Problem 1. (Here is an example of a ring where there is not necessarily a gcd for two given elements. As I said in class I personally don’t find these things fascinating, but this is still an opportunity to practice with ideals/units/irreducibles etc )

In an integral domain $A$, two elements $x$ and $y$ are said to have a gcd if the set of all principal ideals containing $(x, y) = (x) + (y)$ has a smallest element namely there is $d \in A$ such that

- $(x) + (y) \subseteq (d)$ (this means literally that $d$ divides $a$ and $b$).
- for all $d' \in A$, we have $(x) + (y) \subseteq (d')$ implies $(d) \subseteq (d')$ (namely $d'$ divides $x$ and $y$ implies $d'$ divides $d$).

In that case $d$ is called a gcd of $x$ and $y$.

(1) Prove that the gcd of $2$ and $X$ in $\mathbb{Z}[X]$ is $1$.

(2) Let $A = \mathbb{Z}[i\sqrt{3}]$.

(a) What are the units in $A$?

(b) Show that $2$ and $1 \pm i\sqrt{3}$ are irreducible in $A$ (use as usual the norm $N : A \rightarrow \mathbb{Z}$).

(c) Let $x = 4 = 2 \times 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ and $y = 2(1 + i\sqrt{3})$. Notice that $2$ and $1 + i\sqrt{3}$ both divide $x$ and $y$, so

$$ (x) + (y) \subseteq (2) \quad \text{and} \quad (x) + (y) \subseteq (1 + i\sqrt{3}) $$

so if there was a gcd of $x$ and $y$, there would be $d \in A$ such that $(x) + (y) \subseteq (d)$ and

$$ (d) \subseteq (2) \quad \text{and} \quad (d) \subseteq (1 + i\sqrt{3}). $$

so $2$ divides $d$ and $1 + i\sqrt{3}$ divides $d$. Find a contradiction.

In your book they say that $\mathbb{Z}[i\sqrt{3}]$ is a principal ideal domain (§8.2). If it was true it would be a UFD (and there would be a gcd for $x$ and $y$). We can already see that it is not a UFD since we have a non unique decomposition of $4$ into irreducibles.

Problem 2. Let $p$ be an odd prime number. Recall that we set $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

(1) How many squares are there in $(\mathbb{Z}/p\mathbb{Z})^\times$ ?

(2) Decompose the polynomial $X^{(p-1)/2} - 1$ into irreducibles in the unique factorization domain $\mathbb{F}_p[X]$.

(3) Let $x \in \mathbb{Z}$ not divisible by $p$. Show that $x$ is a square mod $p$ (i.e. $x \mod p$ is a square in $\mathbb{Z}/p\mathbb{Z}$) if and only if

$$ x^{(p-1)/2} = 1 \mod p. $$

Problem 3. (This one is just a very easy review on Euclidean division of polynomials).

(1) Let $P \in \mathbb{K}[X]$ and $z \in \mathbb{K}$. What is the remainder of the Euclidean division of $P$ by $X - z$?

(2) Let $A \in \mathbb{R}[X]$, and $B \in \mathbb{R}[X]$ a monic irreductible polynomial of degree 2. What is the remainder of the Euclidean division of $A$ by $B$?

(3) Write the division of $X^3 + 2X^2 + 5X + 1$ by $X^2 + 4X + 1$ in $\mathbb{Q}[X]$ (and check that it actually happens in $\mathbb{Z}[X]$).
(4) What is the Euclidean division of $X^2 + X + 1$ by $2X + 1$ in $\mathbb{Q}[X]$. Does it happen in $\mathbb{Z}[X]$?

**Problem 4.** Chinese remainder theorem Let $(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in \mathbb{R}^n$ and suppose that all $x_i$s are pairwise distinct. Why is there a unique polynomial $P \in \mathbb{R}[X]$ of degree $< n$ such that $P(x_i) = y_i$ for all $i$?

**Problem 5.** This problem introduces the concept of the "content" of a polynomial. It is important. After proving properties of the content of a polynomial, you are able to prove Gauss lemma below. It must be clear to you now that $2X + 2$ is not irreducible in $\mathbb{Z}[X]$ but it is irreducible in $\mathbb{Q}[X]$. How to characterize the irreducible elements in $\mathbb{Z}[X]$? The answer is given by the lemma.

Let $A$ be a commutative unitary ring. We consider the ring $A[X]$ of polynomials with coefficients in $A$.

1. Identify $(A[X])^\times$.
2. Show that $A[X]$ is an integral domain if and only if $A$ is an integral domain.
3. Now we suppose that $A = \mathbb{Z}$. A polynomial $P$ in $\mathbb{Z}[X]$ is called primitive if the only elements of $\mathbb{Z}$ that divide all coefficients of $P$ at once are $\pm 1$. A polynomial $P$ in $\mathbb{Z}[X]$ which is not a unit is called irreducible if $P$ and $P = AB$ where $A, B \in \mathbb{Z}[X]$ implies that $A$ or $B$ is a unit of $\mathbb{Z}[X]$.
   (a) Show that $\mathbb{Z}[X]$ is not principal.
   (b) Show that the product of two primitive polynomials in $\mathbb{Z}[X]$ is primitive.
   (c) Show that a nonzero polynomial $Q \in \mathbb{Q}[X]$ can be written uniquely in the form $Q = c(Q)P$ with $P \in \mathbb{Z}[X]$ primitive and $c(Q) \in \mathbb{Q}$, $c(Q) > 0$. Check that $c(Q) \in \mathbb{Z}$ if and only if $Q \in \mathbb{Z}[X]$. The rational number $c(Q)$ is called the content of $Q$.
   (d) Show that for $A, B \in \mathbb{Q}[X] \setminus \{0\}$ we have $c(AB) = c(A)c(B)$.
   (e) Prove the following statement

   **Lemma** (Gauss Lemma). A non constant polynomial $P \in \mathbb{Z}[X]$ is irreducible if and only if it is primitive and irreducible when seen as a polynomial in $\mathbb{Q}[X]$.

4. Write $\mathbb{Z}[\frac{1}{2}]$ as a quotient ring. Why is this question a bit different from HW2 Problem 1(3)?

**Problem 6.** (Characteristic of a ring)

1. Why can’t there be a field of characteristic $6$? Is there an integral domain of characteristic $6$?
2. Given a prime number $p$ and a field $K$ of characteristic $p$, prove that the cardinality of $K$ is a power of $p$.
3. Give an example of field with cardinality $4$.
4. Is every field of positive characteristic finite?

**Problem 7.** Proof that $A = \mathbb{Z}[i]$ is principal. This is a bit of a side problem. It is good to have seen it once in your life. See the reference to your book given at the end (I’ll mention this reference in class, not sure I’ll go into details).
(1) Find the list of all invertible elements in $A$ (use as usual the norm $N : \mathbb{Q}[i] \to \mathbb{Q}$).

(2) Let $x \in \mathbb{C}$. Show that there is $q \in A$ such that $|q - x| \leq \sqrt{2}/2$ (make a drawing!).

(3) Let $I$ be an ideal of $A$. We are going to prove that $I$ is principal. Let $z_0 \in I$ such that $N(z_0) = \min\{N(z), z \in I - \{0\}\}$. We want to show that $I = z_0A$.

(a) Why does $z_0$ exist?

(b) Let $z \in I$ and let $x := z/z_0 \in \mathbb{Q}[i]$. We need to prove that $x \in A$.

(i) Show that there is $q \in A$ such that $N(x - q) < 1$.

(ii) Compute $N(z - z_0q)$ and conclude.

(c) Note that hidden in this proof is the fact that $A$ is endowed with an Euclidean division (a Euclidean ring is always principal). The direct proof that $A$ is Euclidean is in your book. §8.1 Example (3))