Kapitola I

ZÁKLADNÍ POJMY

§ 1 : OKRUHY, TĚLESA

V tomto paragrafu uvedeme základní algebraické pojmy a jejich vlastnosti v takovém rozsahu, jaký bude potřebný v dalším textu. V případě, že půjde o vlastnost známou z úvodního kurzu algebry, budeme se odkazovat na skripta L. Skuly [9].

Okruhem budeme všude v dalším vždy rozumět *komutativní okruh s jedničkou*, což je tedy množina s dvěma binárními operacemi (sčítáním, násobením), obvykle označovaná

$R = (R,+,.)$ nebo jen stručně R, při čemž :

1. $(R,+)$ je komutativní (abelovská) grupa
2. $(R,.)$ je komutativní pologrupa s jedničkou 1_R
3. násobení je distributivní vzhledem k sčítání, t.j. $a\,.\,(b+c) = a.b + a.c$,

   pro lib. $a,b,c \in R$.

Nejjednoduššími příklady okruhu jsou :

a) množiny Z, Q, R, K s operacemi obyčejného sčítání a násobení čísel

b) množina $G = \{a + bi \mid a,b \in Z\}$ s operacemi obyčejného sčítání a násobení čísel. Tento okruh nazýváme okruhem Gaussových celých čísel.

c) okruhy $Z_m = (Z_m, +, .)$ zbytkových tříd modulo m

d) jednoprvkový okruh $R = \{O_R\}$, který se nazývá triviální okruh. V tomto případě obě operace splývají a je $O_R = 1_R$ (jinak je vždycky $O_R \neq 1_R$!!). Tento okruh budeme většinou z našich úvah vylučovat, t. zn. budeme uvažovat pouze netriviální okruhy.

Příklad 1.1 : Na množině $Z \times Z$ definujeme operace $+$ a $.$ takto :

$$\begin{aligned} (x,y) + (x',y') &= (x+x', y+y') \\ (x,y) \,.\, (x',y') &= (x.x', y.y') \end{aligned} \qquad \text{pro lib. } x,x',y,y' \in Z$$

kde symboly $+$, . na pravé straně značí obyčejné sčítání a násobení čísel. Dostáváme takto okruh $Z \times Z = (Z \times Z\, , +, .)$, jehož jedničkou je zřejmě prvek $(1,1)$.

Příklad 1.2 : Nechť R je okruh a nechť n je pevné přirozené číslo. Kartézský součin $R \times R \times \ldots\ldots \times R$ (n - krát) označme R^n. Dále, symbolem $R^{(R^n)}$ označme množinu všech zobrazení z R^n do R, t.j.

$$R^{(R^n)} = \{\varphi \mid \varphi : R^n \to R\}.$$

Na množině $R^{(R^n)}$ definujeme operace $+$ a . takto : pro $\varphi, \psi \in R^{(R^n)}$ položíme

$$(\varphi + \psi)(r_1, \ldots, r_n) = \varphi(r_1, \ldots, r_n) + \psi(r_1, \ldots, r_n)$$
$$(\varphi . \psi)(r_1, \ldots, r_n) = \varphi(r_1, \ldots, r_n) . \psi(r_1, \ldots, r_n)$$
pro lib. $(r_1, \ldots, r_n) \in R^n$

kde symboly $+$, . na pravé straně značí sčítání, resp. násobení v okruhu R. Je ihned vidět, že $(\varphi + \psi), (\varphi . \psi) \in R^{(R^n)}$ a dále, že jsou splněny axiomy okruhu. Tedy $(R^{(R^n)}, +, .)$ je okruh, jehož jedničkou je zřejmě zobrazení ι definované : $\iota(r_1, \ldots, r_n) = 1_R$.

Ve specielním případě pro $n = 1$ dostáváme takto okruh $R^R = (R^R, +, .)$, jehož prvky jsou tedy zobrazení z R do R. Tento okruh budeme nazývat *okruh funkcí* (na R).

Definice : *Nechť R je okruh, prvek $r \in R$ se nazývá d ě l i t e l n u l y v R, jestliže $r \neq 0$ a existuje $s \in R$, $s \neq 0$ tak, že $r.s = 0$. Netriviální okruh, který neobsahuje dělitele nuly, se nazývá o b o r i n t e g r i t y.*

Příkladem oboru integrity jsou výše zmíněné okruhy $Z, Q, R, K, G,$ resp. okruh zbytkových tříd Z_m v případě, že m je prvočíslo (viz [9], str. 58). Naopak, triviální okruh, okruh $Z \times Z$ a okruh funkcí R^R nejsou obory integrity. Následující věta pak udává jinou charakterizaci oboru integrity.

Věta 1.1 : *Nechť R je netriviální okruh. Pak R je oborem integrity právě když v R platí zákon o krácení (t.j. $a, b, c \in R$, $a \neq 0$, $a.b = a.c \Rightarrow b = c$)*

[D ů k a z : I. nechť R je obor integrity; je-li $a.b = a.c$, $a \neq 0$, pak $a(b - c) = 0$, t. zn. podle předpokladu musí být $b - c = 0$, neboli $b = c$.

II. nechť v R platí zákon o krácení; nechť $a, b \in R$, $a \neq 0$, $a.b = 0$. Pak ale lze psát : $a.b = 0 = a.0$, t. zn. podle zákona o krácení je $b = 0$ a tedy R je obor integrity.]

Definice : *Nechť R je okruh. Prvek $e \in R$; k němuž existuje prvek inverzní (vzhledem k operaci násobení), se nazývá j e d n o t k a o k r u h u R. Množinu všech jednotek okruhu R budeme označovat symbolem $J(R)$.*

Zřejmě jednička 1_R je vždy jednotkou okruhu R , t. zn. $J(R)$ je neprázdná množina, při čemž obecně má okruh více jednotek. Např. okruh Z má právě 2 jednotky (a sice čísla $\pm$ 1), resp. okruh G celých Gaussových čísel má 4 jednotky (čísla ± 1, $\pm\, i$), resp. v okruzích **Q**, **R**, **K** je každý nenulový prvek jednotkou, atd.

Definice : *Okruh R , jehož množina nenulových prvků $R - \{0_R\}$ je grupou vzhledem k operaci násobení, se nazývá t ě l e s o .*

Poznámka : vzhledem k tomu, že operace násobení je všude v tomto textu komutativní, není nutné používat termínu komutativní těleso nebo pole, jak se někdy z důvodů rozlišení dělá. Z definice dále vyplývá, že těleso musí být vždy alespoň dvouprvkové (neboť $R - \{0_R\}$ je grupa, t. zn. neprázdná množina) a že každý nenulový prvek je jednotkou. Příkladem těles jsou např. $Q, R, K,$ při čemž to zdaleka nejsou všechny číselné množiny, které jsou tělesem vzhledem k operacím obyčejného sčítání a násobení, jak ukážeme dále. Na druhé straně, okruh Z , okruh funkcí R^R a okruh $Z \times Z$ zřejmě nejsou tělesa.

Definice : *Nechť $R = (R, +, .)$ je okruh. Je-li podmnožina $S \subseteq R$ vzhledem k operacím $+$, . okruhem (resp. tělesem), pak S se nazývá p o d o k r u h (resp. p o d t ě l e s o) o k r u h u R a R se pak nazývá n a d o k r u h o k r u h u (resp. t ě l e s a) S. Je-li navíc R tělesem, pak říkáme, že S je p o d o k r u h e m (resp. p o d t ě l e s e m) t ě l e s a R, při čemž R v tomto případě nazýváme n a d t ě l e s e m o k r u h u (resp. t ě l e s a) S.*

Je-li S podokruhem okruhu R a platí-li $1_S = 1_R$, pak S nazýváme u n i t á r n í m p o d o k r u h e m o k r u h u R.

Na příklad, okruh Z je unitárním podokruhem okruhu G , resp. okruh Z je podokruhem tělesa R, resp. těleso Q je podtělesem tělesa K. Je-li R těleso a uvážíme-li v okruhu funkcí R^R podmnožinu F všech konstantních zobrazení (t. j. zobrazení tvaru $\varphi(x) = c$, pro každé $x \in R$, kde $c \in R$ je pevný prvek), pak F je zřejmě podtělesem okruhu funkcí R^R. Nakonec si ještě ukažme, že podokruh obecně nemusí být unitárním podokruhem daného okruhu. Například v okruhu $Z \times Z$ (viz příklad 1.1.) je $S = \{(x, 0) \mid x \in Z\}$ podokruhem. Při tom však je:

$$1_S = (1,0) \neq (1,1) = 1_{Z \times Z}$$

a tedy podokruh S není unitárním podokruhem okruhu $Z \times Z$.

Definice : *Nechť R je okruh (resp. těleso); nechť existuje přirozené k s vlastností :*

$$(1) \qquad k.x = \underbrace{x + x + \ldots + x}_{k\text{ - krát}} = O_R \ , \quad \textit{pro každé } x \in R$$

Pak nejmenší takové k se nazývá c h a r a k t e r i s t i k a o k r u h u *(resp.* t ě l e s a *) R. Říkáme pak, že okruh (resp. těleso) R je charakteristiky k. Jestliže žádné přirozené k s vlastností (1) neexistuje, pak říkáme, že okruh (resp. těleso) R je charakteristiky O.*

V našem případě, kdy R má jedničku 1_R, lze určit charakteristiku R pouze vyšetřováním vlastností 1_R, jak ukazuje následující věta.

Věta 1.2: *Nechť R je okruh (resp. těleso). Existuje-li přirozené k takové, že $k.1_R = O_R$, pak nejmenší takové k je charakteristikou okruhu (resp. tělesa) R. Neexistuje-li žádné takové k, pak okruh (resp. těleso) R je charakteristiky O.*

[D ů k a z : nechť k je nejmenší přirozené číslo s vlastností : $k.1_R = O_R$. Pak pro libovolný prvek $r \in R$ je $k.r = r + r + \ldots + r = 1_R.r + 1_R.r + \ldots + 1_R.r = (1_R + 1_R + \ldots + 1_R).r = (k.1_R).r = O_R.r = O_R$, odkud plyne tvrzení.]

Vidíme tedy např., že triviální okruh je charakteristiky 1, okruh Z_m zbytkových tříd modulo m je charakteristiky m, okruh funkcí R^R je stejné charakteristiky jako je okruh R a všechny ostatní výše zmiňované okruhy nebo tělesa, t.j. $Z, G, Q, R, K, Z \times Z$ jsou charakteristiky O.

Definice : *Nechť $R = (R, +, .)$, $R' = (R', \oplus, \odot)$ jsou okruhy (resp. tělesa). Zobrazení $\varphi : R \to R'$ se nazývá* h o m o m o r f i z m u s o k r u h u *(resp.* t ě l e s a *) R* d o o k r u h u *(resp.* t ě l e s a *) R', jestliže pro libovolné $a,b \in R$ platí :*

$$\varphi(a + b) = \varphi(a) \oplus \varphi(b) \ , \quad \varphi(a \cdot b) = \varphi(a) \odot \varphi(b) \ .$$

Je-li navíc zobrazení φ injektivní, pak hovoříme o i z o m o r f i z m u *R do R' nebo též o* v n o ř e n í *R do R'. Je-li φ bijektivní, pak hovoříme o* i z o m o r f i z m u *R* n a *R' a říkáme, že R a R' jsou* i z o m o r f n í.

Poznámka : v dalším budeme obvykle operace sčítání, resp. násobení v R a R' označovat stejnými symboly. Nemůže dojít k nedorozumění, protože ze způsobu zápisu je patrné, zda jde o operaci v R nebo v R'. Základní vlastnosti homomorfizmů jsou probrány v [9]; uveďme si nyní pouze tuto větu :

Věta 1.3 : *Nechť R, R' jsou okruhy; nechť $\varphi : R \to R'$ je homomorfizmus okruhu R do R'. Pak $\varphi(R)$ je podokruhem v R'.*

[D ů k a z : je $\varphi(R) = \{x' \in R' \mid$ existuje $x \in R$ tak, že $\varphi(x) = x'\} \subsetneq R'$. Zřejmě je $\varphi(R) \neq \phi$ a je to množina uzavřená vzhledem k odečítání a násobení v R'. Navíc $\varphi(1_R)$ je jedničkou $\varphi(R)$. (Obecně však nikoliv jedničkou R'!!). Tedy $\varphi(R)$ je podokruhem okruhu R'.] .

Poznámka : je-li $\varphi : R \to R'$ vnořením R do R', pak zřejmě R a $\varphi(R)$ jsou z algebraického hlediska stejné (mají stejné vlastnosti). Můžeme tedy ztotožnit prvky z R s jim odpovídajícími prvky (t.j. jejich obrazy při φ) ve $\varphi(R)$ a okruh R můžeme pak považovat za podokruh okruhu R'.

Definice : *Každý podokruh (resp. podtěleso) tělesa K komplexních čísel nazýváme* č í s e l n ý m o k r u h e m *(resp.* č í s e l n ý m t ě l e s e m *).*

Vidíme tedy, že Z, resp. G jsou číselné okruhy ; Q, resp. R, resp. K jsou číselná tělesa. Další příklady číselných okruhů a těles jsou uvedeny ve cvičení 1. Je zřejmé, že každý netriviální číselný okruh je oborem integrity a je charakteristiky O. Zvláštní postavení mezi číselnými tělesy má těleso Q, které je mezi nimi "nejmenší", přesněji řečeno, je obsaženo v každém číselném tělese. Z obecnějšího hlediska tuto situaci popisuje následující věta.

Věta 1.4: *Nechť R je těleso charakteristiky 0. Pak existuje podtěleso S tělesa R, které je izomorfní s tělesem Q racionálních čísel.*

[D ů k a z : viz [9], důkaz V. 2.2.42.]

Na základě poznámky za V.1.3. můžeme tedy stručně říkat, že každé těleso charakteristiky 0 obsahuje těleso Q racionálních čísel.

§ 2. : DĚLITELNOST V OKRUHU A V OBORU INTEGRITY.

S pojmem dělitelnosti se můžeme setkat již na střední škole při vyšetřování dělitelnosti v oboru celých čísel. Nyní ukážeme, jak lze tyto otázky studovat obecněji v oboru integrity nebo dokonce v libovolném okruhu.

Definice : *Nechť R je okruh, nechť $a,b \in R$. Jestliže existuje prvek $r \in R$ takový, že $b.r = a$, pak říkáme, ze b d ě l í a (nebo též, že p r v e k a j e d ě l i t e l n ý p r v k e m b) a píšeme : $b \mid a$. V opačném případě říkáme, že b n e d ě l í a (nebo též, že a n e n í d ě l i t e l n ý b) a píšeme : $b \nmid a$. Relaci $\mid$ nazýváme relací dělitelnosti na R.*

Poznámka : je-li $a = 0$, pak zřejmě $b \mid 0$ pro každý prvek $b \in R$ (stačí totiž položit $r = 0$). Na druhé straně, je-li $b = 0$, pak $0 \mid a$ jedině v případě, že $a = 0$. Často se budeme při studiu dělitelnosti omezovat pouze na nenulové prvky z R.

Věta 2.1 : *Nechť R je okruh; pak platí :*

1. relace dělitelnosti na R je reflexivní a transitivní

2. jsou-li $a_1, \ldots, a_k, b \in R$ pevné prvky, pro něž $b \mid a_i$ $(i = 1, \ldots, k)$ a jsou-li $u_1, \ldots, u_k \in R$ libovolné, pak :

$$b \mid \sum_{i=1}^{k} a_i . u_i = a_1 u_1 + \ldots + a_k u_k$$

[D ů k a z : 1. zřejmě pro libovolné $a \in R$ je : $1.a = a$, t. zn. $a \mid a$. Dále, je-li $c \mid b$, $b \mid a$, pak podle definice existují $r,s \in R$ tak, že : $c.r = b$, $b.s = a$. Po dosazení je pak : $c.(r.s) = a$, t. zn. $c \mid a$.

2. je-li $b \mid a_i$, pak existuje $r_i \in R$ tak, že $b.r_i = a_i$ $(i = 1, \ldots, k)$ a tedy :

$$\sum_{i=1}^{k} a_i u_i = \sum_{i=1}^{k} b.r_i.u_i = b. \sum_{i=1}^{k} r_i u_i \text{, t. zn. } b \mid \sum_{i=1}^{k} a_i u_i .$$]

Poznámka : pomocí dělitelnosti lze rovněž charakterizovat pojem jednotky v R, definovaný v předchozím paragrafu. Zřejmě prvek $e \in R$ je jednotkou okruhu R právě když $e \mid 1_R$; navíc součin $e_1 \cdot \ldots \cdot e_k$ je jednotkou v R, právě když každé e_i $(i = 1, \ldots, k)$ je jednotkou v R. Odtud pak již lehce plyne, že množina $J(R)$ všech jednotek v R tvoří (vzhledem k operaci násobení v R) grupu.

Definice : *Nechť R je okruh. Jestliže pro $a,b \in R$ existuje jednotka $e \in J(R)$ tak, že platí : $a = b.e$, pak říkáme, že p r v e k a j e a s o c i o v á n s p r v k e m b, a píšeme : $a \sim b$. Jelikož relace $\sim$ je symetrická (jak bude ukázáno níže), budeme obvykle říkat, že p r v k y a, b j s o u a s o c i o v á n y (v R).*

Věta 2.2 : *Nechť R je okruh; pak relace asociovanosti $\sim$ je relací ekvivalence na množině R.*

[D ů k a z : reflexivita : $a = a . 1$, t. zn. $a \sim a$ pro libovolné $a \in R$.

symetrie : nechť $a \sim b$, t. zn. existuje $e \in J(R)$ tak, že $a = b.e$. Ale $e^{-1} \in J(R)$ a po vynásobení tímto prvkem dostáváme : $b = a.e^{-1}$, t. zn. $b \sim a$.

transitivita : nechť $a \sim b$, $b \sim c$, t. zn. existují $e_1, e_2 \in J(R)$ tak, že $a = b.e_1$, $b = c.e_2$, t. zn. dosazením : $a = c.(e_2.e_1)$, přičemž $e_2.e_1 \in J(R)$. Tedy $a \sim c$.]

Poznámka : z předchozí věty plyne, že relace asociovanosti $\sim$ vytváří na R jistý rozklad. Třídy tohoto rozkladu jsou tvořeny vždy navzájem asociovanými

prvky. Prvek O_R sám o sobě vždy vytváří jednu takovou třídu. Dále pak všechny
jednotky okruhu R tvoří další třídu tohoto rozkladu, neboť jsou asociovány s prv-
kem 1_R. Je-li specielně R tělesem, pak všechny nenulové prvky jsou navzájem
asociovány (neboť jsou to jednotky) a tedy rozklad, příslušný relaci $\sim$ má právě
dvě výše zmiňované třídy $\{ O \}$ a $R - \{ O \}$. Z hlediska dělitelnosti je proto
těleso pro nás nezajímavé a v dalších větách se omezíme na situaci, s níž se budeme
nejčastěji setkávat, t. zn. na případ, že R je oborem integrity.

Věta 2.3: *Nechť R je obor integrity; $a,b \in R$. Pak platí :*

$$a \sim b \quad \Leftrightarrow \quad a \mid b \,,\; b \mid a \,.$$

[D ů k a z : " $\Rightarrow$ " je-li $a \sim b$, pak existuje jednotka $e \in J(R)$ tak,
že $a = b.e$. Odtud pak $b = a.e^{-1}$. Tedy je $a \mid b$, $b \mid a$.
" $\Leftarrow$ " nechť $a \mid b$, $b \mid a$. Je-li $a = 0$, pak musí být i
$b = 0$ a tedy $a \sim b$. Nechť tedy $a \neq 0$. Pak existují prvky $r,r' \in R$ tak, že
$a.r = b$, $b.r' = a$, t. zn. po dosazení : $a.(r.r') = a = a.1$, odkud podle
V. 1.1. je $r.r' = 1$ a tedy $r,r' \in J(R)$. Potom však je $a \sim b$.]

Věta 2.4 : *Nechť R je obor integrity ; nechť $a, b, a', b' \in R$. Pak*
1. pro každou jednotku $e \in J(R)$ a každý prvek $r \in R$ platí : $e \mid r$
2. je-li $a' \sim a$, $b' \sim b$, pak $a \mid b$ právě když $a' \mid b'$.

[D ů k a z : ad 1 : platí $r = 1.r = e.(e^{-1}.r)$, t. zn. $e \mid r$.
ad 2 : nechť $a' \sim a$, $b' \sim b$, $a \mid b$. Pak užitím V.2.3. lze
psát : $a' \mid a$, $a \mid b$, $b \mid b'$ odkud vzhledem k transitivitě relace dělitelnosti
dostáváme : $a' \mid b'$. Opačná implikace se dokáže analogicky.]

Poznámka : z předchozích dvou vět vidíme, že každý prvek daného oboru
integrity R je vždy dělitelný všemi jednotkami z R a všemi s ním asociovanými
prvky. Zavedeme proto následující definici.

Definice : *Nechť R je obor integrity, nechť $r \in R$. Pak všechny jednotky*
z R a všechny prvky asociované s r se nazývají n e v l a s t n í d ě l i t e l é
prvku r . Ostatní dělitelé prvku r (pokud existují) se nazývají v l a s t n í d ě -

l i t e l é .

Nechť $p \in R$ je nenulový prvek, který není jednotkou v R . Pak prvek p se nazývá r e d u c i b i l n í (resp. i r e d u c i b i l n í) v R , jestliže má (resp. nemá) vlastní dělitele v R.

Poznámka : jinými slovy řečeno, prvek $p \in R$ je ireducibilní v R , jestliže jej nelze napsat jako součin dvou prvků z R , z nichž žádný není jednotkou, ani není s prvkem p asociován. Z definice dále vidíme, že v tělese (kde každý nenulový prvek je jednotkou) nemá vyšetřování reducibility a ireducibility smysl.

Věta 2.5: *Nechť R je obor integrity; nechť $p , q \in R$ a platí $p \sim q$. Pak : prvek p je ireducibilní v R právě když prvek q je ireducibilní v R.*

[D ů k a z : ze symetrie relace $\sim$ plyne, že stačí dokázat pouze jednu implikaci. Nechť tedy p je ireducibilní v R a dále nechť $e \in J(R)$ je jednotka v R taková, že $p = q.e$. Odtud plyne, že $q \neq 0$, $q \notin J(R)$. Dále sporem : je-li q reducibilní, pak $q = a.b$, kde $a,b \notin J(R)$; a, b nejsou asociovány s q . Pak ale $p = q.e = (e.a).b$, při čemž $e.a, b \notin J(R)$ a zřejmě $e.a, b$ nejsou asociovány s p. Pak p je reducibilní, což je spor. Tedy q je ireducibilní.]

Příklad 2.1 : Okruh Z celých čísel má dvě jednotky, a sice ± 1, t. zn. k danému číslu $c \in Z$ jsou asociovány pouze $\pm c$. Tedy číslo $p \in Z$ je ireducibilním prvkem v Z právě tehdy, když $p \neq 0$, $p \neq \pm 1$. a jeho jedinými děliteli jsou čísla ± 1, $\pm p$. Stručně řečeno, p je ireducibilním prvkem v Z právě když absolutní hodnota z čísla p je prvočíslo.

Definice : *Nechť R je obor integrity, nechť M je neprázdná podmnožina R. Pak prvek $t \in R$ se nazývá společný dělitel množiny M v R , jestliže je $t \mid m$ pro každý prvek $m \in M$. Píšeme pak : $t \mid M$.*

Prvek $d \in R$ se nazývá n e j v ě t š í s p o l e č n ý d ě l i t e l m n o - ž i n y M v R , je-li :

(i) $d \mid M$

(ii) pro $s \in R$ s vlastností $s \mid M$ je $s \mid d$.

V případě, že M je konečná množina, např. $M = \{a_1, a_2, \ldots, a_n\}$, pak hovoříme o společném děliteli (resp. největším společném děliteli) prvků $a_1, a_2, \ldots, a_n$ v R.

Poznámka : z předchozí definice obecně neplyne existence největšího společného dělitele množiny M (ať už konečné nebo nekonečné). Na druhé straně, o jednoznačnosti největšího společného dělitele lze zcela obecně vyslovit tuto větu :

Věta 2.6 : *Nechť R je obor integrity a nechť existuje největší společný dělitel d množiny M v R. Pak $D = \{r \in R \mid r \sim d\}$ je množina všech největších společných dělitelů množiny M v R.*

[D ů k a z : I. nechť $q \in R$ je největší společný dělitel množiny M. Prvek d však splňuje : $d \mid M$, t. zn. podle definice je $d \mid q$. Analogicky je $q \mid d$, neboť d je podle předpokladu největší společný dělitel M. Tedy : $d \mid q$, $q \mid d$ a podle V.2.3. je $q \sim d$, t. zn. $q \in D$.

II. nechť $q \in D$; pak existuje jednotka $e \in J(R)$ tak, že $q = d.e$. Ale z toho, že d je největší společný dělitel M bezprostředně plyne, že $d.e = q$ je také největší společný dělitel množiny M v R.]

Kongruence, rozklad na zbytkové třídy.

Věta: Nechť a, b jsou celá čísla taková, že $b \neq 0$. Potom existují celá čísla q, r splňující vztah:

$a = bq + r$, $0 \leq r < |b|$, přičemž toto vyjádření je jednoznačné.

Poznámka: Je nutno si uvědomit, že zbytek r při dělení je vždy nezáporný, a to i při dělení záporným číslem. Např. a = –26, b = 8, q = –4, r = 6, protože –26 = 8 . (–4) + 6.

Poznámka: Celá čísla a, b jsou nesoudělná, je-li jejich největší společný dělitel roven jedné. V opačném případě se nazývají soudělná. Největší společný dělitel čísel a, b budeme označovat NSD(a, b), nejmenší kladný společný násobek NSN(a, b).

Eulerova funkce $\varphi(n)$ vyjadřuje počet přirozených čísel menších nebo rovných číslu n, nesoudělných s n. Nechť $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, pak platí $\varphi(n) = n \cdot \prod_{i=1}^{k}(1-\frac{1}{p_i})$. Je-li n prvočíslo, pak $\varphi(n) = n - 1$.

Kongruence: $a, b \in \mathbf{Z}$, $m \in \mathbf{N}$, $m \geq 2$. Platí $a \equiv b \Leftrightarrow m \mid (a-b)$. Čteme: Číslo a je kongruentní s číslem b podle modulu m. Dvě čísla kongruentní podle nějakého modulu m dávají při dělení tímto modulem m týž zbytek. Relace kongruence je ekvivalence na množině všech celých čísel (je reflexivní, symetrická a tranzitivní).

Vlastnosti kongruencí:

1) p prvočíslo, pak $a \equiv b \pmod{p^n} \Rightarrow a \equiv b \pmod{p}$

Platí-li kongruence podle modulu, který je mocninou prvočísla, platí i podle modulu rovného tomuto prvočíslu.

2) $a \equiv b \pmod{m_i}$, $i = 1,2,\ldots,k \Rightarrow a \equiv b \pmod{\mathrm{NSN}(m_1,\ldots,m_k)}$

Platí-li kongruence podle několika modulů, platí i podle modulu rovného nejmenšímu společnému násobku těchto modulů.

3) $a_i \equiv b_i \pmod{m}$, $i = 1,\ldots,k \Rightarrow \sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \pmod{m}$, $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{m}$.

Kongruence podle téhož modulu lze sčítat i násobit.

Nechť v dalším platí $a \equiv b \pmod{m}$:

4) $a + x \equiv b + x \pmod{m}$, $a \cdot y \equiv b \cdot y \pmod{m}$

K oběma stranám kongruence lze přičíst stejné celé číslo a obě strany kongruence lze vynásobit týmž celým číslem. **Obecně ale nelze obě strany kongruence dělit týmž celým číslem,** např. 24 ≡ 40 (mod 8), ale po vydělení čtyřmi 6 ≢ 10 (mod 8).

5) $m \mid z \Rightarrow a + z \equiv b \pmod{m}$

Celé číslo, které je násobkem modulu, lze přičíst pouze k jedné straně kongruence.

6) $a^n \equiv b^n \pmod{m}$

Obě strany kongruence lze umocnit na libovolný přirozený exponent.

7) $d \mid a \wedge d \mid b \wedge \mathrm{NSD}(d, m) = 1 \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{m}$

Obě strany kongruence lze vydělit celým číslem nesoudělným s modulem.

8) $ac \equiv bc \pmod{mc}$

Obě strany kongruence i modul lze vynásobit týmž celým kladným číslem.

9) $e \mid a \wedge e \mid b \wedge e \mid c \Rightarrow \frac{a}{e} \equiv \frac{b}{e} \pmod{\frac{m}{e}}$

Obě strany kongruence i modul lze vydělit týmž celým kladným číslem různým od nuly.

10) $a \equiv b \pmod{m} \wedge d \mid m \Rightarrow a \equiv b \pmod{d}$

Platí-li kongruence podle modulu m, platí i podle modulu rovného libovolnému kladnému děliteli čísla m, většímu než jedna.

Eulerova věta: $m \in \mathbf{N}$, $m > 1$, $a \in \mathbf{Z}$, NSD(a, m) = 1, pak $a^{\varphi(m)} \equiv 1 \pmod{m}$.
Je-li specielně p prvočíslo, které není dělitelem čísla a, pak platí $a^{p-1} \equiv 1 \pmod{p}$ (tzv. malá Fermatova věta).