1 Úvod

Poznámka (Informační zdroje)
Stránky, diskuze na google docs, Moodle.

Poznámka (Proč algebra)
Diofanctické rovnice (Fermatovy věty, Gaussova celá čísla), kořeny polynomů (Grupy polynomů), geometrie (nekonstruovatelnost), studium abstraktních struktur běžných objektů.

2 Obory

Definice 2.1 (Okruh)

Okruh R je pětice $(R, +, \cdot, -, 0)$, kde $+, \cdot : R \times R \to R$, $- : R \to R$, $0 \in R$ tak, že $(\forall a, b, c \in R)$:

$$a + (b + c) = (a + b) + c,$$

$$a + b = b + a, a + 0 = a, a + (-a) = 0,$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, a \cdot (b + c) = a \cdot b + a \cdot c, (b + c) \cdot a = b \cdot a + c \cdot b.$$

Definice 2.2 (Komutativní okruh)

Komutativní okruh je okruh, pro který platí $a \cdot b = b \cdot a$.

Definice 2.3 (Okruh s jednotkou)

Okruh s jednotkou je okruh, který má prvek $1 \in R : a \cdot 1 = a$.

Definice 2.4 (Obor (integrity))

Obor (integrity) je komutativní okruh s jednotkou tak, že $0 \neq 1 \wedge (a \neq 0 \wedge b \neq 0 \implies a \cdot b \neq 0)$.

Definice 2.5 (Těleso)

Těleso je komutativní okruh s 1, že $0 \neq 1$ a $\forall 0 \neq a \in R \; \exists b \in R : a \cdot b = 1$.

Definice 2.6 (Podokruh)

Podokruh S okruhu R je $(S, +|_S, \cdot|_S, -|_S, 0)$, kde $0 \in S$ a $\forall a, b \in S : a + b \in S \wedge a \cdot b \in S \wedge -a \in S$. Značíme $R \leq S$.

Definice 2.7 (Podobor)

S je podobor oboru R tehdy, když $S \leq R$ a S je obor.

Definice 2.8 (Podtěleso)

S je podtěleso tělesa R tehdy, když $S \leq R$ a S je těleso.

Definice 2.9 (Gaussova čísla)

$\mathbb{Z}[i] = \{a + b_i | a, b \in \mathbb{Z}\}$ jsou tzv. Gaussova celá čísla.

$\mathbb{Q}[i] = \{a + bi | a, b \in \mathbb{Q}\}$ jsou tzv. Gaussova racionální čísla..

2.1 Základní vlastnosti

Tvrzení 2.1

Mějme množinu X s asociativní (tj. $(a * b) * c = a * (b * c)$) operací $* : X \times X \to X$. Pak hodnota výrazu $a_1 * a_2 * a_3 * \ldots * a_n$ nezávisí na uzávorkování.

Důkaz
Indukcí. □

Tvrzení 2.2 (Základní vlastnosti oborů)

Buď R okruh a $a, b, c \in R$.

$$1) a + c = b + c \implies a = b,$$

$$2) a \cdot 0 = 0,$$

$$3) -(-a) = a,\ -(a + b) = -a + (-b),$$

$$4) -(a \cdot b) = (-a) \cdot b = a \cdot (-b),\ (-a) \cdot (-b) = a \cdot b,$$

$$5) \textit{Je-li } R \textit{ obor, pak } a \cdot c = b \cdot c \wedge c \neq 0 \implies a = b.$$

Důkaz

$$1)(a + c) + (-c) = (b + c) + (-c) \implies a + 0 = b + 0 \implies a = b,$$

$$2) 0 + a \cdot 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \implies 0 = a \cdot 0.$$

□

Tvrzení 2.3 (Každé těleso je obor)

Z existence a^{-a} vyplývá $a \neq 0, b \neq 0 \implies ab \neq 0$.

Důkaz (Sporem)
$a \neq 0, b \neq 0, ab = 0 \implies b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (ab) = a^{-1} \cdot 0$ a podle předchozího tvrzení (část 2) $b = 0$ ↯. □

Tvrzení 2.4

Každý konečný obor je těleso.

Důkaz
Viz skripta. □

Definice 2.10

Nechť R je okruh s jednotkou 1. Charakteristika R je nejmenší přirozené číslo n tak, že $\underbrace{1 + 1 + \ldots + 1}_{n\text{-krát}}$, pokud takové n neexistuje, říkáme, že charakteritika je 0 (případně ∞).

Prvek $\underbrace{1 + 1 + \ldots + 1}_{n\text{-krát}}$ značíme n, obdobně $\underbrace{-1 - 1 - \ldots - 1}_{n\text{-krát}}$ značíme $-n$.

Tvrzení 2.5

Každý obor má charakteristiku 0 nebo p.

Důkaz
Pro 1 je to cvičení. V případě, že charakteristika je $n = k \cdot l$, $k, l \neq 1$, pak $0 = k \cdot l$. Jsme v oboru, tedy $k = 0$ nebo $l = 0$. Spor s minimalitou n. □

2.2 Izomorfismus

Definice 2.11 (Homomorfismus)

Nechť R, S jsou okruhy. Zobrazení $\varphi : R \to S$ je homomorfismus okruhů, pokud $\forall a, b \in R$:

$$\varphi(a + b) = \varphi(a) + \varphi(b) \wedge \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Je-li homeomorfismus φ bijekce, nazývá se izomorfismus.

Poznámka
Inverzní zobrazení k izomorfismu je izomorfismus.

Definice 2.12

Okruhy R, S jsou izomorfní, pokud existuje izomorfismus $\varphi : R \to S$. Značíme $R \simeq S$.

Například
Tzv. prvookruh (tj. všechny prvky tvaru $1 + 1 + \ldots + 1$ nějakého okruhu s jedničkou) je izomorfní $\mathbb{Z}_n$ resp. (v tomto případě musíme zahrnout i $-1 - 1 - \ldots - 1$) $\mathbb{Z}$.

2.3 Podílové těleso

Definice 2.13 (Multiplikativní množina)

Nechť R je obor. Pak $M \subseteq R$ je multiplikativní množina, pokud $0 \notin M, 1 \in M$ a $a, b \in M \implies a \cdot b \in M$.

Například
Nejdůležitější MM je $M = R \setminus \{0\}$.

Definice 2.14 (Podílové těleso)

Nechť R je obor a M multiplikativní množina. Definujeme relaci $\sim$ na $R \times M$:

$$(a, b) \sim (c, d) \equiv ad = bc.$$

Blok $[(a, b)]_\sim$ nazýváme zlomek a značíme $\frac{a}{b}$.

Na $Q = \left\{ \frac{a}{b} | a \in R, b \in M \right\}$ definujeme operace

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \ \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}, \ -\frac{a}{b} = \frac{-a}{b}, \ 0 = \frac{0}{1}, 1 = \frac{1}{1}.$$

Tedy Q je okruh s jednotkou. $(Q, +, -, \cdot, 0, 1)$ se nazývá lokalizace oboru R v MM M. Pokud $M = R \setminus \{0\}$, pak se nazývá podílové těleso.

Tvrzení 2.6

Máme R, N, Q z předchozí definice. 1) Q je obor. 2) $\left\{ \frac{a}{1} | a \in R \right\}$ je podobor Q, který je izomorfní s R. 3) Je-li $M = R \setminus \{0\}$, pak Q je těleso.

Důkaz
1) Ověříme axiomy. Triviální. Důležitý je hlavně součin ne0 prvků.

2) Ověříme uzavřenost a obsah jedničky. Ověříme, že zjevné zobrazení je izomorfizmus.

3) Ověříme axiomy. Na tři řádky. □

3 Polynomy

3.1 Obory polynomů

Poznámka (Značení)
V celé sekci Polynomů je R komutativní okruh s jednotkou.

Definice 3.1 (Polynom)

Polynom v proměnné x nad okruhem R je výraz tvaru

$$a_0 + a_1 \cdot x + a_2 \cdot x^2 + a_n \cdot x^n,$$

kde $n \geq 0$, $a_1, \ldots, a_n \in R$ a $a_n \neq 0$ vyjma $n = 0$. $a_1, \ldots, a_n$ jsou koeficienty, x proměnná. Navíc se dodefinovává $a_m = 0 \forall m > n$.

Číslo $n = \deg f$ je stupeň polynomu f. $\deg 0 = -1$. a_n se nazývá vedoucí koeficient a a_0 absolutní člen.

f je monický, pokud $a_n = 1$. Množinu všech polynomů značíme $R[x]$.

Definice 3.2 (Operace na $R[x]$)

$$\sum_{i=0}^{m} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{max(m,n)} (a_i + b_i) x^i; \; -\sum_{i=0}^{m} a_i x^i = \sum_{i=0}^{m} -a_i x^i;$$

$$\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{m+n} \sum_{j+k=i, j,j\geq 0} (a_j \cdot b_k) x^i$$

Tvrzení 3.1

$R[x]$ je komutativní okruh s jednotkou. Navíc je-li R obor, pak i $R[x]$ je obor $\wedge \deg(fg) = \deg f + \deg g \; \forall f, g \in R[x], f \neq 0 \neq g$.

Důkaz
Jednoduché, ve skriptech. Druhá část přes vedoucí koeficienty (jsou nenulové). □

Definice 3.3 (Polynom více proměnných)

Induktivní definicí: Polynom v proměnných $x_1, x_2, \ldots, x_m$ nad okruhem R je polynom v proměnné x_m nad okruhem $R[x_1, \ldots, x_{m-1}]$.

Značíme $R[x_1, \ldots, x_m] = (R[x_1, \ldots, x_{m-1}])[x_m]$.

Každý $f \in R[x_1, \ldots, x_m]$ jde jednoznačně napsat v distribuovaném tvaru (je potřeba

dokázat, ale tím pádem nezáleží na pořadí proměnných):

$$\sum_{k_1,\ldots,k_m}^{n} a_{k_1,\ldots,k_m} x_1^{k_1} \cdot \ldots \cdot x_m^{k_m}.$$

3.2 Hodnota polynomu

Definice 3.4

$R \leq S$ obory. $f = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n \in R[x], u \in S$. Hodnota polynomu f po dosazení u je definována:

$$f(u) := a_0 + a_1 \cdot u + \ldots + a_n \cdot u^n \in S.$$

(Operace jsou v oboru S.)

Zobrazení $S \to S$, $u \mapsto f(u)$ nazýváme polynomiální zobrazení dané polynomem f.

3.3 Dělení polynomu se zbytkem

Definice 3.5

$f, g \in R[x]$. g dělí f, zapisujeme $g|f$, $\equiv \exists h \in R[x]$ tak, že $f = gh$.

Je-li R obor a $g|f \neq 0 \implies \deg g \leq \deg f$ z tvrzení výše.

Tvrzení 3.2 (Dělení polynomů se zbytkem)

Nechť R je obor, Q podílové těleso. $f, g \in R[x], g \neq 0$. Pak existuje právě jedna dvojice $q, r \in Q[x]$:

$$f = gq + r \wedge \deg r < \deg g.$$

Je-li navíc g monický, pak $q, r \in R$.

$fdivg := q$ *a* $fmodg := r$.

Důkaz
$q_0 = 0, r_0 = f$. Induktivně ($l(f) :=$ vedoucí koeficient polynomu f):

$$q_{i+1} = q_i + \frac{l(r_i)}{l(g)} x^{\deg r_i - \deg g},\ r_{i+1} = r_i - \frac{l(r_i)}{l(g)} x^{\deg r_i - \deg g} \cdot g.$$

Vidíme, že stupeň r_i se snižuje, a když $\deg r_i < \deg g$, tak skončíme a $r = r_i, q = q_i$.

Jednoznačnost:

$$f = gq + r = g\tilde{q} + \tilde{r} \implies g(q - \tilde{q}) = \tilde{r} - r \implies g|\tilde{r} - r \implies \tilde{r} - r = 0.$$

□

3.4 Kořeny a dělitelnost

Definice 3.6

Ať $R \leq S$ jsou obory, $f \in R[x]$, $a \in S$. Pak a je kořen $f \equiv f(a) = 0$.

Tvrzení 3.3

Buď R obor, $f \in R[x]$, $a \in R$. a je kořen $f \Leftrightarrow x - a | f$.

Důkaz
$\implies$: $f = (x - a) \cdot g$ pro nějaké $g \in R[x] \implies f(a) = (a - a) \cdot g(a) = 0$.

Buď $q, r \in R[x]$ podíl a zbytek při dělení f monickým polynomem $x - a$. $f = (x - a) \cdot q + r$, $\deg r < \deg(x - a) = 1 \implies r$ je konstantní polynom. Dosadíme a:

$$0 = f(a) = (a - a)q(a) + r(a) = r(a).$$

r je konstantní $\implies r = 0$. $f = (x - a) \cdot q + 0 \implies x - a | f$. □

Pozorování

$$f mod x - a = f(a)$$

Věta 3.4 (Počet kořenů)

R obor, $0 \neq f \in R[x]$. Pak f má nejvýše $\deg f$ *kořenů v R.*

Důkaz
Indukcí dělením $x -$ kořen. □

Definice 3.7 (Vícenásobný kořen)

Ať $f \in R[x], a \in R$. Pak a je n-násobný kořen $f \equiv (x-a)^n | f$ a $(x-a)^{n-1} \nmid f$.

4 Číselné obory

4.1 Okruhová a tělesová rozšíření

Definice 4.1

Nechť $R \leq S$ jsou komutativní okruhy, $a_1, \ldots, a_n \in S$. Definujeme $R[a_1, \ldots, a_n]$ jako nejmenší podokruh okruhu S, který obsahuje R a $a_1, \ldots, a_n$. Ten nazveme okruhové rozšíření R o prvky $a_1, \ldots, a_n$.

Nechť $R \leq S$ jsou tělesa, $a_1, \ldots, a_n \in S$. Definujeme $R(a_1, \ldots, a_n)$ jako nejmenší podtěleso tělesa S, které obsahuje R a $a_1, \ldots, a_n$. To nazveme tělesové rozšíření R o prvky $a_1, \ldots, a_n$.

Tvrzení 4.1

Mějme $R \leq S$ komutativní okruhy s 1, $a \in R$. Pak $R[a] = \{f(a) | f \in R[x]\}$. Jsou-li R, S navíc tělesa, pak $R(a) = \left\{ \frac{f(a)}{g(a)} | f, g \in q[R], g(a) \neq 0 \right\}$.

Důkaz
Dokážeme, že je to podokruh, že obsahuje R i a a že je nejmenší takový. □

Pozorování
Ať $T \leq S$ jsou tělesa, potom $T[a] \subseteq T(a)$.

Ale např. $\mathbb{Q}[i] = \mathbb{Q}(i)$.

Tvrzení 4.2

Nechť $T \leq S$ jsou tělesa, a není kořenem žádného nenulového polynomu z $T[x]$. Pak $T[a] \neq T(a)$.

Důkaz
Podle předchozího tvrzení $T[a] = \{f(a) | f \in T[x]\}$. Kdyby $T[a] = T(a)$, pak $T[a]$ je těleso, tedy $a^{-1} \in T[a] \implies a^{-1} = f(a)$ pro nějaký $f \in T[x]$, tedy $a \cdot f(a) - 1 = 0$. Tedy a je kořenem $x \cdot f - 1$. ↯. □

4.2 Algebraická a transcendentní čísla

Definice 4.2

$a \in \mathbb{C}$ je algebraické, pokud je kořenem nějakého nenulového polynomu $f \in \mathbb{Z}[x]$.

Jinak a je transcendentní.

Poznámka (První důkaz transcendentního čísla)
Luvil? $\sum_{i=1}^{\infty} 10^{-i!}$.

Další čísla (19. stol): π, e.

Cantor: náhodné reálné číslo je transcendentní (tj. algebraická čísla jsou spočetná / mají míru 0).

Tvrzení 4.3

Množina algebraických čísel je spočetná.

Důkaz
Indexem polynomu $f = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x], f \neq 0$ nazvěme číslo $|a_0| + |a_1| + \ldots + |a_n| + n \in N$. Indexů existuje jen konečně mnoho daného indexu (díky započítání stupně do indexu). Všechny polynomy seřadím podle rostoucího indexu. Nyní už je zřejmě $\mathbb{Z}[x]$ spočetná. Navíc každý polynom má konečně kořenů, tedy, tedy i kořenů je spočetně mnoho. □

Tvrzení 4.4

Množina reálných čísel je nespočetná.

5 Elementární teorie čísel

5.1 Dělitelnost a základní věta aritmetiky

Definice 5.1 (Dělitelnost v celých číslech)

Ať $a, b \in \mathbb{Z}$, b dělí a, značíme $b|a$, pokud $\exists c \in \mathbb{Z} : a = bc$.

± 1 a $\pm a$ se nazývají nevlastní dělitelé, ostatní jsou vlastní.

Tvrzení 5.1

Mějme $a, b \in \mathbb{Z}$, $b \neq 0$. Pak $\exists! q, r \in \mathbb{Z} : a = qb + r, 0 \leq r < |b|$. Značíme $a \div b = q$ $a \bmod b = r$. Navíc $b|a \Leftrightarrow a \bmod b = 0$

Definice 5.2 (Prvočíslo a složené číslo)

Prvočíslo je $p \in \mathbb{Z}, p > 1$, které má pouze nevlastní dělitele. Ostatní přirozená čísla > 1 jsou složená.

Věta 5.2 (Základní věta aritmetiky)

$\forall a \in \mathbb{Z}, a > 1$ *existují po dvou různá prvočísla* $p_1, \ldots, p_n$ *a* $k_1, \ldots, k_n \in \mathbb{N}$ *tak, že* $a = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$. *Tento rozklad je až na pořadí jednoznačný.*

Důkaz
Později. □

5.2 NSD

Definice 5.3 (NSD, NSN)

Největší společný dělitel $a, b \in \mathbb{Z}$ je největší $c \in \mathbb{N}$ takové, že $c|a, c|b$. Značíme ho $\text{NSD}(a, b)$ (neexistuje pro $a = b = 0$).

Nejmenší společný násobek $a, b \in \mathbb{Z} \setminus \{0\}$ je nejmenší $c \in \mathbb{N}$ tak, že $a|c$ a $b|c$. Značíme ho $\text{NSN}(a, b)$.

Poznámka
Základní věta aritmetiky $\implies a \cdot b = \text{NSD}(a, b) \cdot \text{NSN}(a, b)$.

Rychlý algoritmus na hledání NSN je Euklidův algoritmus.

Tvrzení 5.3 (Bézoutova rovnost)

$\forall a, b \in \mathbb{Z}$, $a \neq 0$ *nebo* $b \neq 0$, $\exists u, v \in \mathbb{Z}$ *(Bézoutovy koeficienty) tak, že* $a \cdot u + b \cdot v = \text{NSD}(a, b)$.

Důkaz
Rozšířený Euklidův algoritmus. □

Lemma 5.4

Ať p *je prvočíslo,* $a, b \in \mathbb{Z}$. *Pak* $p|a \cdot b \implies p|a \vee p|b$.

Poznámka
V obecném oboru neplatí. Např. v $\mathbb{Z}[\sqrt{5}]$ $2|(\sqrt{5}+1)(\sqrt{5}-1) = 4$, ale $2 \not| \sqrt{5} \pm 1$

Důkaz
BÚNO $p \not| a$, tedy chceme, aby $p|b$. p je prvočíslo, tudíž nemá vlastní dělitele $\implies$ NSD(p, a) = buď p (to by ale $p|a$), nebo 1. Dle tvrzení o Bézoutově rovnosti $\exists u, v \in \mathbb{Z}$: $pu + av = 1$. Vynásobíme b: $pbu + abv = b$. Ale $p|ab$, takže $p|pbu + abv = b$. □

Lemma 5.5

p prvočíslo, $a_1, \ldots, a_n \in \mathbb{Z}$. $p|a_1 \cdot \ldots \cdot a_n \implies \exists i : p|a_i$.

Důkaz
Indukcí z předchozího tvrzení. □

Důkaz (Základní věta aritmetiky)
Existence: pro spor ať a je nejmenší přirozené číslo, které nemá rozklad na součin. Buď je a prvočíslo, ale pak má rozklad $a = a^1$. Nebo je a složené, tedy $a = b \cdot c, 1 < b, c, < a$, ale a bylo nejmenší číslo, které nemá rozklad, tedy b i c mají rozklad. Ale pak součin těchto rozkladů je a.

Jednoznačnost: a nejmenší přirozené číslo, které má 2 rozklady: $a = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m} = q_1^{l_1} \cdot \ldots \cdot q_n^{l_n}$. Pak $p_1|q_1^{l_1} \cdot \ldots \cdot q_n^{l_n}$. Podle předchozího lemmatu $\exists i : p_1|q_i$. Jsou to prvočísla, tedy $p_1 = q_i$. Potom $p_1^{k_1 - 1} \cdot \ldots \cdot p_m^{k_m} = q_1^{l_1} \cdot \ldots \cdot q_i^{k_i - 1} \ldots \cdot q_n^{l_n}$ jsou dva rozklady čísla $< a$. ↯. □

5.3 Kongruence

Poznámka (Historie)
Symbol $\equiv$ zavedl v roce 1801 Gauss.

Definice 5.4

$a, b, m \in \mathbb{Z}, m \neq 0$. a je kongruentní s b modulo m ($a \equiv b(\mod m)$), pokud $m|a - b$. (Ekvivalentně a, b dávají stejný zbytek po dělení m.)

Pozorování
Být kongruentní mod m je ekvivalence.

Tvrzení 5.6 (Vlastnosti kongruence)

$a, b, c, d, m \in \mathbb{Z}, m \neq 0$. $a \equiv b \mod m, c \equiv d \mod m$.

$a+c = b+d \mod m$, $a-c \equiv b-d \mod m$, $a \cdot c \equiv b \cdot d \mod m$, $a^k \equiv b^k \mod m, k \in \mathbb{N}$.

$c \neq 0 \implies a \equiv b \mod m \Leftrightarrow ac \equiv bc \mod mc$, NSD$(c, m) = 1 \implies a \equiv b \mod m \Leftrightarrow ac \equiv bc$ m

Důkaz
Z definice rozepsáním.

$$a \equiv b \mod m \Leftrightarrow \exists q : a - b = mq \Leftrightarrow ac - bc = mcq \Leftrightarrow ac \equiv bc \mod mc.$$

$cu+mv = 1, cu = 1-mv \implies (ac \equiv bc \mod m \Leftrightarrow a \equiv a(1-mv) \equiv auc \equiv buc \equiv b(1-mv) \equiv b \mod m$

□

5.4 Eulerova věta a RSA

Definice 5.5 (Eulerova funkce)

Eulerova funkce $\varphi(n)$ značí (pro $n \in \mathbb{N}$) počet $k \in \{1, 2, \ldots, n\}$ nesoudělných s n, čili $\mathrm{NSD}(k, n) = 1$.

Tvrzení 5.7

$n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ prvočíselný rozklad, $n > 1$. Pak $\varphi(n) = p_1^{k_1-1}(p_1 - 1) \cdot \ldots \cdot p_m^{k_m-1}(p_m - 1)$.

Důkaz
Příště. □

Věta 5.8 (Eulerova)

Pokud a, m jsou nesoudělná přirozená čísla, pak $a^{\varphi(m)} \equiv 1 \mod m$.

Speciálním případem je Malá Fermatova věta: p prvočíslo, $p \not| a \implies a^{p-1} \equiv 1(\mod p)$.

Důkaz
Φ_m nechť značí množinu $\{k \in [m] | \, \mathrm{NSD}(k, m) = 1\}$. $\varphi(m) = |\Phi_m|$.

Lemma: a, m nesoudělná přirozená čísla, $m \neq 1$. Definujeme zobrazení $f_a : \Phi_m \to \Phi_m$, $k \mapsto ka \mod m$. Pak f_a je dobře definované $\wedge$ je to bijekce.

Důkaz k, a nesoudělná s $m \implies k \cdot a$ nesoudělné s $m \implies k \cdot a \mod m$ nesoudělné s $m \implies k \cdot a \mod m \in \Phi_m$. $f_a(k) = f_a(l) \implies k \cdot a \equiv l \cdot a \mod m \implies k \equiv l \mod m$ (a je nesoudělné s m, tedy můžeme použít tvrzeni výše) $\implies k = l$. f_a je prosté a na konečné množině, tedy je bijekce.

$$\prod_{b \in \Phi_m} b = \prod_{b \in \Phi_m} f_a(b) = \prod_{b \in \Phi_m} (ab \mod m) \equiv a^{\varphi(m)} \prod_{b \in \Phi_m} b$$

$c = \prod_{b \in \Phi_m} b$, $c \equiv a^{\varphi(m)} c \mod m$ a c je nesoudělné s m, tedy dle tvrzení výše je $1 \equiv a^{\varphi(n)} \mod m$. □

Poznámka
Lemma z posledního důkazu nám říká, že každý prvek z Φ_m má inverzi v okruhu $\mathbb{Z}_m$.

Ten můžeme najít buď přes Eulerovu větu, nebo přes Bézoutovu větu. (Druhý způsob je zpravidla rychlejší.)

Poznámka (RSA (Rivest Shamir Adleman))
Šifrovací algoritmus založený na Eulerově větě.

5.5 Čínská zbytková věta

Poznámka
Špatně: Uvedená v knize umění války (počítání vojáků).

Správně: vymyslel ji čínský matematik, který se jmenoval stejně jako legendární generál, autor knihy výše.

Věta 5.9 (Čínská zbytková)

Nechť $m_1, \ldots, m_n \in \mathbb{N}$ po dvou nesoudělná čísla. Označíme $M = m_1 \cdot \ldots \cdot m_N$. Ať $u_1, \ldots, u_n \in \mathbb{Z}$. Pak[a] *$\exists! x \in [M-1]_0$ tak, že $x \equiv u_1 \mod m_1, \ldots, x \equiv u_n \mod m_n$.*

Důkaz
Jednoznačnost: Ať $x, y \in [M-1]_0$, pro které platí všechny kongruence. Potom $\forall i : m_i | x-y$, tedy $M|x-y$. Ale $|x-y| < M$, tudíž $x - y = 0$.

Existence: $f : [M-1]0 \to [m_1-1]_0 \times \ldots \times [m_n-1]_0$, $x \mapsto (x \mod m_1, \ldots, x \mod m_n)$. Korektní definice zobrazení (mimochodem je to dokonce isomorfismus okruhů). f je prosté (díky jednoznačnosti). Množiny jsou stejně velké, tedy je to dokonce bijekce, a proto existuje inverze, tudíž prvek $(u_1, \ldots, u_n)$ musí mít obraz při zobrazení f^{-1}, který z definice splňuje vlastnosti hledaného prvku.. □

[a] $$[M-1]_0 = \{0, 1, \ldots, M-1\}$$

Důkaz (Vzorec pro eulerovu formuli)
1) $\varphi(p^k) = p^{k-1}(p-1)$. 2) a, b nesoudělná $\implies \varphi(ab) = \varphi(a) \cdot \varphi(b)$. Následně se vzorec dokáže aplikováním hodněkrát 2 na rozklad a jedničky nakonec.

1) Počet čísel soudělných s p^k z množiny $[p^k]$ je p^{k-1}, tedy počet nesoudělných je $p^k - p^{k-1}$.

2) Funkce z důkazu čínské zbytkové věty je bijekce. Uvažujme zúžení f na $\Phi_{a \cdot b}$. Chceme:

obraz zúžení je $\Phi_a \times \Phi_b$, tedy $\varphi(ab) = |\Phi_{ab}| = |\Phi_a \times \Phi_b| = \varphi(a) \cdot \varphi(b)$. Důkaz:

a) f zobrazí Φ do $\Phi_a \times \Phi_b$, čili, že $\mathrm{NSD}(x, a \cdot b) = 1$ implikuje $\mathrm{NSD}(x \mod a, a) = 1, \mathrm{NSD}(x \mod b, b) = 1$. b) f zobrazí $\Phi_{a,b}$ na $\Phi_a \times \Phi_b$, čili pokud $\mathrm{NSD}(u, a) = 1, \mathrm{NSD}(v, b) = 1$, pak to jediné x, které se zobrazí na (u, v), leží v $\Phi_{a,b}$.

$\mathrm{NSD}(x, ab) == 1 \Leftrightarrow \mathrm{NSD}(x, a) = 1 \wedge \mathrm{NSD}(x, b) = 1 \Leftrightarrow \mathrm{NSD}(x \mod a, a) = 1 \wedge \mathrm{NSD}(x \mod b, b) = 1.$

a) je zleva doprava a b) je zprava doleva. □

6 Abstraktní dělitelnost

6.1 Dělitelnost a asociovanost

Definice 6.1 (Dělitelnost, asociovanost, inverz)

R obor, $a, b \in R$. b dělí a v R, značíme $b|a$, pokud existuje $c \in R$ tak, že $a = b \cdot c$.

a, b jsou asociované v R, pokud $a|b$, $b|a$. Značíme $a||b$.

$a \in R$ je invertibilní, pokud existuje $b \in R$ tak, že $a \cdot b = 1$ (značíme $b = a^{-1}$).

Pozorování
a je invertibilní $\Leftrightarrow a||1$.

Relace $|$ je reflexivní $\wedge$ tranzitivní.

Tvrzení 6.1

R obor, $a, b \in R$. Pak $a||b \Leftrightarrow \exists$ invertibilní prvek $q \in R$ tak, že $a = bq$.

Důkaz
$\Leftarrow$: $(a = bq \implies b|a) \wedge (b = aq^{-1} \implies a|b)$.

$\Longrightarrow$: $a = 0 \implies b = 0$. Ať $a \neq 0$, $(b|a \implies a = bu) \wedge (a|b \implies b = av) \implies a = bu = auv$. Můžeme vykrátit $a \neq 0$, tj. $1 = uv$, a u, v jsou tedy invertibilní. □

Definice 6.2 (Kongruence)

$a, b, m \in R : a \equiv b \mod m$, pokud $m|a - b$.

Pozorování
Je to ekvivalence, zachovává se přičtením a odečtením, ale nemusí platit krácení.

6.2 Kvadratická rozšíření $\mathbb{Z}$

Definice 6.3 (Kvadratické rozšíření $\mathbb{Z}$)

Kvadratické rozšíření $\mathbb{Z}$ je $\mathbb{Z}[\sqrt{s}] = \{a + b\sqrt{s} | a, b \in \mathbb{Z}\}$, kde $s \in \mathbb{Z}$, s není druhá mocnina celého čísla.

Důkaz (Tvar $\mathbb{Z}\,[sqrts]$)
Dokáže se uzavřenost. □

Definice 6.4

Norma na oboru $\mathbb{Z}[\sqrt{s}]$ je zobrazení $\ni\colon \mathbb{Z}[\sqrt{s}] \to \mathbb{N} \cup \{0\}\,, a + b\sqrt{s} \mapsto |a^1 - b^2 s|$.

Tvrzení 6.2

$\forall u, v \in \mathbb{Z}[\sqrt{s}]$ *platí:*

1. $\ni (u \cdot v) = \ni (u) \cdot \ni (v)$,
2. $\ni (u) = 1 \Leftrightarrow u$ *je invertovatelné.*
3. *Pokud* $u|v$ *a* $v|u$, *pak* $\ni (u) | \ni (v)$ *(víme z 1))* *a* $\ni (u) \neq \ni (v)$.

Důkaz
1) vezmu a ověřím. Nebo využiji, že $\ni (u) = |u \cdot u'|$, kde $u' = a - b\sqrt{s}$, $u = a + b\sqrt{s}$. Zjistíme, že $(u \cdot v)' = u' \cdot v'$. Potom $|u \cdot v \cdot (u \cdot v)'| = |u \cdot u'| \cdot |v \cdot v'|$.

2) $\Leftarrow$: $u \cdot u^{-1} = 1 \implies \ni (u \cdot u^{-1}) = \ni (1) = 1$. A z 1) už plyne $\ni (u) = 1$. $\implies$: $\ni (u) = 1 \implies u \cdot u' = 1 \implies u'$ je hledaná inverze.

3) $u = 0 \implies v = 0 \implies v|u$. Ať tedy $v = uc$ pro $c \in \mathbb{Z}[\sqrt{s}]$. Ať $\ni (u) = \ni (v) = \ni (u \cdot c) = \ni (u) \cdot \ni (c) \implies \ni (c) = 1 \implies c$ je invert $\implies v||u$, čili $v|u$ spor. □

Pozor
Norma nesplňuje trojúhelníkovou nerovnost!

Tvrzení 6.3 (Dělení Gaussových čísel se zbytkem)

$$\forall \alpha, \beta \in \mathbb{Z}[i], \beta \neq 0\ \exists \gamma, \delta \in \mathbb{Z}[i] : \alpha = \beta \cdot \gamma + \delta \wedge \ni (\delta) < \ni (\beta).$$

Důkaz
$\mathbb{Z}[i] \subseteq \mathbb{C}$, tudíž berme $\frac{\alpha}{\beta} \in \mathbb{C}$. Zvolme $\gamma \in \mathbb{Z}[i]$ jako nejbližší hodnotu k $\frac{\alpha}{\beta}$. Položme $\delta = \alpha - \beta \cdot \gamma$. $\frac{\delta}{\beta} = \frac{\alpha}{\beta} - \gamma$, tj. $|\frac{\delta}{\beta}| \leq \frac{\sqrt{2}}{2}$, tj. $\ni \delta \leq \left(\frac{\sqrt{2}}{2}\right)^2 |\beta|^2 < 1 \ni (\beta)$. □

Poznámka
Takováto definice dělení se zbytkem funguje ještě pro $\mathbb{Z}[\sqrt{-2}]$ a $\mathbb{Z}[\sqrt{2}]$, ale pro ostatní $\mathbb{Z}[\sqrt{s}]$ už nefunguje.

6.3 Největší společný dělitel

Definice 6.5 (Největší společný dělitel, nesoudělnost a největší společný násobek)

Pro $a, b \in R$, R obor řekneme, že $c \in R$ je největší společný dělitel a, b, značíme $c = \mathrm{NSD}(a, b)$, pokud 1) $c|a \wedge c|b$ a 2) $\forall d|a, d|b : d|c$.

a, b jsou nesoudělné, pokud $\mathrm{NSD}(a, b) = 1$.

Obdobně definujeme $\mathrm{NSN}(a, b) = c \equiv a|c \wedge b|c \wedge \forall d, a|d, b|d : c|d$.

Poznámka
NSD nemusí existovat. Zároveň není jednoznačně určený. Ale je jednoznačně určený až na asociovanost.

6.4 Ireducibilní prvky a rozklady

Definice 6.6 (Vlastní dělitel a ireducibilní prvek)

R obor. $a \in R \setminus \{0\}$. $b \in R$ je vlastní dělitel a, pokud $b|a$ a $b \not|1$ a $b \not|a$.

$a \neq 0$ je ireducibilní, pokud $a \not|1$ a nemá žádné vlastní dělitele.

Definice 6.7 (Ireducibilní rozklad)

Ireducibilní rozklad prvku a je zápis $a||p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, kde $p_1, \dots, p_n$ jsou ireducibilní prvky a $p_i \not|p_j$, pro $i \neq j$, a kde $k_1, \dots, k_n \in \mathbb{N}$.

Řekneme, že a má jednoznačný ireducibilní rozklad, pokud má právě 1 rozklad až na pořadí a asociovanost.

6.5 Prvočinitelé

Definice 6.8 (Prvočinitel)

R obor, pak $p \in R, p \not| 1$ je prvočinitel, pokud $\forall a, b \in R : p|a \cdot b \implies p|a \vee p|b$.

Pozorování
p je prvočinitel $\implies$ p je ireducibilní.

Důkaz
Ať $p = ab$. Pak $p|a \cdot b \overset{\text{prvočinitel}}{\implies} p|a \vee p|b$. Zároveň zřejmě $a|p$ a $b|p$, tedy $p||a \implies b||1$ nebo $p||b \implies a||1$. Tedy a, b jsou nevlastní dělitelé. □

7 Existence a jednoznačnost ireducibilního rozkladu

7.1 Gaussovské obory

Definice 7.1 (Gaussovský obor)

Obor R je gaussovský, pokud $\forall a \in R, a \neq 0, a \not| 1$, má jednoznačný ireducibilní rozklad.

Příklad (Otevřený problém)
$\mathbb{Z}[\sqrt{s}]$ je gaussovský pro ∞ mnoho s. (Čeká se, že ano.)

Poznámka (Rozšíření definice ireducibilního rozkladu)
$a||1$, pak řekneme, že ireducibilní rozklad a je $a||1 = \ldots^0$.

Tvrzení 7.1 (Vlastnosti gaussovských oborů)

R je gaussovský obor a $a, b \in R$, $a, b \neq 0$. Ať navíc je $a||p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ je ireducibilní rozklad. Pak $b|a \Leftrightarrow b||p_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$ (nemusí být rozklad, protože l_i smí být 0), kde $\forall i : 0 \leq l_i \leq k_i$.

Důkaz
$\Rightarrow$: Ať $b = rp_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$ a $a = q \cdot p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$, kde $r||1||q$. Chci: $b|a$, čili $\exists c : a = b \cdot c$. $c = q \cdot r^{-1} \cdot p_1^{k_1 - l_1} \cdot \ldots \cdot p_n^{k_n - l_n}$.

$\Longrightarrow : b|a \implies \exists c : a = b \cdot c$. Ať $b||q_1^{s_1} \cdot \ldots \cdot q_u^{s_u}$, $c||r_1^{t_1} \cdot \ldots \cdot r_v^{t_v}$ jsou ireducibilní rozklady. Zkombinujeme na rozklad $b \cdot c : B \cdot C||q_1^{s_1'} \cdot \ldots \cdot q_u^{s_u'} \cdot r_{i_1}^{t_{i_1}} \cdot \ldots \cdot r_{i_w}^{t_{i_w}}$ (vyfiltrujeme z rozkladu c ty r_i, který jsou asociovány s nějakým q_j). Máme 2 rozklady $b \cdot c = a$. Z jednoznačnosti rozkladů $q_i = p_{\pi(i)} \wedge s_i' = k_{\pi(i)} \geq s_i$. Tudíž $b||p_{\pi(1)}^{s_1} \cdot \ldots \cdot p_{\pi(n)}^{s_n}$, kde $s_i \leq k_{\pi(i)}$ (a doplníme chybějící p_j^0). $\square$