

## OBSAH.

|                |   |
|----------------|---|
| Úvod . . . . . | 5 |
|----------------|---|

### *I. Dělitelnost, prvočísla.*

|   |    |
|---|----|
| 1. Dělitelnost . . . . .  | 7  |
| 2. $[x]$ , $[x]'$ , $\{x\}$ . . . . .                                     | 7  |
| 3. Modul . . . . .  | 11 |
| 4. Největší společný dělitel (n. s. d.) . . . . .                         | 13 |
| 5. Vlastnosti n. s. d. . . . .  | 14 |
| 6. Výpočet n. s. d. . . . .   | 15 |
| 7. Věty o číslech nesoudělných . . . . .                                  | 16 |
| 8. Zlomky redukované . . . . .  | 17 |
| 9. Nejmenší společný násobek (n. s. n.) . . . . .                         | 18 |
| 10. Prvočísla . . . . .   | 19 |
| 11. Pomočné věty o prvočíslech . . . . .                                  | 20 |
| 12. Rozklad čísel racionálních v prvočinitele . . . . .                   | 21 |
| 13. N. s. d. a n. s. n. čísel vyjádřených součinem prvočinitelů . . . . . | 22 |
| 14. Síto Eratostenovo . . . . .   | 23 |
| 15. Počet a součet celých kladných dělitelů čísla celého . . . . .        | 24 |
| 16. Čísla dokonalá . . . . .  | 25 |
| 17. Součin celých kladných dělitelů čísla celého . . . . .                | 26 |
| 18. Nejvyšší mocnina prvočísla obsažená v $[x]!$ . . . . .                | 26 |

### *II. Kongruence.*

|   |    |
|---|----|
| 19. Definice kongruence . . . . .   | 30 |
| 20. Základní vlastnosti kongruencí . . . . .  | 30 |
| 21. Třídy (mod $m$ ) . . . . .  | 32 |
| 22. Znázornění prvočísel mnohočleny . . . . .   | 33 |
| 23. $ax + b \equiv 0 \pmod{m}$ . . . . .  | 34 |
| 24. Kongruenci $ax + b \equiv 0 \pmod{m}$ lze v případě, že $m$ je číslo složené, převést na řešení kongruencí s modulem prvočíselným . . . . . | 35 |
| 25. Řešení rovnice $ax + by = c$ čísly celými $x, y$ . . . . .  | 39 |
| 26. Eulerova (Bachetova) metoda řešení rovnice neurčité . . . . .   | 40 |
| 27. Řešení rovnice $ax + by = c$ ( $a, b, c$ čísla kladná) kladnými celými čísly $x, y$ . . . . .   | 42 |
| 28. Pravidla dělitelnosti pro čísla celá vyjádřená v soustavě desítkové . . . . .   | 44 |
| 29. Užití kongruencí k verifikaci početních úkonů (zkouška devítková a jedenáctková) . . . . .  | 45 |
| 30. $\varphi(m)$ . . . . .  | 46 |
| 31. Vlastnosti $\varphi(m)$ . . . . .   | 47 |
| 32. Věta Fermatova . . . . .  | 48 |

|       |                                 |    |
|-------|---------------------------------|----|
| § 33. | Kongruence mnohočlenů . . . . . | 49 |
| § 34. | Věta Wilsonova . . . . .        | 51 |
| § 35. | Primitivní kořeny . . . . .     | 51 |

*III. g-adické zlomky.*

|       |  |    |
|-------|--|----|
| § 36. | <i>g</i> -adické zlomky . . . . .                              | 56 |
| § 37. | <i>g</i> -adický algoritmus prvního druhu . . . . .            | 57 |
| § 38. | <i>g</i> -adický algoritmus druhého druhu . . . . .            | 58 |
| § 39. | Rozvoj čísel racionálních ve zlomky <i>g</i> -adické . . . . . | 60 |
| § 40. | Zlomky desetinné . . . . .                                     | 63 |

*IV. Kvadratické zbytky, kvadratický zákon reciprocity  
a znázornění prvočísel formami  $x^2 + my^2$ .*

|       |   |    |
|-------|---|----|
| § 41. | Kvadratické zbytky a nezbytky . . . . .   | 66 |
| § 42. | Legendreův symbol . . . . .   | 67 |
| § 43. | Gaussovo lemma . . . . .  | 69 |
| § 44. | Scheringova a Kroneckerova definice symbolu $\left(\frac{a}{p}\right)$ . . . . .                    | 70 |
| § 45. | Kvadratický zákon reciprocity . . . . .   | 72 |
| § 46. | Stanoviti <i>n</i> tak, aby $\left(\frac{m}{n}\right) = 1$ resp. $-1$ . . . . .                     | 77 |
| § 47. | Rozklad $P_{13} = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$ v prvočinitele . . . . . | 82 |
| § 48. | Znázornění prvočísel formami $x^2 + my^2$ v některých jednoduchých případech . . . . .              | 82 |

*V. Znázornění čísel celých kladných formou  $x_1^2 + x_2^2 + x_3^2 + x_4^2$ .*

|       |  |    |
|-------|--|----|
| § 49. | Každé číslo celé kladné je možno znázorniti jako součet nejvyšší čtyř čtverců celých čísel . . . . . | 88 |
|-------|--|----|

*VI. Pythagorovy trojúhelníky, velká věta Fermatova pro  $n=4$ , racionální trojúhelníky.*

|       |  |    |
|-------|--|----|
| § 50. | Velká věta Fermatova . . . . .             | 93 |
| § 51. | Trojúhelníky Pythagorovy . . . . .         | 94 |
| § 52. | Velká věta Fermatova pro $n = 4$ . . . . . | 96 |
| § 53. | Trojúhelníky racionální . . . . .          | 98 |