'_1 = 1 - \sqrt{-5}$ nejsou spolu associována (3). π_1 přiřaďme prvodivisor $\mathfrak{p}_1$, π'_1 pak prvodivisor $\mathfrak{p}'_1$, takže $(3) = \mathfrak{p}_1\,\mathfrak{p}'_1$. Podobně je kongruence $z^2 \equiv -5 \pmod 7$ řešitelná a má kořen 3, není $3^2 \equiv -5 \pmod{7^2}$, takže $7 \sim (3 + \sqrt{-5})\,(3 - \sqrt{-5})$ (7) a prvočísla (7) $\pi_2 = 3 + \sqrt{-5}$, $\pi'_2 = 3 - \sqrt{-5}$ nejsou spolu associována (7). π_2 přiřadíme prvodivisor $\mathfrak{p}_2$, π'_2 prvodivisor $\mathfrak{p}'_2$; i bude $(7) = \mathfrak{p}_2\,\mathfrak{p}'_2$. Naproti tomu kongruence $z^2 \equiv 5 \pmod{11}$ není řešitelná. Zůstává tedy 11 v $R(\sqrt{-5})$ prvočíslem. Divisor $\mathfrak{q}_1$ není hlavní: nepřísluší mu číslo v $R(\sqrt{-5})$ Kdyby bylo $\mathfrak{q}_1 = (x + y\sqrt{-5})$, ($x$, y racionálná čísla celá), musilo by býti $N(x + y\sqrt{-5}) = N\mathfrak{q}_1 = 2$, $x^2 + 5y^2 = 2$, kteroužto rovnici nelze splniti.

*) Zde značí $N\alpha$ normu čísla α, $N(\alpha)$ normu hlavního divisoru (α).

Všimněme si rozkladů v nerozložitelné činitele: 1) $6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Zde je $(2) = \mathfrak{q}_1^2$, $(3) = \mathfrak{p}_1 \mathfrak{p}'_1$. Čísla $1+\sqrt{-5}$ a $1-\sqrt{-5}$ dlužno uvažovati vzhledem k prvočinitelům 2,3 jich normy 6. I je $1+\sqrt{-5} = \varkappa_1, (2)$; $= \pi_1, (3)$; takže $(1+\sqrt{-5}) = \mathfrak{q}_1 \mathfrak{p}_1$ a pro číslo sdružené $(1-\sqrt{-5}) = \mathfrak{q}_1 \mathfrak{p}'_1$. Konečně je $6 = \mathfrak{q}_1^2 \mathfrak{p}_1 \mathfrak{p}'_1$. 2) $9 = 3.3 = (2+\sqrt{-5})(2-\sqrt{-5})$. Zde je $(3) = \mathfrak{p}_1 \mathfrak{p}'_1$. Ježto $N(2+\sqrt{-5}) = N(2-\sqrt{-5}) = 9$, dlužno čísla ta uvažovati vzhledem ku 3. I je $(1-\sqrt{-5})^2 = -2(2+\sqrt{-5})$, takže $2+\sqrt{-5} \sim \pi'^2_1$ (3), $(2+\sqrt{-5}) \doteq \mathfrak{p}'^2_1$, $(2-\sqrt{-5}) = \mathfrak{p}_1^2$; $9 = \mathfrak{p}_1^2 \mathfrak{p}'^2_1$. 3) $21 = 3.7 = (4+\sqrt{-5})(4-\sqrt{-5}) = (1+2\sqrt{-5})(1-2\sqrt{-5})$; (3) $= \mathfrak{p}_1 \mathfrak{p}'_1$; (7) $= \mathfrak{p}_2 \mathfrak{p}'_2$; $4+\sqrt{-5} = 3+(1+\sqrt{-5}) = 7-(3-\sqrt{-5})$ takže $4+\sqrt{-5} \sim \pi_1, (3)$; $\sim \pi'_2$, (7); i je $(4+\sqrt{-5}) = \mathfrak{p}_1 \mathfrak{p}'_2, (4-\sqrt{-5}) = \mathfrak{p}'_1 \mathfrak{p}_2$; podobně $1+2\sqrt{-5} = 3\sqrt{-5} + (1-\sqrt{-5}) = 7-2(3-\sqrt{-5})$ a proto $1+2\sqrt{-5} \sim \pi'_1$, (3); $\sim \pi'_2$, (7); takže $(1+2\sqrt{-5}) = \mathfrak{p}'_1 \mathfrak{p}'_2$. $1-2\sqrt{-5} = \mathfrak{p}_1 \mathfrak{p}_2$; $21 = \mathfrak{p}_1 \mathfrak{p}'_1 \mathfrak{p}_2 \mathfrak{p}'_2$.

Experimentální stanovení čísla π užitím počtu pravděpodobnosti.

Napsal Dr. **Antonín Hrazdil.**

V druhé polovici osmnáctého století francouzský mathematik a fysiolog G. L. Buffon (*1707 — †1788) předložil k řešení úlohu, známou pod jménem „problém jehly“ (problème de l'aiguille), která umožnila užitím počtu pravděpodobnosti ustanoviti experimentálně číslo π.

Problém ten zněl: „Na vodorovnou tabuli, pokrytou systémem aequidistantních rovnoběžek ve vzdálenosti $2a$ od sebe, hází se válcová jehla délky $2c$ ($\leq 2a$); jak velká jest pravděpodobnost, že jehla padne křížem přes některou z těch rovnoběžek?“

Řešení tohoto problému podal jednak Buffon sám, jednak — a to mnohem elegantněji — Laplace v „Théorie analytique des Probabilités“ str. 359—362. Leč oba byli nuceni použiti k němu počtu vyššího, infinitesimálního. Experimentálně zkoušel jejich výsledky R. Wolf a našel z 5000 hodů pro π hodnotu 3·159.