Recall that an element x in a (commutative) ring A is called *irreducible* if $x \notin A^\times$, $x \neq 0$, and for all $a, b \in A$

$$x = ab \implies a \in A^\times \text{ or } b \in A^\times.$$

Exercise 1. When A is a (commutative) ring, we say that an element $p \in A$ is *prime* if pA is a nonzero prime ideal of A.

(i) Assume that A is a domain. Show that every prime element of A is irreducible.

(ii) Assume that A is a principal ideal domain. Show that every irreducible element of A is prime. (Hint: Show that the ideal generated by an irreducible is maximal.)

Exercise 2. Let A be a principal ideal domain. Let $a \in A$ be such that $a \neq 0$ and $a \notin A^\times$.

(i) Show that there exist irreducible elements $p_1, \dots, p_n$ in A such that

$$a = p_1 \dots p_n.$$

(Hint: Consider the set of ideals generated by elements $a \notin A^\times \cup \{0\}$ which admit no such decomposition, and use the fact that A is noetherian.)

(ii) Show that the elements $p_1, \dots, p_n$ are uniquely determined by a, up to their ordering and multiplication by units of A.

Exercise 3. We are going to solve the equation

$$y^3 = x^2 + 1, \quad \text{with } x, y \in \mathbb{Z}.$$

We consider the ring of Gaussian integers $\mathbb{Z}[i]$.

(i) Show that the element $1 + i$ is prime in $\mathbb{Z}[i]$.

(ii) Let $x \in \mathbb{Z}$. Let us pick $d \in \mathbb{Z}[i]$ such that $d\mathbb{Z}[i]$ is the ideal generated by $x - i$ and $x + i$. Show that $d = u(1+i)^n$, where $u \in \mathbb{Z}[i]^\times$, and $n \in \{0, 1, 2\}$.

(iii) Assume that $x, y \in \mathbb{Z}$ are such that $x^2 + 1 = y^3$. Show that the ideal generated by $x + i$ and $x - i$ in $\mathbb{Z}[i]$ is the whole ring $\mathbb{Z}[i]$.

(iv) Find all solutions to the equation

$$y^3 = x^2 + 1, \quad \text{with } x, y \in \mathbb{Z}.$$

Exercise 4. Let $\pi \in \mathbb{Z}[i]$ be a prime element. Show that there exists a prime number $p \in \mathbb{N}$ such that $\mathrm{N}(\pi) = p$ or $\mathrm{N}(\pi) = p^2$. (Here $\mathrm{N}\colon \mathbb{Z}[i] \to \mathbb{Z}$ is the norm function defined in the lectures.)

Exercise 5. Consider an integer $x \in \mathbb{N}$, and its prime decomposition in $\mathbb{Z}$

$$n = \prod_p p^{v_p(n)},$$

where p runs over the prime numbers, and $v_p(n) \in \mathbb{N}$.

Show that the following conditions are equivalent:

(a) there exist $a, b \in \mathbb{N}$ such that $n = a^2 + b^2$,

(b) for each prime number p congruent to 3 modulo 4, the integer $v_p(n)$ is even.

(Hint: Use the previous exercise.)

Exercise 6. Let $p \in \mathbb{N}$ be a prime number.

(i) If $p = 2$, show that $p \in \mathbb{Z}[i]$ can be written as $p = ab$ where $a, b \in \mathbb{Z}[i]$ are prime elements generating the same ideal in $\mathbb{Z}[i]$.

(ii) If $p = 3 \mod 4$, then $p \in \mathbb{Z}[i]$ is a prime element. (Hint: Use the results from the lectures.)

(iii) If $p = 1 \mod 4$, then $p \in \mathbb{Z}[i]$ can be written as $p = ab$, where $a, b \in \mathbb{Z}[i]$ are prime elements generating different ideals in $\mathbb{Z}[i]$.