(1) Rozložte v $\mathbb{Z}[i]$ na součin ireducibilních prvků:
- $17$
- $5+i$
- $12+3i$

**Řešení.** Budeme používat tvrzení z přednášky o tom, že pokud $a \mid b$, pak $||a||$ dělí $||b||$. Speciálně, je-li $||b||$ prvočíslo, pak je $b$ ireducibilní.
- $17 = (4+i)(4-i)$
  $\|4 \pm i\| = 16 + 1 = 17$, což je prvočíslo, tedy $4 \pm i$ je ireducibilní.
- $5 + i = (1+i)(3-2i)$
  $\|1+i\| = 2$ a $\|3-2i\| = 13$, což jsou prvočísla, tedy tyto prvky jsou ireducibilní.
- $12 + 3i = 3(4+i)$
  3 je ireducibilní, protože jeho norma je 9 a prvky normy 3 v $\mathbb{Z}[i]$ nejsou.

(2) Dokažte, že pokud je $p$ prvočíslo, tak platí:
(a) $x^{p-1} - 1 = \prod_{n=1}^{p-1}(x-n)$ v oboru $\mathbb{Z}_p[x]$
(b) pokud je $p$ tvaru $4k-1$ pro $k \in \mathbb{N}$, tak rovnice $x^{2k}+1$ má v $\mathbb{Z}_p$ vždy řešení
(c) pokud je $p$ tvaru $4k-1$ pro $k \in \mathbb{N}$, tak v $\mathbb{Z}_p$ existuje druhá odmocnina z $-1$

**Řešení.** (a) Budeme zkoumat kořeny polynomu $f = x^{p-1} - 1$. Podle malé Fermatovy věty platí $a^{p-1} \equiv 1 \pmod p$ pro každé $a \in \{1, 2, \ldots, p-1\}$, tj. $f(a) = a^{p-1} - 1 = 0$ v $\mathbb{Z}_p$. Tedy každý monočlen $x - a \mid f$, a protože jsou tyto monočleny navzájem nesoudělné, platí

$$\prod_{a=1}^{p-1}(x-a) \mid f.$$

Oba polynomy jsou monické a stejného stupně, musí se tedy rovnat.

(b) Vycházíme z právě dokázané rovnosti. Položíme $p = 4k-1$ a vidíme, že $x^{4k} - 1 = \prod_{n=1}^{4k}(x-n)$, tedy polynom $x^{4k}-1$ má $4k$ kořenů. Platí ale také rovnost

$$x^{4k} - 1 = \left(x^{2k} - 1\right)\left(x^{2k} + 1\right),$$

a protože polynom může mít maximálně tolik kořenů, kolik je jeho stupeň, musí platit, že každý z polynomů $x^{2k} \pm 1$ má právě $2k$ kořenů. (Implicitně používáme fakt, že $\mathbb{Z}_p$ je obor integrity, ve smyslu že pokud $(fg)(a) = f(a)g(a) = 0$, pak $f(a) = 0$ nebo $g(a) = 0$.)

(c) Podle předchozího víme, že $x^{2k}+1$ má kořen v $\mathbb{Z}_p$, zvolme tedy $a \in \mathbb{Z}_p$ takové, že $a^{2k} + 1 \equiv 0 \pmod p$. Tedy $\left(a^k\right)^2 \equiv -1 \pmod p$ a $a^k$ je druhá odmocnina z $-1$ v $\mathbb{Z}_p$.