

Základy aritmetiky a algebry I

1. **Úvod.** Co je matematika, aritmetika, algebra. Jazyk matematiky, definice, věty, důkazy. Struktura definic, vět a důkazů.
2. **Množiny.** Množinová symbolika, množinové operace, Vennovy diagramy. Potenční množina, svaz podmnožin dané množiny.
3. **Relace.** Relace mezi množinami, relace na množině. Ekvivalence, disjunktí rozklad množiny, faktorová množina. Uspořádání, úplné uspořádání.
4. **Zobrazení.** Speciální typy zobrazení: injekce, surjekce, bijekce. Zobrazení jako relace, graf zobrazení. Rozklad zobrazení na surjekci, bijekci a injekci; disjunktí rozklad výchozí množiny, jádro a obraz. Transformace a permutace množiny. Binární operace. Mohutnost množin, konečné a nekonečné množiny, spočetné a nespočetné množiny. Mohutnost číselných oborů (přirozená čísla, celá čísla, racionální čísla, reálná čísla, komplexní čísla).
5. **Přirozená čísla.** Peanovy axiomy, matematická indukce, dobré uspořádání, důkazy indukci. Součty mocnin přirozených čísel.
6. **Dělitelnost přirozených čísel.** Dělitel a násobek. Největší společný dělitel a nejmenší společný násobek. Nesoudělná čísla. Přirozená čísla jako svaz. Prvočísla a čísla složená. Rozklady přirozených čísel na součin prvočísel. Eukleidova věta o nekonečném počtu prvočísel. Fermatova čísla a prvočísla.
7. **Dělení se zbytkem.** Eukleidův algoritmus, Bézoutova věta, Eukleidovo lemma. Základní věta aritmetiky. Vyjádření největšího společného dělitele a nejmenšího společného násobku dvou čísel pomocí rozkladu na mocniny prvočísel. Zápis čísel v jiných číselných soustavách.
8. **Prvočísla.** Eratosthenovo síto. Matijasevičova parabola. Dokonalá čísla. Mersennova čísla a prvočísla. Vztah Mersennových prvočísel a sudých dokonalých čísel: Eukleidova věta, Eulerova věta.
9. **Konstrukce.** Konstrukce oboru (oboru integrity) celých čísel, konstrukce oboru (pole) racionálních čísel. Abstraktní podstata těchto konstrukcí.
10. **Kongruence.** Kongruence modulo n , zbytková reprezentace čísel. Malá Fermatova věta. Základní kritéria dělitelnosti.
11. **Řetězové zlomky.** Vyjádření racionálních čísel řetězovými zlomky. Konvergency.
12. **Grupy.** Definice grupy, podgrupy, svaz podgrup. Grupy symetrií pravidelných mnohoúhelníků. Cyklické grupy. Homomorfismy, speciální homomorfismy, věta o homomorfismu.
13. **Permutace.** Permutace konečné množiny. Znázornění permutace grafem. Skládání permutací, jeho vlastnosti. Symetrická grupa stupně n . Inverze permutace, znaménko permutace, sudé a liché permutace, znaménko složené permutace. Alternující grupa stupně n . Rozklad na cykly a transpozice. Trojcykly.
14. **Algebraické struktury.** Okruhy, obory integrity, tělesa, pole. Podstruktury, ideály. Homomorfismy, speciální homomorfismy, věta o homomorfismu. Gaussova celá čísla, „podivné“ obory integrity.