## Section 2 Unique Factorization Domains

**2.1.** Factor the following polynomials into irreducible factors in $\mathbb{F}_p[x]$.
**(a)** $x^3 + x^2 + x + 1$, $p = 2$, **(b)** $x^2 - 3x - 3$, $p = 5$, **(c)** $x^2 + 1$, $p = 7$

**2.2.** Compute the greatest common divisor of the polynomials $x^6 + x^4 + x^3 + x^2 + x + 1$ and $x^5 + 2x^3 + x^2 + x + 1$ in $\mathbb{Q}[x]$.

**2.3.** How many roots does the polynomial $x^2 - 2$ have, modulo 8?

**2.4.** Euclid proved that there are infinitely many prime integers in the following way: If $p_1, \ldots, p_k$ are primes, then any prime factor $p$ of $(p_1 \cdots p_k) + 1$ must be different from all of the $p_i$. Adapt this argument to prove that for any field $F$ there are infinitely many monic irreducible polynomials in $F[x]$.

**2.5.** *(partial fractions for polynomials)*

**(a)** Prove that every element of $\mathbb{C}(x)$ $x$ can be written as a sum of a polynomial and a linear combination of functions of the form $1/(x - a)^i$.

**(b)** Exhibit a basis for the field $\mathbb{C}(x)$ of rational functions as vector space over $\mathbb{C}$.

**2.6.** Prove that the following rings are Euclidean domains.
**(a)** $\mathbb{Z}[\omega]$, $\omega = e^{2\pi i/3}$, **(b)** $\mathbb{Z}[\sqrt{-2}]$.

**2.7.** Let $a$ and $b$ be integers. Prove that their greatest common divisor in the ring of integers is the same as their greatest common divisor in the ring of Gauss integers.

**2.8.** Describe a systematic way to do division with remainder in $\mathbb{Z}[i]$. Use it to divide $4 + 36i$ by $5 + i$.

**2.9.** Let $F$ be a field. Prove that the ring $F[x, x^{-1}]$ of Laurent polynomials (Chapter 11, Exercise 5.7) is a principal ideal domain.

**2.10.** Prove that the ring $\mathbb{R}[[t]]$ of formal power series (Chapter 11, Exercise 2.2) is a unique factorization domain.

## Section 3 Gauss's Lemma

**3.1.** Let $\varphi$ denote the homomorphism $\mathbb{Z}[x] \to \mathbb{R}$ defined by
**(a)** $\varphi(x) = 1 + \sqrt{2}$, **(b)** $\varphi(x) = \frac{1}{2} + \sqrt{2}$.
Is the kernel of $\varphi$ a principal ideal? If so, find a generator.

**3.2.** Prove that two integer polynomials are relatively prime elements of $\mathbb{Q}[x]$ if and only if the ideal they generate in $\mathbb{Z}[x]$ contains an integer.

**3.3.** State and prove a version of Gauss's Lemma for Euclidean domains.

**3.4.** Let $x, y, z, w$ be variables. Prove that $xy - zw$, the determinant of a variable $2 \times 2$ matrix, is an irreducible element of the polynomial ring $\mathbb{C}[x, y, z, w]$.

**3.5.** **(a)** Consider the map $\psi: \mathbb{C}[x, y] \to \mathbb{C}[t]$ defined by $f(x, y) \rightsquigarrow f(t^2, t^3)$. Prove that its image is the set of polynomials $p(t)$ such that $\frac{dp}{dt}(0) = 0$.

**(b)** Consider the map $\varphi: \mathbb{C}[x, y] \to \mathbb{C}[t]$ defined by $f(x, y) \rightsquigarrow (t^2 - t, t^3 - t^2)$. Prove that $\ker \varphi$ is a principal ideal, and find a generator $g(x, y)$ for this ideal. Prove that the image of $\varphi$ is the set of polynomials $p(t)$ such that $p(0) = p(1)$. Give an intuitive explanation in terms of the geometry of the variety $\{g = 0\}$ in $\mathbb{C}^2$.