Name:

1. The *Gaussian Integers*, denoted $\mathbb{Z}[i]$ is the set

$$\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$$

where i is the complex number $i = \sqrt{-1}$. Addition and multiplication in $\mathbb{Z}[i]$ is inherited from $\mathbb{C}$.

(a) Prove that $\mathbb{Z}[i]$ is a ring.

Solution:

- Addition and multiplication are binary operations for the set $\mathbb{Z}[i]$:

$$\begin{aligned}(a+bi)+(c+di) =&(a+c)+(b+d)i \in \mathbb{Z}[i]\\ (a+bi)(c+di) =&(ac-bd)+(ad+bc)i \in \mathbb{Z}[i]\end{aligned}$$

- $\mathbb{Z}[i]$ is an abelian group under addition. This requires showing that
  - Addition is associate (inherited from $\mathbb{C}$)
  - Addition is commutative (inherited from $\mathbb{C}$)
  - There is an identity for addition. $(0 \in \mathbb{Z}[i])$
  - Every element has an additive inverse: $((a+bi)+(-a-bi)=0)$
- Mutiplication is associative (inherited from $\mathbb{C}$)
- Mutiplication is distributive over addition (inherited from $\mathbb{C}$)

2. Let $d = \gcd(1386, 350)$.

(a) Find d using the Euclidean algorithm.

Solution:

$$\begin{aligned}1386 =&3 \cdot 350 + 336\\ 350 =&1 \cdot 336 + 14\\ 336 =&24 \cdot 14\end{aligned}$$

$\gcd(1386, 350) = 14$

(b) Using the Euclidean algorithm, find a and b so that $d = 1386a + 350b$.

Solution: $14 = 1386 \cdot (-1) + 350 \cdot 4$

3. Let $f, g \in \mathbb{Q}[x]$:

$$\begin{aligned}f =&x^4 + 2x^3 + x^2 + 2x\\ g =&2x^3 + 4x^2 + 3x + 6\\ d =&\gcd(f, g)\end{aligned}$$

Find d using the Euclidean algorithm.

Solution:

$$\begin{aligned}x^4 + 2x^3 + x^2 + 2x =&(2x^3 + 4x^2 + 3x + 6)(x/2) - (x^2 + 2x)/2\\ 2x^3 + 4x^2 + 3x + 6 =&(x^2 + 2x)(2x) + (3x + 6)\end{aligned}$$

$$x^2 + 2x = x(x+2) + 0$$

$\gcd(x^4 + 2x^3 + x^2 + 2x, 2x^3 + 4x^2 + 3x + 6) = x + 2$

4. Show that for any $n \geq 1$, $x^n - 1$ is divisible by $x - 1$.

   Solution: This is the remainder or factor theorem. We know that $x - 1$ is a factor of $f(x)$ if and only if $f(1) = 0$. In this case, $f(x) = x^n - 1$ and $f(1) = 1$.

5. A complex number α is called *algebraic* if it is a root of a polynomial with integer coefficients.

   (a) Show that $\sqrt{2}$ is algebraic.
   Solution: All we need to do is find a polynomial in $\mathbb{Z}[x]$: $x^2 - 2$.

   (b) Show that $2 - i\sqrt{3}$ is algebraic.
   Solution: $x^2 - 4x + 7$

   (c) π is not algebraic. What would you need to do to be able to prove this?
   Solution: You would need to show that there is no polynomial that has π as a root. This is considerably more difficult than exhibiting a polynomial that has a given root as in the previous questions.

6. Let K be a field and $K[x]$ be the ring of polynomials with coefficients in K. As *ideal* in $K[x]$ is a set I, with the properties:

   - If $a, b \in I$ then $a \pm b \in I$.
   - If $a \in I$ and $b \in K[x]$ then $ab \in I$.

   Let I be a nonzero idea of $K[x]$. Prove that there is some polynomial $f \in I$ such that every element of I is a multiple if f. (This shows that every idea in $K[x]$ is a principal ideal.)

   Solution: Let $f \in I$ have minimal, non-negative degree. Such an f exists since I is nonzero. Then, given any $g \in I$, divide f by g:

   $$f = g \cdot q + r$$

   Since $g \in I$ and $q \in K[x]$, we must have $g \cdot q \in I$ (by the definition of an ideal). Also, $r = f - gq$ and therefore $r \in I$. By the minimal assumption of $\deg f$, we must have $r = 0$ and we are done. (We proved any g in I is a multiple of f.)