14.6 Prove Theorem 14.1: Let F be a field and let $m(x)$ be a polynomial in $F[x]$ of positive degree n. Every polynomial $a(x)$ in $F[x]$ is congruent modulo $m(x)$ to exactly one polynomial of degree less than n

14.10 Give a description of all the polynomials in each of the following congruence classes.

1. The congruence class of $x^5 + 3$ in $\mathbb{R}[x]$ modulo x
2. The congruence class of $x^3 + x^2 + 1$ in $\mathbb{F}_2[x]$ modulo $x + 1$

14.13 Let F be a field and let $m(x)$ be a polynomial of positive degree in $F[x]$. Consider two polynmoials $a(x), b(x)$ in $F[x]$

1. Suppose $e(x)$ is a polynomial in the congruence class $[a(x)]_{m(x)}$ and $f(x)$ is a polynomial in the congruence class $[b(x)]_{m(x)}$. Show that

$[e(x) + f(x)]_{m(x)} = [a(x) + b(x)]_{m(x)}$

and $[e(x)f(x)]_{m(x)} = [a(x)b(x)]_{m(x)}$

2. Define addition and multiplication for the set of congruence classes of $F[x]$ modulo $m(x)$ by setting the sum of congruence classes $[a(x)]_{m(x)} + [b(x)]_{m(x)}$ equal to the congruence class

$[a(x) + b(x)]_{m(x)}$

and product $[a(x)]_{m(x)}[b(x)]_{m(x)} = [a(x)b(x)]_{m(x)}$

3. Show that with respect to these rules of addition and multiplication, $[0]_{m(x)}$ is an additive identity and $[1]_{m(x)}$ is a multiplicative identity. Show further than the collection of congruence classes modulo $m(x)$ forms a ring.

We can write $F[x]_{m(x)}$ for the new ring we constructed, the ring of congruence classes of polynomials in $F[x]$ modulo $m(x)$

14.15 Assume that $m(x)$ is a polynomial of positive degree in $F[x]$.

1. Show that in $F[x]_{m(x)}$, the collection of congruence classes of degree-zero polynomials (constants) is closed under addition and multiplication. Thus, this collection forms a ring inside $F[x]_{m(x)}$
2. EIdentify this ring with F
3. Explain how this exercise generalizes part 3 of the previous exercise.

14.18 Prove Theorem 14.7 by imitating the proof of theorem 14.6

Theorem 14.7: Let F be a field, let $a(x), b(x)$ be polynomials in $F[x]$ with greatest common divisor $d(x)$, and let $e(x)$ be a polynomial in $F[x]$. Then the equation $a(x)U + b(x)V = e(x)$ has a polynomial solution if and only if $d(x)$ divides $e(x)$. In particular, the equation $a(x)U + b(x)V = 1$ has a polynomial solution if and only if $a(x), b(x)$ are relatively prime

14.21 Prove theorem 14.8 (Hint: interpret 14.7 as terms of congruences)

Theorem 14.8: Let F be a field. Let $a(x), m(x)$ be polynomials of $F[x]$ with $m(x)$ of postiive degree. The congruence $a(x)U \equiv 1(mod m(x))$ is solvable if and only if $gcd(a(x), m(x)) = 1$

14.24 Let F be a field and suppose $m(x)$ is an irreducible polynomial in $F[x]$. Show that $F[x]_{m(x)}$ is a field.

15.2 Prove Theorem 15.2 using theorem 15.1

Theorem 15.2: Let R be the ring of integers or the ring of polynomials over a field. Suppose r is an element of R that is not zero or a unit.

1. If $r = ab$ is a nontrivial factorization of r, then $N(a) < N(r)$ and $N(b) < N(r)$.
2. Either r is irreducible or r is a product of irreducible elements

15.5 We have observed that a ring satisfying the conclusions of theorem 15.1 should satisfy the conclusion of theorem 15.2. Verify this for the rings $\mathbb{Z}[\sqrt{-m}]$ by proving theorem 15.5 using theorem 15.3.

Theorem 15.5: Let m be a square free integer, let R be the ring $\mathbb{Z}[\sqrt{-m}]$, and suppose r is an element of R that is not zero or a unit.

1. If $r = ab$ is a nontrivial factorization of r, then $N(a) < N(r)$ and $N(b) < N(r)$.
2. Either r is irreducible or r is a product of irreducible elements

15.8 Use the division theorem for $\mathbb{Z}[i]$ to prove theorem 15.10 below.

Theorem 15.10: $\mathbb{Z}[i]$ is a Euclidean ring.