Příklad (1.1)
Nalezněte všechna celá čísla x splňující $x^2 + 5x \equiv 0 (\mathrm{mod}\ 19)$.

Řešení
Upravíme levou stranu: $x(x+5) \equiv 0 (\mathrm{mod}\ 19)$. Víme, že počítat modulo 19 znamená počítat v $\mathbb{Z}_{19}$ a že $\mathbb{Z}_{19}$ je těleso (tj. i obor), tedy součin dvou čísel je 0, pokud je jedno z nich nulové. Tedy buď $x \equiv 0 (\mathrm{mod}\ 19)$ nebo $x + 5 \equiv 0 (\mathrm{mod}\ 19)$ (to lze ještě upravit na $x \equiv -5 (\mathrm{mod}\ 19)$). Tudíž z definice modulárního počítání je výsledek:

$$x \in \{19k | k \in \mathbb{Z}\} \cup \{19k - 5 \in \mathbb{Z}\}\,.$$

Příklad (1.2)
Pomocí rozšířeného Euklidova algoritmu určete $\mathrm{NSD}(325, 123)$ a příslušné Bézoutovy koeficienty.

Řešení
Prostě budeme postupovat podle algoritmu:

$$\begin{pmatrix} 325 & 123 & 79 & 44 & 35 & 9 & 8 & 1 & 0 \\ 1 & 0 & 1 & -1 & 2 & -3 & 11 & -14 & - \\ 0 & 1 & -2 & 3 & -5 & 8 & -29 & 37 & - \end{pmatrix}$$

Čísle přečteme z posledního sloupce, kde není nula v prvním řádku:

$$\mathrm{NSD}(325, 123) = 1 = 325 \cdot 37 - 14 \cdot 123.$$

Příklad (1.3)
Označme $\varphi = \frac{1}{2}(\sqrt{5}+1)$. Dokažte, že množina $R_1 = a + b\varphi | a, b \in \mathbb{Z}$ tvoří podobor tělesa reálných čísel.

Důkaz
Stačí ukázat, že R_1 obsahuje jednotku, nulu a je uzavřená na sčítání, opačný prvek a násobení, protože jejich vlastnosti pak plynou z toho, že $\mathbb{R}$ je těleso[a]. Jednotka a nula v reálných číslech jsou zřejmě 1 a 0, které jsou tvaru $1 + 0\varphi \in R_2$ a $0 + 0\varphi \in R_2$.

Uzavřená na opačný prvek rozhodně je, protože pokud $a, b \in \mathbb{Z}$, tak zřejmě $-a, -b \in \mathbb{Z}$ a $-(a + b\varphi) = -a - b\varphi \in R_2$. Stejně tak součet (z asociativity + na $\mathbb{R}$): $a, b, c, d \in \mathbb{Z} \implies a + c, b + d \in \mathbb{Z}$ a $(a + b\varphi) + (c + d\varphi) = (a + c) + (b + d)\varphi \in R_2$. Největší problém je asi násobení, tedy $\forall a, b, c, d \in \mathbb{Z}$:

$$\left(a + b\frac{1}{2}(\sqrt{5}+1)\right) \cdot \left(c + d\frac{1}{2}(\sqrt{5}+1)\right) = ac + (ad+bc) \cdot \frac{1}{2}(\sqrt{5}+1) + bd\frac{1}{4}(5+2\sqrt{1}+1) =$$

$$= (ac + bd) + (ad + bc + bd) \cdot \frac{1}{2}(\sqrt{5}+1) \in R_2,$$

jelikož $ac + bd, ad + bc + bd \in \mathbb{Z}$. □

[a] Ještě je samozřejmě potřeba dokázat, že $R_2 \subseteq \mathbb{R}$, ale to je možná příliš jasné i na poznámku pod čarou.

Příklad (1.4)
Dokažte, že R_1 z předchozího bodu není isomorfní podoboru $R_2 = \left\{a + b\sqrt{2} | a, b \in Z\right\} \leq \mathbb{R}$.

Důkaz (Sporem)
Nechť tedy existuje isomorfismus $h : R_1 \to R_2$. Odhadneme (z následujícího výpočtu a z toho, jak se neisomorfismus standardně dokazuje), že nás zajímá ku příkladu obraz $(1 - 2\varphi)^2 \in R_1$. Podle výpočtu v předchozím příkladu je

$$(1-2\varphi)^2 = (a\cdot a+b\cdot b)+(a\cdot b+b\cdot a+b\cdot b)\varphi = (1^2+(-2)^2)+(1\cdot(-2)+(-2)\cdot 1+(-2)^2)\varphi = 5.$$

Izomorfismus součtu je součet isomorfismů, tedy levou stranu zobrazíme jako (zřejmě $R_1 \ni 1 = 1 \in R_2$, tedy $h(1) = 1$):

$$h(5) = h(1 + 1 + 1 + 1 + 1) = h(1) + h(1) + h(1) + h(1) + h(1) = 1 + 1 + 1 + 1 + 1 = 5.$$

Stejně tak, protože isomorfismus součinu je součin isomorfismů, můžeme zobrazit pravou stranu ($c, d \in \mathbb{Z}$):

$$h\left((1 - 2\varphi)^2\right) = h\left(1 - 2\varphi\right) \cdot h\left(1 - 2\varphi\right) = \left(c + d\sqrt{2}\right)^2.$$

A jelikož h je isomorfismus, tedy bijekce, tak si obrazy musí být rovny:

$$\left(c + d\sqrt{2}\right)^2 = c^2 + 2cd\sqrt{2} + 2d^2 = 5.$$

Teď $c = 0$, ale pak $5 = \left(d\sqrt{2}\right)^2 = 2d^2$, tj. $\mathbb{Q} \setminus \mathbb{Z} \ni \frac{5}{2} = d^2 \in \mathbb{Z}$, což je spor, nebo $d = 0$, ale pak $5 = c^2$, tj. $\mathbb{Z} \ni c = \sqrt{5} \in \mathbb{R} \setminus \mathbb{Q}$, což je taktéž spor[a]. Poslední možnost je tedy $c \neq 0 \neq d$:

$$\mathbb{R} \setminus \mathbb{Q} \ni \sqrt{2} = \frac{5 - c^2 - 2d^2}{2cd} \in \mathbb{Q}. \lightning$$

□

[a] Že je $\sqrt{5}$ (resp. $\sqrt{2}$ dále) iracionální dokážeme např. sporem: vyjádřením ve tvaru zlomku v základním tvaru, umocněním na druhou a pak ukázáním, že 5 (resp. 2) musí dělit čitatel i jmenovatel, což je ve sporu se základním tvarem.