1. Euklidův algoritmus

Nechť $a_0 \geq a_1$ jsou dvě přirozená čísla. Připomeňme Euklidův algoritmus hledání největšího společného dělitele (NSD) čísel a_0 a a_1:

Známe-li a_{i-1} a a_i spočteme $a_{i+1} = (a_{i-1}) \bmod a_i$. Tedy víme, že existuje takové $q_i \in \mathbf{N}$ a $a_{i+1} < a_i$, že $a_{i-1} = q_i a_i + a_{i+1}$. Algoritmus skončí, když $a_{n+1} = 0$, potom $a_n = \mathrm{NSD}(a_0, a_1)$.

1.1. Najděte pomocí Euklidova algoritmu největší společný dělitel čísel 72 a 93. Najděte dále taková celá čísla x a y, aby $\mathrm{NSD}(72, 93) = x \cdot 72 + y \cdot 93$.

První část úkolu je snadná, sepišme si i jakým způsobem jednotlivé zbytky po celočíselném dělení získáme:
$a_0 = 93$,
$a_1 = 72$,
$a_2 = 93 - 72 = 21$,
$a_3 = 72 - 3 \cdot 21 = 9$,
$a_4 = 21 - 2 \cdot 9 = 3 = \mathrm{NSD}(93, 72)$
$a_5 = 0$.
Druhou část úlohy vyřešíme rovněž pomocí Euklidova algoritmu, stačí si uvědomit, že každé z čísel a_{i+1} dostaneme jako celočíselnou lineární kombinaci dvou předchozích hodnot a_{i-1} a a_i. Jednoduchou indukční úvahou zjistíme, že každé číslo a_{i+1} je celočíselnou lineární kombinaci hodnot a_0 a a_1. Konkrétně:
$a_2 = 21 = 93 - 72$,
$a_3 = 9 = 72 - 3 \cdot 21 = 72 - 3 \cdot (93 - 72) = 4 \cdot 72 - 3 \cdot 93$,
$a_4 = 3 = \mathrm{NSD}(93, 72) = 21 - 2 \cdot 9 = (93 - 72) - 2 \cdot (4 \cdot 72 - 3 \cdot 93) = 7 \cdot 93 - 9 \cdot 72$.
Zjistili jsme, že $x = -9$ a $y = 7$. □

1.2. Najděte celá čísla x a y tak, aby $x \cdot 18 + y \cdot 25 = 1$.

Protože $\mathrm{NSD}(18, 25) = 1$, zaručuje nám Euklidův algoritmus existenci požadovaných čísel $x, y \in \mathbf{Z}$. Použijeme ho tedy (podobně jako v předchozí úloze) i k jejich nalezení:
$a_0 = 25$,
$a_1 = 18$,
$a_2 = 7 = 25 - 18$,
$a_3 = 4 = 18 - 2 \cdot 7 = 18 - 2 \cdot (25 - 18) = 3 \cdot 18 - 2 \cdot 25$,
$a_4 = 3 = 7 - 4 = 25 - 18 - (3 \cdot 18 - 2 \cdot 25) = 3 \cdot 25 - 4 \cdot 18$,
$a_5 = \mathrm{NSD}(25, 18) = 1 = 4 - 3 = 3 \cdot 18 - 2 \cdot 25 - (3 \cdot 25 - 4 \cdot 18) = 7 \cdot 18 - 5 \cdot 25$. □

1.3. Najděte všechna celočíselná řešení rovnice $x \cdot 18 + y \cdot 25 = 1$.

V předchozím příkladě jsme našli jedno řešení, označme ho (x_0, y_0). Uvažujme nyní libovolné další řešení (x, y). Stejnou úvahou jako při hledání všech řešení lineárních rovnic nad tělesem dostaneme

$$(x - x_0) \cdot 18 + (y - y_0) \cdot 25 = 0.$$

Všechna racionální řešení této rovnice jsou tvaru $(q \cdot 25, -q \cdot 18)$, kde $q \in \mathbf{Q}$. Protože 25 a 18 jsou nesoudělná, tvoří celočíselné dvojice řešení dané homogenní rovnice právě dvojice $(c \cdot 25, -c \cdot 18)$ pro $c \in \mathbf{Z}$. Tedy jsme zjistili, že platí $(x - x_0) = c.25$ a $(y - y_0) = -c.18$ pro vhodné celé c, proto $\{(7 + c \cdot 25, -5 - c \cdot 18)|\ c \in \mathbf{Z}\}$ tvoří množinu všech celočíselných řešení rovnice. □

1.4. Najděte všechna celočíselná řešení rovnice $x \cdot 18 + y \cdot 25 = 10$.

Vynásobíme-li již vyřešenou rovnici $7 \cdot 18 - 5 \cdot 25 = 1$ desítkou, okamžitě vidíme, že rovnici $x \cdot 18 + y \cdot 25 = 10$ řeší $x = 10 \cdot 7 = 70$ a $y = -5 \cdot 10 = -50$. Úvaha, kterou nalezneme všechna řešení bude zcela stejná jako v předchozím příkladě (a analogická hledání řešení nehomogenní soustavy rovnic nad tělesem). Tedy množina všech celočíselných řešení rovnice je tvaru $\{(70 + c \cdot 25, -50 - c \cdot 18)|\ c \in \mathbf{Z}\}$. □

1.5. Najděte všechna celočíselná řešení rovnice $x \cdot 18 + y \cdot 24 = 10$.

Protože $\mathrm{NSD}(18, 24) = 6$, musela by pro libovolné celočíselné řešení rovnice $x \cdot 18 + y \cdot 24 = 10$ šestka dělit její levou a proto i pravou stranu. Ovšem 6 nedělí 10, proto množina všech celočíselných řešení zadané rovnice je prázdná. □

1.6. Najděte všechna celočíselná řešení rovnice $x \cdot 18 + y \cdot 24 = 12$.

Tentokrát vidíme, že $\mathrm{NSD}(18, 24)/12$, můžeme tedy celou rovnici vydělit hodnotou $\mathrm{NSD}(18, 24)$ $(= 6)$ a řešit upravenou rovnici $x \cdot 3 + y \cdot 4 = 2$. Snadno nahlédneme, že $(2, -1)$ je jedním řešením rovnice, a protože jsou čísla 3 a 4 nesoudělná, je množina všech celočíselných řešení tvaru $\{(2 + c \cdot 4, -1 - c \cdot 3)|\ c \in \mathbf{Z}\}$. □

1.7. Najděte všechna celočíselná řešení rovnice $x \cdot 18 - y \cdot 24 + 6 = 0$.

Obvyklým způsobem zjistíme, že , že $-1 \cdot 18 + 1 \cdot 24 = 6$, což snadno upravíme na tvar $1 \cdot 18 - 1 \cdot 24 + 6 = 0$. Našli jsme tedy jedno řešení $(1, 1)$ diofantické rovnice. Nyní obvyklou lineárně algebraickou úvahou najdeme celočíselná řešení homogenní soustavy $x \cdot 18 - y \cdot 24 = 0$, jíž jsou právě celočíselné násobky vektoru $(4, 3)$, tedy množina všech celočíselných řešení tvaru $\{(1 + c \cdot 4, 1 + c \cdot 3)|\ c \in \mathbf{Z}\}$. □

Pozorování 1.8. V předchozích úlohách jsme našli obecně fungující algoritmus, pro popis množiny všech celočíselných řešení (tzv. lineární diofantické) rovnice $ax + by = c$, kde $a, b, c \in \mathbf{N}$. Nejprve najdeme Euklidovým algoritmem $\mathrm{NSD}(a, b)$. Jestliže $\mathrm{NSD}(a, b)/c$, najdeme rozšířeným Euklidovým algoritmem jedno řešení (x_0, y_0) a množina všech celočíselných řešení je tvaru $\{(x_0 + \frac{b \cdot c}{\mathrm{NSD}(a,b)}, y_0 - \frac{a \cdot c}{\mathrm{NSD}(a,b)})|\ c \in \mathbf{Z}\}$. Jestliže $\mathrm{NSD}(a, b)$ nedělí c, je množina všech řešení prázdná.

8.10./12.10.

Připomeňme, že *prvočíslem* rozumíme každé přirozené číslo $p > 1$ splňující pro všechna přirozená a, b podmínku $p = a.b \Rightarrow p = a$ nebo $p = a$.

1.9. Dokažte, že lze každé přirozené číslo $n > 1$ napsat jako součin prvočísel.

Dokážeme snadno indukcí podle n. Číslo 2 je zřejmě prvočíslo. Pokud n není prvočíslo existují taková přirozená čísla $k,\ l < n$, že $n = k \cdot l$. Obě jsou samozřejmě větší než jedna a podle indukčního předpokladu máme prvočíselný rozklad čísel $k = p_1 \cdot \ldots \cdot p_r$ a $l = q_1 \cdot \ldots \cdot q_s$. Tedy číslo n je součinem prvočísel $p_1 \cdot \ldots \cdot p_r \cdot q_1 \cdot \ldots \cdot q_s$. □

1.10. Dokažte, že přirozené číslo a_n z popisu Euklidova algoritmu je rovno právě $\mathrm{NSD}(a_0, a_1)$.

Indukcí podle i dokážeme rovnost $\mathrm{NSD}(a_i, a_{i+1}) = \mathrm{NSD}(a_{i-1}, a_i)$. Položme $c = \mathrm{NSD}(a_{i-1}, a_i)$ a $d = \mathrm{NSD}(a_i, a_{i+1})$. Protože d/a_i i d/a_{i+1}, d dělí i $a_{i-1} = q_i \cdot a_i + a_{i+1}$, proto $d \leq c$. Podobně nahlédneme, že c/a_i i $c/a_{i-1} = q_i \cdot a_i + a_{i+1}$ tedy $c \leq d$ a $c = d$. Protože a_n/a_{n-1}, vidíme, že $a_n = \mathrm{NSD}(a_{n-1}, a_n)$, a tudíž $a_n = \mathrm{NSD}(a_n, a_{n-1}) = \mathrm{NSD}(a_{n-1}, a_{n-2}) = \cdots = \mathrm{NSD}(a_0, a_1)$. □

1.11. Definujme posloupnosti x_i a y_i tak, že $x_0 = y_1 = 1$, $x_1 = y_0 = 0$, a pro $i \geq 1$ položme $x_{i+1} = x_{i-1} - x_i \cdot q_i$ a $y_{i+1} = y_{i-1} - y_i \cdot q_i$, kde $a_{i-1} = a_i \cdot q_i + a_{i+1}$. Dokažte, že $a_i = x_i \cdot a_0 + y_i \cdot a_1$, a proto $x_n \cdot a_0 + y_n \cdot a_1$ je $\mathrm{NSD}(a_0, a_1)$.

Ověříme indukcí podle i. Zřejmě tvrzení platí pro $i = 0$ a $i = 1$.

Předpokládejme, že tvrzení platí pro i a $i - 1$, tedy $a_i = x_i \cdot a_0 + y_i \cdot a_1$ a $a_{i-1} = x_{i-1} \cdot a_0 + y_{i-1} \cdot a_1$, a dokážeme ho pro $i + 1$. Dosadíme za a_i a a_{i-1} do vztahu

$$a_{i+1} = a_{i-1} - a_i \cdot q_i = (x_{i-1} \cdot a_0 + y_{i-1} \cdot a_1) - (x_i \cdot a_0 + y_i \cdot a_1) \cdot q_i =$$

$$= (x_{i-1} - x_i \cdot q_i) \cdot a_0 + (y_{i-1} - y_i \cdot q_i) \cdot a_1 = x_{i+1} \cdot a_0 + y_{i+1} \cdot a_1,$$

čímž jsme dokončili důkaz. □

1.12. Ověřte , že přirozené číslo p je prvočíslem právě tehdy, platí-li pro všechna přirozená a, b implikace $p/a \cdot b \Rightarrow p/a$ nebo p/b.

Nejprve předpokládejme, že p je prvočíslo a zvolíme libovolná přirozená a, b, pro něž $p/a \cdot b$. Protože $\mathrm{NSD}(p, a) = 1$ (p má pouze dělitele 1 a p), existují díky úvaze Příkladu 1.10 a 1.11 taková celá x a y, že $1 = a \cdot x + p \cdot y$. Proto $b = abx + pby$. Protože p dělí abx i pby, platí, že p/b.

Naopak, nechť pro přirozené číslo p a všechna přirozená a, b platí, že $p/a \cdot b \Rightarrow p/a$ nebo p/b, a položme $p = a \cdot b$. Potom a/p i b/p, tedy $a \leq p$ a $b \leq p$ a navíc $p = a \cdot b/a \cdot b$. Využijeme-li náš předpoklad, pak buď p/a, proto $p \leq a$ a následně $p = a$ nebo p/b, a tudíž $p = b$, čímž jsme dokázali obrácenou implikaci dokazované ekvivalence. □

1.13. Dokažte pro každé prvočísl p a pro všechna přirozená $a_1, a_2, \ldots, a_k$ platí implikace $p/a_1 a_2 \ldots a_k \Rightarrow$ existuje takové i, že p/a_i.

Indukční rozšíření předchozího pozorování. □

1.14. Dokažte, že je prvočíselný rozklad přirozeného čísla určen jednoznačně až na pořadí prvočísel.

Dokážeme tvrzení pro přirozené číslo n indukcí podle n. Je-li n prvočíslo (speciálně $n = 2$), je prvočíselný rozklad zřejmě určen jednoznačně. Platí-li tvrzení pro všechna $k < n$ a $n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot p_s$ jsou dva prvočíselné rozklady, potom podle tvrzení 1.13 existuje takové j, že p_1/q_j. Bez újmy na obecnosti můžeme předpokládat, že $j = 1$. Protože p_1 i q_1 jsou prvočísla, máme $p_1 = q_1$. Nyní stačí použít indukční předpoklad pro $p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot p_s < n$. □

15.10./19.10.

2. Monoidy

Připomeňme, že prvek s monoidu $(S, \cdot, 1)$ je (oboustranně) *invertibilní*, existuje-li takový prvek $s^{-1} \in S$, že $s^{-1} \cdot s = s \cdot s^{-1} = 1$. Prvek s^{-1} nazveme *inverzním prvkem* prvku s.

2.1. Dokažte, že množina všech invertibilních prvků monidu $(G, \cdot, 1)$ tvoří jeho podmonoid.

Vezmeme-li prvky g_1 a g_2 z G^*, platí, že existují prvky $h_1, h_2 \in G$, pro něž $g_i h_i = h_i g_i = 1$, kde $i = 1, 2$. Tedy $(g_1 g_2)(h_2 h_1) = g_1(g_2 h_2)h_1 = g_1 1 h_1 = g_1 h_1 = 1$ a symetricky $(h_2 h_1)(g_1 g_2) = 1$. Zřejmě $1 \cdot 1 = 1$, proto G^* obsahuje prvek 1. Tedy G^* je podmonoid monidu $(G, \cdot, 1)$. □

2.2. Nechť $(G, \cdot, 1)$ je monoid a G^* podmonoid všech jeho invertibilních prvků. Označme $\cdot_{G^*}$ restrikci operace $\cdot$ na množinu $G^* \times G^*$ a definujeme unární operaci $^{-1}$ tak, že a^{-1} je právě inverzní prvek pro každé $a \in G^*$. Ověřte, že $(G^*, \cdot_{G^*}, ^{-1}, 1)$ je grupa.

V úloze 2.1 jsme dokázali, že G^* je podmonoidem monoidu $G(\cdot, 1)$. Vezmeme-li operaci omezenou na tento podmonoid $\cdot|_{G^* \times G^*}$, je $(G^*, \cdot_{G^*}, 1)$ monoid. Protože víme, že inverzní prvek je díky asociativitě operace určen jednoznačně a množina G^* je na operaci inverzního prvku uzavřena, $(G^*, \cdot_{G^*}, ^{-1}, 1)$ splňuje všechny axiomy grupy. □

2.3. Uvažujme monoid $(\mathbf{Z}_n, \cdot, 1)$ s operací $\cdot$ definovanou jako násobení modulo n. Označme $\mathbf{Z}_n^*$ množinu všech invertibilních prvků tohoto momoidu. Dokažte, že $\mathbf{Z}_n^* = \{k \in \mathbf{Z}_n | \text{ NSD}(k, n) = 1\}$.

Stačí si uvědomit, že $k \in \mathbf{Z}_n$ je invertibilní právě tehdy, když existuje m takové, že $(k \cdot m) \text{mod } n = 1$. Jestliže $\text{NSD}(k, n) = 1$, umíme pomocí Euklidova algoritmu najít $x \in \mathbf{Z}_n$ a celé y, aby $kx + ny = 1$, tedy hledané $m = (x) \text{mod } n$. Naopak, jestliže $\text{NSD}(k, n) = c > 1$, pak pro libovolné m je buď $(km) \text{mod } n = 0$ nebo $c/(km) \text{mod } n$. Tím jsme ověřili, že $\mathbf{Z}_n^* = \{k < n | \text{ NSD}(k, n) = 1\}$. □

2.4. Nechť p je prvočíslo a k přirozené číslo. Určete počet invertibilních prvků monidu $(\mathbf{Z}_{p^k}, \cdot, 1)$.

Číslo menší než p^k je soudělné s p^k, právě když je násobkem čísla p. Nezáporných násobků čísla p menších než p^k je zřejmě právě p^{k-1}. To znamená, že naopak čísel nesoudělných s p^k máme $|\mathbf{Z}^*_{p^k}| = |Z_{p^k}| - p^{k-1} = p^k - p^{k-1} = (p-1)p^{k-1}$. □

Zobrazení $\varphi : \mathbf{N} \to \mathbf{N}$ dané předpisem $\varphi(n) = |\{k < n |\ k \in \mathbf{N},\ \mathrm{NSD}(k, n) = 1\}|$ nazveme *Eulerovou funkcí.*

2.5. Ověřte, že $\varphi(n)$ udává počet invertibilních prvků monidu $(\mathbf{Z}_n, \cdot, 1)$.

Tvrzení plyne okamžitě z úlohy 2.3 a definice Eulerovy funkce. □

Uvažujme monoidy $(M_j, \cdot, 1)$ pro $j = 1, \dots, k$ a definujme na kartézském součinu $(\prod_{j=1}^k M_i, \cdot, (1, \dots, 1))$ po složkách operaci $\odot$, tj.

$$(m_1, \dots, m_k) \odot (n_1, \dots, n_k) = (m_1 \cdot n_1, \dots, m_k \cdot n_k).$$

2.6. Ověřte, že $\mathcal{M} = (\prod_{j=1}^k M_i, \cdot, (1, \dots, 1))$ je opět monoid a že prvek $(m_1, \dots, m_k)$ monoidu $\mathcal{M}$ je invertibilní, právě když jsou všechny prvky m_j, $j = 1, \dots, k$ invertibilní.

Vezměme $(m_1, \dots, m_k), (n_1, \dots, n_k), (r_1, \dots, r_k) \in M$. Pak

$$(m_1, \dots, m_k) \odot ((n_1, \dots, n_k) \odot (r_1, \dots, r_k)) = (m_1, \dots, m_k) \odot (n_1 \cdot r_1, \dots, n_k \cdot r_k) =$$
$$= (m_1 \cdot (n_1 \cdot r_1), \dots, m_k \cdot (n_k \cdot r_k)) = ((m_1 \cdot n_1) \cdot r_1, \dots, (m_k \cdot n_k) \cdot r_k) =$$
$$= (m_1 \cdot n_1, \dots, m_k \cdot n_k) \odot (r_1, \dots, r_k) = ((m_1, \dots, m_k) \odot (n_1, \dots, n_k)) \odot (r_1, \dots, r_k)$$

a

$$(m_1, \dots, m_k) \odot (1, \dots, 1) = (m_1, \dots, m_k) = (1, \dots, 1) \odot (m_1, \dots, m_k),$$

čímž jsme ověřili, že je $\mathcal{M}$ monoid. Nyní stačí uvážit, kdy existuje prvek $(r_1, \dots, r_k)$, pro který

$$(m_1, m_2, \dots, m_k) \odot (r_1, r_2, \dots, r_k) = (m_1 \cdot r_1, m_2 \cdot r_2, \dots, m_k \cdot r_k) = (1, 1, \dots, 1)$$

a

$$(r_1, r_2, \dots, r_k) \odot (m_1, m_2, \dots, m_k) = (r_1 \cdot m_1, r_2 \cdot m_2, \dots, r_k \cdot m_k) = (1, 1, \dots, 1).$$

□

2.7 (Čínská věta o zbytcích)**.** Nechť $n_1, n_2, \dots, n_k$ jsou po dvou nesoudělná kladná celá čísla a $n = n_1 \cdot n_2 \cdot \dots \cdot n_k$, Dokažte, že zobrazení $f : \mathbf{Z}_n \to \prod_{i=1}^k \mathbf{Z}_{n_i}$ dané předpisem $f(x) = (x \bmod n_1,\ x \bmod n_2, \dots, x \bmod n_k)$ je izomorfismus grup $(\mathbf{Z}_n, +, -, 0)$ a $(\prod_{i=1}^k \mathbf{Z}_{n_i}, +, -, \mathbf{0})$ a monoidů $(\mathbf{Z}_n, \cdot, 1)$ a $(\prod_{i=1}^k \mathbf{Z}_{n_i}, \cdot, \mathbf{1})$.

Přímo z definice snadno vidíme, že je f zobrazení slučitelné se všemi operacemi. Zbývá nahlédnout, že jde o bijekci. Protože jsou $\mathbf{Z}_n$ a $\prod_{i=1}^k \mathbf{Z}_{n_i}$ stejně velké konečné množiny, stačí nahlédnout, že je f prosté. Nechť pro $a \leq b \in \mathbf{Z}_n$ platí, že $f(a) = f(b)$. Potom $f(b-a) = 0$, tedy $n_i / b - a$ pro všechna $i = 1, \dots, k$. Protože jsou n_i po dvou nesoudělná a $0 \leq b - a \leq n - 1$, máme i $n / b - a$, tudíž $b = a$. □

22.10./26.10.

2.8. Uvažujme zobrazení $f : \mathbf{Z}_{45} \to \mathbf{Z}_5 \times \mathbf{Z}_9$ z 2.7, tj.$f(a) = (a \bmod 5, a \bmod 9)$. Určete (jednoznačně určené) $a \in \mathbf{Z}_{45}$, pro které $f(a) = (3, 2)$.

Hledáme $a \in \mathbf{Z}_{45}$ pro něž existují taková $x \in \mathbf{Z}_9$ a $y \in \mathbf{Z}_5$, že $5x + 3 = a$ a $9y + 2 = a$, tedy musí platit $5x + 3 = 9y + 2$. Upravíme-li rovnici na tvar $9y - 5x = 1$, řešíme obvyklou úlohu. Snadno zjistíme, že $9 \cdot 4 - 5 \cdot 7 = 1$, tedy $a = 5 \cdot 7 + 3 = 9 \cdot 4 + 3 = 38$. □

2.9. Uvažujme zobrazení $f : \mathbf{Z}_{720} \to \mathbf{Z}_5 \times \mathbf{Z}_9 \times \mathbf{Z}_{16}$ z 2.7. Najděte $b \in \mathbf{Z}_{720}$, pro které $f(b) = (3, 2, 13)$.

Definujme zobrazení $g : \mathbf{Z}_{45} \times \mathbf{Z}_{16} \to \mathbf{Z}_5 \times \mathbf{Z}_9 \times \mathbf{Z}_{16}$ předpisem $g(u, v) = (u \bmod 5, u \bmod 9, v)$ a zobrazení $h : \mathbf{Z}_{720} \to \mathbf{Z}_{45} \times \mathbf{Z}_{16}$ z Čínské věty o zbytcích, tj. $h(w) = (w \bmod 45, w \bmod 16)$. Všimněme si, že $f = gh$, navíc jsou obě zobrazení g a h bijekce a $f^{-1}(3, 2, 13) = h^{-1}(g^{-1}(3, 2, 13))$. Protože je zobrazení g součinem bijekce z 2.7 a identity a vzor dvojice $(3, 2)$ už jsme spočítali v předchozí úloze, vidíme, že $g^{-1}(3, 2, 13) = (38, 13)$. Zbývá nám tedy stejnou úvahou jako v předchozím příkladu najít vzor $h^{-1}(38, 13)$, tj. vyřešit rovnice $45x + 38 = b$ a $16y + 13 = b$ pomocí diofantické rovnice $16y - 45x + = 25$. Obvyklým způsobem zjistíme například, že $5 \cdot 45 - 14 \cdot 16 = 1$, proto $25 = 125 \cdot 45 - 350 \cdot 16 = 10 \cdot 16 - 3 \cdot 45$. Tedy $b = 45 \cdot 3 + 38 = 16 \cdot 10 + 13 = 173$. □

2.10. Buď $p_1 < p_2 < \cdots < p_k$ prvočísla a $r_1, r_2, \ldots, r_k$ kladná celá čísla. Dokažte, že $\varphi(\prod_{i=1}^k p_i^{r_i}) = \prod_{i=1}^k \varphi(p_i^{r_i}) = \prod_{i=1}^k (p_i - 1)p_i^{r_i - 1}$.

Položme pro přehlednost $n_i = p_i^{r_i}$ a $n = \prod_{i=1}^k n_i$. Protože čísla n_i a n_j jsou pro všechna $i \neq j$ nesoudělná, můžeme využít úlohu 2.7, podle níž jsou monoidy $(\mathbf{Z}_n, \cdot, 1)$ a $(\prod_{i=1}^k \mathbf{Z}_{n_i}, \cdot, (1, \ldots, 1)$ izomorfní, proto mají stejné počty invertibilních prvků. Použijeme-li dále 2.6 dostáváme: $\varphi(n) = |(\mathbf{Z}_n^*| = |\prod_{i=1}^k \mathbf{Z}_{n_i}^*| = \prod_{i=1}^k |\mathbf{Z}_{n_i}^*| = \prod_{i=1}^k \varphi(n_i) = \prod_{i=1}^k \varphi(p_i^{r_i})$. Konečně poslední rovnost dostáváme z úloh 2.4 a 2.5. □

2.11. Určete počet invertibilních prvků monoidu $(\mathbf{Z}_{1352}, \cdot, 1)$.

Podle 2.3 potřebujeme určit hodnotu $\varphi(1352)$ Eulerovy funkce na prvku 1352. Prvočíselný rozklad čísla 1352 je $2^3 \cdot 13^2$ a z 2.10 dostáváme, že $|\mathbf{Z}_{1352}^*| = \varphi(1352) = (13 - 1) \cdot 13^1 \cdot (2 - 1) \cdot 2^2 = 624$. □

2.12. Rozhodněte, zda jsou izomorfní monoidy $(\mathbf{Z}_4, +, 0)$ a $(\mathbf{Z}_8^*, \cdot, 1)$.

Stačí si rozmyslet, že pro všechny prvky a ze $\mathbf{Z}_8^* = \{1, 3, 5, 7\}$ platí $a \cdot a = 1$. V monoidu $(\mathbf{Z}_4, +, 0)$ máme $3 + 3 = 2$, což je různé od neutrálního prvku 0, tedy monoidy nejsou izomorfní. □

2.13. Rozhodněte, zda jsou izomorfní monoidy $(\mathbf{Z}_2 \times \mathbf{Z}_2, +, 0)$ a $(\mathbf{Z}_8^*, \cdot, 1)$.

Sestrojíme-li bijekci $g : \mathbf{Z}_2 \times \mathbf{Z}_2 \to \mathbf{Z}_8^*$ výčtem $g((0, 0)) = 1$, $g((0, 1)) = 3$, $g((1, 0)) = 5$ a $g((1, 1)) = 7$, snadno ověříme, že se jedná o homomorfismus, tedy dané monoidy jsou izomorfní. □

2.11./5.11.

3. Grupy

3.1. Nechť p a s jsou permutace z grupy S_n a nechť $p(a) = b$, kde $a, b \in \{1, \dots, n\}$. Dokažte, že $[sps^{-1}](s(a)) = s(b)$.

Důkaz tvrzení je zcela přímočarý. Důležitým důsledkem je ovšem pozorování, že permutace p a sps^{-1} mají stejný počet stejných cyklů, neboť jsme právě dokázali, že

$$s \circ [\dots (\dots ab \dots) \dots] \circ s^{-1} = \dots (\dots s(a)s(b) \dots) \dots .$$

$\square$

3.2. Mějme $p = (1346)(27)(589)$ a $q = (16)(29)(345)$ dvě permutace z grupy S_9. Spočítejte hodnoty pqp^{-1} a qpq^{-1}.

Postupujeme podle předchozího pozorování:

$$[(1346)(27)(589)] \circ [(16)(29)(345)] \circ [(1346)(27)(589)]^{-1} = (31)(75)(468)$$

a

$$[(16)(29)(345)] \circ [(1346)(27)(589)] \circ [(16)(29)(345)]^{-1} = (6451)(97)(382).$$

$\square$

3.3. Mějme permutace $p_1 = (126)(37)(458)$ a $p_2 = (12)(345)(678)$ z grupy S_8. Rozhodněte, zda jsou permutace p_1 a p_2 konjugované, tj. zda existuje permutace $q \in S_8$ s vlastností $qp_1q^{-1} = p_2$ a případně takovou permutaci q najděte.

Využijeme opačný postup k postupu v předchozím příkladu. Obě permutace jsou stejného typu (což je zřejmě nutná podmínka, aby permutace q existovala). Seřaďme stejnými n-cykly pod sebe, například:

$$\begin{matrix} (126)(37)(458) \\ (345)(12)(678) \end{matrix}$$

Zřejmě potom permutace $q = (13)(24657)(8)$ splňuje podmínku $qp_1q^{-1} = p_2$. $\square$

3.4. Ověřte, že alternující grupa na čtyřech prvcích A_4 neobsahuje žádnou podgrupu řádu 6.

Uvědomme si, že $A_4 = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$. Předpoládejme, že máme podgrupu H řádu alespoň 6. To určitě znamená, že H obsahuje alespoň dva trojcykly, tj. permutace tvaru (abc), bez újmy na obecnosti můžeme předpokládat, že A_4 obsahuje trojcyklus (123). Podle Lagrangeovy věty je index podgrupy H v grupě A_4 nejvýše 2. Využijeme-li Příkladu 1.37(1) a (2) z přednášky, vidíme, že jak podgrupa indexu 1, tak podgrupa indexu 2 je normální, proto je H normální podgrupa A_4. To ovšem znamená, že $p(123)p^{-1} = (p(1)p(2)p(3)) \in H$ pro každé $p \in A_4$. Nyní snadno spočítáme, že

$$(214) = (12)(34) \circ (123) \circ ((12)(34))^{-1},$$

$$(341) = (13)(24) \circ (123) \circ ((13)(24))^{-1},$$

$$(432) = (14)(23) \circ (123) \circ ((14)(23))^{-1}.$$

Protože je H normální podgrupa, leží (214), (341) i (432) v H, navíc v H leží i inverzní permutace (124), (143) a (243), tedy H obsahuje více než 6 prvků. Z Lagrangeovy věty už plyne, že $|H| = 12$, proto $H = A_4$. □

3.5. Ověřte, že pro každý prvek g konečné grupy G platí, že $g^{|G|} = 1$.

Z Poznámky 1.32 okamžitě plyne, že $g^{|\langle g\rangle|} = 1$. Nyní stčí použít Lagrangeovu větu a pozorování, že $(g^a)^b = g^{ab}$ pro všechna $a, b \in \mathbf{N}$. Proto $g^{|G|} = (g^{|\langle g\rangle|})^{\frac{|G|}{|\langle g\rangle|}} = 1^{\frac{|G|}{|\langle g\rangle|}} = 1$. □

3.6. [Malá Fermatova věta] Dokažte, že pro každé a nesoudělné s n platí, že $(a^{\varphi(n)})\mathrm{mod} n = 1$.

Stačí vzít jako grupu G z předchozího příkladu grupu invertibillních prvků monoidu $(\mathbf{Z}_n, \cdot, 1)$ tj. prvků nesoudělných s n. □

Připomeňme, že $(G, \cdot, ^{-1}, 1)$ je cyklická grupa, existuje-li její prvek g, pro nějž $\langle g\rangle = G$, tj. jednoprvková množina $\{g\}$ generuje celou nosnou množinu grupy. Všimněme si, že $\langle g\rangle = \{g^n |\ n \in \mathbf{Z}\}$, kde $g^0 = 1$, $g^n = g \cdot g^{n-1}$ pro $n > 0$ a $g^n = (g^{-1})^{|n|}$ pro $n < 0$.

9.11./12.11.

3.7. Spočítejte $(53^{65})\mathrm{mod}120$.

Díky Malé Fermatově větě víme, že $(53^{\varphi(120)})\mathrm{mod}120 = (53^{32})\mathrm{mod}120 = 1$. Tedy$(53^{65})\mathrm{mod}120 = (((53^{32})^2)\mathrm{mod}120 \cdot 53)\mathrm{mod}120 = 1 \cdot 53 = 53$. □

3.8. Nechť $(G, \cdot, ^{-1}, 1)$ je grupa, H její podgrupa řádu 70 a K její podgrupa řádu 16. Určete počet prvků G, vite-li, že $|G| < 1000$, a rozhodněte, zda je průnik $H \cap K$ nutně komutativní grupa.

Podle Lagrangeovy věty musí řád podgrup H i K dělit $|G|$, proto $70/|G|$ a $16/|G|$ a tudíž $560 = \mathrm{nsn}(70, 16)/|G|$. Protože $|G| < 1000$, máme $|G| = 560$.

Zabývejme se nyní grupou $H \cap K$. Opět použijeme Lagrangeovu větu, tentokrát pro $H \cap K$ jako podgrupu grupy H i K. Velikost průniku $H \cap K$, proto musí dělit řád obou grup H i K, tedy $|H \cap K|/\mathrm{NSD}(70, 16) = 2$. Proto je průnik $H \cap K$ jednoprvková nebo dvouprvková, tedy v obou případech komutativní grupa. □

3.9. Najděte nějakou grupu, která by měla 560 prvků a obsahovala podgrupy řádu 70 a 16.

Stačí, abychom vzali grupu $(\mathbf{Z}_{560}, +, -, 0)$. Její podgrupou řádu 70 je cyklická grupa $\langle 8\rangle$ a podgrupou řádu 16 cyklická grupa $\langle 35\rangle$. □

3.10. Popište množinu generátorů cyklické grupy $(\mathbf{Z}_n, +, -, 0)$.

Uvědomme si, že číslo k je generátorem právě tehdy, když podgrupa $\langle k\rangle$ obsahuje prvek 1 a to nastává právě tehdy, když je $\mathrm{NSD}(k,n)=1$. Vidíme, že množinu generátorů cyklické grupy $(\mathbf{Z}_n,+,-,0)$ tvoří právě invertibilní prvky monoidu $(\mathbf{Z}_n,\cdot,1)$. □

3.11. Určete počet generátorů cyklické grupy $(\mathbf{Z}_{50},+,-,0)$.

Podle úvahy z 3.10 a popisu množiny invertibilních prvků monoidu $(\mathbf{Z}_n,\cdot,1)$ úlohy 2.10 potřebujeme určit hodnotu Eulerovy funkce na prvku 50. Prvočíselný rozklad čísla 50 je $5^2\cdot 2$, proto $\varphi(50)=(5-1)\cdot 5^1\cdot(2-1)=20$. □

3.12. Určete počet generátorů cyklické grupy řádu 81.

Uvážíme-li, že cyklická grupa řádu 81 je izomorfní grupě $(\mathbf{Z}_{81},+,-,0)$, postujpujeme stejně jako v předchozím příkladu: prvočíelný rozklad čísla 81 je 3^4, tedy počet generátorů cyklické grupy řádu 81 je $\varphi(81)=(3-1)\cdot 3^3=54$. □

3.13. Nechť G je konečná cyklická grupa, $|G|=n$, a nechť k dělí n. Ukažte, že existuje právě jedna podgrupa grupy G, která má k prvků.

K důkazu využijeme charakterizace cyklických grup (Důsledek 1.47 z přednášky), díky němuž stačí tvrzení dokázat pro (izomorfní) grupu $(\mathbf{Z}_n,+,-,0)$. Jestliže $k=1$, je tvrzení triviální, předpokládejme tedy, že $k>1$, a položme $a=\frac{n}{k}$. Potom snadno nahlédneme, že $\langle a\rangle=\{0,a,2a,\dots,(k-1)a\}$, tudíž $|\langle a\rangle|=k$. Mějme nyní nějakou podgrupu H řádu k grupy $\mathbf{Z}_n$. Podle Lagrangeovy věty (Věta 1.29 z přednášky) řád grupy $\langle h\rangle$ dělí k pro každý prvek $h\in H$, proto $(k\cdot h)\mathrm{mod}n=0$. Tudíž $k\cdot h=c\cdot n$ pro vhodné celé číslo c, tedy $h=\frac{c\cdot n}{k}=c\cdot a$. Tím jsme ověřili, že H je částí podgrupy $\langle a\rangle$. Protože se ovšem jedná o dvě konečné stejně velké množiny dostáváme, že $H=\langle a\rangle$, čímž jsme ověřili jednoznačnost volby. □

3.14. Kolik podgrup obsahuje cyklická grupa řádu 98?

Využijeme úvahu úlohy 3.13: každému děliteli řádu cyklické grupy odpovídá právě jedna její podgrupa. Potřebujeme tedy jen spočítat dělitele čísla 98, kterých je 6 (tj. $1,2,7,14,49,98$). □

16.11./19.11.

Zvolme pro následující úvahy p a q dvě různá lichá prvočísla a položme $m=\mathrm{nsn}(p-1,q-1)$.

3.15. Dokažte, že pro každé nezáporné celé číslo x platí rovnosti $(x^{m+1})\mathrm{mod}p=(x)\mathrm{mod}p$ a $(x^{m+1})\mathrm{mod}q=(x)\mathrm{mod}q$.

Tvrzení samozřejmě stačí dokázat jen pro prvočíslo p.

Předně zvolme x a uvědomme si, že $x=x_0+p\cdot\alpha$ pro vhodné $x_0\in Z_p$ a α celé nezáporné, což znamená, že $x_0=(x)\mathrm{mod}p$. Proto

$$(x^{m+1})\mathrm{mod}p=(x_0^{m+1}+p\cdot(\dots))\mathrm{mod}p=(x_0^{m+1})\mathrm{mod}p.$$

Z 3.6 dostáváme, že $(x_0^{m+1})\mathrm{mod}p=x_0$ pro nenulové x_0 a pro $x_0=0$ je tvrzení triviální. Tedy $(x^{m+1})\mathrm{mod}p=x_0=(x)\mathrm{mod}p$. □

3.16. Dokažte, že pro každé $x \in \mathbf{Z}_{pq}$ platí rovnosti $(x^{m+1})\mathrm{mod} pq = x$.

Tentokrát využijeme 2.7 pro (bijekci) $f : \mathbf{Z}_{pq} \to \mathbf{Z}_p \times \mathbf{Z}_q$. Protože podle předchozí úlohy máme $f(x^{m+1}) = f(x)$ jsou v monoidu $(\mathbf{Z}_{pq}, \cdot, 1)$ hodnoty x^{m+1} a x stejné, což je právě tvrzení, jež jsme měli dokázat. □

3.17 (Rivest, Shamir, Adleman)**.** Zvolme $e < m$ nesoudělné s m a pak (například pomocí Euklidova algoritmu) najdeme takové $d < m$, že $(ed)\mathrm{mod} m = 1$. Nyní pro každé $a \in \mathbf{Z}_{pq}$ platí, že $(a^e)^d = a^{ed} = a^{um+1} = a$ (počítáno v $\mathbf{Z}_{pq}$, tedy modulo pq).

Pomocí vlastnosti čísel p, q, m, d, e můžeme nyní popsat protokol asymetrického šifrování známý pod zkratkou RSA. Položíme-li $n = p \cdot q$, je veřejným klíčem je dvojice čísel (pq, e) a soukromý klíč tvoří *tajný exponent d*. Chceme-li informaci vyjádřenou posloupností hodnot $a_1, \dots, a_k \in \mathbf{Z}_{pq}$ adresovat majiteli soukromého klíče, stačí ji zašifrovat pomocí mocnění veřejně známou hodnotou e v monoidu $\mathbf{Z}_{pq}(\cdot, 1)$, tj. odeslat zprávu $(a_1^e)\mathrm{mod} pq, \dots, (a_k^e)\mathrm{mod} pq$. K jejímu rozluštění stačí umocnit v $\mathbf{Z}_{pq}(\cdot, 1)$ pomocí tajného exponentu, protože $(a_i^e)^d = a_i^{ed} = a_i$. Naopak, zveřejnění-li majitel soukromého klíče zašifrovanou zprávu $(a_1^d) mod\ pq, \dots,$ $(a_k^d) mod\ pq$, mohou si příjemci zprávy stejným způsobem (tj. umocněním na veřejně známý exponent e: $((a_1^d)^e) mod\ pq, \dots, ((a_k^d)^e) mod\ pq = a_1, \dots, a_k$) ověřit, že odesilatel zprávy opravdu zná tajný exponent.

Poznamenejme, že je ze znalosti n a e obtížné najít d (odpovídá to nalezení prvočíselného rozkladu čísla n, což je úloha, pro níž není znám algoritmus polynomiální složitosti), zatímco mocnění čísel v $\mathbf{Z}_{pq}$ je (i pro velké exponenty a velké pq) velmi snadné a rychlé.

Další úlohy

(1) Najděte všechna celočíselná řešení rovnice $324 \cdot x + 88 \cdot y = c$ postupně pro $c = 0, 2, 88, -4, -88$.
(2) Najděte všechna celočíselná řešení rovnice $15 \cdot x - 44 \cdot y = c$ postupně pro $c = 1, 2, -2$.
(3) Najděte (všechna) celočíselná řešení rovnice $15 \cdot x + 18 \cdot y + 10 \cdot z = 1$.
(4) Spočítejte v tělese $\mathbf{Z}_{83}$ hodnoty 15^{-1} a $(3^{-1} + 6 \cdot 53^{-1})^{-1}$.
(5) Vyřešte v tělese $\mathbf{Z}_{97}$ rovnici $7^{-1} \cdot x = 51^{-1}$.
(6) Ověřte, že algoritmus popsaný v Pozorování 1.8 pracuje správně.
(7) Dokažte pro všechna kladná celá čísla a, b platí, že $\mathrm{nsn}(a, b) = \frac{a \cdot b}{NSD(a,b)}$.
(8) Najděte $a \in \mathbf{Z}_{315}$, o kterém víte, že $(a)\mathrm{mod}5 = 3$, $(a)\mathrm{mod}7 = 4$, $(a)\mathrm{mod}9 = 5$.
(9) Najděte $a \in \mathbf{Z}_{2520}$, o kterém víte, že $(a)\mathrm{mod}8 = 1$ $(a)\mathrm{mod}5 = 3$, $(a)\mathrm{mod}7 = 4$, $(a)\mathrm{mod}9 = 5$.
(10) Najděte $a \in \mathbf{Z}_{630}$, o kterém víte, že $(a)\mathrm{mod}2 = 1$ $(a)\mathrm{mod}5 = 3$, $(a)\mathrm{mod}7 = 4$, $(a)\mathrm{mod}9 = 5$.
(11) Rozhodněte, zda existuje $a \in \mathbf{Z}_{999}$ splňující podmínku, že $(a)\mathrm{mod}9 = 5$ $(a)\mathrm{mod}3 = 2$, $(a)\mathrm{mod}11 = 4$.
(12) Rozhodněte, zda existuje $a \in \mathbf{Z}_{999}$ splňující podmínku, že $(a)\mathrm{mod}9 = 5$ $(a)\mathrm{mod}3 = 2$, $(a)\mathrm{mod}37 = 4$.

(13) Popište obor hodnot zobrazení $\beta : \mathbf{Z}_{300} \to \mathbf{Z}_{20} \times \mathbf{Z}_{15}$ daného předpisem $\beta(a) = ((a)\mathrm{mod}20, (a)\mathrm{mod}15)$.
(14) Rozhodněte, zda jsou izomorfní grupy $(\mathbf{Z}_4, +, -, 0)$ a $(\mathbf{Z}_2 \times \mathbf{Z}_2, +, -, 0)$.
(15) Rozhodněte, zda jsou izomorfní grupy $(\mathbf{Z}_6, +, -, 0)$ a $(\mathbf{Z}_2 \times \mathbf{Z}_3, +, -, 0)$.
(16) Rozhodněte, zda jsou izomorfní grupy $(\mathbf{S}_3, \circ, ^{-1}, \mathrm{Id})$ a $(\mathbf{Z}_2 \times \mathbf{Z}_3, +, -, 0)$.
(17) Rozhodněte, zda je grupa $(\mathbf{Z}_{20} \times \mathbf{Z}_{30}, +, -, 0)$ cyklická.
(18) Rozhodněte, zda je grupa $(\mathbf{Z}_{21} \times \mathbf{Z}_{31}, +, -, 0)$ cyklická.
(19) Rozhodněte, zda jsou permutace p_1 a p_2 konjugované v S_9, jestliže
a) $p_1 = (13)(259)$ a $p_2 = (247)(58)$,
b) $p_1 = (13)(259)$ a $p_2 = (13)(259)(48)$
(20) Rozhodněte, zda jsou permutace $(13)(259)$ a $(247)(58)$ konjugované v A_9.
(21) Dokažte, že pro každé přirozené n existuje nekonečně neizomorfních konečných grup obsahujících právě n podgrup.