Cíl. *Nejprve stručně nastíníme, jak se formálně definují přirozená čísla, a hned poté se pustíme do základních poznatků o dělitelnosti: existence a jednoznačnost rozkladu na prvočísla (Základní věta aritmetiky); Eukleidův algoritmus a Bézoutova rovnost; Čínská věta o zbytcích; Eulerova funkce a Eulerova věta. Naučíme se pracovat s šikovným značením pomocí kongruencí* $\equiv \pmod n$.

3.1. Přirozená čísla.

Přirozenými čísly intuitivně rozumíme množinu $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$. Formálně vzato však tento zápis nedává valný smysl ze dvou důvodů: jednak nekonečnou množinu nemůžeme definovat výčtem prvků, a pak také není jasné, co vlastně symboly 1,2,3 atd. znamenají. V tomto odstavci nastíníme, jak lze přirozená čísla zavést formálně. Protože však u čtenáře nepředpokládáme žádnou znalost matematické logiky, nebudeme se pouštět do detailů a některé pojmy z logiky budeme používat bez dalšího vysvětlení na intuitivní úrovni. Z jistých důvodů se v logice zavádějí přirozená čísla i s nulou, čehož se v tomto odstavci přidržíme.

Jeden ze způsobů, jak přirozená čísla zavést, je zformulovat sadu *axiomů*, z nichž se budou všechna tvrzení o přirozených číslech dokazovat. Standardním přístupem je tzv. *Peanova axiomatika*. Přirozená čísla s nulou zavedeme jako teorii, v níž máme konstantu 0, unární funkční symbol s a následující axiomy:

(1) pro každé a existuje právě jedno b takové, že $s(a) = b$;
(2) pro každé a je $s(a) \neq 0$;
(3) pro každé $a \neq b$ platí $s(a) \neq s(b)$;
(4) je-li V vlastnost taková že
   (a) 0 má vlastnost V;
   (b) pro každé a platí následující: jestliže má a vlastnost V, pak $s(a)$ má také vlastnost V;

   pak má každé a vlastnost V.

Číslovky pak můžeme zavést jako $1 = s(0)$, $2 = s(1)$, atd. Interpretace symbolu s je taková, že „číslu" přiřadí „číslo o jedna větší". První tři axiomy říkají, že s je prostá funkce, v jejímž oboru hodnot není 0. Poslednímu axiomu se říká *matematická indukce*.

Na základě těchto axiomů můžeme induktivně definovat standardní operace: sčítání předpisy $a + 0 = a$ a $a + s(b) = s(a + b)$ (tj. umíme-li spočítat $a + b$, definujeme na jeho základě $a + s(b)$), násobení předpisy $a \cdot 0 = 0$ a $a \cdot s(b) = a \cdot b + a$, atd. Uspořádání definujeme předpisem $a \leq b \Leftrightarrow \exists c\, a + c = b$ a podobně lze postupovat pro další známé pojmy a vlastnosti.

Z Peanových axiomů lze logicky odvodit všechna tvrzení o přirozených číslech, na která si vzpomenete – i když zpravidla nejde vůbec o jednoduchou práci (zkuste např. dokázat, že sčítání je komutativní!). Přesto má tato metoda své limity: slavná Gödelova věta o neúplnosti říká, že existují tvrzení, jež z těchto axiomů nelze dokázat ani vyvrátit. A ještě hůře: dokonce neexistuje žádná „hezká" sada axiomů, která by tuto nepříjemnou vlastnost neměla. Naštěstí se ukazuje, že taková tvrzení jsou poměrně obskurní, Gödelovou větou se tedy nemusíme příliš trápit.

Druhým přístupem, který uvedeme, je vybudování *modelu* přirozených čísel (s nulou) v rámci nějaké dobře známé teorie, např. teorie množin. Standardním modelem v teorii množin jsou tzv. *von Neumannova čísla*, definovaná jako nejmenší množina ω splňující

(1) $\emptyset \in \omega$;
(2) jestliže $A \in \omega$, pak $A \cup \{A\} \in \omega$.

Tedy ω obsahuje postupně množiny

$$\emptyset, \quad \{\emptyset\}, \quad \{\emptyset, \{\emptyset\}\}, \quad \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \quad \ldots$$

Tímto způsobem můžeme definovat číslovky $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$ atd. Všimněte si, že v tomto značení je $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, atd. Pokud iterpretujeme symbol s jako $s(A) = A \cup \{A\}$, pro von Neumannova čísla budou platit Peanovy axiomy.

Na závěr stručně uvedeme, jak se formálně zavádějí ostatní číselné obory. Celá čísla lze definovat jako sjednocení čísel kladných, záporných a nuly, přičemž záporným číslem rozumíme formální zápis $-a$, kde a je přirozené číslo; operace se definují zřejmým způsobem. Celá čísla s operacemi sčítání, odčítání a násobení tvoří strukturu, které se říká *obor integrity*. Racionální čísla se pak definují jako *podílové těleso* tohoto oboru (viz Tvrzení 4.4). Způsobů, jak formálně zavést čísla reálná je celá řada, jeden příklad za všechny: jde o tzv. *zúplnění* uspořádaného tělesa racionálních čísel – doplníme suprema a infima všech omezených podmožin a pomocí limit na ně přeneseme operace (detaily konstrukce patří spíše do topologie). Na komplexní čísla pak lze nahlížet jako na *algebraický uzávěr* čísel reálných (viz Věta 27.4).

3.2. Základní věta aritmetiky.

Výklad teorie čísel začneme větou o prvočíselném rozkladu. Všechna fakta z tohoto odstavce byla známa již starořeckým matematikům a v moderní podobě byly formulovány Carlem Friedrichem Gaussem v jeho slavné knize *Disquisitiones Arithmeticae* z roku 1801, která položila základ moderní teorie čísel.

Čísly budeme nadále rozumět přirozená čísla. Jak známo, pro každou dvojici čísel a, b existuje právě jedna dvojice čísel q, r, kde $r \in \{0, \ldots, b-1\}$, splňující vztah

$$a = q \cdot b + r.$$

Číslo q se nazývá *celočíselný podíl* čísel a, b, značí se $a \operatorname{div} b$, a číslo r se nazývá *zbytek* po dělení, značí se $a \bmod b$. Existence podílu a zbytku plyne ze známého algoritmu celočíselného dělení, ale jak to je s jednoznačností? Kdyby $a = q_1 b + r_1 = q_2 b + r_2$, pak $b(q_1 - q_2) = r_2 - r_1$, tedy $b \mid r_2 - r_1$, avšak $r_2 - r_1 \in \{-(b-1), \ldots, b-1\}$, takže $r_2 - r_1 = 0$. Z toho plyne $r_1 = r_2$ i $q_1 = q_2$.

Řekneme, že číslo b *dělí* číslo a, píšeme $b \mid a$, pokud existuje číslo q splňující $a = b \cdot q$ (tj. pokud je zbytek $r = 0$). Pro každé a platí $1 \mid a$ a $a \mid a$; tito dělitelé se nazývají *nevlastní*. Číslo $p \neq 1$, které má pouze nevlastní dělitele, se nazývá *prvočíslo*; ostatní čísla se nazývají *složená*. Zcela základním poznatkem teorie čísel je fakt, že každé číslo lze jednoznačně vyjádřit jako součin prvočísel.

Věta 3.1 (Základní věta aritmetiky). *Pro každé přirozené číslo $a \neq 1$ existují různá prvočísla $p_1, p_2, \ldots, p_n$ a přirozená čísla $k_1, k_2, \ldots, k_n$ splňující*

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$$

(tomuto vyjádření se říká prvočíselný rozklad*). Tento zápis je jednoznačný až na pořadí činitelů.*