Časopis pro pěstování matematiky a fysiky

Karel Rychlík

O rozšíření pojmu kongruence

Časopis pro pěstování matematiky a fysiky, Vol. 58 (1929), No. 1-2, 92--94

Persistent URL: http://dml.cz/dmlcz/108911

O rozšíření pojmu kongruence.

K. Rychlík.

§ 1. Budeme uvažovati konečná i nekonečná množství P různých přirozených prvočísel. Množství všech takových prvočísel označíme $\bigvee$, příslušné „množství nulové“ neobsahující prvočísel označme $\bigwedge$.

§ 2. Je-li $P \neq \bigwedge$, nazveme čísla tvaru $p_1^{k_1}, p_2^{k_2} \dots p_m^{k_m}$, kdež $p_1, p_2, \dots p_m$ jsou prvočísla $2P$ a $k_1, k_2, \dots k_m$ celá čísla racionální, čísly v P znázornitelnými.

V $\bigvee$ je každé kladné racionální číslo znázornitelné. Za jediné číslo znázornitelné v $\bigwedge$ budeme považovati 1.

Racionální číslo $a \neq 0$ lze psáti ve tvaru

$$a = a_1 a_2 \operatorname{sgn} a,$$

kdež a_1 je znázornitelné v P, a_2 v $\bar{P}$, množství komplementární k P. Označme $a_1 = |a|_P$, tedy $a_2 = |a|_{\bar{P}}$. I jest

$$a = |a|_P \,.\, |a|_{\bar{P}} \,.\, \operatorname{sgn} a. \tag{1}$$

Položíme-li $|0|_P = 0$, bude (1) platiti i pro $a = 0$.

Pro $P = \bigvee$ je $|a|_\vee = |a|$.

Pro $P = \bigwedge$ je $|a|_\wedge = 1$, při $a \neq 0$, $|0|_\wedge = 0$.

Pro $|a|_P$ platí

$$|ab|_P = |a|_P \, |b|_P,$$

$$\left|\frac{a}{b}\right|_P = \frac{|a|_P}{|b|_P}, \text{ jestliže } b \neq 0.$$

§ 3. Racionální číslo a nazveme celým vzhledem k P, je-li $|a|_P$ celé (v obyčejném slova smyslu). Je-li e i $\frac{1}{e}$ celé vzhledem k P, nazveme e jednotkou vzhledem k P. Pak $|e|_P = 1$.

Je-li $a = bc$, kdež c je celé vzhledem k P, řekneme, ža a je dělitelno b vzhledem k P.

Vzhledem k $\bigvee$ jsou čísly celými čísla celá v obyčejném slova smyslu, dělitelnost vzhledem k $\bigvee$ je dělitelnost v obyč. sl. smyslu, jednotky jsou ± 1.

Vzhledem k $\bigvee$ jsou celými všechna čísla racionální, jednotkami jsou čísla racionální $\neq 0$.

Čísla celá vzhledem k P tvoří obor celistvosti, jehož podílovým tělesem je těleso čísel racionálních.

§ 4. Budiž m racionální číslo celé vzhledem k P. Jsou-li a, b čísla celá vzhledem k P a $a - b$ je dělitelno m vzhledem k P, řekneme, že a je kongruentní s b pro mod. m vzhledem k P,

$$a \equiv b \quad (\mathrm{mod}\, m;\, P)$$

Tato kongruence je vztah reflexivní, symetrický, transitivní.

Pro $m = 0$ přejde kongruence v rovnost; je-li m jednotka vzhledem k P, jsou spolu všechna čísla celá vzhledem k P kongruentní vzhledem k P.

Snadno lze nahlédnouti, že platí $a \equiv b$ (mod m; P) tehdy a jen tehdy, je-li $a \equiv b$ (mod $|m|_P$; P). Pro $m \neq 0$ stačí tedy uvažovati pouze případ, kdy m je celé číslo znázornitelné v P.

Budeme tedy předpokládati, že m je celé číslo znázornitelné v P. Každé číslo celé vzhledem k P, a, je kongruentní mod m; P s jediným z čísel $0, 1, 2, \ldots m - 1$ (nejmenší zbytky kladné).

Budiž $a = \dfrac{a'}{a''}$ znázornění a redukovaným zlomkem; a', a'' jsou čísla celá, nesoudělná a ježto a je celé vzhledem k P, je a'' nesoudělné s m. Lze tedy určiti celá čísla x, y tak, že bude

$$a''x + my = a',$$

tedy

$$\frac{a'}{a''} = x + m\,\frac{y}{a''}.$$

Bude tudíž $a \equiv x$ (mod m; P). Celé číslo x je mod m, tedy i mod m; P kongruentní s jediným z čísel $0, 1, 2, \ldots m - 1$.

Čísla spolu kongruentní (mod m; P) shrneme do téže třídy (mod m; P); libovolné číslo této třídy nazveme jejím representantem. Těchto tříd je na počet m a za representanty lze zvoliti čísla $0, 1, 2, \ldots m - 1$.

Z kongruence

$$a \equiv a', \quad (\mathrm{mod}\, m;\, P)$$
$$b \equiv b', \quad (\mathrm{mod}\, m;\, P)$$

plyne

$$a \pm b \equiv a' \pm b', \quad (\mathrm{mod}\, m;\, P)$$
$$ab \equiv a'\,b'. \quad (\mathrm{mod}\, m;\, P)$$

Lze tedy pro třídy (mod m; P) definovati sčítání, odčítání a násobení takto:

Je-li a representant třídy A,
b „ „ B,
bude $A + B$ třídu o representantu a $+ b$,
$A - B$ „ „ $a - b$,
AB „ „ ab.

Při takto definovaném sčítání a násobení tvoří třídy (mod m;P) okruh O (m, P). Označme O (m) okruh tvořený třídami (mod m). Je patrně

$$O\,(m) = O\,(m, \vee).$$

Pak platí věta:

Okruh O (m, P) je isomorfní s okruhem O (m).

Budiž A_P třída v O m; P). Jejím representantem ze soustavy nejmenších zbytků kladných nechť je a. Prvku a nechť v O (m) jako representantu odpovídá třída A. Tak je dán vzájemně jednoznačný vztah mezi A_P a A. A je to isomorfismus, ježto, odpovídá-li si A_P a A, B_P a B, odpovídají si též

$$A_P + B_P \text{ a } A + B,$$
$$A_P B_P \quad \text{ a } AB.$$

Uvedené úvahy bylo by možno rozšířiti i na případ algebraického tělesa číselného konečného stupně.

*

Sur une extension de la notion de congruence.

(Extrait de l'article précédent.)

Soient a, b, m deux nombres rationnels entiers par rapport (p. r.) à un ensemble de nombres premiers rationnels P[1]) . $a \equiv b$ (mod m; P) signifie que $a - b$ est divisible par m p. r. à P. Les nombres rationnels entiers p. r. à P, congrus p. r. à P à un nombre rationnel, entier p. r. à P, fixe, forment une classe p. r. à P. Si l'on définit l'addition et la multiplication pour ces classes, on obtient un anneau O $(m; P)$. Cet anneau est isomorphe à l'anneau O $(|m|_P)$, formé par les classes mod $|m|_P$. L'extension à un corps algébrique numérique d'ordre fini est imédiate.

[1]) Sur la notion des nombres entiers p. r. à P et de la divisibilité p. r. à P voir mon mémoire »Zur Theorie der Teilbarkeit in algebraischen Zahlkörpern«, Mémoires de la Société Royale des Sciences de Bohême, 1923, II. classe.