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.

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 $p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot p_s < n$. □

1.15 (Čínská věta o zbytcích)**.** Nechť $n_1, n_2, \ldots, n_k$ jsou po dvou nesoudělná kladná celá čísla a $n = n_1 \cdot n_2 \cdot \cdots \cdot n_k$, Dokažte, že zobrazení $f : \mathbf{Z}_n \to \prod_{i=1}^{k} \mathbf{Z}_{n_i}$ dané předpisem $f(x) = (x \bmod n_1,\ x \bmod n_2, \ldots, x \bmod n_k)$ 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 $i = 1, \ldots, k$. Protože jsou n_i po dvou nesoudělná a $0 \leq b - a \leq n - 1$, máme i $n/b - a$, tudíž $b = a$. □

1.16. Uvažujme zobrazení $f : \mathbf{Z}_{45} \to \mathbf{Z}_5 \times \mathbf{Z}_9$ z 1.15, 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 $a = 5 \cdot 7 + 3 = 9 \cdot 4 + 3 = 38$. □

1.17. Uvažujme zobrazení $f : \mathbf{Z}_{720} \to \mathbf{Z}_5 \times \mathbf{Z}_9 \times \mathbf{Z}_{16}$ z 1.15. 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 1.15 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 $b = 45 \cdot 3 + 38 = 16 \cdot 10 + 13 = 173$. □