Masarykova univerzita
Fakulta informatiky

Elektronická podpora výuky algebry a teorie čísel

Bakalářská práce

Valdemar Švábenský

Brno, jaro 2014

Prohlášení

Prohlašuji, že tato bakalářská práce je mým původním autorským dílem, které jsem vypracoval samostatně. Všechny zdroje, prameny a literaturu, které jsem při vypracování používal nebo z nich čerpal, v práci řádně cituji s uvedením úplného odkazu na příslušný zdroj.

Vedoucí práce: Mgr. Michal Bulant, Ph.D.

Poděkování

Rád bych poděkoval vedoucímu své práce Mgr. Michalu Bulantovi, Ph.D. za jeho cenné rady a připomínky k řešení této práce. Dále děkuji mým rodičům, Evě a Valdemarovi za jejich neustálou pomoc a podporu během mého studia.

Shrnutí

Cílem práce je tvorba výukových materiálů z oblasti algebry a teorie čísel podporujících samostatnou přípravu studentů, a to zejména v předmětech FI:MB104 a FI:MB204. Tyto výukové materiály sestávají ze sbírky příkladů spolu s jejich řešeními ve formě textu a v některých případech i videa. Pro interaktivní použití jsou k dispozici pracovní listy do matematického výpočetního prostředí Sage spolu s návodem na jeho obsluhu. Součástí práce je rovněž aplikace pro generování příkladů. Tato aplikace vytváří zadání náhodně dle zvolené obtížnosti nebo dle uživatelem zadaných parametrů. Umožňuje také zobrazit řešení konkrétního příkladu nebo jeho export do PDF souboru.

Klíčová slova

e-learning, výukové materiály, matematika, algebra, teorie čísel, sbírka příkladů, výuková videa, Sage, Java

Obsah

1 **Úvod** . . . 3
2 **Sbírka příkladů** . . . 5
2.1 Dělitelnost a prvočísla . . . 5
2.2 Kongruence . . . 7
2.3 Grupy . . . 8
2.3.1 Cyklické grupy . . . 9
2.3.2 Grupy permutací . . . 11
2.3.3 Homomorfismy grup . . . 12
2.4 Okruhy . . . 12
2.5 Polynomy . . . 13
2.6 Kódování a šifrování . . . 14
2.7 Řešení příkladů . . . 15
2.7.1 Dělitelnost a prvočísla . . . 15
2.7.2 Kongruence . . . 21
2.7.3 Grupy . . . 27
Cyklické grupy . . . 28
Grupy permutací . . . 31
Homomorfismy grup . . . 32
2.7.4 Okruhy . . . 34
2.7.5 Polynomy . . . 35
2.7.6 Kódování a šifrování . . . 36
2.8 Výuková videa . . . 38
3 **Matematický systém Sage** . . . 39
3.1 Úvod do Sage . . . 39
3.2 Základní poznatky pro práci se systémem . . . 40
3.3 Práce s proměnnými a funkcemi . . . 41
3.4 Teorie čísel . . . 43
3.5 Algebra . . . 45
3.6 Grupy permutací . . . 46
3.7 Kódování a šifrování . . . 47
3.8 Interaktivita . . . 49
3.9 Příklady . . . 50
3.10 Řešení příkladů . . . 51
4 **Generátor příkladů Numbermat** . . . 55
4.1 Uživatelské rozhraní . . . 55

4.2 Použité technologie . . . 57
4.3 Typy příkladů . . . 57
4.3.1 Největší společný dělitel . . . 57
4.3.2 Bezoutova rovnost . . . 58
4.3.3 Inverze modulo n . . . 58
4.3.4 Eulerova funkce φ . . . 58
4.3.5 Lineární kongruence . . . 59
4.3.6 Soustava lineárních kongruencí . . . 60
4.3.7 Řád prvku grupy jednotek . . . 60
4.3.8 Modulární umocňování . . . 61
4.3.9 Legendreův symbol . . . 61
4.3.10 Kvadratická kongruence (binomická) . . . 62
4.3.11 Kvadratická kongruence (obecná) . . . 63
4.3.12 Binomická kongruence . . . 64
4.3.13 Řád permutace . . . 65
5 **Závěr** . . . 66
A **Obsah přiloženého CD** . . . 69

Kapitola 1

Úvod

Informatika je od svých počátků úzce svázána s matematikou. Pravděpodobně každý pokrok v informatice byl dosažen na základě matematických znalostí a schopnost matematicky myslet je důležitá pro pochopení klíčových principů stojících za každou z mnoha oblastí informatiky. Matematika je proto nedílnou součástí studia informatiky, které by mělo studentovi poskytnout dobrý teoretický základ.

Také anglický termín *computer science* implikuje, že informatika je v první řadě vědecká disciplína, i když s řadou praktických aplikací. Ve srovnání s obdobím před několika desítkami let je dnes mnoho z nich přístupných i bez detailních teoretických znalostí, což potvrzuje, že pro praktické ovládání informatických aplikací matematika není nezbytná. Nicméně, jedním z rozdílů mezi informatikem a tím, kdo umí pouze využívat informační technologie, je právě znalost teoretických konceptů, na kterých ony technologie stojí. Učební osnovy Fakulty informatiky Masarykovy univerzity (dále jen FI MU) proto zahrnují i teoretické předměty, jejichž studium umožňuje nabýt obecného přehledu o různých oblastech informatiky.

Algebra a teorie čísel, jakožto matematické disciplíny s aplikacemi zejména v kódování a kryptografii, jsou hlavním tématem této bakalářské práce. Cílem práce je tvorba výukových materiálů podporujících samostatnou přípravu studentů FI MU, obzvlášť v předmětech MB104 a MB204. Tyto výukové materiály se skládají ze tří hlavních částí:

- sbírky příkladů s řešeními ve formě textu a v některých případech i videa,
- návodu pro práci s matematickým výpočetním systémem Sage spolu se sadou příkladů a interaktivních pracovních listů,
- aplikace pro generování příkladů a jejich řešení.

Kapitola 2 obsahuje zadání a řešení 118 příkladů z oblasti algebry a teorie čísel. Text práce neobsahuje znění definic, vět a jejich důkazů, se kterými se studenti obeznámí na přednáškách a v citované literatuře, ale zaměřuje se pouze na příklady, čímž doplňuje cvičení předmětů. Primárním teoretickým podkladem práce je učební text Matematika drsně a svižně [1], na který se při použití teoretických pojmů odkazuji. Studenti si tak budou moci snáze dohledat konkrétní definice. Při tvorbě příkladů dále pracuji s různými matematickými učebnicemi [2], [3], [4], [5]. Příklady jsou seřazeny s ohledem na sylaby předmětů MB104 a MB204. Jejich řešení jsou vysázena systémem LaTeX do textu práce, a pokud je to žádoucí, rovněž nahrána na videa, která jsou k dispozici na přiloženém CD.

Pro dosažení větší míry interaktivity využívám matematické prostředí Sage [6]. Práci s ním popisuji v kapitole 3. Návod uvedený v textu práce vychází z oficiálních příruček k systému [7], [8] a od základu vysvětluje použití Sage pro výpočty z oblasti algebry a teorie čísel. Každý popisovaný aspekt systému je doplněn ukázkami kódu, které demonstrují chování systému v konkrétních případech. Kód vytvořený v průběhu psaní práce je zároveň k dispozici v přiložených interaktivních pracovních listech, se kterými uživatelé mohou dále experimentovat. Kapitolu zakončuje zadání 20 úloh k procvičení práce se Sage. Řešení úloh jsou znovu uvedena v textu práce a také v pracovních listech.

Pro 13 vybraných typů příkladů nakonec v jazyce Java implementuji generátor příkladů sloužících k dalšímu procvičení látky. Aplikace má název Numbermat a vytváří zadání náhodně dle zvolené obtížnosti nebo dle uživatelem zadaných parametrů. Umožňuje také zobrazit řešení konkrétního příkladu nebo jeho export do zdrojového TEX souboru a odpovídajícího PDF souboru. Použití aplikace a implementační detaily popisuje kapitola 4. Při programování algoritmů teorie čísel jako reference slouží anglická učebnice Handbook of Applied Cryptography [9]. Přiložené CD obsahuje distribuci programu a kompletní dokumentované zdrojové kódy.

Kapitola 2

Sbírka příkladů

2.1 Dělitelnost a prvočísla

1. Nalezněte koeficienty v Bezoutově rovnosti [1, s. 591] pro čísla $2^{60} - 1$, $2^{32} - 1$.

2. Dokažte pro všechna $a, b \in \mathbb{N}$, že $[a, b] = ab$ právě tehdy, když $(a, b) = 1$.

3. Fibonacciho posloupnost definujeme induktivně: $f_1 = 1$, $f_2 = 1$ a $f_{n+2} = f_{n+1} + f_n$ pro všechna $n \in \mathbb{N}$. Dokažte, že:

   a) $f_n < 2^n$;

   b) f_n a f_{n+1} jsou nesoudělná;

   c) $f_1 + f_2 + \ldots + f_n = f_{n+2} - 1$;

   d) $f_{n+1} \cdot f_{n-1} = f_n^2 + (-1)^n$;

   e) $f_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$ [2, s. 33].

4. Nechť $p \geq 2$. Dokažte, že pokud $2^p - 1$ je prvočíslo (tzv. Mersenneho [1, s. 597]), pak i p je prvočíslo.

5. Nalezněte všechna $n \in \mathbb{N}$, pro která je $\varphi(n)$ [1, s. 597] liché.

6. Dokažte, že pro všechna $n \in \mathbb{N}$ jsou nesoudělná čísla:

   a) $2n + 9$, $3n + 13$;

   b) $2n + 3$, $11n + 17$.

7. Najděte $(3k + 11, 5k + 12)$ jako funkci k.

8. Najděte všechna prvočísla r, která lze vyjádřit jako součet a rozdíl dvou jiných prvočísel [4, s. 6].

9. Dokažte nebo vyvraťte tvrzení, že změnou jediné cifry libovolného $n \in \mathbb{N}$ lze získat prvočíslo [4, s. 8].

10. Vezměte libovolné $n \in \mathbb{N}$. Nahraďte jej součtem druhých mocnin jeho cifer. Tento proces opakujte, dokud se nedostanete k číslu 1 nebo se nezaseknete v nekonečné smyčce. Pokud se tímto způsobem dostanete k číslu 1, zvolené n nazýváme *šťastné*. Najděte největší trojciferné šťastné číslo.

11. Diofantická rovnice [1, s. 623] je rovnice, která dovoluje proměnným nabývat hodnot pouze z oboru celých čísel. Určete podmínky pro řešení a nalezněte obecný tvar řešení pro lineární diofantické rovnice:

    a) o jedné proměnné, tedy rovnice tvaru $ax = b$;
    b) o dvou proměnných, tedy rovnice tvaru $ax + by = c$.

12. Dokažte, že $n \in \mathbb{N}$, kde $n > 1$ je prvočíslem právě tehdy, když není dělitelné žádným prvočíslem p, přičemž $1 < p \leq \sqrt{n}$.

13. Dokažte, že pokud p, $p^2 + 2$ jsou prvočísla, pak $p = 3$ [2, s. 34].

14. Nechť $a, b, n \in \mathbb{N}$. Dokažte, že pokud $a^n | b^n$, pak $a | b$.

15. Spočtěte $[1, 2, \ldots, 20]$.

16. Rozložte číslo $16!$ na součin prvočísel.

17. Nalezněte $\nu_p(n!)$, tedy největší exponent mocniny prvočísla p, které děli $n!$.

18. Dokažte, že $(n, n + 2)$ je rovno 1 pro lichá n a 2 pro sudá $n \in \mathbb{N}$.

19. Dokažte, že všechna prvočísla větší než 3 mají zbytek 1 nebo 5 po dělení číslem 6.

20. Číslo n je dokonalé, pokud součet všech jeho dělitelů $\sigma(n) = 2n$ [1, s. 596].

    a) Dokažte pro všechna sudá $n \in \mathbb{N}$, že n je dokonalé, pokud $n = 2^{p-1} \cdot (2^p - 1)$, kde p, $2^p - 1$ jsou prvočísla.
    b) Ověřte, že první 3 dokonalá čísla jsou 6, 28 a 496.

21. Čísla $a, b \in \mathbb{N}$ nazýváme *spřátelená*, pokud $\sigma(a) = \sigma(b)$ [3, s. 252]. Která z dvojic čísel $(220, 284)$, $(234, 260)$ jsou spřátelená?

22. Dokažte pro všechna $n \in \mathbb{N}$, že $n^3 - n$ je dělitelné číslem 6.

23. Najděte všechna trojciferná $n \in \mathbb{N}$, pro která platí, že $11 | n$ a $\frac{n}{11}$ je rovno součtu čtverců cifer čísla n.

24. Nechť $a \in \mathbb{N}$. Číslo b vzniklo permutací cifer a. Ukažte, že rozdíl mezi čísly a, b je dělitelný číslem 9.

25. Existuje mocnina čísla 2, ze které po přeuspořádání cifer dostaneme jinou mocninu čísla 2?

26. Dokažte, že $(1 + i)^2 | 2$ v $\mathbb{Z}[i]$ [5, s. 16].

2.2 Kongruence

27. Dokažte, že $a \in \mathbb{Z}$ je dělitelné 3, pokud je součet jeho cifer dělitelný 3.
28. Dokažte pro všechna $x, y, z \in \mathbb{N}$, že $x^2 + y^2 = z^2 \implies xyz \equiv 0 \pmod{60}$.
29. Nalezněte poslední dvě cifry čísla 3^{45}.
30. Nalezněte poslední cifru čísla $99^{98^{97}}$.
31. Určete poslední 3 cifry čísla $2003^{2002^{2001}}$.
32. Nalezněte zbytek po dělení:
    a) čísla 2^{30} číslem 5;
    b) čísla 72^{11} číslem 17;
    c) čísla 7^{51} číslem 144;
    d) čísla $13^{12} + 12^{11} + 11^{10}$ číslem 9.
33. Ukažte, že číslo $8^{12} + 11 \cdot 2^{10}$ je dělitelné číslem 5.
34. Ukažte, že číslo $2^{70} + 3^{70}$ je dělitelné číslem 13 [4, s. 1].
35. Ukažte, že číslo $20^{15} - 1$ je dělitelné číslem 20801 [4, s. 1].
36. Demonstrujte Eulerovu větu [1, s. 604] pro hodnoty $n = 1573$ a $a = 27$.
37. Ukažte, že 645 je Fermatovo pseudoprvočíslo [1, s. 627] o základu $a = 2$.
38. Ukažte, že 561 je Carmichaelovo číslo [1, s. 625].
39. Někdo si nesprávně zapamatoval Malou Fermatovu větu [1, s. 604] a tvrdí, že pokud $p \nmid a$, pak $a^p \equiv 1 \pmod{p}$. Popište množinu takových dvojic (a, p), pro které toto ve skutečnosti platí.
40. Nalezněte všechna řešení následujících kongruencí:
    a) $3x \equiv 2 \pmod{7}$;
    b) $5x \equiv 12 \pmod{23}$;
    c) $5x \equiv 12 \pmod{26}$;
    d) $49x \equiv 3 \pmod{5}$;
    e) $17x \equiv 1 \pmod{6}$;
    f) $3x \equiv 1 \pmod{6}$;
    g) $37x \equiv 1 \pmod{101}$;
    h) $21x \equiv 6 \pmod{9}$;
    i) $x^2 \equiv 2 \pmod{47}$;
    j) $x^2 + x - 2 \equiv 0 \pmod{5}$;
    k) $x^2 + 16x \equiv -5 \pmod{11}$;
    l) $373^{121} \equiv x \pmod{18}$;
    m) $2^{3^{4^5}} \equiv x \pmod{9}$.

41. Nalezněte všechna řešení následujících soustav kongruencí:

a) $x \equiv 3 \pmod 4$
$x \equiv 4 \pmod 5$;

b) $x \equiv 3 \pmod 4$
$x \equiv 4 \pmod 5$
$x \equiv 1 \pmod 9$
$x \equiv 5 \pmod{14}$;

c) $x \equiv 3 \pmod 5$
$x \equiv 0 \pmod 8$
$x \equiv 1 \pmod{11}$
$x \equiv 2 \pmod{14}$;

d) $x \equiv 1 \pmod 3$
$3x \equiv 2 \pmod 5$
$3x \equiv -2 \pmod 8$;

e) $4x \equiv 9 \pmod{11}$
$12x \equiv 3 \pmod{45}$
$28x \equiv 35 \pmod{42}$;

f) $7x + 10y \equiv -5 \pmod{23}$
$4x + 3y \equiv 4 \pmod{23}$.

42. Dokažte, že poslední 4 cifry čísla 5^n, kde $n \in \{4, 5, 6, \dots\}$ tvoří periodickou posloupnost. Najděte periodu této posloupnosti [4, s. 19].

43. ISBN je kód, který má 10 cifer a platí $(x_1, x_2, \dots, x_{10}) \cdot (10, 9, \dots, 1) \equiv 0 \pmod{11}$. Někdy se stane, že $x_{10} = 10$, v takovém případě je poslední cifra nahrazena písmenem X. Ověřte, že 0-451-52493-4 a 1-236-89135-X jsou validní ISBN kódy.

44. Metodou binárního umocňování [1, s. 624] vypočtěte $3^{352} \pmod{1000}$.

45. Dokažte, že existuje nekonečně mnoho prvočísel $p \equiv -1 \pmod 6$ [5, s. 36].

46. Nechť p je liché prvočíslo. Dokažte, že kongruence $x^2 \equiv -1 \pmod p$ nemá řešení pro žádné $p \equiv 3 \pmod 4$.

47. Dokažte, že kongruence $x^2 \equiv 1 \pmod{2^b}$ má:

a) jedno řešení pro $b = 1$;
b) dvě řešení pro $b = 2$;
c) čtyři řešení pro $b = 3$ [5, s. 37].

48. Dokažte, že pro všechna $n \in \mathbb{N}_0$ existuje $k \in \{0, 1, \dots, 8\}$, že $n \equiv 2k \pmod 9$.

2.3 Grupy

49. Tvoří množina $\{a, b, c, d\}$ s operací $\circ$ danou následující tabulkou grupu [1, s. 641]?

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

50. Tvoří množina $\mathbb{Q}$ s operací $\circ$ danou předpisem $a \circ b = |a \cdot b|$ monoid [1, s. 642]?

51. Nechť $S = \mathbb{R} \setminus \{-1\}$. Definujme binární operaci $\circ$ na S předpisem $a \circ b = a + b + ab$. Dokažte, že $(S, \circ)$ je komutativní grupa.

52. Dokažte tvrzení: existuje dihedrální grupa [1, s. 646] $\mathbb{D}_{2n}$, která je komutativní.

53. Nechť a, b jsou prvky grupy G. Dokažte, že $ab^n a^{-1} = (aba^{-1})^n$ pro všechna $n \in \mathbb{N}$.

54. Tvoří iracionální čísla $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$ podgrupu [1, s. 642] grupy $(\mathbb{R}, +)$ nebo $(\mathbb{R}^*, \cdot)$?

2.3.1 Cyklické grupy

55. Nalezněte všechny generátory [1, s. 650] grup:

    a) $(\mathbb{Z}_{16}, +)$;
    b) $(\mathbb{Z}_{17}, +)$;
    c) $(\mathbb{Z}_n, +)$.

56. Dokažte nebo vyvraťte tvrzení: grupa $(\mathbb{Z}_{60}, +)$ má pouze prvočíselné generátory.

57. Vypište prvky:

    a) podgrupy $(\mathbb{Z}_{24}, +)$ generované prvkem $[15]$;
    b) všech podgrup $(\mathbb{Z}_{12}, +)$;
    c) všech podgrup $(\mathbb{Z}_{32}, +)$ řádu 8;
    d) všech podgrup $(\mathbb{Z}_{40}, +)$ řádu 6;
    e) všech podgrup $(\mathbb{Z}_4 \times \mathbb{Z}_2, +)$.

58. Nalezněte řád [1, s. 605] prvku a v grupě G:

    a) $a = [5]$, $G = (\mathbb{Z}_{16}, +)$;
    b) $a = [5]$, $G = (\mathbb{Z}_{16}^{\times}, \cdot)$;
    c) $a = [\sqrt{3}]$, $G = (\mathbb{R}, +)$;
    d) $a = [\sqrt{3}]$, $G = (\mathbb{R}^*, \cdot)$;
    e) $a = [-i]$, $G = (\mathbb{C}^*, \cdot)$;
    f) $a = [(3, 4)]$, $G = (\mathbb{Z}_4 \times \mathbb{Z}_6, +)$;
    g) $a = [(7, 63)]$, $G = (\mathbb{Z}_{14} \times \mathbb{Z}_{70}, +)$;
    h) $a = [(10, 11, 12)]$, $G = (\mathbb{Z}_{20} \times \mathbb{Z}_{30} \times \mathbb{Z}_{40}, +)$;
    i) $a = [(4, 8, 12)]$, $G = (\mathbb{Z}_{16} \times \mathbb{Z}_{16} \times \mathbb{Z}_{16}, +)$;
    j) $a = [(6, 6, 6)]$, $G = (\mathbb{Z}_{30} \times \mathbb{Z}_{24} \times \mathbb{Z}_{60}, +)$.

59. Nalezněte řády všech prvků v grupě:

    a) $(\mathbb{Z}_{18}, +)$;
    b) $(\mathbb{Z}_{18}^{\times}, \cdot)$ spolu s inverzemi všech prvků.

60. Nalezněte všechny prvky konečného řádu v grupě:

    a) $(\mathbb{Z}, +)$;
    b) $(\mathbb{Q}^*, \cdot)$;
    c) $(\mathbb{R}^*, \cdot)$.

61. Je-li prvek a řádu 24 v grupě G, jaké jsou možné řády grupy G? Jaké jsou možné řády dalších prvků grupy G?

62. Nechť G je konečná grupa s prvkem g řádu 5 a prvkem h řádu 7. Jaký nejmenší řád může mít grupa G?

63. Nechť G je konečná grupa s 60 prvky. Jaké řády můžou mít podgrupy grupy G?

64. Je pravdivé tvrzení, že každá vlastní podgrupa grupy $(\mathbb{Z}, +)$ má konečný řád?

65. Nechť $a \in G$. Dokažte, že řád prvku a v grupě G je stejný, jako řád prvku a^{-1}.

66. Uveďte příklad komutativní grupy řádu 2016 a její podgrupy řádu 3 nebo dokažte, že neexistuje.

67. Uveďte příklad nekomutativní grupy řádu většího než 6, ale dělitelného 6 a její podgrupy řádu 6 nebo dokažte, že neexistuje.

68. Uveďte příklad necyklické komutativní grupy řádu 11 nebo dokažte, že neexistuje.

69. Uveďte příklad necyklické komutativní grupy řádu 12 nebo dokažte, že neexistuje.

70. Nalezněte cyklickou grupu s:

    a) právě jedním generátorem;
    b) právě dvěma různými generátory;
    c) právě 10 různými generátory.

71. Nechť p, q jsou různá prvočísla. Kolik různých generátorů má grupa $(\mathbb{Z}_{pq}, +)$?

72. Určete grupu danou jejími generátory:

    a) $\langle 35, 49 \rangle_{\mathbb{Z}}$;
    b) $\langle 16, 19, 37 \rangle_{\mathbb{Z}}$;
    c) $\langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \rangle_{\mathbb{Z}_2}$.

2.3.2 Grupy permutací

73. Rozložte následující permutace [1, s. 643] na součin nezávislých cyklů:

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$;

b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$;

c) $(1,4,7,5) \circ (2,3) \circ (1,7,3,2,5)$;

d) $(2,3,4) \circ (1,2,5) \circ (3,6,1,7)$;

e) $(1,3,4,5) \circ (2,3,4)$;

f) $(3,4) \circ (3,4,1,2)$;

g) $(1,2,3)^2 \circ (1,2,5,3) \circ (4,2,3,5)^{-1}$.

74. Zapište permutaci $(1,4,5,6,2) \circ (1,4,3,7,8)$ jako součin transpozic [1, s. 644] a určete její paritu [1, s. 645].

75. Najděte takovou permutaci $\pi \in \mathbb{S}_5$, že $(1,3,2) \circ \pi \circ (3,5,2) \circ (1,4) = (2,4) \circ (1,5)$.

76. Vypište všechny prvky grupy $(\mathbb{S}_4, \circ)$. Poté rozhodněte, zda následující množiny tvoří podgrupu grupy $(\mathbb{S}_4, \circ)$:

a) $\{\pi \in \mathbb{S}_4 : \pi(1) = 3\}$;

b) $\{\pi \in \mathbb{S}_4 : \pi(4) = 4\}$;

c) $\{\pi \in \mathbb{S}_4 : \pi(1) = 3 \wedge \pi(4) = 4\}$.

77. Nalezněte všechny řády prvků grupy:

a) $(\mathbb{S}_7, \circ)$;

b) $(\mathbb{A}_7, \circ)$.

78. Uveďte příklad prvku řádu a v grupě G, nebo dokažte, že neexistuje:

a) $a = 15$, $G = (\mathbb{S}_8, \circ)$;

b) $a = 16$, $G = (\mathbb{S}_9, \circ)$;

c) $a = 10$, $G = (\mathbb{A}_7, \circ)$;

d) $a = 26$, $G = (\mathbb{A}_{13}, \circ)$;

e) $a = 6$, $G = (\mathbb{A}_8, \circ)$.

79. Nalezněte nejvyšší možný řád prvku grupy $(\mathbb{S}_n, \circ)$ pro všechna $n \in \{1, 2, \ldots, 10\}$.

80. Pokud je π sudá permutace, dokažte, že π^{-1} je také sudá. Platí to i pro liché permutace?

2.3.3 Homomorfismy grup

81. Které z následujících zobrazení je homomorfismem [1, s. 645]? Určete jádro a obraz homomorfismů.

    a) $f\colon (\mathbb{Z},+) \mapsto (\mathbb{Z},+)$, $f(a) = 11a$;

    b) $f\colon (\mathbb{Z},+) \mapsto (\mathbb{Z},+)$, $f(a) = a+5$;

    c) $f\colon (\mathbb{Z},+) \mapsto (\mathbb{Z},+)$, $f(a) = a^3$;

    d) $f\colon (\mathbb{Z},+) \mapsto (\mathbb{Z},+)$, $f(a) = 1$;

    e) $f\colon (\mathbb{Z},+) \mapsto (\mathbb{Z},+)$, $f(a) = 0$;

    f) $f\colon (\mathbb{R}^*,\cdot) \mapsto (GL_2(\mathbb{R}),\cdot)$, $f(a) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right)$;

    g) $f\colon (\mathbb{R},+) \mapsto (GL_2(\mathbb{R}),\cdot)$, $f(a) = \left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)$;

    h) $f\colon (GL_2(\mathbb{R}),\cdot) \mapsto (\mathbb{R},+)$, $f(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) = a+d$.

82. Popište izomorfismus $\mathbb{Z}_5^\times \cong \mathbb{Z}_4$.

83. Dokažte, že $(\mathbb{Z}_8^\times,\cdot) \cong (\mathbb{Z}_{12}^\times,\cdot)$, ale $(\mathbb{Z}_8,+) \ncong (\mathbb{Z}_{12},+)$.

84. Dokažte, že $(\mathbb{Z}_5^\times,\cdot) \cong (\mathbb{Z}_{10}^\times,\cdot)$, ale $(\mathbb{Z}_{12}^\times,\cdot) \ncong (\mathbb{Z}_{10}^\times,\cdot)$.

85. Popište všechny homomorfismy z grupy $(\mathbb{Z},+)$ do grupy $(\mathbb{Z},+)$.

86. Popište všechny homomorfismy z grupy $(\mathbb{Z},+)$ do grupy $(\mathbb{Z}_n,+)$.

87. Popište všechny homomorfismy z grupy $(\mathbb{Z}_n,+)$ do grupy $(\mathbb{Z},+)$.

88. Nechť G je komutativní grupa a $n \in \mathbb{N}$. Dokažte, že zobrazení $f\colon G \mapsto G$, $f(g) = g^n$ je homomorfismem grup. Platí to i pro nekomutativní grupy?

89. Popište všechny komutativní grupy řádu 360.

90. Najděte izomorfismus z grupy $(\mathbb{C},+)$ do grupy $(\mathbb{R}\times\mathbb{R},+)$.

2.4 Okruhy

91. Tvoří množina $M = \{a,b,c,d\}$ s operacemi $\oplus$, $\odot$ danými následujícími tabulkami okruh [1, s. 656]?

$\oplus$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	a	b
d	d	c	b	a

$\odot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	a	a	a
d	a	b	c	d

92. Tvoří množina $\mathbb{Z}_{12}$ s operacemi $+,\cdot$ modulo n okruh? Je to obor integrity?

93. Dokažte, že $(\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2}; a,b \in \mathbb{Q}\},+,\cdot)$ tvoří těleso [1, s. 657].

94. Dokažte, že množina $R = \{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\}$ matic nad $\mathbb{Z}_2$ s operacemi sčítání a násobení matic tvoří těleso.

95. Popište jednotky [1, s. 661] v následujících okruzích:

    a) $(\mathbb{Z}_{10}, +, \cdot)$;
    b) $(\mathbb{Z}_7, +, \cdot)$;
    c) $(Mat_{2\times 2}(\mathbb{Z}), +, \cdot)$;
    d) $(Mat_{2\times 2}(\mathbb{Z}_2), +, \cdot)$.

96. Nalezněte jednotku okruhu $\mathbb{Z}_4[x]$ stupně nejméně 2.

97. Dokažte, že okruh $\mathbb{Z}_6[x]$ není okruh s jednoznačným rozkladem [1, s. 661].

2.5 Polynomy

98. Dokažte, že polynom $p(x)$ je ireducibilní nad okruhem R:

    a) $p(x) = 16x^5 - 9x^4 + 3x^2 + 6x - 21$, $R = \mathbb{Q}[x]$;
    b) $p(x) = x^3 + 3x - 2$, $R = \mathbb{Z}[x]$;
    c) $p(x) = x^7 + 2$, $R = \mathbb{Z}[x]$;
    d) $p(x) = x^4 - 2x^3 + x + 1$, $R = \mathbb{Q}[x]$;
    e) $p(x) = x^4 + x^3 + x^2 + x + 1$, $R = \mathbb{Z}_2[x]$.

99. Faktorizujte následující polynomy nad $\mathbb{Z}_2[x]$:

    a) $x^5 - 1$;
    b) $x^9 - 1$;
    c) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

100. Faktorizujte následující polynomy nad $\mathbb{Z}_5[x]$:

    a) $x^5 + 3x^3 + x + 3$;
    b) $2x^5 + x^4 - 2x^3 - x^2 - 4x - 2$.

101. Nalezněte dvě různé faktorizace polynomu $x^2 + x + 8$ v $\mathbb{Z}_{10}[x]$ [2, s. 284].

102. Určete $(2x^3 + 1, x^4 - x^3 + 2x^2 - x - 1)$ v $\mathbb{Z}_3[x]$.

103. Určete $(x^6 - x^4 - x^2 + 1, x^4 + 3x^3 + 3x^2 + 3x + 2)$ v $\mathbb{Z}_5[x]$.

104. Nalezněte dva polynomy p, q v $\mathbb{Z}_n[x]$ pro Vámi zvolené $n \in \mathbb{N}$, pro které není podíl a zbytek po dělení [1, s. 661] jednoznačně určen.

105. Uveďte příklad polynomu nad $\mathbb{Z}_4$, který má víc kořenů, než je jeho stupeň.

106. Uveďte příklad polynomu nad $\mathbb{Z}_5$, který má víc kořenů, než je jeho stupeň.

107. Dokažte nebo vyvraťte tvrzení: $x^p + a$ je ireducibilní nad $\mathbb{Z}_p[x]$ pro libovolné $a \in \mathbb{Z}_p$, kde p je prvočíslo [2, s. 284].

108. Dokažte, že $x^p - x$ má p různých kořenů v $\mathbb{Z}_p$ pro všechna prvočísla p [2, s. 284].

109. Nechť F je těleso a $a \in F$. Dokažte, že pokud $p(x) \in F[x]$, pak $p(a)$ je zbytek po dělení $p(x)$ výrazem $x - a$ [2, s. 284].

110. Dokažte, že polynom $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ je ireducibilní nad $\mathbb{Q}[x]$ pro všechna prvočísla p [2, s. 284].

2.6 Kódování a šifrování

111. Zakódujte zprávu 11010_2 pomocí kódu generovaného polynomem [1, s. 698] $p(x) = x + x^3$.

112. Nechť C je $(6, 3)$-kód nad abecedou $\{0, 1\}$. Najděte generující matici G a matici kontroly H [1, s. 700] kódu C, pokud

$$P = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

113. Nechť C je $(6, 3)$-kód nad abecedou $\{0, 1\}$. Zakódujte všechny možné zprávy, pokud je kód generován maticí

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}^T.$$

114. Demonstrujte protokol výměny klíčů Diffie-Hellman [1, s. 636] s parametry $p = 61, g = 7$ a Vámi zvolenými a, b.

115. Demonstrujte protokol RSA [1, s. 633] s parametry $p = 23, q = 29$ a Vámi zvoleným e. Zašifrujte zprávu $m = 25$ a následně jí dešifrujte.

116. Dešifrujte zprávu $c = 34$ zašifrovanou RSA s parametry $n = 5893, d = 81$.

117. Nechť parametry RSA jsou $n = 143 = 11 \cdot 13, e = 7, d = 103$.

    a) Podepište zprávu $m = 8$.
    b) Ověřte vzniklý podpis.
    c) Je $s = 42$ podpisem zprávy $m = 26$?

118. Najděte čísla n, e, x: $x^e \equiv x \pmod{n}$. Jsou tato čísla vhodná jako parametry RSA?

2.7 Řešení příkladů

2.7.1 Dělitelnost a prvočísla

1. $2^{60} - 1 = 2^{28} \cdot (2^{32} - 1) + 2^{28} - 1$
   $2^{32} - 1 = 2^4 \cdot (2^{28} - 1) + 2^4 - 1$
   $2^{28} - 1 = (2^{24} + 2^{20} + 2^{16} + 2^{12} + 2^8 + 2^4 + 1) \cdot (2^4 - 1) + 0.$

   $$\begin{aligned} 2^4 - 1 &= 2^{32} - 1 - 2^4 \cdot (2^{28} - 1) \\ &= 2^{32} - 1 - 2^4 \cdot [2^{60} - 1 - 2^{28} \cdot (2^{32} - 1)] \\ &= (2^{32} + 1)(2^{32} - 1) - 2^4 \cdot (2^{60} - 1). \end{aligned}$$

2. Pokud známe tvrzení $(a, b) \cdot [a, b] = a \cdot b$ [1, s. 592], pak je důkaz triviální.

   Jiný způsob: zaveďme

   $$\begin{aligned} a &= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}, \alpha_i \in \mathbb{N}_0, \\ b &= p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}, \beta_i \in \mathbb{N}_0, \\ [a, b] &= p_1^{\max(\alpha_1,\, \beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n,\, \beta_n)}, \\ (a, b) &= p_1^{\min(\alpha_1,\, \beta_1)} \cdot \ldots \cdot p_n^{\min(\alpha_n,\, \beta_n)}, \\ [a, b] \cdot (a, b) &= p_1^{\max(\alpha_1,\, \beta_1) + \min(\alpha_1,\, \beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n,\, \beta_n) + \min(\alpha_n,\, \beta_n)}. \end{aligned}$$

   „$\Longrightarrow$“: Pokud $\max(\alpha_i,\, \beta_i) = \alpha_i$, pak $\min(\alpha_i,\, \beta_i) = \beta_i$ a opačně. V každém případě ale $\max(\alpha_i,\, \beta_i) + \min(\alpha_i,\, \beta_i) = \alpha_i + \beta_i$.

   $$\begin{aligned} [a, b] = ab &= p_1^{\alpha_1 + \beta_1} \cdot \ldots \cdot p_n^{\alpha_n + \beta_n} \\ &= p_1^{\max(\alpha_1,\, \beta_1) + \min(\alpha_1,\, \beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n,\, \beta_n) + \min(\alpha_n,\, \beta_n)}. \end{aligned}$$

   Proto $(a, b) = 1$.

   „$\Longleftarrow$“: Pokud $(a, b) = 1$, pak $\min(\alpha_i,\, \beta_i) = 0$.

   $$[a, b] \cdot 1 = p_1^{\max(\alpha_1,\, \beta_1) + 0} \cdot \ldots \cdot p_n^{\max(\alpha_n,\, \beta_n) + 0}.$$

   Bez ohledu na hodnoty $\max(\alpha_i,\, \beta_i)$ vidíme, že a, b nemají žádné společné faktory, proto $[a, b] = ab$. $\square$

3. a) Báze pro $n \in \{1, 2, 3\}$: $f_1 = 1 < 2^1$, $f_2 = 1 < 2^2$, $f_3 = 2 < 2^3$.
   Indukční předpoklad: $\forall k \geq 3\colon\ f_k < 2^k$, tedy $f_{k-2} + f_{k-1} < 2^{k-2} + 2^{k-1}$.
   Indukční krok:

   $$\begin{aligned} f_{k+1} &< 2^{k+1} \\ f_{k-1} + f_k &< 2^{k-1} + 2^k \end{aligned}$$

$$\begin{aligned} 2^{k-1} + 2^k &< 2^{k+1} \qquad / \cdot 2^k \\ 2^{-1} + 1 &< 2 \\ \frac{3}{2} &< 2. \end{aligned}$$

□

b) Báze pro $n = 1$: $(f_n, f_{n+1}) = (f_1, f_2) = (1, 1) = 1$.
Indukční předpoklad: $\forall k \geq 1\colon (f_k, f_{k+1}) = 1$.
Indukční krok: $(f_{k+1}, f_{k+2}) = (f_{k+1}, f_{k+1} + f_k) = (f_{k+1}, f_k) = 1$. □

c) Báze pro $n = 1$: $f_1 = 1 = 2 - 1 = f_3 - 1$.
Indukční předpoklad: $\forall k \geq 1\colon f_1 + f_2 + \cdots + f_k = f_{k+2} - 1$.
Indukční krok:

$$\begin{aligned} f_1 + f_2 + \cdots + f_k + f_{k+1} &= f_{k+3} - 1 \\ f_{k+2} - 1 + f_{k+1} &= f_{k+3} - 1 \\ f_{k+2} + f_{k+1} &= f_{k+3}. \end{aligned}$$

□

d) Báze pro $n = 2$: $f_3 \cdot f_1 = 2 \cdot 1 = 1^2 + 1 = f_2^2 + (-1)^2$.
Indukční předpoklad: $\forall k \geq 2\colon f_{k+1} \cdot f_{k-1} = f_k^2 + (-1)^k$.
Indukční krok:

$$\begin{aligned} f_{k+2} \cdot f_k &= f_{k+1}^2 + (-1)^{k+1} \\ (f_{k+1} + f_k) \cdot f_k &= f_{k+1}^2 + (-1)^{k+1} \\ f_{k+1} \cdot f_k + f_k^2 - f_{k+1}^2 &= (-1)^{k+1} \\ f_{k+1}(f_k - f_{k+1}) + f_k^2 &= (-1)^{k+1} \\ f_{k+1}(f_k - f_k - f_{k-1}) + f_k^2 &= (-1)^{k+1} \\ -(f_{k+1} \cdot f_{k-1}) + f_k^2 &= (-1)^{k+1} \\ -(f_k^2 + (-1)^k) + f_k^2 &= (-1)^{k+1} \\ -(-1)^k &= (-1)^{k+1} \\ (-1)^{k+1} &= (-1)^{k+1} \\ 0 &= 0. \end{aligned}$$

□

e) Báze pro $n = 1$ a $n = 2$:

$$f_1 = \frac{(1+\sqrt{5})^1 - (1-\sqrt{5})^1}{2^1\sqrt{5}} \qquad f_2 = \frac{(1+\sqrt{5})^2 - (1-\sqrt{5})^2}{2^2\sqrt{5}}$$

$$1 = \frac{2\sqrt{5}}{2\sqrt{5}}, \qquad 1 = \frac{4\sqrt{5}}{4\sqrt{5}}.$$

Indukční předpoklad:

$$\forall k \geq 1\colon f_k = \frac{(1+\sqrt{5})^k - (1-\sqrt{5})^k}{2^k\sqrt{5}},\ f_{k+1} = \frac{(1+\sqrt{5})^{k+1} - (1-\sqrt{5})^{k+1}}{2^{k+1}\sqrt{5}}.$$

Indukční krok:

$$\begin{aligned}
f_{k+2} &= \frac{(1+\sqrt{5})^{k+2} - (1-\sqrt{5})^{k+2}}{2^{k+2}\sqrt{5}} \\
f_{k+2} &= f_k + f_{k+1} \\
&= \frac{(1+\sqrt{5})^k - (1-\sqrt{5})^k}{2^k\sqrt{5}} + \frac{(1+\sqrt{5})^{k+1} - (1-\sqrt{5})^{k+1}}{2^{k+1}\sqrt{5}} \\
&= \frac{2(1+\sqrt{5})^k - 2(1-\sqrt{5})^k + (1+\sqrt{5})^k(1+\sqrt{5}) - (1-\sqrt{5})^k(1-\sqrt{5})}{2^{k+1}\sqrt{5}} \\
&= \frac{(1+\sqrt{5})^k(3+\sqrt{5}) - (1-\sqrt{5})^k(3-\sqrt{5})}{2^{k+1}\sqrt{5}}.
\end{aligned}$$

$$\begin{aligned}
\frac{(1+\sqrt{5})^{k+2} - (1-\sqrt{5})^{k+2}}{2^{k+2}\sqrt{5}} &= \frac{(1+\sqrt{5})^k(3+\sqrt{5}) - (1-\sqrt{5})^k(3-\sqrt{5})}{2^{k+1}\sqrt{5}} \\
(1+\sqrt{5})^k(3+\sqrt{5}) - (1-\sqrt{5})^k(3-\sqrt{5})^2 &= (1+\sqrt{5})^k(3+\sqrt{5}) - (1-\sqrt{5})^k(3-\sqrt{5}) \\
0 &= 0.
\end{aligned}$$

□

4. Obměnou implikace získáme tvrzení: pokud p není prvočíslo, pak $2^p - 1$ není prvočíslo. Z toho vyplývá, že $p = a \cdot b$, kde $a, b > 1$ a $2^p - 1 = 2^{ab} - 1 = (2^a)^b - 1$.

   Platí: $x^b - 1 = (x-1)(x^{b-1} + x^{b-2} + \ldots + x + 1)$. V našem případě $x = 2^a \geq 4$, proto $(x-1) > 1$ a zároveň $(x^{b-1} + x^{b-2} + \ldots + x + 1) > 1$, tedy $2^{ab} - 1$ je složené. □

5. $\varphi(1) = \varphi(2) = 1$. Pro $n \geq 3$ je $\varphi(n)$ sudé [1, s. 598].

6. Z Euklidova algoritmu [1, s. 591]:

   a) $(2n+9, 3n+13) = (2n+9, n+4) = (n+4, n+5) = (n+4, 1) = 1.$ □

   b) $(2n+3, 11n+17) = (2n+3, n+2) = (n+2, n+1) = (n+1, 1) = 1.$ □

7. $(3k+11, 5k+12) = (3k+11, 2k+1) = (2k+1, k+10) = (k+10, -19) = (k+10, 19)$.

   Pro $k \equiv 9 \pmod{19}$ je $(k+10, 19) = 19$, jinak 1.

8. Zřejmě $r > 2$, tedy r je liché prvočíslo. Protože r je součtem dvou prvočísel a rozdílem dvou prvočísel, jedno z nich je sudé, tedy 2. Proto $r = p+2 = q-2$. Čísla $p, r = p+2, q = r+2$ jsou tři po sobě jdoucí lichá prvočísla. Protože z každé trojice po sobě jdoucích lichých čísel je jedno z nich dělitelné číslem 3, jediná možná trojice je $(p, r, q) = (3, 5, 7)$. Hledané číslo je tedy jenom $r = 5 = 3 + 2 = 7 - 2$.

9. Předpokládejme, že z čísla 200 je možné dostat prvočíslo změnou poslední cifry (protože změnou první nebo druhé cifry prvočíslo nezískáme) za jedno z čísel $1, 3, 7, 9$. Avšak $3|201, 7|203, 3|207$ a $11|209$. Tvrzení je tedy nepravdivé. $\square$

10. Pokud vyzkoušíme největší trojciferné číslo 999, po několika krocích se zacyklíme v sekvenci $4, 16, 37, 58, 89, 145, 42, 20$. Číslo 999 tedy není šťastné. Největší trojciferné šťastné číslo je 998:

$$\begin{aligned}
998 &\to 9^2 + 9^2 + 8^2 = 226\\
226 &\to 2^2 + 2^2 + 6^2 = 44\\
44 &\to 4^2 + 4^2 = 32\\
32 &\to 3^2 + 2^2 = 13\\
13 &\to 1^2 + 3^2 = 10\\
10 &\to 1^2 + 0^2 = 1.
\end{aligned}$$

11. a) Rovnice $ax = b$ má řešení, pokud b je násobkem a. Řešení je jediné: $\frac{b}{a}$.

    b) Rovnice $ax+by = c$, má řešení, pokud c je násobkem (a, b). Partikulární řešení v tvaru (x_0, y_0) nalezneme pomocí koeficientů v příslušné Bezoutově rovnosti. Rovnice má dále pro $k \in \mathbb{Z}$ nekonečně mnoho řešení tvaru $(x_0 + bk, y_0 - ak)$. Např.:

$$\begin{aligned}
16x + 28y &= 72\\
(16, 28) &= 4|72\\
4x + 7y &= 18\\
(4, 7) &= 1\\
1 &= 2 \cdot 4 - 1 \cdot 7\\
18 &= 36 \cdot 4 - 18 \cdot 7\\
(x, y) &= (36 + 7k, -18 - 4k), \text{ kde } k \in \mathbb{Z}.
\end{aligned}$$

12. „ $\Longrightarrow$ “: Zřejmé.

    „ $\Longleftarrow$ “: Obměnou implikace získáme tvrzení: pokud n je složené, pak je dělitelné nějakým prvočíslem p, kde $1 < p \leq \sqrt{n}$. Nechť $n = ab$ pro $a, b \in \mathbb{N}$, kde $a, b > 1$. Dle základní věty aritmetiky lze a, b rozložit na součin prvočísel. Dále musí platit, že $a \leq \sqrt{n}$ nebo $b \leq \sqrt{n}$, protože jinak $ab > \sqrt{n} \cdot \sqrt{n} = n$. Proto nalezneme nejméně jednoho dělitele n nejvýše do $\sqrt{n}$. V opačném případě je n prvočíslem. $\square$

13. Předpokládejme, že p je prvočíslo a $p \neq 3$. Pak $p = 3k \pm 1$ pro nějaké $k \in \mathbb{N}$. Potom ale $p^2 + 2 = 9k^2 \pm 6k + 3 = 3(3k^2 \pm 2k + 1)$ je dělitelné 3 a tedy není prvočíslem. Jediná možnost je proto $p = 3$. $\square$

14. Nechť $d = (a, b)$. Pak $a = dx$, $b = dy$, kde $x, y \in \mathbb{N}$ a $(x, y) = 1$.

    $a^n | b^n \implies b^n = k \cdot a^n \implies d^n y^n = k \cdot d^n x^n \implies y^n = k \cdot x^n \implies x^n | y^n$.

    Pak ale nutně $x = 1$, protože jinak by bylo x dělitelné nějakým prvočíslem p, které by dělilo i y^n a tedy i y a to by bylo ve sporu s tím, že $(x, y) = 1$.

    $x = 1 \implies a = d, b = dy \implies a | b$. □

15. Hledaný nejmenší společný násobek musí být dělitelný všemi čísly od 1 po 20. Nejmenší takové číslo je $2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 232792560$.

16. $16! = 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot 2 \cdot 3 \cdot 7 \cdot 2^3 \cdot 3^2 \cdot 2 \cdot 5 \cdot 11 \cdot 2^2 \cdot 3 \cdot 13 \cdot 2 \cdot 7 \cdot 3 \cdot 5 \cdot 2^4 = 2^{15} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$.

17. Číslo $\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$ je tzv. *p-adickou valuací* čísla $n!$.

    Důkaz: $n! = 1 \cdot 2 \cdot \ldots \cdot n$. Pro pevně zvolené prvočíslo p je ve výrazu $\nu_p(n!)$ celkem $\lfloor \frac{n}{p} \rfloor$ čísel dělitelných p, $\lfloor \frac{n}{p^2} \rfloor$ čísel dělitelných p^2 atd. Obecně v rozkladu $n!$ existuje $\lfloor \frac{n}{p^k} \rfloor$ čísel dělitelných p^k. Proto pro nalezení exponentu jednoduše sečteme členy $\lfloor \frac{n}{p^k} \rfloor$ pro všechna $k \geq 1$. Tato suma konverguje, protože existuje takové k, že $p^k > n$. □

    Dále pro $n = p^r$:

$$\begin{aligned}
\nu_p(n!) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{n}{p^{r-1}} \right\rfloor + \left\lfloor \frac{n}{p^r} \right\rfloor \\
&= p^{r-1} + p^{r-2} + \ldots + p + 1 \\
&= \frac{p^r - 1}{p - 1} = \frac{n - 1}{p - 1}.
\end{aligned}$$

18. Z Euklidova algoritmu $(n, n + 2) = (n, 2)$. Pro lichá n dostáváme $(2k + 1, 2) = 1$, pro sudá n zase $(2k, 2) = 2$. □

19. Všechna $n \in \mathbb{N}$ jsou tvaru $6k + a$, kde $a \in \{0, 1, 2, 3, 4, 5\}$ a $k \in \mathbb{N}$. Pro $a \in \{0, 2, 3, 4\}$ je n složené, proto prvočísla větší než 3 jsou vždy tvaru $6k + 1$ nebo $6k + 5$ a tedy mají zbytek 1 nebo 5 po dělení 6. □

20. a) Nejprve dokážeme, že funkce $\sigma(n)$ je multiplikativní, tedy že pro nesoudělná a, b platí: $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$. Nechť dělitele čísla a jsou $x_1, \ldots, x_k$ a dělitele čísla b jsou $y_1, \ldots, y_l$. Protože $(a, b) = 1$, všechny dělitele čísla ab jsou tvaru $x_i \cdot y_j$ pro nějaké i, j. Pak součinem $(x_1 + \ldots + x_k) \cdot (y_1 + \ldots + y_l) = \sigma(a) \cdot \sigma(b)$ získáme všechny dělitele čísla ab, tedy $\sigma(a \cdot b)$. □

    V důkazu dále využijeme, že $\sigma(2^k) = 2^{k+1} - 1$ a $\sigma(p) = 1 + p$.

$$\begin{aligned}
n &= 2^{p-1} \cdot (2^p - 1) \\
\sigma(n) &= \sigma(2^{p-1} \cdot (2^p - 1)) \\
\sigma(n) &= \sigma(2^{p-1}) \cdot \sigma(2^p - 1) \\
\sigma(n) &= (2^p - 1) \cdot (1 + 2^p - 1) \\
\sigma(n) &= (2^p - 1) \cdot 2^p = 2n.
\end{aligned}$$

□

b) Pro první 3 prvočísla dostáváme:
$p = 2 \implies 2^2 - 1 = 3$ je prvočíslo $\implies n = 2^1 \cdot 3 = 6$,
$p = 3 \implies 2^3 - 1 = 7$ je prvočíslo $\implies n = 2^2 \cdot 7 = 28$,
$p = 5 \implies 2^5 - 1 = 31$ je prvočíslo $\implies n = 2^4 \cdot 31 = 496$.

21. První dvojici tvoří spřátelená čísla, protože $\sigma(220) = \sigma(284) = 504$, ale druhou ne, protože $\sigma(234) = 546$ a $\sigma(260) = 588$.

22. Stačí ukázat, že $n^3 - n = n(n+1)(n-1)$ je dělitelné 2 a 3 zároveň. Protože $n-1, n, n+1$ jsou tři po sobě jdoucí přirozená čísla, jedno z nich bude dělitelné 3 a alespoň jedno z nich bude dělitelné 2. Jejich součin bude proto dělitelný 6. $\square$

23. Nechť $n = \overline{abc}$, kde $a \neq 0$. Pak $11|n \iff 11|c + a - b \iff c + a - b \in \{0, 11\}$.
Ze zadání $\frac{100a+10b+c}{11} = a^2 + b^2 + c^2 \iff 100a + 10b + c = 11(a^2 + b^2 + c^2)$.
Pokud $c + a - b = 0$, t.j. $b = a + c$, pak

$$\begin{aligned} 100a + 10(a+c) + c &= 11(a^2 + (a+c)^2 + c^2) \\ 110a + 11c &= 11(2a^2 + 2ac + 2c^2) \\ 10a + c &= 2a^2 + 2ac + 2c^2 \\ 2a^2 + 2ac - 10a + 2c^2 - c &= 0 \\ a^2 + (c-5)a + c^2 - \frac{c}{2} &= 0. \end{aligned}$$

Diskriminant této rovnice je $-3c^2 - 8c + 25 \geq 0 \iff c \in \{0, 1\}$.
$c = 0 \implies a^2 - 5a = 0 \implies a = 5, b = 5$. Prvním hledaným číslem je 550.
$c = 1 \implies a, b \notin \mathbb{N}$.
Pokud $c + a - b = 11$, t.j. $b = a + c - 11$, pak

$$\begin{aligned} 100a + 10(a+c-11) + c &= 11(a^2 + (a+c-11)^2 + c^2) \\ 110a + 11c - 110 &= 11(2a^2 + 2ac + 2c^2 - 22a - 22c + 121) \\ 10a + c - 10 &= 2a^2 + 2ac + 2c^2 - 22a - 22c + 121 \\ 2a^2 + 2ac - 32a + 2c^2 - 23c + 131 &= 0 \\ a^2 + (c-16)a + c^2 - \frac{23}{2}c + \frac{131}{2} &= 0. \end{aligned}$$

Diskriminant této rovnice je $-3c^2 + 14c - 6 \geq 0 \iff c \in \{1, 2, 3, 4\}$.
$c = 1 \vee c = 2 \vee c = 4 \implies a, b \notin \mathbb{N}$.
$c = 3 \implies a^2 - 13a + 40 = 0 \implies a = 8, b = 0$. Druhým hledaným číslem je 803.

24. Každou permutaci je možné reprezentovat jako sekvenci záměn jednoho páru cifer. Stačí proto ukázat, že rozdíl čísel a, b je dělitelný 9 po výměně dvou cifer.

Nechť $a = 10^n k_n + \ldots + 10^i k_i + \ldots + 10^j k_j + \ldots + 10k_1 + k_0$. Můžeme předpokládat $i > j$ a zaměnit cifry k_i, k_j. Pak $b = 10^n k_n + \ldots + 10^i k_j + \ldots + 10^j k_i + \ldots + 10k_1 + k_0$. Rozdíl je pak

$$\begin{aligned} a - b &= (10^i k_i + 10^j k_j) - (10^i k_j + 10^j k_i) \\ &= 10^i(k_i - k_j) - 10^j(k_i - k_j) \\ &= (k_i - k_j)(10^i - 10^j) \\ &= (k_i - k_j)(10^{i-j} - 1)10^j. \end{aligned}$$

$(10^{i-j} - 1) = (10^m - 1) = (10 - 1)(10^{m-1} + 10^{m-2} + \ldots + 10^2 + 10 + 1) = 9s.$ □

25. Předpokládejme, že cifry čísla 2^a se dají přeuspořádat na 2^b, kde $a < b$. Na základě výsledku předešlého příkladu víme, že $9|2^b - 2^a$.

    Protože $2^3 < 10 < 2^4$, existují nejvýše čtyři mocniny dvojky se stejným počtem cifer. Může proto nastat jedna z možností $b = a + 1$, $b = a + 2$, $b = a + 3$.

    $b = a + 1 \implies 2^b = 2^{a+1} \implies 2^b = 2 \cdot 2^a \implies 2^b - 2^a = 2^a.$

    $b = a + 2 \implies 2^b = 2^{a+2} \implies 2^b = 4 \cdot 2^a \implies 2^b - 2^a = 3 \cdot 2^a.$

    $b = a + 3 \implies 2^b = 2^{a+3} \implies 2^b = 8 \cdot 2^a \implies 2^b - 2^a = 7 \cdot 2^a.$

    V každém případě ale 9 nikdy nebude dělit $2^b - 2^a$. To je spor s naším předpokladem a proto hledané číslo neexistuje. □

26. $2 = -2i^2 = -i(2i) = -i(1 + i)^2.$ □

2.7.2 Kongruence

27. $a = 10^n k_n + \ldots + 10k_1 + k_0 \equiv k_n + \ldots + k_1 + k_0 \equiv 0 \pmod 3.$ □

    Tímto jsme zároveň dokázali, že číslo a je kongruentní se součtem svých cifer modulo 3, tedy že $S(a) \equiv a \pmod 3$. To samé platí modulo 9. Proto můžeme jiným způsobem dokázat příklad 24:

    $S(b) \equiv S(a) \pmod 9 \implies b \equiv a \pmod 9 \implies b - a \equiv 0 \pmod 9.$ □

28. Stačí ukázat, že xyz je dělitelné 3, 4 a 5 zároveň.

    Dělitelnost 3: Protože $0^2 \equiv 0 \pmod 3$ a $1^2 \equiv 2^2 \equiv 1 \pmod 3$, všechny druhé mocniny jsou kongruentní s 0 nebo 1 modulo 3. Aby byla řešitelná kongruence $x^2 + y^2 \equiv z^2 \pmod 3$, musí být x^2 (a tedy zároveň x) nebo y^2 (a tedy zároveň y) kongruentní s 0 modulo 3. Proto je součin xyz dělitelný 3.

    Dělitelnost 4: Protože součet dvou lichých čísel je sudý a součet dvou sudých čísel je sudý, právě jedno z čísel x, y, z je sudé nebo všechna jsou sudá. Protože $0^2 \equiv 4^2 \equiv 0 \pmod 8$, $2^2 \equiv 6^2 \equiv 4 \pmod 8$ a $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$, všechny druhé mocniny jsou kongruentní s 0, 1 nebo 4 modulo 8.

Pokud jsou x, y, z sudá, pak má kongruence $x^2 + y^2 \equiv z^2 \pmod 8$ tvar $0 + 0 \equiv 0 \pmod 8$ nebo $0+4 \equiv 4+0 \equiv 4 \pmod 8$. V každém případě je alespoň jedno z čísel x^2, y^2, z^2 dělitelné 8 a tedy alespoň jedno z čísel x, y, z je dělitelné 4.

Pokud je sudé jenom jedno z nich (předpokládejme bez újmy na obecnosti x), pak aby byla řešitelná kongruence $x^2 + y^2 \equiv z^2 \pmod 8$, musí platit: $x \equiv 0 \pmod 8$ a $y \equiv z \equiv 1 \pmod 8$. Proto $4|x$ a součin xyz je dělitelný 4.

Dělitelnost 5: Protože $0^2 \equiv 0 \pmod 5$, $1^2 \equiv 4^2 \equiv 1 \pmod 5$ a $2^2 \equiv 3^2 \equiv -1 \pmod 5$, všechny druhé mocniny jsou kongruentní s $0, 1$ nebo -1 modulo 5. Pokud by nebylo žádné z čísel x, y, z dělitelné 5, kongruence $x^2 + y^2 \equiv z^2 \pmod 5$ může mít po dosazení tvar $\pm 1 \pm 1 \equiv \pm 1 \pmod 5$, což ale není možné. V každém případě je alespoň jedno z čísel x, y, z dělitelné 5, proto také xyz je dělitelné 5. $\square$

29.
$$\begin{aligned}
3^{45} &\equiv x && \pmod{100} \\
3^5 \cdot 3^{40} &\equiv x && \pmod{100} \\
3^{40} &\equiv 1 && \pmod{100} \quad \Longleftarrow \text{ Z Eulerovy věty } \varphi(100) = 40 \\
3^5 \cdot 3^{40} &\equiv 3^5 \cdot 1 && \pmod{100} \\
3^5 &\equiv 43 && \pmod{100} \\
x &= 43.
\end{aligned}$$

30.
$$\begin{aligned}
99^{98^{97}} &\equiv x && \pmod{10} \\
(-1)^{98^{97}} &\equiv x && \pmod{10} \\
98^{97} &\equiv y && \pmod{2} \\
y &\equiv 0 && \pmod{2} \\
(-1)^{98^{97}} &\equiv (-1)^0 && \pmod{10} \\
x &= 1.
\end{aligned}$$

31.
$$\begin{aligned}
2003^{2002^{2001}} \equiv 3^{2002^{2001}} &\equiv x && \pmod{1000} \\
\varphi(1000) = 400 \implies 3^{400} &\equiv 1 && \pmod{1000} \\
2002^{2001} \equiv 2^{2001} &\equiv y && \pmod{400} \\
2^4 \cdot 2^{1997} &\equiv y && \pmod{2^4 \cdot 25} \\
2^{1997} &\equiv z && \pmod{25} \\
\varphi(25) = 20 \implies 2^{20} &\equiv 1 && \pmod{25} \\
2^{17} &\equiv z && \pmod{25} \\
z &\equiv 22 && \pmod{25} \\
2^4 \cdot 22 &\equiv y && \pmod{400} \\
y &\equiv 352 && \pmod{400} \\
3^{352} &\equiv x && \pmod{1000} \\
x &= 241.
\end{aligned}$$

K výpočtu $3^{352} \pmod{1000}$ můžeme použít algoritmus binárního umocňování, viz. příklad 44.

32. a) $2^{30} = (2^2)^{15} \equiv (-1)^{15} \equiv -1 \equiv 4 \pmod 5$.

    b) $72^{11} = 4^{11} \cdot 18^{11} \equiv 4^{11} \equiv 4 \cdot (4^2)^5 \equiv 4 \cdot (-1)^5 \equiv -4 \equiv 13 \pmod{17}$.

    c) $\varphi(144) = 48 \implies 7^{51} = 7^3 \cdot 7^{48} \equiv 7^3 \equiv 55 \pmod{144}$.

    d) $13^{12} + 12^{11} + 11^{10} \equiv 4^{12} + 3^{11} + 2^{10} \equiv (4^3)^4 + 3 \cdot (3^2)^5 + 2 \cdot (2^3)^3 \equiv$
    $\equiv 1^4 + 3 \cdot 0^5 + 2 \cdot (-1)^3 \equiv 8 \pmod 9$.

33. $8^{12} + 11 \cdot 2^{10} \equiv 3^{12} + 1 \cdot 2^{10} \equiv (3^2)^6 + (2^2)^5 \equiv (-1)^6 + (-1)^5 \equiv 0 \pmod 5$.

34. $2^{70} \equiv (2^5)^2 \cdot (2^{12})^5 \equiv 6^2 \cdot 1^5 \equiv -3 \pmod{13}$.

    $3^{70} \equiv 3 \cdot (3^3)^{23} \equiv 3 \cdot 1^{23} \equiv 3 \pmod{13}$.

    $2^{70} + 3^{70} \equiv 0 \pmod{13}$.

35. Protože $20801 = 11 \cdot 31 \cdot 61$, stačí ukázat, že $20^{15} - 1$ je dělitelné postupně čísly 11, 31 a 61, neboli že $20^{15} \equiv 1 \pmod k$, kde $k \in \{11, 31, 61\}$.

    $20^{15} = (20^5)^3 = ((2 \cdot 10)^5)^3 = (2^5 \cdot 10^5)^3 \equiv ((-1) \cdot (-1)^5)^3 \equiv 1^3 \equiv 1 \pmod{11}$.

    $20^{15} = (20^3)^5 \equiv 2^5 \equiv 1 \pmod{31}$.

    $20^{15} = (2^2 \cdot 5)^{15} = 2^{30} \cdot (5^3)^5 \equiv (-1) \cdot 3^5 \equiv (-1) \cdot (-1) \equiv 1 \pmod{61}$.

36.
$$\begin{aligned}
(27, 1573) &= 1 \\
27^{\varphi(1573)} &\equiv 1 \pmod{1573} \\
\varphi(1573) = \varphi(11^2 \cdot 13) &= 1320 \\
27^{1320} &\equiv 1 \pmod{1573} \\
27^5 \equiv 1 \implies 27^{1320} &\equiv 1 \pmod{1573}.
\end{aligned}$$

37. $645 = 3 \cdot 5 \cdot 43$ není prvočíslem, ale $2^{644} \equiv 1 \pmod{645}$:

$$\begin{aligned}
2^{644} &\equiv 1 \pmod 3 \\
(2^2)^{322} &\equiv 1 \pmod 3 \\
1^{322} &\equiv 1 \pmod 3.
\end{aligned}
\qquad
\begin{aligned}
2^{644} &\equiv 1 \pmod 5 \\
(2^4)^{161} &\equiv 1 \pmod 5 \\
1^{161} &\equiv 1 \pmod 5.
\end{aligned}
\qquad
\begin{aligned}
2^{644} &\equiv 1 \pmod{43} \\
2^{42} &\equiv 1 \pmod{43} \\
2^{644} &\equiv 2^{14} \pmod{43} \\
2^{14} &\equiv (2^7)^2 \pmod{43} \\
(2^7)^2 &\equiv (-1)^2 \pmod{43} \\
(-1)^2 &\equiv 1 \pmod{43}.
\end{aligned}$$

38. Použijeme Korseltovo kritérium [1, s. 626]: $561 = 3 \cdot 11 \cdot 17$ není dělitelné čtvercem a platí: $2|560$, $10|560$, $16|560$. Proto je 561 Carmichaelovým číslem.

39. Správně platí $a^{p-1} \equiv 1 \pmod{p}$. Z kongruence $a^p \equiv a^{p-1} \pmod{p}$ dostáváme po vydělení výrazem a^{p-1} výsledek: $a \equiv 1 \pmod{p}$.

Ukázka pro $a \in \{1, \dots, 15\}$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
p	p	–	2	3	2	5	2, 3	7	2	3	2, 5	11	2, 3	13	2, 7

40. a)
$$\begin{aligned} 3x &\equiv 2 \pmod{7} \\ 15x &\equiv 10 \pmod{7} \\ x &\equiv 3 \pmod{7}. \end{aligned}$$

b)
$$\begin{aligned} 5x &\equiv 12 \pmod{23} \\ 70x &\equiv 168 \pmod{23} \\ x &\equiv 7 \pmod{23}. \end{aligned}$$

c)
$$\begin{aligned} 5x &\equiv 12 \pmod{26} \\ 25x &\equiv 60 \pmod{26} \\ -x &\equiv 8 \pmod{26} \\ x &\equiv 18 \pmod{26}. \end{aligned}$$

d)
$$\begin{aligned} 49x &\equiv 3 \pmod{5} \\ -x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{5}. \end{aligned}$$

e)
$$\begin{aligned} 17x &\equiv 1 \pmod{6} \\ -x &\equiv 1 \pmod{6} \\ x &\equiv 5 \pmod{6}. \end{aligned}$$

f)
$$\begin{aligned} 3x &\equiv 1 \pmod{6} \\ (3,6) &\neq 1 \implies \nexists x. \end{aligned}$$

g)
$$\begin{aligned} 37x &\equiv 1 \pmod{101} \\ 111x &\equiv 3 \pmod{101} \\ 10x &\equiv 3 \pmod{101} \\ 100x &\equiv 30 \pmod{101} \\ -x &\equiv 30 \pmod{101} \\ x &\equiv 71 \pmod{101}. \end{aligned}$$

h)
$$\begin{aligned} 21x &\equiv 6 \pmod{9} \\ 3x &\equiv 6 \pmod{9} \\ x &\equiv 2 \pmod{3}. \end{aligned}$$

i)
$$\begin{aligned} x^2 &\equiv 2 \pmod{47} \\ x^2 &\equiv 2 + 47 \pmod{47} \\ x^2 &\equiv 49 \pmod{47} \\ x &= \pm 7. \end{aligned}$$

j)
$$\begin{aligned} x^2 + x - 2 &\equiv 0 \pmod{5} \\ (x+2)(x-1) &\equiv 0 \pmod{5} \\ x \equiv -2 \ \vee\ x &\equiv 1 \pmod{5}. \end{aligned}$$

k)
$$\begin{aligned} x^2 + 16x &\equiv -5 \pmod{11} \\ x^2 + 16x + 64 &\equiv 59 \pmod{11} \\ (x+8)^2 &\equiv 59 \pmod{11}. \\ y &= x + 8 \\ y^2 &\equiv 4 \pmod{11} \\ y^2 &\equiv \pm 2 \pmod{11} \\ x \equiv 5 \ \vee\ x &\equiv 1 \pmod{11}. \end{aligned}$$

l)
$$\begin{aligned} 373^{121} &\equiv x \pmod{18} \\ 13^{121} &\equiv x \pmod{18} \\ 13^3 &\equiv 1 \pmod{18} \\ 121 &\equiv y \pmod{3} \\ y &\equiv 1 \pmod{3} \\ x &\equiv 13 \pmod{18}. \end{aligned}$$

m)
$$\begin{aligned} 2^{3^{4^5}} &\equiv x \pmod{9} \\ 2^6 &\equiv 1 \pmod{9} \\ 3^{4^5} &\equiv y \pmod{6} \\ \forall a \in \mathbb{N}\colon 3^a &\equiv 3 \pmod{6} \\ 2^{3^{4^5}} &\equiv 2^3 \pmod{9} \\ x &\equiv 8 \pmod{9}. \end{aligned}$$

41. a)

$$\begin{aligned} x &= 4k+3 \\ \hline x &\equiv 4 && \pmod 5 \\ 4k &\equiv 1 && \pmod 5 \\ k &\equiv 4 && \pmod 5 \\ k &= 5l+4 \\ x &= 20l+19 \\ x &\equiv 19 && \pmod{20}. \end{aligned}$$

b)

$$\begin{aligned} x &= 20k+19 \\ \hline x &\equiv 1 && \pmod 9 \\ k &\equiv 0 && \pmod 9 \\ k &= 9l \\ x &= 180l+19 \\ \hline x &\equiv 5 && \pmod{14} \\ 12l &\equiv 0 && \pmod{14} \\ l &\equiv 0 && \pmod 7 \\ x &= 1260m+19 \\ x &\equiv 19 && \pmod{1260}. \end{aligned}$$

c)

$$\begin{aligned} x &= 5k+3 \\ \hline x &\equiv 0 && \pmod 8 \\ k &\equiv 1 && \pmod 8 \\ k &= 8l+1 \\ x &= 40l+8 \\ \hline x &\equiv 1 && \pmod{11} \\ 7l &\equiv -7 && \pmod{11} \\ l &\equiv 10 && \pmod{11} \\ l &= 11m+10 \\ x &= 440m+408 \\ \hline x &\equiv 2 && \pmod{14} \\ 6m &\equiv 0 && \pmod{14} \\ 3m &\equiv 0 && \pmod 7 \\ m &= 7n \\ x &= 3080n+408 \\ x &\equiv 408 && \pmod{3080}. \end{aligned}$$

d)

$$\begin{aligned} x &= 3k+1 \\ \hline 3x &\equiv 1 && \pmod 5 \\ k &\equiv 1 && \pmod 5 \\ k &= 5l+1 \\ x &= 15l+4 \\ \hline 3x &\equiv -2 && \pmod 8 \\ l &\equiv 2 && \pmod 8 \\ l &= 8m+2 \\ x &= 120m+34 \\ x &\equiv 34 && \pmod{120}. \end{aligned}$$

e)

$$\begin{aligned} 28x &\equiv 35 && \pmod{42} \\ 4x &\equiv 5 && \pmod 6 \\ -2x &\equiv -1 && \pmod 6 \\ 2x &\equiv 1 && \pmod 6 \end{aligned}$$

$(2,6) \neq 1 \implies \nexists x.$

f)

$$\begin{aligned} 7x+10y &\equiv -5 && \pmod{23} \\ 4x+3y &\equiv 4 && \pmod{23} \\ \hline 7x+10y &\equiv -5 && \pmod{23} \\ 4x+26y &\equiv 4 && \pmod{23} \\ \hline 7x+10y &\equiv -5 && \pmod{23} \\ 2x+13y &\equiv 2 && \pmod{23} \\ \hline 9x+23y &\equiv -3 && \pmod{23} \\ 9x &\equiv -3 && \pmod{23} \\ 3x &\equiv -1 && \pmod{23} \\ 3x &\equiv 24 && \pmod{23} \\ x &\equiv 8 && \pmod{23} \\ \hline 32+3y &\equiv 4 && \pmod{23} \\ 3y &\equiv 18 && \pmod{23} \\ y &\equiv 6 && \pmod{23}. \end{aligned}$$

42. Nejprve ukážeme, že pro všechna $n \geq 4$ platí: $5^n \equiv 5^{n+4} \pmod{10000}$.

Báze pro $n = 4$: $5^4 \equiv 5^8 \equiv 625 \pmod{10000}$.

Indukční předpoklad: $\forall k \geq 4\colon 5^k \equiv 5^{k+4} \pmod{10000}$.

Indukční krok: $5^{k+1} \equiv 5^{k+5} \equiv 5^{k+4} \cdot 5 \equiv 5^k \cdot 5 \equiv 5^{k+1} \pmod{10000}$.

Protože pro všechna $a \in \mathbb{N}$ platí: $5^{4a} \equiv 625 \pmod{10000}$, $5^{5a} \equiv 3125 \pmod{10000}$, $5^{6a} \equiv 5625 \pmod{10000}$ a $5^{7a} \equiv 8125 \pmod{10000}$, poslední 4 cifry čísla 5^n, kde $n \in \{4, 5, 6, \dots\}$ tvoří periodickou posloupnost s periodou $0625, 3125, 5625, 8125$.

43. $(0, 4, 5, 1, 5, 2, 4, 9, 3, 4) \cdot (10, \dots, 1) = 176 \equiv 0 \pmod{11}$.

$(1, 2, 3, 6, 8, 9, 1, 3, 5, 10) \cdot (10, \dots, 1) = 220 \equiv 0 \pmod{11}$.

44.

krok	0	1	2	3	4	5	6	7	8	9
základ	3	9	81	561	721	841	281	961	521	441
exponent	352	176	88	44	22	11	5	2	1	0
výsledek	1						841	321		241

45. Předpokládejme, že prvočísel tvaru $6k - 1$ existuje jenom konečně mnoho a seřaďme je: $p_1 < \dots < p_n$. Uvažme ale číslo $N = 6 \cdot p_1 \cdot \dots \cdot p_n - 1$.

Pokud je N prvočíslem, pak jsme došli k sporu, protože $N > p_n$ a N je opět tvaru $6k - 1 \equiv -1 \pmod 6$.

Pokud je N složené, pak existuje prvočíslo q, $q|N$ a $q \notin \{p_1, \dots, p_n\}$. Tedy $N = q_1 \cdot \dots \cdot q_m$. Pro všechna $q > 3$ platí: $q \equiv \pm 1 \pmod 6$. Kdyby pro všechna i platilo, že $q_i \equiv 1 \pmod 6$, pak $N \equiv 1 \pmod 6$, proto existuje takové i, že $q_i \equiv -1 \pmod 6$. Našli jsme další prvočíslo tvaru $6k - 1$. □

46. Předpokládejme, že existuje řešení dané kongruence pro nějaké $p \equiv 3 \pmod 4$. Pak $r = \frac{p-1}{2}$ je liché.

Nechť $a^2 \equiv -1 \pmod p$ pro nějaké $a \in \mathbb{N}$. Pak $(a^2)^r \equiv (-1)^r \equiv -1 \pmod p$, ale dle Malé Fermatovy věty $(a^2)^r = a^{2r} = a^{p-1} \equiv 1 \pmod p$. To implikuje, že $1 \equiv -1 \pmod p$, což je spor s tím, že p je liché prvočíslo. □

47. a) Hledáme řešení kongruence $x^2 \equiv 1 \pmod 2$.
Pokud $x \equiv 0 \pmod 2$, pak $x^2 \equiv 0 \pmod 2$.
Pokud $x \equiv 1 \pmod 2$, pak $x^2 \equiv 1 \pmod 2$.
Jediným řešením je $x \equiv 1 \pmod 2$. □

b) Hledáme řešení kongruence $x^2 \equiv 1 \pmod 4$.
Pokud $x \equiv 0 \pmod 4$ nebo $x \equiv 2 \pmod 4$, pak $x^2 \equiv 0 \pmod 4$.
Pokud $x \equiv 1 \pmod 4$ nebo $x \equiv 3 \pmod 4$, pak $x^2 \equiv 1 \pmod 4$.
Kongruence má dvě řešení: $x \equiv 1 \pmod 4$ a $x \equiv 3 \pmod 4$. □

c) Analogicky jako v předešlých případech nalezneme 4 řešení:
$x \equiv 1 \pmod 8$, $x \equiv 3 \pmod 8$, $x \equiv 5 \pmod 8$ a $x \equiv 7 \pmod 8$. □

48. Tvrzení vlastně říká, že libovolné $n \in \mathbb{N}_0$ je kongruentní modulo 9 s jedním z čísel $0, 2, 4, 6, 8, 10, 12, 14, 16$, nebo, modulo 9: $0, 2, 4, 6, 8, 1, 3, 5, 7$. To je ale zřejmé, neboť se jedná o všechny možné zbytky po dělení 9.

    Uvažujeme $n \in \{0, 1, \ldots, 8\}$. Řešením kongruence $2k \equiv n \pmod 9$ je $k \equiv 5n \pmod 9$. Odpovídající hledaná k jsou proto $0, 5, 1, 6, 2, 7, 3, 8, 4$. □

2.7.3 Grupy

49. Postupně ověříme všechny vlastnosti, které musí splňovat grupa.

    - Uzavřenost množiny $\{a, b, c, d\}$ na operaci $\circ$: zřejmě platí.
    - Operace $\circ$ je dokonce komutativní (matice, která jí zadává je symetrická), což sníží počet kombinací, které je nutno otestovat při ověřování asociativity.
    - Asociativita operace $\circ$: platí.
    - Existence neutrálního prvku: $e = a$.
    - Existence inverzního prvku: $a^{-1} = a$, $b^{-1} = d$, $c^{-1} = c$, $d^{-1} = d$.

    Závěr: $(\{a, b, c, d\}, \circ)$ tvoří komutativní grupu.

50. Ne, neexistuje neutrální prvek.

51. $(S, \circ)$ tvoří komutativní grupu:

    - Uzavřenost množiny S na operaci $\circ$:
      Chceme ukázat, že $a, b \neq -1 \implies a + b + ab \neq -1$:

      $$\begin{aligned} a + b + ab &\neq -1 \\ a(1+b) &\neq -1 - b \\ a(1+b) &\neq -(1+b), (1+b) \neq 0 \\ a &\neq -1. \end{aligned} \qquad \begin{aligned} a + b + ab &\neq -1 \\ b(1+a) &\neq -1 - a \\ b(1+a) &\neq -(1+a), (1+a) \neq 0 \\ b &\neq -1. \end{aligned}$$

    - Komutativita operace $\circ$:

      $$\begin{aligned} a \circ b &= b \circ a \\ a + b + ab &= b + a + ba. \end{aligned}$$

    - Asociativita operace $\circ$:

      $$\begin{aligned} (a \circ b) \circ c &= a \circ (b \circ c) \\ (a + b + ab) \circ c &= a \circ (b + c + bc) \\ a + b + ab + c + (a + b + ab)c &= a + b + c + bc + a(b + c + bc) \\ a + b + ab + c + ac + bc + abc &= a + b + c + bc + ab + ac + abc. \end{aligned}$$

– Existence neutrálního prvku:

$$\begin{aligned} a \circ e &= a \\ a + e + ae &= a \\ e(1+a) &= 0 \\ (1+a) \neq 0 \implies e &= 0. \end{aligned}$$

– Existence inverzního prvku:

$$\begin{aligned} a \circ a^{-1} &= e \\ a + a^{-1} + aa^{-1} &= 0 \\ a^{-1}(1+a) &= -a \\ (1+a) \neq 0 \implies a^{-1} &= \frac{-a}{1+a}. \end{aligned}$$

□

52. Pro $n = 1$ je komutativní grupa D_2, kterou si lze představit jako úsečku s dvěma operacemi: identita a zrcadlení. Skládání těchto operací je zřejmě komutativní. □

53. $(aba^{-1})^n = \underbrace{(ab\boldsymbol{a^{-1}})(\boldsymbol{a}ab\boldsymbol{a^{-1}})\dots(\boldsymbol{a}ba^{-1})}_{n\text{-krát}} = ab^n a^{-1}$. □

54. $(\mathbb{R}, +)$: Ne, protože např. $\sqrt{2} + (-\sqrt{2}) = 0 \notin \mathbb{I}$.
$(\mathbb{R}^*, \cdot)$: Ne, protože např. $\sqrt{2} \cdot \sqrt{2} = 2 \notin \mathbb{I}$.

Cyklické grupy

55. a) $1, 3, 5, 7, 9, 11, 13, 15$.
    b) $1, 2, \dots, 16$.
    c) Všechny prvky $[a]_n$ takové, že $1 \leq a < n$ a $(a, n) = 1$.

56. Tvrzení je nepravdivé: 1 je generátorem každé grupy $(\mathbb{Z}_n, +)$. Také generátor 49 není prvočíselný. Zbylé generátory $7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59$ ale prvočíselné jsou. □

57. a) $\{15, 6, 21, 12, 3, 18, 9, 0\} = 3\mathbb{Z}$ (protože $(24, 15) = 3$).
    b) Stačí zvážit všechny dělitele 12: 1, 2, 3, 4, 6, 12. Dostáváme 6 podgrup: $\{0\}$ (triviální), $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, $\{0, 2, 4, 6, 8, 10\}$, $\mathbb{Z}_{12}$ (původní grupa).
    c) $\{0, 4, 8, 12, 16, 20, 24, 28\}$.
    d) Žádná neexistuje (protože $6 \nmid 40$).
    e) 1) Triviální podgrupa $\{(0, 0)\}$,
       2) $\{(0, 0), (2, 0)\}$,

3) $\{(0,0),(0,1)\}$,
4) $\{(0,0),(2,1)\}$,
5) $\{(0,0),(0,1),(2,0),(2,1)\}$,
6) $\{(0,0),(1,0),(2,0),(3,0)\}$,
7) $\{(0,0),(1,1),(2,0),(3,1)\}$,
8) Celá grupa $\mathbb{Z}_4 \times \mathbb{Z}_2$.

58. a) Řád grupy: 16. Možné řády prvků: $1, 2, 4, 8, 16$.
Řád prvku $[5]$ je 16, protože $5 \cdot 16 \equiv 0 \pmod{16}$ a čísla menší než 16 nevyhovují.

b) Řád grupy: $\varphi(16) = 8$. Možné řády prvků: $1, 2, 4, 8$.
Řád prvku $[5]$ je 4, protože $5^4 \equiv 1 \pmod{16}$ a čísla menší než 4 nevyhovují.

c) Řád prvku $[\sqrt{3}]$ je ∞, protože rovnice $x \cdot \sqrt{3} = 0$ má řešení jen pro $x = 0$, ale řád prvku je definovaný jako kladné číslo nebo nekonečno.

d) Řád prvku $[\sqrt{3}]$ je ∞, protože rovnice $\sqrt{3}^x = 1$ má řešení jen pro $x = 0$.

e) Řád prvku $[-i]$ je 4, protože $(-i)^4 = 1$.

f) Řád prvku $[3]$ v $\mathbb{Z}_4$ je 4. Řád prvku $[4]$ v $\mathbb{Z}_6$ je 3.
Řád prvku $[(3,4)]$ v $\mathbb{Z}_4 \times \mathbb{Z}_6$ je $[4,3] = 12$.

g) $(7,14) = 2 \implies$ řád prvku $[7]$ v $\mathbb{Z}_{14}$ je $\frac{14}{2} = 7$.
$(63,70) = 7 \implies$ řád prvku $[63]$ v $\mathbb{Z}_{70}$ je $\frac{70}{7} = 10$.
Řád prvku $[(7,63)]$ v $\mathbb{Z}_{14} \times \mathbb{Z}_{70}$ je $[7,10] = 70$.

h) $(10,20) = 10 \implies$ řád prvku $[10]$ v $\mathbb{Z}_{20}$ je $\frac{20}{10} = 2$.
$(11,30) = 1 \implies$ řád prvku $[11]$ v $\mathbb{Z}_{30}$ je $\frac{30}{1} = 30$.
$(12,40) = 4 \implies$ řád prvku $[12]$ v $\mathbb{Z}_{40}$ je $\frac{40}{4} = 10$.
Řád prvku $[(10,11,12)]$ v $\mathbb{Z}_{20} \times \mathbb{Z}_{30} \times \mathbb{Z}_{40}$ je $[2,30,10] = 30$.

i) Řád prvku $[4]$ v $\mathbb{Z}_{16}$ je 4. Řád prvku $[8]$ v $\mathbb{Z}_{16}$ je 2. Řád prvku $[12]$ v $\mathbb{Z}_{16}$ je 4.
Řád prvku $[(4,8,12)]$ v $\mathbb{Z}_{16} \times \mathbb{Z}_{16} \times \mathbb{Z}_{16}$ je $[4,2,4] = 4$.

j) Řád prvku $[6]$ v $\mathbb{Z}_{30}$ je 5. Řád prvku $[6]$ v $\mathbb{Z}_{24}$ je 4. Řád prvku $[6]$ v $\mathbb{Z}_{60}$ je 10.
Řád prvku $[(6,6,6)]$ v $\mathbb{Z}_{30} \times \mathbb{Z}_{24} \times \mathbb{Z}_{60}$ je $[5,4,10] = 20$.

59. a)
- Prvky řádu 1: $[0]$.
- Prvky řádu 2: $[9]$.
- Prvky řádu 3: $[6]$, $[12]$.
- Prvky řádu 6: $[3]$, $[15]$.
- Prvky řádu 9: $[2]$, $[4]$, $[8]$, $[10]$, $[14]$, $[16]$.
- Prvky řádu 18: $[1]$, $[5]$, $[7]$, $[11]$, $[13]$, $[17]$.

b)

prvek	[1]	[5]	[7]	[11]	[13]	[17]
řád	1	6	3	6	3	2
inverze	1	11	13	5	7	17

60. a) Prvek $[0]$ řádu 1.
    b) Prvek $[1]$ řádu 1 a prvek -1 řádu 2.
    c) Prvek $[1]$ řádu 1 a prvek -1 řádu 2.

61. Číslo 24 jako řád prvku dělí řád grupy G, tedy řád grupy je ve tvaru $24k$, kde $k \in \mathbb{N}$. Možné řády dalších prvků jsou dělitele $24k$.

62. Aby řád obou prvků dělil řád grupy, musí mít grupa G řád nejméně $[5, 7] = 35$.

63. Podgrupy G mohou mít řády dělitelů 60, tedy 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.

64. Tvrzení je nepravdivé: např. grupa $(2\mathbb{Z}, +)$ má nekonečný řád. □

65. Označme k řád prvku a, tedy $|a| = |a^{-1}| = k$. Platí: $(a^k)^{-1} = a^{-k} = (a^{-1})^k$.

    1) $a^k = e \implies (a^k)^{-1} = e^{-1} = (a^{-1})^k = e$. Tedy $|a^{-1}| \leq |a|$.
    2) $(a^{-1})^k = e \implies ((a^{-1})^{-1})^k = e^{-1} = a^k = e$. Tedy $|a| \leq |a^{-1}|$. □

66. $(\mathbb{Z}_{2016}, +)$ a její podgrupa $672\mathbb{Z}_3 = \{0, 672, 1344\}$.

67. $\mathbb{S}_4$ a její podgrupa $\mathbb{S}_3$.

68. Každá grupa prvočíselného řádu je cyklická:

    Nechť p je prvočíslo a G je grupa, $|G| = p$. Nechť $g \in G$, přičemž $g \neq e_G$. Pak $\langle g \rangle$ obsahuje víc než jeden prvek, tedy $|\langle g \rangle| > 1$. Zároveň $|\langle g \rangle|$ dělí p. Proto $|\langle g \rangle| = p = |G|$, tedy $\langle g \rangle = G$ a tedy G je cyklická. □

    Každá cyklická grupa je také komutativní:

    Všechny prvky cyklické grupy G jsou tvaru a^n, kde $n \in \mathbb{Z}$.
    Nechť $x, y \in G : x = a^p, y = a^q$. Pak $xy = a^p a^q = a^{p+q} = a^{q+p} = a^q a^p = yx$. □

69. $(\mathbb{Z}_2 \times \mathbb{Z}_6, +)$.

70. a) Např. $(0, +)$ nebo $\mathbb{Z}_3^\times$ (generátor 2).
    b) Např. $\mathbb{Z}_5^\times$ (generátory $2, 3$) nebo $\mathbb{Z}_7^\times$ (generátory $3, 5$).
    c) Grupa $\mathbb{Z}_p^\times$ má $\varphi(p-1)$ různých generátorů. Rovnice $\varphi(p-1) = 10$ má řešení pro $p - 1 = 11$ a $p - 1 = 22$. Hledanou grupou je tedy např. $\mathbb{Z}_{23}^\times$.

71. $(\mathbb{Z}_p, +)$ má $p - 1$ generátorů, $(\mathbb{Z}_q, +)$ má $q - 1$ generátorů.

    Generátory $(\mathbb{Z}_{pq}, +)$ jsou taková $n \in \mathbb{N}$, že $1 \leq n < pq$ a zároveň $(n, pq) = 1$.

    $\mathbb{Z}_{pq}$ má pq prvků, z kterých:

    – prvky p, $2p$, $3p$, …, $(q-1)p$ negenerují $\mathbb{Z}_{pq}$,
    – prvky q, $2q$, $3q$, …, $(p-1)q$ negenerují $\mathbb{Z}_{pq}$,

– prvek 0 negeneruje $\mathbb{Z}_{pq}$.

Zbylé prvky generují $\mathbb{Z}_{pq}$ a jejich počet je $pq-(q-1)-(p-1)-1=(p-1)(q-1)=\varphi(pq)$.

72. a) $49-35=14$, $35-14-14=7$, tedy $\langle 35,49\rangle_{\mathbb{Z}}=7\mathbb{Z}$.
    b) $19-16=3$, $37-12\cdot 3=1$, tedy $\langle 16,19,37\rangle_{\mathbb{Z}}=\mathbb{Z}$.
    c) $GL_2(\mathbb{Z}_2)=\{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)\}$.

Grupy permutací

73. a) $(1,2,4,5,3)$.
    b) $(1,4)\circ(3,5)$.
    c) $(1,5,4,7,2)$.
    d) $(1,7,4,2,5)\circ(3,6)$.
    e) $(2,4)\circ(3,5)$.
    f) $(1,2,4)$.
    g) $(4,2)\circ(5,3)$.

74. $(1,5)\circ(5,6)\circ(6,2)\circ(4,3)\circ(3,7)\circ(7,8)$. Permutace je sudá.

75. $\pi=(1,3,2)^{-1}\circ(2,4)\circ(1,5)\circ(3,5,2)^{-1}\circ(1,4)^{-1}=(1,3,4,5)$.

76. Prvky grupy $(\mathbb{S}_4,\circ)$:
    – Řád 1: id.
    – Řád 2: $(1,2)$, $(1,3)$, $(1,4)$, $(2,3)$, $(2,4)$, $(3,4)$.
    – Řád 3: $(1,2,3)$, $(1,2,4)$, $(1,3,2)$, $(1,3,4)$, $(1,4,2)$, $(1,4,3)$, $(2,3,4)$, $(2,4,3)$.
    – Řád 4: $(1,2,3,4)$, $(1,2,4,3)$, $(1,3,2,4)$, $(1,3,4,2)$, $(1,4,2,3)$, $(1,4,3,2)$, $(1,2)\circ(3,4)$, $(1,3)\circ(2,4)$, $(1,4)\circ(2,3)$.

    a) $\{(1,3),(1,3)\circ(2,4),(1,3,2),(1,3,4),(1,3,2,4),(1,3,4,2)\}$.
    Není to podgrupa: chybí např. prvek $(1,3)\circ(1,3)=id$.
    b) $\{id,(1,2),(1,3),(2,3),(1,2,3),(1,3,2)\}$.
    Je to podgrupa.
    c) $\{(1,3),(1,3,2)\}$.
    Není to podgrupa: chybí např. prvek $(1,3)\circ(1,3)=id$.

77. a) $1, 2, 3, 4, 5, 6, 7, 10, 12$.
    b) $1, 2, 3, 4, 5, 6, 7$.

78. a) $(1,2,3,4,5)\circ(6,7,8)$.
    b) Neexistuje, protože $16=4\cdot 4=2\cdot 2\cdot 4=2\cdot 2\cdot 2\cdot 2$, cykly s takovými délkami mají ale řády $4,4$, resp. 2.

c) Neexistuje, protože prvek řádu 10 získáme jenom jako součin cyklů permutací délky 2 a 5, což je ale součin liché a sudé permutace, tedy lichá permutace, která není prvkem $\mathbb{A}_7$.

d) Neexistuje, protože $26 = 2 \cdot 13$, tedy potřebujeme součin liché a sudé permutace, což je lichá permutace.

e) $(1, 2, 3) \circ (4, 5) \circ (6, 7)$.

79.

n	1	2	3	4	5	6	7	8	9	10
Nejvyšší řád prvku	1	2	3	4	6	8	12	15	20	21

80. Nechť $\pi = (a_1, a_2, \ldots, a_n)$. Pak $\pi^{-1} = (a_1, a_2, \ldots, a_n)^{-1} = (a_1, a_n, \ldots, a_2)$. Obě permutace se dají rozložit na stejný počet transpozic, proto se parita permutace u její inverze nemění. $\square$

Homomorfismy grup

81. a) $f(a+b) = f(a) + f(b)$
$11(a+b) = 11a + 11b.$
Injektivní homomorfismus:
$\mathrm{Ker} f = \{0\}$, $\mathrm{Im} f = 11\mathbb{Z}$.

b) $f(a+b) \neq f(a) + f(b)$
$a + b + 5 \neq a + 5 + b + 5$
$a + b + 5 \neq a + b + 10.$
Nejde o homomorfismus.

c) $f(a+b) \neq f(a) + f(b)$
$(a+b)^3 \neq a^3 + b^3$
$3a^2b + 3ab^2 \neq 0.$
Nejde o homomorfismus.

d) $f(a+b) \neq f(a) + f(b)$
$1 \neq 1 + 1.$
Nejde o homomorfismus.

e) $f(a+b) = f(a) + f(b)$
$0 = 0 + 0.$
Injektivní homomorfismus:
$\mathrm{Ker} f = \{0\}$, $\mathrm{Im} f = \{0\}$.

f) $f(a \cdot b) = f(a) \cdot f(b)$
$\left(\begin{smallmatrix} 1 & 0 \\ 0 & ab \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right).$
Izomorfismus: $\mathrm{Ker} f = f^{-1}(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = \{1\}$,
$\mathrm{Im} f = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right) \mid a \in \mathbb{R}^*\}$.

g) $f(a+b) = f(a) \cdot f(b)$
$\left(\begin{smallmatrix} 1 & 0 \\ 0 & a+b \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right).$
Izomorfismus: $\mathrm{Ker} f = f^{-1}(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = \{0\}$,
$\mathrm{Im} f = \{\left(\begin{smallmatrix} 1 & 0 \\ a+b & 1 \end{smallmatrix}\right) \mid a, b \in \mathbb{R}\}$.

h) $f(a \cdot b) \neq f(a) + f(b)$
$f(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)) \neq f(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) + f(\left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right))$
$f(\left(\begin{smallmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{smallmatrix}\right) \neq a + d + e + h$
$ae + bg + cf + dh \neq a + d + e + h.$
Nejde o homomorfismus.

82. $[1]_5 \mapsto [0]_4$, $[2]_5 \mapsto [1]_4$, $[3]_5 \mapsto [3]_4$, $[4]_5 \mapsto [2]_4$.

83. $(\mathbb{Z}_8^\times, \cdot) \cong (\mathbb{Z}_{12}^\times, \cdot)$: $[1]_8 \mapsto [1]_{12}$, $[3]_8 \mapsto [5]_{12}$, $[5]_8 \mapsto [7]_{12}$, $[7]_8 \mapsto [11]_{12}$.
$(\mathbb{Z}_8, +) \ncong (\mathbb{Z}_{12}, +)$: $|\mathbb{Z}_8| = 8 \neq |\mathbb{Z}_{12}| = 12$.

84. Všimněme si inverzí prvků:

$$\begin{aligned}\mathbb{Z}_5^\times &: 1^{-1} = 1, 2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 4.\\ \mathbb{Z}_{10}^\times &: 1^{-1} = 1, 3^{-1} = 7, 7^{-1} = 9, 9^{-1} = 9.\\ \mathbb{Z}_{12}^\times &: 1^{-1} = 1, 5^{-1} = 5, 7^{-1} = 7, 11^{-1} = 11.\end{aligned}$$

Proto $(\mathbb{Z}_5^\times, \cdot) \cong (\mathbb{Z}_{10}^\times, \cdot)$: $[1]_5 \mapsto [1]_{10}$, $[2]_5 \mapsto [3]_{10}$, $[3]_5 \mapsto [7]_{10}$, $[4]_5 \mapsto [9]_{10}$.

85. $\forall a \in \mathbb{Z}: x \mapsto ax$.

86. $\forall a \in \{0, 1, \ldots, n-1\}: x \mapsto ax \pmod n$.

87. $x \mapsto 0$.

88. Pokud $f(g \circ h) = f(g) \circ f(h)$, pak $(g \circ h)^n = g^n \circ h^n$.
Báze pro $n = 1$: $(g \circ h)^1 = g^1 \circ h^1$.
Indukční předpoklad: $\forall k \geq 1: (g \circ h)^k = g^k \circ h^k$.
Indukční krok:

$$\begin{aligned}(g \circ h)^{k+1} &= g^{k+1} \circ h^{k+1}\\ (g \circ h)^k \circ (g \circ h) &= g^k \circ g \circ h^k \circ h.\end{aligned}$$

Jen v komutativních grupách: $(g \circ h)^k \circ g \circ h = g^k \circ h^k \circ g \circ h$. □
U nekomutativních grup tvrzení neplatí, např v $\mathbb{S}_4$:

$$\begin{aligned}((1,2,3) \circ (2,3,4))^2 \circ (1,2,3) \circ (2,3,4) &\neq (1,2,3)^2 \circ (2,3,4)^2 \circ g(1,2,3) \circ (2,3,4)\\ ((2,1) \circ (3,4))^2 \circ (2,1) \circ (3,4) &\neq (1,3,2) \circ (2,4,3) \circ (1,2,3) \circ (2,3,4)\\ id \circ (2,1) \circ (3,4) &\neq (2,3) \circ (4,1).\end{aligned}$$

89. $360 = 2^3 \cdot 3^2 \cdot 5$. Dle [1, s. 651] máme 6 možností:

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$,
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$,
- $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$,
- $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$,
- $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$,
- $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$.

90. $a + bi \mapsto (a, b)$. Ukážeme, že jde o homomorfismus, který je injektivní a surjektivní.

$$\begin{aligned}f((a+bi) + (c+di)) &= f(a+bi) + f(c+di)\\ f((a+c) + (b+d)i) &= (a,b) + (c,d)\\ (a+c, b+d) &= (a+c, b+d).\end{aligned}$$

Jde o homomorfismus.
$\mathrm{Ker} f = f^{-1}((0,0)) = \{0\}$. Homomorfismus je injektivní.
$\mathrm{Im} f = \mathbb{R} \times \mathbb{R}$. Homomorfismus je surjektivní.

2.7.4 Okruhy

91. Nejedná se o okruh, operace $\oplus$ totiž není komutativní, např. $b \oplus c = c$, ale $c \oplus b = d$.

92. $(\mathbb{Z}_{12}, +, \cdot)$ je komutativní okruh. Platí, že $(\mathbb{Z}_{12}, +)$ je komutativní grupa a operace $\cdot$ modulo n je asociativní, komutativní, distributivní a existuje jednička: 1.

    Nejedná se ale o obor integrity: např. $3 \cdot 4 \equiv 0 \pmod{12}$.

93. $(\mathbb{Q}(\sqrt{2}), +)$ je komutativní grupa:

    - Uzavřenost: $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, protože $a, b, c, d \in \mathbb{Q} \implies (a + c), (b + d) \in \mathbb{Q}$.
    - Asociativita a komutativita sčítání je zřejmá.
    - Neutrálním prvkem je 0.
    - $(a + b\sqrt{2})^{-1} = -a - b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

    $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ je komutativní okruh:

    - Uzavřenost: $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, protože $a, b, c, d \in \mathbb{Q} \implies (ac + 2bd), (ad + bc) \in \mathbb{Q}$.
    - Asociativita a komutativita násobení je zřejmá.
    - Jedničkou je 1.

    Zbývá tedy už jen dokázat, že každý nenulový prvek má inverzi:

    $$(a + b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

    protože $a, b, c, d \in \mathbb{Q} \implies (a^2 - 2b^2 \neq 0) \wedge \frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q}$. Jedná se o těleso. $\square$

94. Platí, že $(R, +)$ je komutativní grupa: množina R je uzavřená na sčítání, sčítání matic je komutativní a asociativní, neutrálním prvkem je nulová matice a každý prvek je sám sobě inverzí. Dále platí, že $(R, +, \cdot)$ je okruh. Operace násobení matic je asociativní, distributivní a jedničkou je jednotková matice.

    Pokud označíme prvky množiny R postupně A, B, C, D, pak D je nulový prvek a pro zbylé prvky platí: $A^{-1} = A$, $B^{-1} = C$, $C^{-1} = B$. Jedná se tedy o těleso. $\square$

95. a) $\{1, 3, 7, 9\} = \mathbb{Z}_{10}^{\times}$.
    b) $\{1, 2, 3, 4, 5, 6\} = \mathbb{Z}_7^{\times}$.
    c) $\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in \mathbb{Z} \wedge ad - bc \neq 0\} = GL_2(\mathbb{Z})$.
    d) $\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)\} = SL_2(\mathbb{Z}_2)$.

96. $(2x^2 + 1)^2 = 4x^4 + 4x^2 + 1 \equiv 1 \pmod{4}$.

97. Vezmeme nenulový polynom z tohoto okruhu, který není jednotkou a ukážeme jeho alespoň dva možné rozklady na různé ireducibilní faktory. Např. $x^2+3x+2 = (x+2)(x+1) = (x+5)(x+4)$. □

2.7.5 Polynomy

98. a) Použijeme Eisensteinovo kritérium pro $p = 3$. □

    b) Kubický polynom je ireducibilní, pokud nemá kořen. Možné kořeny musí dělit absolutní člen, tedy v úvahu přichází čísla ± 1, ± 2. Prostým vyzkoušením ale zjistíme, že žádné z těchto čísel není kořenem daného polynomu. □

    c) Použijeme Eisensteinovo kritérium pro $p = 2$. □

    d) Polynom není možné rozložit na součin polynomů stupně 1 a 3, protože ani jedno z čísel ± 1 není kořenem polynomu. Zbývá tedy ukázat, že polynom není možné rozložit na součin dvou kvadratických polynomů. Předpokládejme ale, že to je možné. Pak

$$\begin{aligned} x^4 - 2x^3 + x + 1 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + cx^3 + dx^2 + ax^3 + acx^2 + adx + bx^2 + bcx + bd \\ &= x^4 + (a+c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd. \end{aligned}$$

    Z toho $a + c = -2$, $ac + b + d = 0$, $ad + bc = 1$, $bd = 1$, tato soustava rovnic ale nemá v $\mathbb{Q}$ řešení. □

    e) Polynom nemá kořen (stačí vyzkoušet čísla 0 a 1) a není jej možné ani rozložit na součin dvou kvadratických polynomů, protože soustava rovnic $a + c = 1$, $ac + b + d = 1$, $ad + bc = 1$, $bd = 1$ nemá v $\mathbb{Z}_2$ řešení. □

99. a) $(x+1)(x^4 + x^3 + x^2 + x + 1)$.

    b) $(x+1)(x^2 + x + 1)(x^6 + x^3 + 1)$.

    c) $(x^3 + x^2 + 1)(x^3 + x + 1)$.

100. a) $(x+2)(x^2 + x + 1)(x^2 + 2x + 4)$.

     b) $(x+2)(x+3)(2x+1)(x^2+3)$.

101. $x^2 + x + 8 = (x+2)(x+9) = (x+7)(x+4)$.

102. $x + 1$.

103. $x^3 + x^2 + x + 1$.

104. Např. v $\mathbb{Z}_4[x]$ vezměme $p = q = 2x + 1 = 1 \cdot (2x+1) + 0 = 2x \cdot (2x+1) + 1$.

105. Např. polynom $2x$ má stupeň 1 a dva kořeny 0, 2.

106. Takový polynom neexistuje, $\mathbb{Z}_5[x]$ je totiž obor integrity [1, s. 662].

107. Nechť $p = 2, a = 1$. Pak x^2+1 je reducibilní nad $\mathbb{Z}_2[x]$, protože $x^2+1 = (x+1)(x+1)$. Tvrzení je tedy nepravdivé. □

108. $x^p - x = x(x^{p-1} - 1) = 0$ právě tehdy, když $x \equiv 0 \pmod p$ nebo $x^{p-1} \equiv 1 \pmod p$. Toto platí pro všechna $x \in \mathbb{Z}_p$ (jedná se totiž o Malou Fermatovu větu). Kořenem je tedy každý prvek z množiny $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ a počet kořenů je p. □

109. Nechť $(x - a) \in F[x]$, kde $(x - a) \neq 0$. Pak existují polynomy $q(x), r(x) \in F[x]$ takové, že $p(x) = q(x) \cdot (x - a) + r(x)$. Protože $\deg(r) < \deg(x - a) = 1$, $r(x)$ je konstantní. Za x dosadíme a: $p(a) = q(a) \cdot (a - a) + r$, tedy $p(a) = r$. □

110.
$$\begin{aligned}
\Phi_p(x+1) &= \frac{(x+1)^p - 1}{x+1-1} \\
&= \frac{\left(\sum_{k=0}^{p} \binom{p}{k} x^{p-k}\right) - 1}{x} \\
&= \frac{\binom{p}{0}x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \ldots + \binom{p}{p-2}x^2 + \binom{p}{p-1}x + \binom{p}{p} - 1}{x} \\
&= x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \ldots + \binom{p}{p-2}x + p.
\end{aligned}$$

Tento polynom splňuje Eisensteinovo kritérium pro p. □

2.7.6 Kódování a šifrování

111. Protože délka vstupní zprávy je $k = 5$ a stupeň generujícího polynomu je $n-k = 3$, jedná se o $(8, 5)$-kód. Zprávu reprezentujeme jako $m(x) = 1 + x + x^3$ a kódové slovo $v(x)$ získáme jako $r(x) + x^{n-k}m(x)$, kde:

$$\begin{aligned}
x^{n-k}m(x) &= x^3(1 + x + x^3) = x^3 + x^4 + x^6 \\
r(x) = x^{n-k}m(x) \bmod p(x) &= (x^3 + x^4 + x^6) \bmod (x + x^3) = -x \equiv x \pmod 2 \\
v(x) = r(x) + x^{n-k}m(x) &= x + x^3 + x^4 + x^6
\end{aligned}$$

Výsledná zpráva má délku $n = 8$ a je tvaru 01011010.

112.
$$G = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}^T, \qquad H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

113. Délka zpráv, které budeme kódovat je $k = 3$. Můžeme tedy zakódovat celkem $2^3 = 8$ různých zpráv. Budeme je reprezentovat jako sloupcové vektory, které označíme m_i a které budou obsahovat číslo i zapsané v binární soustavě, přičemž nejméně významný bit bude na prvním místě (*Little endian*). Tedy

$$m_0 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \quad m_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad m_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad m_3 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix},$$

$$m_4 = \begin{pmatrix}0\\0\\1\end{pmatrix}, \quad m_5 = \begin{pmatrix}1\\0\\1\end{pmatrix}, \quad m_6 = \begin{pmatrix}0\\1\\1\end{pmatrix}, \quad m_7 = \begin{pmatrix}1\\1\\1\end{pmatrix}.$$

Kódové slovo délky $n = 6$ pak získáme jako $w_i = G \cdot m_i$:

$$\begin{aligned}
w_0 &= \begin{pmatrix}0 & 0 & 0 & 0 & 0 & 0\end{pmatrix}^T, & w_4 &= \begin{pmatrix}1 & 0 & 1 & 0 & 0 & 1\end{pmatrix}^T,\\
w_1 &= \begin{pmatrix}1 & 1 & 1 & 1 & 0 & 0\end{pmatrix}^T, & w_5 &= \begin{pmatrix}0 & 1 & 0 & 1 & 0 & 1\end{pmatrix}^T,\\
w_2 &= \begin{pmatrix}1 & 0 & 0 & 0 & 1 & 0\end{pmatrix}^T, & w_6 &= \begin{pmatrix}0 & 0 & 1 & 0 & 1 & 1\end{pmatrix}^T,\\
w_3 &= \begin{pmatrix}0 & 1 & 1 & 1 & 1 & 0\end{pmatrix}^T, & w_7 &= \begin{pmatrix}1 & 1 & 0 & 1 & 1 & 1\end{pmatrix}^T.
\end{aligned}$$

114. 1) Alice si zvolí $a = 8$, spočte $7^8 \pmod{61} = 57$ a výsledek sdělí Bobovi.
   2) Bob si zvolí $b = 12$, spočte $7^{12} \pmod{61} = 34$ a výsledek sdělí Alici.
   3) Sdílené tajemství je $34^8 \pmod{61} = 57^{12} \pmod{61} = 20$.

115. 1) $n = pq = 667$,
   2) $\varphi(n) = (p-1)(q-1) = 616$,
   3) $e = 487$, $(\varphi(n), e) = 1$,
   4) $c = m^e \pmod{n} = 25^{487} \pmod{667} = 169$,
   5) $ed = 1 \pmod{\varphi(n)} \implies d = 191$,
   6) $m = c^d \pmod{n} = 169^{191} \pmod{667} = 25$.

116. $m = c^d \pmod{n} = 34^{81} \pmod{5893} = 2014$.

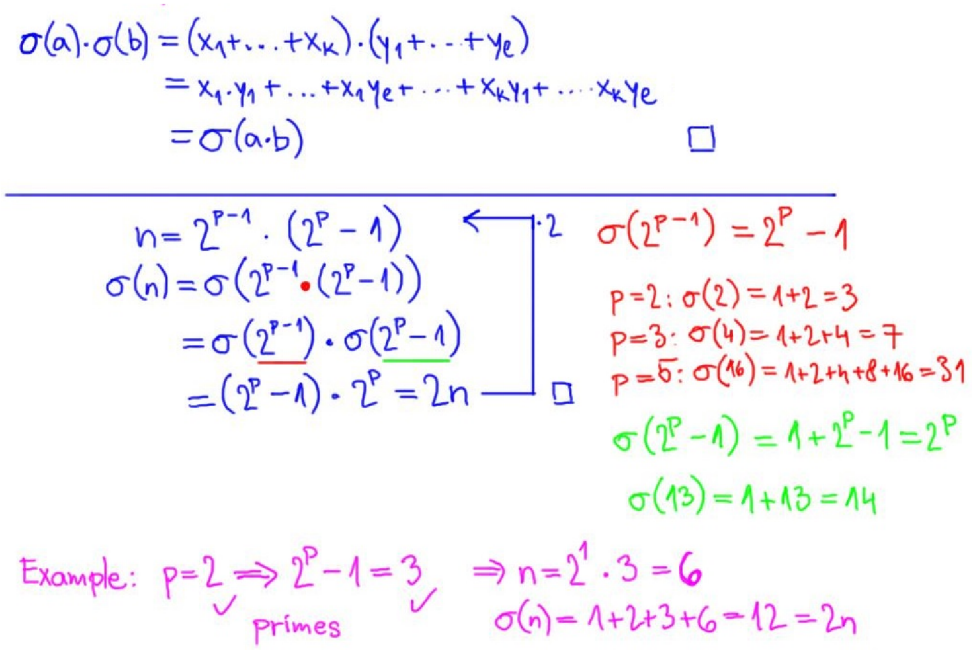
117. a) Podpisem je $s = m^d \pmod{n}$. V našem případě: $8^{103} \pmod{143} \equiv 83$.
   b) Musí platit: $s^e \equiv m \pmod{n}$, tedy $83^7 \equiv 8 \pmod{143}$. Podpis je platný.
   c) $42^7 \equiv 81 \not\equiv 26 \pmod{143}$, dané s tedy není podpisem zprávy m.

118. Z Eulerovy věty: $x^{\varphi(n)} \equiv 1 \pmod{n} \implies x^{\varphi(n)+1} \equiv x \pmod{n}$. Hledaná čísla jsou $n, x \in \mathbb{N}$: $(n, x) = 1$ a $e = \varphi(n) + 1$. Tato čísla ale nejsou vhodná jako parametry RSA, protože při šifrování pak nastane situace, že $c = m^e = m^{\varphi(n)+1} \equiv m \pmod{n}$.

2.8 Výuková videa

Ze sbírky příkladů jsem zvolil 10 příkladů, jejichž řešení jsem nahrál na video. Jde o příklady 3d), 3e), 14, 20, 23, 28, 46, 71, 98 a 110. Jedná se o příklady důkazového typu, jejichž řešení může být jednodušší sledovat krok za krokem právě ve videu.

Na základě návrhu vedoucího práce jsem videa nahrával v anglickém jazyce. Postupoval jsem podle vzoru výukové webové stránky Khan Academy [10]. Pro psaní jsem využil grafický tablet Wacom Intuos 5, jako tabule sloužil program Autodesk SketchBook Express 2011 [11] a pro následnou úpravu a střih videa program Camtasia Studio 7 [12]. Výsledná videa ve formátu MP4 a tabule na psaní ve formátu PNG ke každému příkladu jsou dostupná na přiloženém CD.



Obrázek 2.1: Část tabule z videa k řešení příkladu 20.

Kapitola 3

Matematický systém Sage

3.1 Úvod do Sage

Sage [6] je volně dostupný počítačový systém pro matematické výpočty. Skládá se z několika desítek programových balíčků s otevřeným zdrojovým kódem sdružených do jednoho rozhraní založeného na jazyce Python. Cílem projektu Sage[1] je poskytnout bezplatnou alternativu k matematickým systémům jako je Magma, Maple, Mathematica a Matlab [13]. Sage je možné použít pro aritmetické výpočty, úpravy výrazů, řešení rovnic a nerovnic a jejich soustav, algebru, geometrii, kalkul, grafy, maticové výpočty, vykreslování interaktivní 2D a 3D grafiky a mnoho jiného. K méně tradičním aplikacím patří i vestavěné funkce pro řešení sudoku nebo Rubikovy kostky.

Instalace Sage je přímočará na Linuxových distribucích a na Mac OS X. Nativní verze pro operační systém Windows zatím neexistuje, jeho uživatelé proto k instalaci musí využít virtualizaci. Autory doporučený je program VirtualBox[2]. K dispozici je ale i řada online řešení, z nichž nejrozšířenější je Sage Notebook[3]. V roce 2013 byl spuštěn také Sage Cloud[4]. Nejrychlejším způsobem pro vyzkoušení možností systému je Sage Cell[5] – jediná buňka, ve které je možné vyhodnotit jednoduchý příkaz. Studenti a zaměstnanci MU mohou využít také Sage Notebook Server na webu Přírodovědecké fakulty[6].

Pro účely této práce využívám online Sage Notebook, jelikož nevyžaduje instalaci ani dlouhé nastavování. K práci stačí webový prohlížeč. V následující části textu uvedu pokyny pro práci se Sage, aby jej v rozsahu práce mohli využít i ti uživatelé, kteří se systémem nemají žádné předešlé zkušenosti. Předpokládám ale přinejmenším intuitivní znalost významu elementárních pojmů z oblasti programování (funkce, operátor a pod.), proto nebudu detailně opisovat každý aspekt. Čerpal jsem z oficiálních návodů od vývojového týmu Sage [6], [7], [8] (v angličtině). Užitečnými zdroji v češtině jsou návody doc. Mgr. Roberta Maříka, Ph.D., absolventa MU a docenta na Mendelově univerzitě v Brně [14] a také bakalářská práce Martina Haupta na Přírodovědecké fakultě MU [15], která popisuje práci se systémem krok za krokem.

---

1. Projekt začínal s názvem SAGE (akronym pro Software for Arithmetic Geometry Experimentation), jeho autor William Stein ale později začal používat jednoduše název Sage, který už nemá funkci akronymu [13].
2. https://www.virtualbox.org/wiki/VirtualBox
3. http://sagenb.org/
4. https://cloud.sagemath.com
5. https://sagecell.sagemath.org/
6. http://sage.math.muni.cz

Před začátkem práce je nutné vytvoření účtu na stránce http://sagenb.org/. Možné je i přihlášení bez registrace, např. pod OpenID nebo účtem Google. Po přihlášení do systému se zobrazí „zápisník“ (angl. *notebook*) uživatele, který sestává z jednotlivých „listů“ (angl. *worksheet*). Po vytvoření nového listu (volba *Create New Worksheet*) se zobrazí okno složené z buněk – jednotlivých políček, do kterých uživatel zadává příkazy k vyhodnocení. Doporučuji zapnout volbu *Typeset*, která způsobí, že se výsledky výpočtu zobrazí typograficky vysázené[7] (např. 2π namísto 2*pi).

3.2 Základní poznatky pro práci se systémem

V této sekci se nachází vysvětlení základních vlastností Sage spolu s příklady použití. Řádek začínající výrazem `sage:` označuje uživatelský vstup. Modrou barvou jsou zvýrazněna rezervovaná slova Sage. Pokud kód obsahuje tři tečky, tyto nejsou součástí příkazů, pouze demonstrují fakt, že kód je odřádkován nebo odsazen v rámci jedné buňky. Příklady uvedené v této a následující sekci jsou k dispozici v přiloženém souboru `01Zaklady.sws`.

- Do buněk je možné vkládat příkazy složené z
  - matematických konstant (např. `42, -29, 5.37, pi, e`),
  - operátorů `+, -, *, /, //, %, ^, ., =, ==, <=, >=, <, >, <>` s obvyklým významem[8] (`//` je určen pro celočíselné dělení, synonymem pro operátor `^` je `**`, operátor `.` slouží pro přístup k členům objektu, přiřazení do proměnné se provádí pomocí `=` a pro test na rovnost pak slouží `==`),
  - funkcí (např. `sqrt()` pro druhou odmocninu),
  - symbolu podtržítko, kterým je možné odkázat se na výsledek vyhodnocení předešlé buňky.

```
sage: 8/5 - 0.4
1.20000000000000
sage: 8 // 5
1
sage: a = 5
sage: a == 5
True
sage: not _
False
sage: sqrt(25)
5
```

- Výraz v buňce se vyhodnotí po kliknutí na tlačítko *Evaluate* nebo stiskem kombinace kláves Shift+Enter.

7. Sage Notebook využívá na zobrazování matematiky ve webovém prohlížeči systém MathJax (http://www.mathjax.org/) [16].
8. Operátory blíže popisuje Martin Haupt v kapitole 2 své práce [15].

- Stisk samotné klávesy Enter způsobí přechod na nový řádek. Tímto způsobem se odděluje více příkazů v jedné buňce, přičemž po vyhodnocení se vypíše výstup posledního příkazu. Druhým způsobem je zápis více příkazů na jednom řádku oddělených středníkem. Po vyhodnocení se pak vypíšou i částkové výsledky.

```
sage: a = 1
...   a + 1
...   b = 4
...   b + 3
...   a + b
5
sage: a = 1; a + 1; b = 4; b + 3; a + b
2
7
5
```

- Nápovědu k objektu (např. k funkci nebo proměnné) a ukázky jeho použití Sage zobrazí po vyhodnocení příkazu `objekt?`, např. `sqrt?`. Detailní nápovědu pak Sage zobrazí po vyhodnocení příkazu `objekt??`, např. `Integer??`.
- Nápověda pro dokončení aktuálně rozepsaného příkazu se zobrazí po stisku klávesy Tab v rámci buňky.
- Všechny uživatelské výpočty se ukládají na server. Pro stažení pracovního listu (ve formátu .sws) slouží volba *Save worksheet to file*. Pracovní list je možné nahrát z paměťového média na server pomocí volby *Upload*.
- Pro komentáře slouží symbol `#`.
- Umístění kurzoru nad buňku způsobí zobrazení modrého pruhu na šířku zápisníku. Následné kliknutí na tento pruh způsobí přidání nové buňky. Kliknutí se současným podržením klávesy Shift způsobí přidání bloku pro textovou anotaci. Její další úprava se provádí dvojím kliknutím na text. Pro smazání buňky slouží klávesa Backspace.

3.3 Práce s proměnnými a funkcemi

- Tzv. symbolické proměnné, které nemají hodnotu, ale vyskytují se ve výrazech nebo v zápisu funkcí jako je `sin(y)` je nutné definovat příkazem `y = var('y')`. Více proměnných najednou je možné definovat jednoduše `y,z = var('y,z')`. Jediná předdefinovaná symbolická proměnná je `x`. Alternativou k definici symbolických proměnných je vyhodnocení příkazu `automatic_names(True)`.

```
sage: y = pi/2
sage: 3 * sin(y)
3
sage: 5 * (y - pi/2 + 7)
35
```

```
sage: 5 * (x + 4)
5*x+20
sage: 5 * (z + 4)
Traceback (click to the left of this block for traceback)
...
NameError: name 'z' is not defined
sage: z = var('z')
sage: 5 * (z + 4)
5*z+20
```

- Syntax volání funkcí je `funkce(argument)`. Také je možné aplikovat funkci na objekt, t.j. `objekt.funkce()`. Seznam všech dostupných operací na objektu je možné zobrazit zápisem `objekt.` a následným stiskem klávesy Tab.

```
sage: y = pi/2
sage: sin(y)
1
sage: y.cos()
0
```

- Při násobení je nutné vždy zadávat znaménko `*`, tedy povolený zápis je jenom `4*(x+1)` a ne `4(x+1)`, který je běžný při psaní rukou. Toto chování je možné obejít vyhodnocením příkazu `implicit_multiplication(True)`.

- Na výstup slouží funkce `print()` pro výpis jednoduchého textu (tzv. *plain text*) a `show()` pro matematickou sazbu výstupu (výchozí chování při zapnuté volbě *Typeset*). Funkce `latex()` zase vypíše svůj argument jako formuli do LaTeXu, kterou je možné vysadit v matematickém módu. Sage tedy může být nápomocný i při tvorbě dokumentů.

```
sage: print(4*x^5 + factorial(x) + sqrt(pi/2))
4*x^5 + sqrt(1/2)*sqrt(pi) + factorial(x)
sage: show(4*x^5 + factorial(x) + sqrt(pi/2))
```

$$4\,x^5 + \sqrt{\tfrac{1}{2}}\sqrt{\pi} + x!$$

```
sage: latex(4*x^5 + factorial(x) + sqrt(pi/2))
4 \, x^{5} + \sqrt{\frac{1}{2}} \sqrt{\pi} + x!
```

- Syntax definice vlastních funkcí: `def jméno_funkce(seznam_parametrů): tělo funkce`, které musí obsahovat výraz `return hodnota`. V definici je možné použít základní konstrukty jazyka Python[9] (např. `if`, `else`, `for` a jiné). Při definici funkce na více řádků obvykle dojde k zanořování, kdy je nutné dodržovat povinné odsazení.

```
sage: def even(n): return n % 2 == 0
sage: even(8)
True
sage: def parity(n):
```

9. Pro práci se Sage není nutná znalost jazyka Python, nicméně může být výhodou právě v případech, jako je definice vlastních funkcí. Kvalitní návod (v angličtině) je k dispozici na stránkách Google Developers [17].

```
...         if n % 2 == 0:
...             return "Even"
...         else:
...             return "Odd"
sage: parity(17)
'Odd'
```

3.4 Teorie čísel

V této sekci se nachází popis a příklady použití standardních funkcí Sage pro práci s aparátem teorie čísel. Ukázkové výpočty a příklady uvedené v této sekci jsou k dispozici v přiloženém souboru `02TeorieCisel.sws`.

- `is_prime(n)` – test na prvočíselnost čísla n.
- `next_prime(n)`, resp. `previous_prime(n)` – výpočet nejbližšího následujícího, resp. nejbližšího předešlého prvočísla od zadaného čísla n.
- `prime_pi(n)` – počet všech prvočísel menších než n.
- `prime_range(a, b)` – výpis všech prvočísel v intervalu $[a, b)$.
- `random_prime(a, proof=True)` – generování náhodného prvočísla v intervalu $[2, a]$. Pokud je druhý argument nahrazen za `proof=False` nebo vynechán, existuje malá pravděpodobnost, že vygenerované číslo nebude prvočíslem.
- `n.str(q)` – převod čísla n na řetězec cifer do soustavy o základu q.
- `len(s)` – délka řetězce s.
- `n.ndigits()` – počet cifer čísla n.

```
sage: is_prime(8197)
False
sage: next_prime(1000000)
1000003
sage: prime_pi(100)
25
sage: prime_range(11, 19)
[11, 13, 17]
sage: random_prime(10^18)
616949403645979499
sage: _.str(2)
'1000100011111101100000110110110000001011010100101011011011'
sage: len(100.str(2))
7
sage: 616949403645979499.ndigits()
18
sage: for p in primes(20):
...         if is_prime(2^p - 1):
...             print p, 2^p - 1
2 3
3 7
```

```
5 31
7 127
13 8191
17 131071
19 524287
```

- `lcm(a, b)` – výpočet nejmenšího společného násobku dvou čísel a, b.
- `gcd(a, b)` – výpočet největšího společného dělitele dvou čísel a, b.
- `xgcd(a, b)` – výpočet největšího společného dělitele a koeficientů v Bezoutově rovnosti. Výstupem jsou čísla d, x, y taková, že $ax + by = d$.
- `factor(n)` – faktorizace (rozklad na prvočísla) čísla n.
- `divisors(n)` – výpočet všech dělitelů čísla n.
- `euler_phi(n)` – výpočet Eulerovy funkce φ pro číslo n.

```
sage: lcm(113, 50)
5650
sage: gcd(113, 50)
1
sage: xgcd(113, 50)
(1, -23, 52)
sage: factor(1234567890)
2 * 3^2 * 5 * 3607 * 3803
sage: divisors(12345)
[1, 3, 5, 15, 823, 2469, 4115, 12345]
sage: euler_phi(2014)
936
```

- `Integers(n)` – konstrukce okruhu $\mathbb{Z}_n$.
- `list(R)` – výčet prvků okruhu R.
- `power_mod(a, m, n)` – výpočet $a^m \pmod{n}$.
- `multiplicative_order(a)` – řád prvku $a \in \mathbb{Z}_n$.
- `inverse_mod(a, n)` – výpočet multiplikativní inverze čísla a modulo n.
- `solve_mod(a == b, n)` – řešení kongruence $ax \equiv b \pmod{n}$.
- `crt(a, b, m, n)`[10] – výpočet takového x, že $x \equiv a \pmod{m}$ a $x \equiv b \pmod{n}$.
- `CRT_list([a1, ..., an], [m1, ... mn])` – výpočet takového x, že $x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_n \pmod{m_n}$.

10. Chinese remainder theorem [1, s. 613]

```
sage: Z6 = Integers(6)
sage: list(Z6)
[0, 1, 2, 3, 4, 5]
sage: a = Z6(2)
sage: b = Z6(5)
sage: a + b; a*b
1
4
sage: power_mod(3, 2, 7)
2
sage: multiplicative_order(b)
2
sage: inverse_mod(3, 5)
2
sage: solve_mod(2*x == 4, 6)
[(2,), (5,)]
sage: crt(2, 3, 3, 5)
8
sage: CRT_list([2,3,2], [3,5,7])
23
```

3.5 Algebra

Tato sekce obsahuje popis a příklady použití standardních funkcí Sage pro práci s okruhy, tělesy a polynomy. Ukázkové výpočty a příklady uvedené v této sekci jsou k dispozici v přiloženém souboru `03Algebra.sws`.

- Číselné obory $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ se v Sage značí postupně `ZZ`, `Integers(n)`, `QQ`, `RR` a `CC`. Symbol `I` značí $\sqrt{-1}$.

- Konstrukce okruhu polynomů: `jméno_okruhu.<proměnná> = obor[]`.

  Např. konstrukce okruhu $\mathbb{Z}_7[x]$: `myMod7PolyRing.<x> = Integers(7)[]`.

```
sage: intpoly.<x> = ZZ[]
sage: f = x^2 - 4
sage: g = x^3 + 7
sage: f + g; f - g; f * g; f / g; f^2
x^3 + x^2 + 3
-x^3 + x^2 - 11
x^5 - 4*x^3 + 7*x^2 - 28
(x^2 - 4)/(x^3 + 7)
(x^3 + 7)/(x^2 - 4)
x^4 - 8*x^2 + 16
```

- `factor(f)`, resp. `f.factor()` – rozklad polynomu f na kořenové činitele. Výsledek závisí od toho, do jakého okruhu patří f.

- `expand(f)` – úprava polynomu f na rozšířený tvar.

- `f(x).simplify_full()` – úprava polynomu $f(x)$ na základní tvar. (Musí být specifikována proměnná).

```
sage: intpoly.<x> = ZZ[]
sage: factor(x^2 - 4)
(x - 2) * (x + 2)
sage: ratpoly.<y> = QQ[]
sage: factor(y^2 - 5)
y^2 - 5
sage: realpoly.<z> = RR[]
sage: factor(z^2 - 5)
(z - 2.23606797749979) * (z + 2.23606797749979)
sage: f = (x^3 - 1)^2 - (x^2 - 1)^2
sage: factor(f)
(x - 1)^2 * x^2 * (x^2 + 2*x + 2)
sage: expand(f)
x^6 - x^4 - 2*x^3 + 2*x^2
sage: P(x) = (x - 2)^3 * (x^3 - 4*x + 3)
sage: P(x).simplify_full()
x^6 - 6*x^5 + 8*x^4 + 19*x^3 - 66*x^2 + 68*x - 24
```

- `f(a)` – vyhodnocení polynomu f v bodě a.
- `x.n()` – numerická aproximace výrazu x.
- `f.gcd(g)` – největší společný dělitel polynomů f, g.
- `f.roots()` – výpočet kořenů polynomu f ve formě dvojic *(kořen, násobnost)*.
- `solve(x == k, x)` – řešení rovnic.

```
sage: P(pi)
-(4*pi - pi^3 - 3)*(pi - 2)^3
sage: P(pi).n()
31.8974800335401
sage: a = 3*y^3 + y
sage: b = 9*y^2 + 9*y
sage: a.gcd(b)
y
sage: b.roots()
[(0, 1), (-1, 1)]
sage: R.<w> = PolynomialRing(Integers(7))
sage: h = w^3 + 1
sage: h.roots()
[(6, 1), (5, 1), (3, 1)]
sage: h(6)
0
sage: solve_mod(h(x) == 0, 7)
[(3,), (5,), (6,)]
sage: solve(h(x) == 2, x)
[x = 1/2 i sqrt(3) - 1/2, x = -1/2 i sqrt(3) - 1/2, x = 1]
```

3.6 Grupy permutací

V této sekci se nachází popis a příklady použití standardních funkcí Sage pro práci s grupami permutací. Ukázkové výpočty a příklady uvedené v této sekci jsou k dispozici v přiloženém souboru `04GrupyPermutaci.sws`.

- `SymmetricGroup(n)` – konstrukce grupy permutací $\mathbb{S}_n$ o $n!$ prvcích.
- `AlternatingGroup(n)` – konstrukce alternující grupy $\mathbb{A}_n$ o $\frac{n!}{2}$ prvcích.
- `CyclicPermutationGroup(n)` – konstrukce cyklické grupy generované permutací $(1, \ldots, n)$ o n prvcích.
- `DihedralGroup(n)` – konstrukce dihedrální grupy $\mathbb{D}_{2n}$ symetrií pravidelného n-úhelníku o $2n$ prvcích.

```
sage: G = SymmetricGroup(5)
sage: sigma = G("(1,4)(5,2,3)")
sage: sigma^-1
(1,4)(2,5,3)
sage: sigma * sigma
(2,5,3)
sage: sigma.order()
6
sage: sigma.sign()
-1
sage: triangle = SymmetricGroup(3)
sage: triangle.list()
[(), (2,3), (1,2), (1,2,3), (1,3,2), (1,3)]
sage: triangle.cayley_table(names=['id','u1','u3','r1','r2','u2'
    ])
 *  id u1 u3 r1 r2 u2
  +------------------
id| id u1 u3 r1 r2 u2
u1| u1 id r1 u3 u2 r2
u3| u3 r2 id u2 u1 r1
r1| r1 u2 u1 r2 id u3
r2| r2 u3 u2 id r1 u1
u2| u2 r1 r2 u1 u3 id

sage: C = CyclicPermutationGroup(4)
sage: for g in C: print g.order(), "  ", g
1     ()
4     (1,2,3,4)
2     (1,3)(2,4)
4     (1,4,3,2)
```

3.7 Kódování a šifrování

V této sekci se nachází popis a příklady použití standardních funkcí Sage pro výpočty související s kódováním a šifrováním. Ukázkové výpočty a příklady uvedené v této sekci jsou k dispozici v přiloženém souboru `05KodyASifry.sws`.

- Cyklický kód z generujícího polynomu:

```
sage: P.<x> = PolynomialRing(GF(2),"x")
sage: C = CyclicCodeFromGeneratingPolynomial(5, 1 + x); C
Linear code of length 5, dimension 4 over Finite Field of size 2
sage: C.gen_mat()
[1 1 0 0 0]
```

```
[0 1 1 0 0]
[0 0 1 1 0]
[0 0 0 1 1]
sage: C.check_mat()
[1 1 1 1 1]
sage: m = vector([0, 1, 1, 0])
sage: result = m * C.gen_mat(); result
(0, 1, 0, 1, 0)
sage: C.check_mat() * result
(0)
```

- RSA šifrování:

  1. Vytváření páru klíčů pro Alici začne generováním tajných prvočísel p, q (která mají v praxi velikost minimálně 1024 bitů) a veřejného $n = pq$. Dále se vytváří veřejný šifrovací exponent e nesoudělný s $\varphi(n)$ a soukromý dešifrovací exponent d, který je multiplikativní inverzí e modulo $\varphi(n)$.

```
sage: p_a = next_prime(10^5)
sage: q_a = next_prime(p_a)
sage: n_a = p_a * q_a; n_a
10002200057
sage: phi_a = euler_phi(n_a); phi_a
10002000036
sage: e_a = 85
sage: d_a = inverse_mod(e_a, phi_a); d_a
5177505901
```

  2. Alice vytvoří zprávu ze čtyř znaků ASCII tabulky a konvertuje je na jejich ordinální hodnoty, tedy čísla mezi 0 až 127. Ty následně převede na číslo o základu 128. Výsledná hodnota pak bude menší, než $128^4 = 268435456$, což musí být menší, než Alicina hodnota n, protože další aritmetika se bude provádět modulo n.

```
sage: word = 'Sage'
sage: digits = [ord(letter) for letter in word]; digits
[83, 97, 103, 101]
sage: message = ZZ(digits, 128)
sage: message # 83*128^0 + 97*128^1 + 103*128^2 + 101*128^3
213512403
```

  3. Alice podepíše zprávu svým soukromým exponentem d. (V praxi se ovšem podepisuje tzv. hash zprávy.)

```
sage: signedMessage = power_mod(message, d_a, n_a)
sage: signedMessage
9883085805
```

  4. Vytváření páru klíčů na straně Boba:

```
sage: p_b = next_prime(5*10^5)
sage: q_b = next_prime(p_b)
sage: n_b = p_b * q_b
sage: phi_b = euler_phi(n_b)
```

```
sage: e_b = 77
sage: d_b = inverse_mod(e_b, phi_b)
```

5. Podepsanou zprávu Alice zašifruje veřejným klíčem Boba a odešle ji.

```
sage: encryptedMessage = power_mod(signedMessage, e_b, n_b)
sage: encryptedMessage
55899273667
```

6. Bob dešifruje zprávu svým soukromým klíčem. Následně ověří Alicin podpis za použití jejího veřejného klíče.

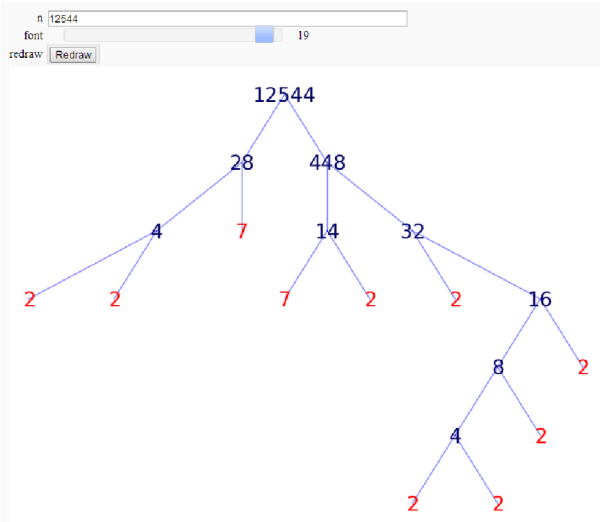
```
sage: decryptedMessage = power_mod(encryptedMessage, d_b, n_b)
sage: decryptedMessage
9883085805
sage: receivedMessage = power_mod(decryptedMessage, e_a, n_a)
sage: receivedMessage
213512403
```

7. Bob transformuje číselnou reprezentaci zprávy zpátky na ASCII znaky.

```
sage: digits = receivedMessage.digits(base=128)
sage: letters = [chr(ascii) for ascii in digits]
sage: ''.join(letters)
'Sage'
```

3.8 Interaktivita

Sage je možné využít také pro tvorbu interaktivních aplikací. Ukázkou je faktorizační strom. Zdrojový kód je převzat ze Sage Wiki [18] a je k dispozici v přiloženém souboru `06Interaktivita.sws`.



Obrázek 3.1: Interaktivní aplikace v Sage.

3.9 Příklady

Tato sekce obsahuje ukázkové výpočty a příklady, které jsou k dispozici také v přiloženém souboru `07Priklady.sws`.

1. Funkce pro výpis podílu a zbytku po dělení dvou čísel je `quo_rem()`. Dle vestavěné nápovědy zjistěte syntaxi použití a otestujte funkci s čísly 963852, 852741.
2. Určete počet cifer nejbližšího prvočísla od $5 \cdot 10^{100}$ a počet bitů, které zabere při reprezentaci v binární soustavě.
3. Spočtěte $2 + 3 \pmod 4$. Nalezněte příkaz na vypsání tabulky sčítání v grupě $\mathbb{Z}_4$.
4. Vytvořte prvek 3 v grupě $\mathbb{Z}_7$. Určete aditivní a multiplikativní řád prvku.
5. Pomocí funkce `list_of_elements_of_multiplicative_group()` vypište prvky grupy jednotek z aditivní grupy $\mathbb{Z}_{42}$. Dvěma různými způsoby spočtěte počet prvků grupy $\mathbb{Z}_{42}^{\times}$. Nápověda: použijte také funkci `unit_group_order()`.
6. Vytvořte dva netriviální prvky σ, ρ grupy $\mathbb{S}_9$ tak, aby $\sigma \cdot \rho = \sigma \cdot \rho^{-1}$. (Pozor na pořadí vyhodnocování, nejedná se o skládání permutací.)
7. Spočtěte dvěma různými způsoby počet prvků grupy $\mathbb{S}_{42}$. Ověřte, že se výsledky výpočtů rovnají.
8. Napište funkci pro výpis řádů všech podgrup $\mathbb{S}_5$. Použijte funkci `subgroups()`[11].
9. Funkce `all()` vyhodnotí seznam logických hodnot a provede mezi nimi logický součin. Např. `all([True, True, False, True])` se vyhodnotí na `False`. Pomocí této funkce demonstrujte správnost Malé Fermatovy věty pro zvolené a a všechna prvočísla v rozsahu $[10, 1000)$.
10. Pro všechna prvočísla p v rozsahu $[10, 1000)$ ověřte, že řád grupy $\mathbb{Z}_p^{\times}$ je $p - 1$.
11. Ověřte, že dihedrální grupa symetrií trojúhelníku je izomorfní grupě $\mathbb{S}_3$.
12. Ověřte, že grupa $\mathbb{C}_3 \times \mathbb{C}_5$ je izomorfní grupě $\mathbb{C}_{15}$. Experimentujte s izomorfismy různých grup.
13. Vytvořte okruh $\mathbb{Z}_{11}$. Zjistěte, jestli je konečný, komutativní, obor integrity a těleso. Vypište jeho generátory a zjistěte, zda je prvek 3 jednotkou. Jak se změní vlastnosti, pokud budeme pracovat s okruhem $\mathbb{Z}_{12}$?
14. Vytvořte okruh polynomů $\mathbb{Z}_8[x]$ a vyhodnoťte polynom $3x^2 + 2x + 4$ ve všech možných bodech v $\mathbb{Z}_8$.

11. Viz. také návod na URL http://www.sagemath.org/doc/tutorial/programming.html#lists-tuples-and-sequences.

15. Demonstrujte Eisensteinovo kritérium ireducibility v okruhu $\mathbb{Z}[x]$ pro zvolený polynom f a prvočíslo p.

16. Proveďte co nejúplnější faktorizaci polynomu $x^3 + 4x - 1$ v okruzích $\mathbb{Z}_5[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ a $\mathbb{C}[x]$.

17. Definujte polynomy $p = x^3 + 2x^2 + 2x + 4$, $q = x^4 + 2x^2$ v okruhu $\mathbb{Z}[x]$. Spočtěte (p, q) pomocí vestavěné funkce a ověřte výsledek pomocí aritmetických operátorů. Nalezněte koeficienty v Bezoutově rovnosti pro tyto polynomy.

18. Pomocí RSA odešlete podepsanou zprávu od Alice k Bobovi. Simulujte změnu zprávy přičtením nějakého čísla před tím, než Bob ověří podpis.

19. Simulujte protokol Diffie-Hellman pro $q = 93450983094850938450983409623$.

20. Implementujte v Sage funkci pro binární modulární umocňování.

3.10 Řešení příkladů

Při tvorbě řešení jsem pracoval s [19].

1.
```
sage: 963852.quo_rem(852741)
(1, 111111)
```

2.
```
sage: p = next_prime(5*10^100)
sage: p.ndigits()
101
sage: len(p.str(2))
335
```

3.
```
sage: Z4 = Integers(4)
sage: Z4(2) + Z4(3)
1
sage: Z4.addition_table(names='elements')
+  0 1 2 3
 +--------
0| 0 1 2 3
1| 1 2 3 0
2| 2 3 0 1
3| 3 0 1 2
```

4.
```
sage: x = Integers(7)(3)
sage: addOrd = x.additive_order()
sage: mulOrd = x.multiplicative_order()
sage: addOrd; mulOrd
7
6
sage: x * addOrd; x^mulOrd
0
1
```

5.
```
sage: Z42 = Integers(42)
sage: Z42x = Z42.list_of_elements_of_multiplicative_group()
sage: Z42xOrd = Z42.unit_group_order()
sage: Z42x
[1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41]
sage: Z42xOrd; euler_phi(42)
12
12
```

6.
```
sage: S9 = SymmetricGroup(9)
sage: sigma = S9("(8,9,2,5,1,3)")
sage: ro = S9("(1,7)(5,6)")
sage: sigma * ro; sigma * ro^-1;
(1,3,8,9,2,6,5,7)
(1,3,8,9,2,6,5,7)
```

7.
```
sage: S42 = SymmetricGroup(42)
sage: a = S42.order()
sage: b = factorial(42)
sage: print a; print b; a == b
1405006117752879898543142606244511569936384000000000
1405006117752879898543142606244511569936384000000000
True
```

8.
```
sage: S5 = SymmetricGroup(5)
sage: list = [s.order() for s~in S5.subgroups()]
sage: sorted(Set(list))
[1, 2, 3, 4, 5, 6, 8, 10, 12, 20, 24, 60, 120]
```

9.
```
sage: a = 6
sage: all(a^p % p == a for p in prime_range(10, 1000))
True
```

10.
```
sage: all(Integers(p).unit_group_order() == p - 1 for p in
    prime_range(10, 1000))
True
```

11.
```
sage: G = DihedralGroup(3)
sage: H = SymmetricGroup(3)
sage: G.is_isomorphic(H)
True
```

12.
```
sage: D1 = CyclicPermutationGroup(3)
sage: D2 = CyclicPermutationGroup(5)
sage: DP = direct_product_permgroups([D1,D2])
sage: C  = CyclicPermutationGroup(15)
sage: DP.is_isomorphic(C)
True
```

13.
```
sage: R = Integers(11)
sage: R.is_finite()
True
sage: R.is_commutative()
True
sage: R.is_integral_domain()
True
sage: R.is_field();
```

```
True
sage: R.zero();
0
sage: R.gens();
(1,)
sage: R(3).is_unit();
True
```

14.
```
sage: R.<x> = Integers(8)[]
sage: p = 4 + 2*x + 3*x^2
sage: [p(a) for a in Integers(8)]
[4, 1, 4, 5, 4, 1, 4, 5]
```

15.
```
sage: S.<y> = ZZ[]
sage: f = 2*y^4 + 5*y^3 + 10*y^2 + 10*y + 5
sage: f.is_irreducible()
True
```

16.
```
sage: P.<x> = Integers(5)[]
sage: p = x^3 + 4*x - 1
sage: p.factor()
(x + 3) * (x^2 + 2*x + 3)
sage: Q.<x> = QQ[]
sage: q = x^3 + 4*x - 1
sage: q.factor()
x^3 + 4*x - 1
sage: R.<x> = RR[]
sage: r = x^3 + 4*x - 1
sage: r.factor()
(x - 0.246266172167723) * (x^2 + 0.246266172167723*x +
   4.06064702755414)
sage: S.<x> = CC[]
sage: s~= x^3 + 4*x - 1
sage: s.factor()
(x - 0.246266172167723) * (x + 0.123133086083861 -
   2.01133917345275*I) *
(x + 0.123133086083861 + 2.01133917345275*I)
```

17.
```
sage: R.<x> = ZZ[]
sage: p = x^3 + 2*x^2 + 2*x + 4
sage: q = x^4 + 2*x^2
sage: gcd = p.gcd(q)
sage: gcd
x^2 + 2
sage: p / gcd; p % gcd
x + 2
0
sage: q / gcd; q % gcd;
x^2
0
sage: xgcd = p.xgcd(q)
sage: xgcd
(4*x^2 + 8, -x + 2, 1)
sage: xgcd[0] == xgcd[1]*p + xgcd[2]*q
True
```

18.
```
sage: n = next_prime(10^8) * next_prime(6*10^8)
sage: e = 7
```

```
sage: d = inverse_mod(e, euler_phi(n))
sage: word = 'Hello from Alice'
sage: print word
sage: digits = [ord(letter) for letter in word]
sage: message = ZZ(digits, 128)
sage: signedMessage = power_mod(message, d, n)
sage: print signedMessage
sage: tamperedMessage = signedMessage + 1
sage: receivedMessage = power_mod(tamperedMessage, e, n)
sage: print receivedMessage
sage: digits = receivedMessage.digits(base=128)
sage: letters = [chr(ascii) for ascii in digits]
sage: ''.join(letters)
Hello from Alice
10022258900065460
12686638977972135
"'o3\reMD\x16"
```

19.

```
sage: q = 93450983094850938450983409623
sage: is_prime(q)
True
sage: is_prime((q-1)//2)
True
sage: g = Mod(-2, q)
sage: g.multiplicative_order()
93450983094850938450983409622
sage: n = 18319922375531859171613379181
sage: m = 82335836243866695680141440300
sage: g^n
45416776270485369791375944998
sage: g^m
15048074151770884271824225393
sage: (g^n)^m
85771409470770521212346739540
sage: (g^m)^n
85771409470770521212346739540
```

20.

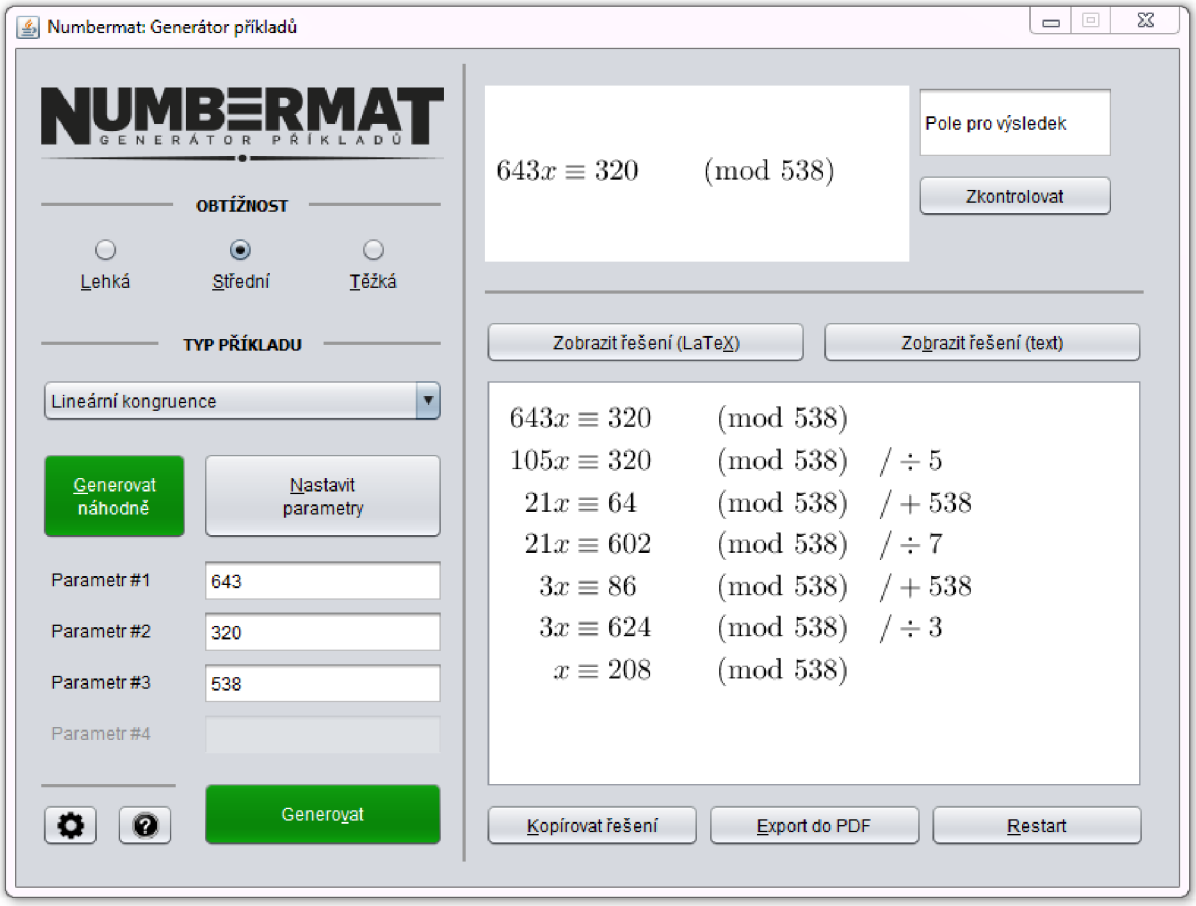
```
def modular_pow(base, exp, mod):
    result = 1
    base = base % mod
    while (exp > 0):
        if (exp % 2 == 1):
           result = (result * base) % mod
        exp = exp // 2
        base = (base * base) % mod
    return result
```

Kapitola 4

Generátor příkladů Numbermat

4.1 Uživatelské rozhraní

Numbermat je aplikace, která generuje zadání a řešení příkladů a to buď náhodně, nebo dle uživatelem zadaných parametrů. Uživatelské rozhraní programu sestává z jediného okna, které vypadá pod systémem Windows 7[1] následovně:



Obrázek 4.1: Ukázkové zadání a řešení vygenerovaného příkladu.

1. Vzhled jednotlivých prvků se může mírně lišit v závislosti od platformy.

- *Obtížnost*: Pokud bude uživatel generovat příklad náhodně, má možnost omezit rozsah hodnot, ze kterých se budou vybírat čísla v zadání. Význam jednotlivých tlačítek závisí od vybraného příkladu a je blíže popsán v 4.3. Výchozí volba je střední obtížnost. Při generovaní příkladu dle uživatelem zadaných parametrů nemá zvolená obtížnost žádný vliv.
- *Typ příkladu*: Seznam, ze kterého si uživatel zvolí jeden ze 13 typů příkladů. Jednotlivé typy jsou blíže popsané v 4.3. Výchozí volba je příklad na výpočet největšího společného dělitele.
- *Generovat náhodně*: Na základě zvolené obtížnosti a typu příkladu se náhodně vygeneruje zadání a zpřístupní se prvky v pravé části okna oddělené svislou čárou (které jsou jinak neaktivní).
- *Nastavit parametry*: Na základě zvoleného typu příkladu se zpřístupní odpovídající počet polí pro zadání parametrů a tlačítko Generovat.
- *Nastavení*: Tlačítko s ozubeným kolečkem zpřístupní nastavení programu, kde je možné specifikovat cestu k souboru pro překlad PDFLaTeX-em (viz. dále).
- *Nápověda*: Tlačítko s otazníkem zpřístupní nápovědu programu: krátký popis jednotlivých typů příkladů, klávesové zkratky a informace o programu.
- *Generovat*: Na základě zvoleného typu příkladu a zadaných parametrů se vygeneruje zadání a zpřístupní se prvky v pravé části okna oddělené svislou čárou.
- *Pole pro výsledek*: Slouží pro zadání výsledku výpočtu. Uživatel musí zadat výsledek v definovaném formátu (viz. nápověda programu).
- *Zkontrolovat*: Tlačítko pro následnou kontrolu uživatelem zadaného výsledku.
- *Zobrazit řešení (LaTeX)*: Zobrazí matematicky vysázený postup řešení. Tato volba je zabudovaná přímo v programu a nevyžaduje žádné další nástroje.
- *Zobrazit řešení (text)*: Zobrazí postup řešení jako text ve formě ASCII znaků.
- *Kopírovat řešení*: Zkopíruje textové řešení příkladu do schránky.
- *Export do PDF*: Exportuje zadání a řešení příkladu jako soubor ve formátu `.tex` do uživatelem zvolené složky. Aplikace se následně automaticky pokusí přeložit zdrojový soubor programem PDFLaTeX (je potřeba standardní instalace TeX-ové distribuce nebo specifikace cesty k spustitelnému souboru pro překlad PDFLaTeX-em v nastavení programu). Aplikace nakonec smaže soubory vzniklé při překladu a automaticky otevře vzniklý PDF soubor.
- *Restart*: Má stejný účinek jako vypnutí a opětovné zapnutí programu.

4.2 Použité technologie

K implementaci aplikace jsem zvolil jazyk Java verze 7, jelikož je to platformně nezávislý jazyk, který obsahuje množství funkcí už v základních knihovnách a poskytuje rozsáhlé možnosti využití knihoven třetích stran. Při vývoji jsem pracoval v prostředí NetBeans 7.3 a využil jsem systém Subversion pro správu verzí. Jelikož korektnost výpočtu je v tomto případě důležitá, ke každé výpočetní funkci jsem napsal jednotkové testy, k čemu jsem využil framework JUnit. Grafické uživatelské rozhraní jsem navrhl za pomocí nástroje GUI Builder vestavěného v IDE NetBeans a implementoval ho pomocí knihovny Swing.

Pro matematickou sazbu příkladů přímo v okně aplikace využívám knihovnu JLaTeXMath 1.0.3 [20] licencovanou pod GNU General Public License version 2[2]. Pro export příkladů ve formátu PDF využívám knihovnu Java LaTeX Report (JLR) 2.1 [21] licencovanou pod Apache License version 2.0. Z tohoto důvodu je výsledná aplikace licencována pod GNU General Public License version 3 [22]. Tato licence je kompatibilní s oběma licencemi použitých knihoven.

4.3 Typy příkladů

Sekce obsahuje popis všech 13 typů příkladů, které umožňuje generovat Numbermat. U každé položky jsou specifikovány požadované vstupy a očekávané výstupy, nastavení obtížnosti při náhodném generování, implementace výpočtu a implementace kroků řešení, které se uživateli zobrazí po kliknutí na tlačítko *Zobrazit řešení (LaTeX)*, resp. *Zobrazit řešení (text)*. Obecně platí:

- Může nastat situace, že uživatel zadá platné parametry, s nimiž daný příklad nemá řešení. Při náhodném generování se ale generují vždy jenom řešitelné příklady.
- V modulární aritmetice se jednotlivé parametry v průběhu výpočtu obvykle normalizují na nejmenší možné nezáporné číslo, t.j. např. kongruence $x \equiv -7 \pmod 5$ se převede na $x \equiv 3 \pmod 5$.
- Vzhledem k ekvivalentním třídám řešení [1, s. 610] jsou výsledky vždy nejmenší možné a vždy nezáporné. Tedy např. místo řešení $x \equiv 0 \pmod 4 \vee x \equiv 2 \pmod 4$ nebo $x \equiv 10 \pmod 2$ aplikace vyhodnotí jako správné $x \equiv 0 \pmod 2$.

4.3.1 Největší společný dělitel

- Vstup: Čísla $a, b \in \mathbb{Z}$.
- Výstup: Číslo $(a, b) \in \mathbb{N}_0$.
- Nastavení obtížnosti:

2. Licence obsahuje přidanou klauzuli „or later“, která umožňuje odvozená díla licencovat pod pozdějšími verzemi GNU General Public License.

  - Lehká: a, b se generují z rozsahu $[1, 127]$.
  - Střední: a, b se generují z rozsahu $[128, 1023]$.
  - Těžká: a, b se generují z rozsahu $[512, 4095]$.

- Implementace výpočtu: Euklidův algoritmus [9, s. 66]. Při zadání záporného čísla se toto číslo vynásobí -1 a v případě, že $a < b$ se čísla zamění.
- Implementace postupu řešení pro uživatele: Kroky Euklidova algoritmu.

4.3.2 Bezoutova rovnost

- Vstup: Čísla $a, b \in \mathbb{N}_0$.
- Výstup: Čísla $d \in \mathbb{N}_0$, $x, y \in \mathbb{Z}$ taková, že $ax + by = d = (a, b)$.
- Nastavení obtížnosti: Stejné jako u 4.3.1.
- Implementace výpočtu: Rozšířený Euklidův algoritmus [9, s. 67]. Pokud $a < b$, čísla se zamění, aby vstup vyhovoval vstupu citovaného algoritmu.
- Implementace postupu řešení pro uživatele: Jednotlivé kroky výpočtu největšího společného dělitele a následné zpětné dosazování. Viz. Obrázek 4.2.

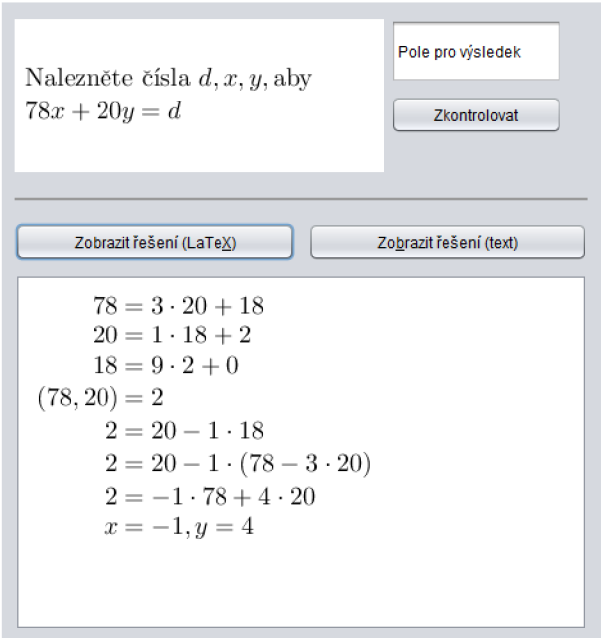
4.3.3 Inverze modulo n

- Vstup: Čísla $a, n \in \mathbb{N}$, kde $(a, n) = 1$.
- Výstup: Číslo $x \in \mathbb{N}$ takové, že $ax \equiv 1 \pmod{n}$.
- Nastavení obtížnosti: Stejné jako u 4.3.1.
- Implementace výpočtu: Stejná jako u 4.3.2.
- Implementace postupu řešení pro uživatele: Stejná jako u 4.3.2.

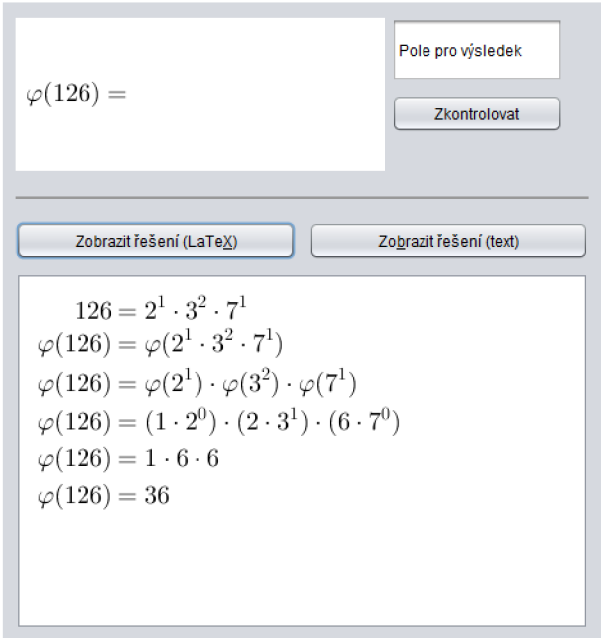
4.3.4 Eulerova funkce φ

- Vstup: Číslo $n \in \mathbb{N}$.
- Výstup: Číslo $\varphi(n) \in \mathbb{N}$.
- Nastavení obtížnosti:
  - Lehká: n se generuje z rozsahu $[1, 99]$.
  - Střední: n se generuje z rozsahu $[100, 999]$.
  - Těžká: n se generuje z rozsahu $[1000, 2999]$.

- Implementace výpočtu: Faktorizace n a výpočet $\varphi(n)$ z definice [1, s. 597].
- Implementace postupu řešení pro uživatele: Jednotlivé kroky výpočtu z definice.



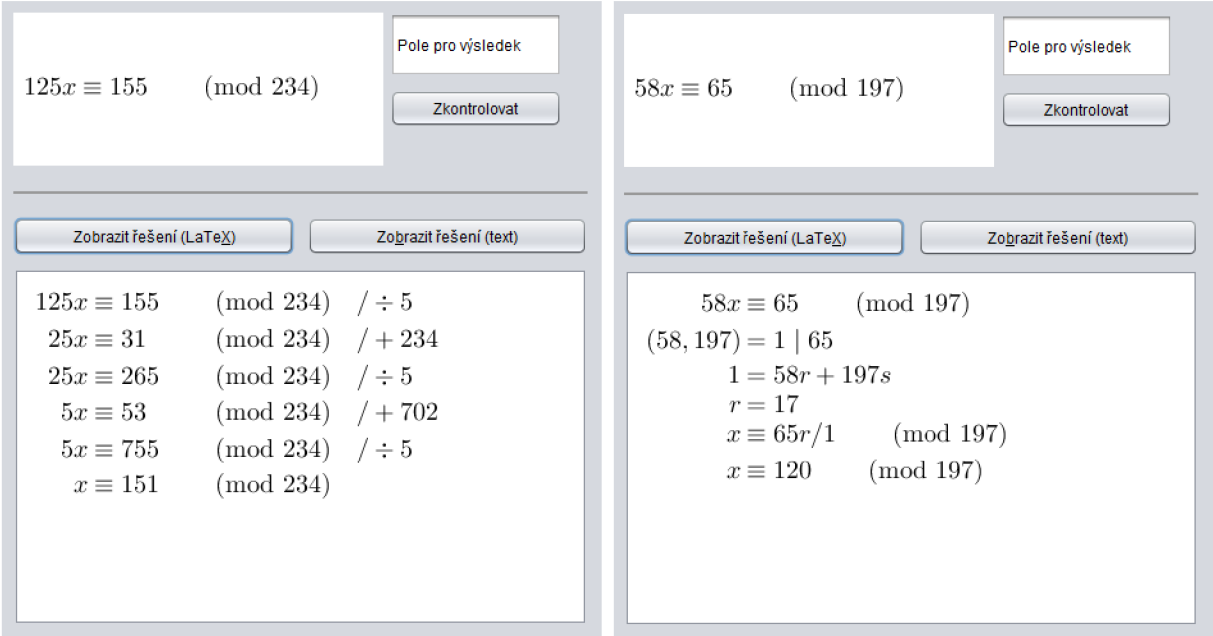
Obrázek 4.2: Bezoutova rovnost.



Obrázek 4.3: Eulerova funkce.

4.3.5 Lineární kongruence

- Vstup: Čísla $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$.
- Výstup: Čísla $r \in \mathbb{N}_0$, $t \in \mathbb{N}$ taková, že $x \equiv r \pmod{t}$ je řešením kongruence $ax \equiv b \pmod{n}$.
- Nastavení obtížnosti:
  - Lehká: a, b, n se generují z rozsahu $[11, 50]$.
  - Střední: a, b, n se generují z rozsahu $[50, 300]$.
  - Těžká: a, b, n se generují z rozsahu $[300, 700]$.
- Implementace výpočtu: Vychází se z Věty 10.24 [1, s. 611], přičemž řešení se hledá pomocí koeficientů v Bezoutově rovnosti, jako to popisuje [3, s. 51].
- Implementace postupu řešení pro uživatele: Program se pokusí nalézt řešení pomocí ekvivalentních úprav kongruence. Pokud se mu to nepovede, zobrazí kroky výpočtu pomocí koeficientů v Bezoutově rovnosti.



(a) Řešení pomocí ekvivalentních úprav. (b) Řešení pomocí Bezoutovy rovnosti.

Obrázek 4.4: Řešení lineárních kongruencí.

4.3.6 Soustava lineárních kongruencí

- Vstup: Počet kongruencí $1 \leq k \leq 4$ a tři posloupnosti $(a_m)_{i=1}^k$, $(b_m)_{i=1}^k$, $(n_m)_{i=1}^k$ koeficientů, přičemž $a_i, b_i \in \mathbb{Z}$ a $n_i \in \mathbb{N}$.
- Výstup: Čísla $r \in \mathbb{N}_0, t \in \mathbb{N}$ taková, že $x \equiv r \pmod{t}$ je řešením všech kongruencí $a_i x \equiv b_i \pmod{n_i}$.
- Nastavení obtížnosti:
  - Lehká: Generují se 2 kongruence a čísla b, n z rozsahu $[2, 15]$. Koeficient a je u obou kongruencí roven 1.
  - Střední: Generují se 2 kongruence a čísla a, b, n z rozsahu $[15, 25]$.
  - Těžká: Generují se 3 kongruence a čísla a, b, n z rozsahu $[10, 30]$.
- Implementace výpočtu: Vyřeší se kongruence i a pokud $i < k$, výsledek se dosadí do kongruence $i + 1$. Následně se i inkrementuje. Viz. také [1, s. 612].
- Implementace postupu řešení pro uživatele: Výsledek řešení každé z částkových kongruencí a krok dosazení do následující kongruence.

4.3.7 Řád prvku grupy jednotek

- Vstup: Čísla $a, n \in \mathbb{N}$, přičemž $n \geq 2$ a $a \in \mathbb{Z}_n^\times$.

- Výstup: Řád prvku a v grupě $\mathbb{Z}_n^\times$, t.j. $k \in \mathbb{N}$ takové, že $a^k = 1$ [1, s. 605, 650].
- Nastavení obtížnosti:
  - Prvek a se generuje vždy z rozsahu $[2, 9]$.
  - Lehká: n se generuje z rozsahu $[5, 11]$.
  - Střední: n se generuje z rozsahu $[11, 37]$.
  - Těžká: n se generuje z rozsahu $[37, 97]$.
- Implementace výpočtu: Vygeneruje se rostoucí posloupnost možných řádů (dělitele $\varphi(n)$ [1, s. 652]) všech prvků dané grupy a prvek a se postupně umocňuje na jednotlivé možné řády, dokud se nenajde výsledek.
- Implementace postupu řešení pro uživatele: Výpis prvků dané grupy, výpis možných řádů a jednotlivé kroky výpočtu.

4.3.8 Modulární umocňování

- Vstup: Čísla $b \in \mathbb{Z}$, $e \in \mathbb{N}_0$, $m \in \mathbb{N}$.
- Výstup: Číslo $x \in \mathbb{N}_0$ takové, že $b^e \equiv x \pmod{m}$.
- Nastavení obtížnosti:
  - Lehká: b, e, m se generují z rozsahu $[5, 11]$.
  - Střední: b, e, m se generují z rozsahu $[11, 37]$.
  - Těžká: b, e, m se generují z rozsahu $[37, 97]$.
  - Existuje 20% šance, že m se inicializuje na hodnotu 100. V takovém případě je zadání ekvivalentní hledání posledních dvou cifer čísla b^e.
- Implementace výpočtu: funkce `modPow` [23].
- Implementace postupu řešení pro uživatele: Program spočte $\varphi(m)$ a pokusí se znormalizovat exponent na hodnotu e modulo $\varphi(m)$. Pokud $b \in \mathbb{Z}_m^\times$, najde řád k prvku a znormalizuje exponent na hodnotu e modulo k. Nakonec faktorizuje m na $p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$ a pokud $n > 1$, vyřeší jednotlivé kongruence $b^e \equiv x_i \pmod{p_i^{e_i}}$ a odvodí hledané x. Viz. Obrázek 4.5.

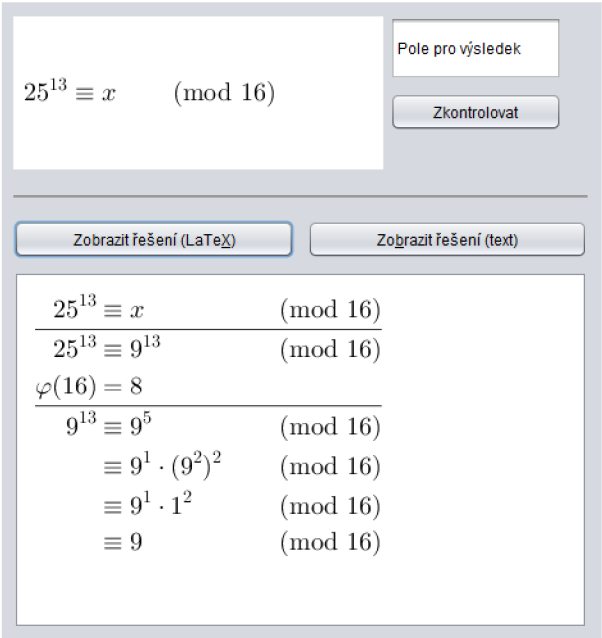
4.3.9 Legendreův symbol

- Vstup: Číslo $a \in \mathbb{Z}$ a liché prvočíslo p.
- Výstup: Hodnota Legendreova symbolu $(\frac{a}{p})$, tedy jedno z čísel 0, 1 nebo -1.
- Nastavení obtížnosti:

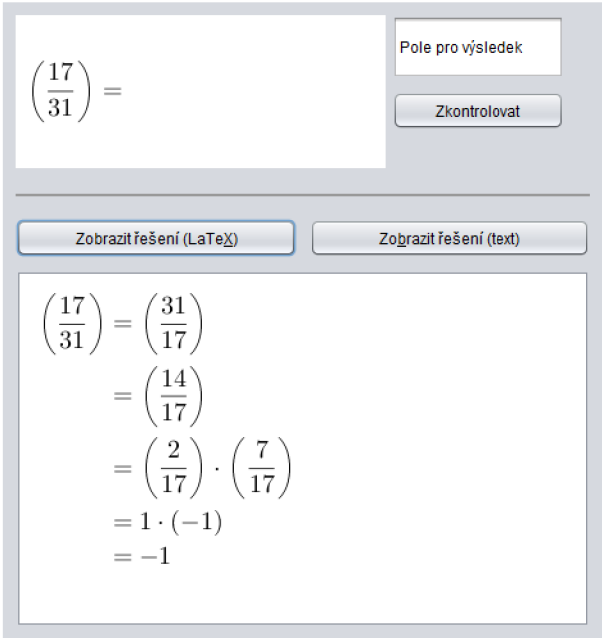
  - Lehká: a, p se generují z rozsahu $[2, 49]$.
  - Střední: a, p se generují z rozsahu $[10, 79]$.
  - Těžká: a, p se generují z rozsahu $[49, 119]$.

- Implementace výpočtu: Z definice (Lemma 10.33 [1, s. 617]) algoritmem pro modulární umocňování.

- Implementace postupu řešení pro uživatele: Program se pokusí aplikovat věty na zjednodušení Legendreova symbolu [1, s. 617, 621]. Pokud $a < p$ a a je liché prvočíslo, prohodí a, p. Nakonec faktorizuje a a spočte jednotlivé symboly zvlášť.



Obrázek 4.5: Modulární umocňování.



Obrázek 4.6: Legendreův symbol.

4.3.10 Kvadratická kongruence (binomická)

- Vstup: Čísla $a \in \mathbb{Z}$, $m \in \mathbb{N}$.

- Výstup: Čísla $r_1, \ldots, r_n \in \mathbb{N}_0$, $t \in \mathbb{N}$ taková, že $x \equiv r_i \pmod{t}$ je řešením kongruence $x^2 \equiv a \pmod{m}$[3].

- Nastavení obtížnosti:

3. Od 4.3.11 řešení obecných kvadratických kongruencí tvaru $ax^2 + bx + c \equiv 0 \pmod{m}$ jsem se rozhodl oddělit případ $x^2 \equiv a \pmod{m}$ zvlášť, jelikož je často využíván např. při hledání kvadratických reziduí a při zadávání parametrů se uživatel vyhne opakování koeficientů $a = 1$, $b = 0$ pro obecné kongruence.

  - Lehká: a, m se generují z rozsahu $[2, 39]$, m je prvočíslo.
  - Střední: a se generuje z rozsahu $[11, 99]$, m je dvojciferné číslo, které je součinem dvou různých prvočísel.
  - Těžká: a se generuje z rozsahu $[11, 199]$, m je dvojciferné číslo, které je součinem dvou různých prvočísel.

- Implementace výpočtu: K číslu a se postupně přičítá m, dokud a není druhou mocninou nějakého k; v takovém případě dostáváme řešení $\pm\sqrt{k}$. Pokračuje se, až dokud nenalezneme (maximálně) 4 řešení nebo počet pokusů nepřekročí m. Využívají se teoretické poznatky definované v [1, s. 617] a kapitolách 4 a 5 v [5].

- Implementace postupu řešení pro uživatele: Program faktorizuje m na $m_1 \cdot \ldots \cdot m_n = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$. Pokud $2 \leq n \leq 4$, zkontroluje, zda má každá z kongruencí $x^2 \equiv a \pmod{m_i}$ řešení (odpovídající Legendreův symbol je 0 nebo 1) [1, s. 613]. Pokud nemá, program vypíše m_i, pro které řešení neexistuje a výpočet odpovídajícího Legendreova symbolu. Pokud existuje řešení pro každou z částkových kongruencí, výpočet vede na řešení soustav lineárních kongruencí.

4.3.11 Kvadratická kongruence (obecná)

- Vstup: Čísla $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$, kde $a \neq 0$ a $(a, m) = 1$.

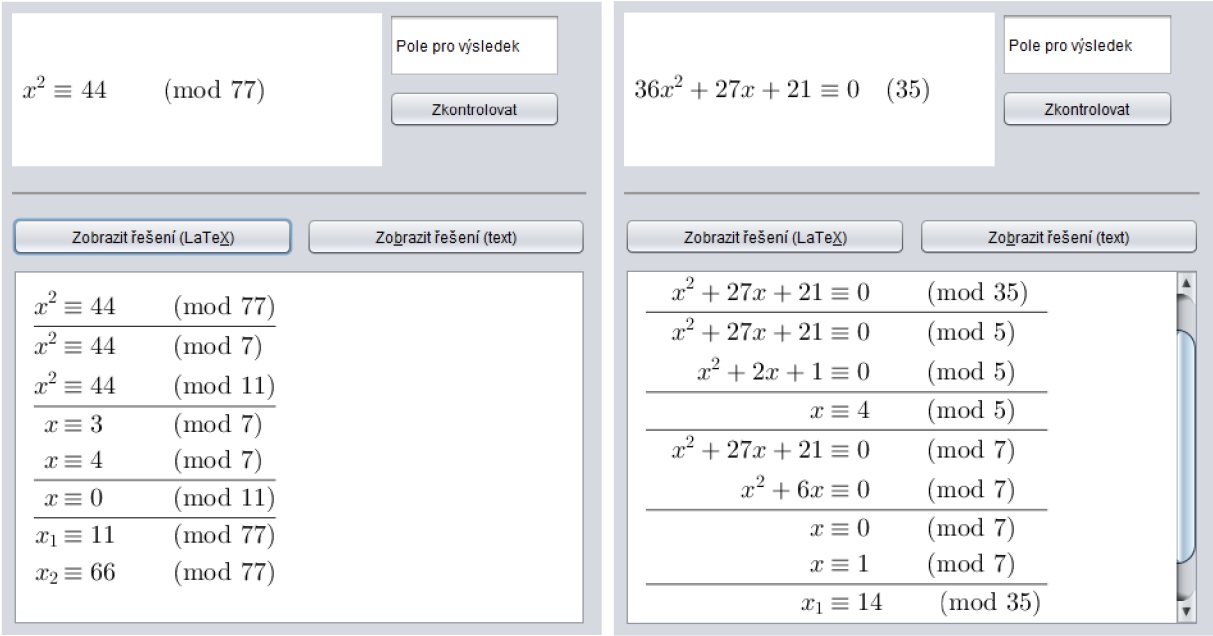
- Výstup: Čísla $r_1, \ldots, r_n \in \mathbb{N}_0$, $t \in \mathbb{N}$ taková, že $x \equiv r_i \pmod{t}$ je řešením kongruence $ax^2 + bx + c \equiv 0 \pmod{m}$.

- Nastavení obtížnosti:

  - Lehká: a, b, c, m se generují z rozsahu $[2, 19]$, m je prvočíslo.
  - Střední: a, b, c se generují z rozsahu $[11, 39]$, m je dvojciferné číslo, které je součinem dvou různých lichých prvočísel.
  - Těžká: a, b, c se generují z rozsahu $[11, 99]$, m je dvojciferné číslo, které je součinem dvou různých lichých prvočísel.

- Implementace výpočtu: Nejprve se vyřeší (binomická) kvadratická kongruence $t^2 \equiv b^2 - 4ac \pmod{4m}$. Následně se pro každé t ověří, že $t \equiv b \pmod{2}$ a řeší se kongruence $ax \equiv (t - b)/2 \pmod{m}$.

- Implementace postupu řešení pro uživatele: Program faktorizuje m na $m_1 \cdot \ldots \cdot m_n = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$ a vyřeší každou z kongruencí $ax^2 + bx + c \equiv 0 \pmod{m_i}$. Pokud se mu nepovede nalézt řešení touto cestou, vypíše kroky výpočtu pomocí diskriminantu.



(a) Binomická kvadratická kongruence. (b) Obecná kvadratická kongruence.

Obrázek 4.7: Kvadratické kongruence.

4.3.12 Binomická kongruence

- Vstup: Čísla $n, m \in \mathbb{N}$, $a \in \mathbb{Z}$.
- Výstup: Čísla $r_1, \ldots, r_n \in \mathbb{N}_0$, $t \in \mathbb{N}$ taková, že $x \equiv r_i \pmod{t}$ je řešením kongruence $x^n \equiv a \pmod{m}$.
- Nastavení obtížnosti:
  - Exponent n se vždy generuje z rozsahu $[3, 5]$.
  - Lehká: a, m se generují z rozsahu $[2, 11]$.
  - Střední: a, m se generují z rozsahu $[9, 19]$.
  - Těžká: a se generuje z rozsahu $[2, 37]$, m je dvojciferné číslo, které je součinem dvou různých prvočísel.
- Implementace výpočtu: Hledání řešení zkoušením všech možností v rozsahu od 0 do m. Pokud $(a, m) = 1$ a existují primitivní kořeny modulo m [1, s. 607], využije se Věta o řešitelnosti binomických kongruencí [1, s. 616].
- Implementace postupu řešení pro uživatele: Pokud se dá použít výše uvedená Věta, program vypíše kroky její použití. Nakonec vypíše všechna řešení nalezená metodou zkoušení.

4.3.13 Řád permutace

- Vstup: Číslo $n \in \mathbb{N}$, permutace $\sigma \in \mathbb{S}_n$.
- Výstup: Řád k permutace σ, t.j. číslo takové, že $\sigma^k = id$.
- Nastavení obtížnosti:
  - Lehká: n se generuje z rozsahu $[2, 5]$.
  - Střední: n se generuje z rozsahu $[6, 8]$.
  - Těžká: $n = 9$[4].
- Implementace výpočtu: Program rozloží permutaci na součin nezávislých cyklů a řád vypočte jako nejmenší společný násobek řádů jednotlivých cyklů.
- Implementace postupu řešení pro uživatele: Program zobrazí rozklad zadané permutace na součin nezávislých cyklů a výpočet řádu.

4. Nalezení řádu 9-prvkové permutace zřejmě není zvlášť těžký úkol, nicméně toto omezení existuje z důvodu relativně malého rozměru plochy pro zobrazení zadání příkladu.

Kapitola 5

Závěr

Výsledkem této práce jsou následující materiály pro elektronickou podporu výuky algebry a teorie čísel:

- sbírka příkladů spolu s jejich řešeními,
- výuková videa k vybraným příkladům,
- návod pro práci s výpočetním systémem Sage,
- sbírka příkladů do Sage spolu s jejich řešeními,
- interaktivní pracovní listy do Sage,
- aplikace pro generování příkladů.

Pokud budou výsledky mé práce využity při výuce matematiky na FI nebo k samostudiu, věřím, že budou pro jejich uživatele přínosné. Všechny výstupy jsou kromě archivu práce k dispozici rovněž na přiloženém CD, jehož obsah je podrobně popsán v Příloze A. V případě budoucího rozšíření výsledků práce považuji za vhodné zvětšit integraci se systémem Sage pro dosažení vyšší míry interaktivity a doplnit generátor příkladů o nové typy úloh.

Literatura

[1] SLOVÁK, Jan – PANÁK, Martin – BULANT, Michal. *Matematika drsně a svižně*. První vydání. Brno: Masarykova univerzita, 2013. 776 s. ISBN 978-80-210-6308-2. Dostupné z URL: http://www.math.muni.cz/Matematika_drsne_svizne.

[2] JUDSON, Thomas W. *Abstract Algebra: Theory and Applications*. Srpen 2013. 434 s. Dostupné z URL: http://abstract.pugetsound.edu/download/aata-20130816.pdf.

[3] NATHANSON, Melvyn B. *Elementary Methods in Number Theory*. New York: Springer, c2000. 513 s. ISBN 0-387-98912-9.

[4] SIERPIŃSKI, Wacław. *250 Problems in Elementary Number Theory*. New York: American Elsevier Publishing Company, 1970. 125 s. ISBN 0-444-00071-2.

[5] IRELAND, Kenneth a Michael ROSEN. *A Classical Introduction to Modern Number Theory*. Druhé vydání. New York: Springer, 1990. 389 s. ISBN 0-387-97329-X.

[6] STEIN, William. *Sage Mathematics Software (Version 6.1.1)* [online]. Únor 2014 [cit. 12. května 2014]. Dostupné z URL: http://www.sagemath.org/.

[7] THE SAGE DEVELOPMENT TEAM. *Sage Tutorial Release 6.1.1* [online]. Únor 2014 [cit. 12. května 2014]. 105 s. Dostupné z URL: http://www.sagemath.org/pdf/en/tutorial/SageTutorial.pdf.

[8] THE SAGE DEVELOPMENT TEAM. *Sage Constructions Release 6.1.1* [online]. Únor 2014 [cit. 12. května 2014]. 87 s. Dostupné z URL: http://www.sagemath.org/pdf/en/constructions/constructions.pdf.

[9] MENEZES, Alfred J. – VAN OORSCHOT, Paul C. – VANSTONE, Scott A. *Handbook of Applied Cryptography*. První vydání. Boca Raton: CRC Press, 1996. 780 s. ISBN 0-849-38523-7.

[10] KHAN ACADEMY. *Khan Academy* [online]. c2014 [cit. 12. května 2014]. Dostupné z URL: http://www.khanacademy.org.

[11] AUTODESK INC. *Autodesk SketchBook Express v.5.5.1.* [online]. c2012 [cit. 12. května 2014]. 29 s. Dostupné z URL: http://www.sketchbook.com/storage/documentation/ENU_SketchBook_Express_icloud2.pdf.

[12] TECHSMITH. *Camtasia Studio Online Help Version 7.0* [online]. [2010] [cit. 12. května 2014]. 267 s. Dostupné z URL: http://assets.techsmith.com/Docs/pdf-camtasiaStudio/Camtasia_Studio_7_Online_Help.pdf.

[13] STEIN, William. *Introduction to Sage: History, Goals, Demo* [online]. Srpen 2010 [cit. 12. května 2014]. Dostupné z URL: http://www.vimeo.com/13986940.

[14] MAŘÍK, Robert. *Sage prakticky* [online]. 2010 [cit. 12. května 2014]. Dostupné z URL: http://user.mendelu.cz/marik/sage/.

[15] HAUPT, Martin. *Systém počítačové algebry Sage* [online]. Květen 2009 [cit. 12. května 2014]. Dostupné z URL: http://is.muni.cz/th/208258/fi_b/.

[16] BEEZER, Rob. *Sage, LaTeX and Friends* [online]. Květen 2010 [cit. 12. května 2014]. Dostupné z URL: http://www.sagenb.org/doc/static/tutorial/latex.html.

[17] GOOGLE DEVELOPERS. *Google's Python Class* [online]. Prosinec 2012 [cit. 12. května 2014]. Dostupné z URL: https://developers.google.com/edu/python/.

[18] STEIN, William. *Sage Wiki: Interact: Number Theory* [online]. Květen 2012 [cit. 12. května 2014]. Dostupné z URL: http://wiki.sagemath.org/interact/number_theory.

[19] STEIN, William. *Elementary Number Theory: Primes, Congruences, and Secrets*. Springer, Listopad 2011. 165 s. ISBN 0-387-85524-6. Dostupné z URL: http://www.wstein.org/ent/ent.pdf.

[20] LEDRU Sylvestre – DENIZET Calixte – ELIAS Antoine. *JLaTeXMath – A Java API to render LaTeX* [online]. Únor 2014 [cit. 12. května 2014]. Dostupné z URL: http://forge.scilab.org/index.php/p/jlatexmath/.

[21] NIXO-SOFT. *Java LaTeX Report* [online]. Srpen 2013 [cit. 12. května 2014]. Dostupné z URL: http://www.nixo-soft.de/en/category/Downloads/page/libs/JavaLatexReport.php.

[22] FREE SOFTWARE FOUNDATION. *GNU General Public License* [online]. Duben 2014 [cit. 12. května 2014]. Dostupné z URL: http://www.gnu.org/copyleft/gpl.html.

[23] ORACLE. *Class BigInteger* [online]. c1993–2014 [cit. 12. května 2014]. Dostupné z URL: http://docs.oracle.com/javase/7/docs/api/java/math/BigInteger.html#modPow(java.math.BigInteger,java.math.BigInteger).

Příloha A

Obsah přiloženého CD

Součástí této práce je také přiložené CD. Obsahuje veškeré materiály, které byly v rámci práce vytvořeny. Struktura souborů na CD je následovná:

```
/
├── Bakalářská práce
│   ├── img ..................................... Složka s obrázky použitými v práci
│   ├── bibliografie.bib ........................ Bibliografická databáze práce
│   ├── bp.tex ................................... Zdrojový kód práce
│   └── bp.pdf ................................... Hotová práce
├── Numbermat
│   ├── Distribuce .............................. Distribuce programu Numbermat
│   ├── Javadoc ................................. Javadoc k programu Numbermat
│   └── Zdroj ................................... Kompletní zdrojové kódy programu Numbermat
├── Sage ........................................ Pracovní listy do systému Sage
└── Video ....................................... Složka s videami a tabulemi z výpočtů
```

Soubory související s programem Numbermat jsou kromě CD rovněž dostupné na webové stránce projektu na Google Code[1].

1. https://code.google.com/p/numbermat/

Seznam obrázků

2.1 Část tabule z videa k řešení příkladu 20. *38*
3.1 Interaktivní aplikace v Sage. *49*
4.1 Ukázkové zadání a řešení vygenerovaného příkladu. *55*
4.2 Bezoutova rovnost. *59*
4.3 Eulerova funkce. *59*
4.4 Řešení lineárních kongruencí. *60*
4.5 Modulární umocňování. *62*
4.6 Legendreův symbol. *62*
4.7 Kvadratické kongruence. *64*