(1) Co plyne z rovnosti součinů $\sqrt{2}\sqrt{2} = \left(-4 + 3\sqrt{2}\right)\left(4 + 3\sqrt{2}\right)$ pro gaussovskost oboru $\mathbb{Z}[\sqrt{2}]$?

**Řešení.** V gaussovských oborech platí jednoznačnost rozkladů na ireducibilní prvky až na pořadí a asociovanost. Podle tvrzení ze skript platí, že dva prvky $a$, $b$ jsou asociované právě tehdy, když existuje invertibilní prvek $q$ takový, že $a = bq$. Máme

$$\pm 4 + 3\sqrt{2} = \left(3 \pm 2\sqrt{2}\right)\sqrt{2},$$

ale přitom $\left(3 + 2\sqrt{2}\right)\left(3 - 2\sqrt{2}\right) = 1$, tedy prvky $3 \pm 2\sqrt{2}$ jsou invertibilní a platí

$$\pm 4 \pm 3\sqrt{2} \parallel \sqrt{2}$$

Uvedená rovnost součinů tedy gaussovskost oboru nevyvrací, protože uvedené prvky jsou navzájem asociované, a ani ji nepotrvrzuje. Takže z této rovnosti nám pro gaussovskost oboru $\mathbb{Z}[\sqrt{2}]$ neplyne nic.

(2) Rozložte 29 na součin ireducibilních prvků:
a) v $\mathbb{Z}[i\sqrt{2}]$
b) v $\mathbb{Z}[\sqrt{17}]$

**Řešení.** V obou oborech platí, že $N(29) = 29^2$ a obecně platí (tvrzení ze cvičení), že $N(xy) = N(x)\,N(y)$. Pokud se tedy 29 rozkládá, musí se rozkládat na prvky s normou 29. Ty už musí být ireducibilní, protože 29 je prvočíslo.
a) hledáme prvek s normou 29, tedy prvek $a + bi\sqrt{2}$, pro který platí

$$N\left(a + bi\sqrt{2}\right) = a^2 + 2b^2 = 29$$

Pro $a \geq 6$ a $b \geq 4$ je $N\left(a + bi\sqrt{2}\right) > 29$, a po ověření všech možností $a \in \{0, 1, 2, 3, 4, 5\}$ a $b \in \{0, 1, 2, 3\}$ vidíme, že prvek s normou 29 v $\mathbb{Z}[i\sqrt{2}]$ neexistuje. Tedy 29 je ireducibilní.
b) hledáme prvky tvaru $a + b\sqrt{7}$ takové, že platí

$$N\left(a + b\sqrt{7}\right) = a^2 - 7b^2 = 29$$

Zároveň vidíme, že pokud $29 = xy$, potom $x = a + b\sqrt{7}$ a $y = a - b\sqrt{7}$, protože $\left(a + b\sqrt{7}\right)\left(a - b\sqrt{7}\right) = a^2 - 7b^2 = 29$. Tyto rovnosti jsou splněny např. pro $a = 6$ a $b = 1$, takže

$$29 = \left(6 + \sqrt{7}\right)\left(6 - \sqrt{7}\right)$$

je rozklad na ireducibilní prvky v $\mathbb{Z}[\sqrt{7}]$.

(3) Spočtěte největšího společného dělitele a Bézoutovy koeficienty v oboru $\mathbb{Z}[i\sqrt{2}]$ pro
a) $3,\ 5 - i\sqrt{2}$
b) $-7 + 5i\sqrt{2},\ -8 + i\sqrt{2}$

**Řešení.** Pro hledání největšího společného dělitele a Bézoutových koeficientů použijeme Eukleidův algoritmus.
a) Nejprve spočítáme normy prvků: $N(3) = 9$ a $N\left(5 - i\sqrt{2}\right) = 27$, položíme tedy $a_0 = 5 - i\sqrt{2}$ a $a_1 = 3$ a pokračujeme podle Eukleidova algoritmu:

| $a_i$ | $u_i$ | $v_i$ |
|---|---|---|
| $5 - i\sqrt{2}$ | 1 | 0 |
| 3 | 0 | 1 |
| $2 - i\sqrt{2}$ | 1 | $-1$ |
| $1 + i\sqrt{2}$ | $-1$ | 2 |
| 0 | | |

Výsledek je

$$NSD\left(3, 5 - i\sqrt{2}\right) = 1 + i\sqrt{2} = -\left(5 - i\sqrt{2}\right) + 2 \cdot 3.$$

b) $N\left(-7 + 5i\sqrt{2}\right) = 99$ a $N\left(-8 + i\sqrt{2}\right) = 66$, položíme tedy $a_0 = -7 + 5i\sqrt{2}$ a $a_1 = -8 + i\sqrt{2}$ a provedeme Eukleidův algoritmus:

| $a_i$ | $u_i$ | $v_i$ |
|---|---|---|
| $-7 + 5i\sqrt{2}$ | 1 | 0 |
| $-8 + i\sqrt{2}$ | 0 | 1 |
| $1 + 4i\sqrt{2}$ | 1 | $-1$ |
| 0 | | |

Výsledek je

$$NSD\left(-7 + 5i\sqrt{2}, -8 + i\sqrt{2}\right) = 1 + 4i\sqrt{2} = \left(-7 + 5i\sqrt{2}\right) + (-1)\left(-8 + i\sqrt{2}\right).$$