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 $n$

Given $a(x)$, we know by theorem 9.5 that there exists unique $q(x), r(x)$ such that $a(x) = m(x)q(x) + r(x)$ for $r(x)$ degree less than $n$

Then $a(x) - r(x) = m(x)q(x)$

Then $m(x)$ divides $a(x) - r(x)$

Then $a(x), r(x)$ are congruent modulo $m(x)$

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

$x^5 + 3 = x * x^4 + 3$

So when divided by $x$, it has remainder 3.

So the congruence class of $x^5 + 3$ in $\mathbb{R}[x]$ modulo $x$ includes polynomials in the form $xp(x) + 3$

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

In $\mathbb{F}_2[x]$

$x^3 + x^2 + 1 = (x + 1)(x^2) + 1$

So remainder 1

So the congruence class includes polynomials in the form $xp(x) + 1$

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

Know that $e(x)\ equiva(x)$, $f(x) \equiv b(x) \bmod m(x)$

Then when divided by $m(x)$, $e(x), a(x)$ have the same remainder, call it $r(x)$. And $f(x), b(x)$ have the same remainder, call it $s(x)$

Then let $e(x) = m(x)q_1(x) + r(x)$

And let $a(x) = m(x)q_2(x) + r(x)$

$f(x) = m(x)q_3(x) + s(x)$

$f(x) = m(x)q_4(x) + s(x)$

For addition,

Then $f(x) + e(x) = m(x)(q_1(x) + q_3(x)) + s(x) + r(x)$

And $a(x) + b(x) = m(x)(q_2(x) + q_4(x)) + s(x) + r(x)$

Then $[f(x) + e(x)]_{m(x)} = [s(x) + r(x)]_{m(x)}$

And $[a(x) + b(x)]_{m(x)} = [s(x) + r(x)]_{m(x)}$

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

For multiplication,

Then $f(x)e(x) = m(x)q_1(x)m(x)q_3(x) + m(x)q_1(x)s(x) + m(x)q_3(x)r(x) + r(x)s(x)$

Then $[e(x)f(x)]_{m(x)} = [r(x)s(x)]_{m(x)}$

And $a(x)b(x) = m(x)q_2(x)m(x)q_4(x) + m(x)q_2(x)s(x) + m(x)q_4(x)r(x) + r(x)s(x)$

Then $[a(x)b(x)]_{m(x)} = [r(x)s(x)]_{m(x)}$

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

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.

0 is the additive identity if $[0 + a(x)]_{m(x)} = [a(x)]_{m(x)}$

$[0]_{m(x)} = 0$

$0 + [a(x)]_{m(x)} = [a(x)]_{m(x)}$

This is true.

1 is the multiplicative identity if $[1 * a(x)]_{m(x)} = [a(x)]_{m(x)}$

$[1]_{m(x)} = 1$, since $m(x)$ polynomial of positive degree

Then $[1 * a(x)] = 1 * [a(x)]_{m(x)}$

This is also true.

Show that it is ring:

Show that it is closed under addition:

Given $a(x), b(x)$,

$[a(x)] + [b(x)] = [a(x) + b(x)]$, which is another element in $F[x]_{m(x)}$

Show that it is closed under multiplication

$[a(x)] * [b(x)] = [a(x)b(x)]$, which is another element in $F[x]_{m(x)}$

So it is 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 $F[x]_{m(x)}$

The collection of congruence classes of degree zero polynomials all have the quality that for a degree 0 polynomial $j$, $j$ divided by $m(x)$ is itself.

Just like in the previous problem, this collection is just all of the constants that are in $F$, which is a field.

And since $F$ is a field, it is closed under addition and multiplication.

2. Identify this ring with $F$

3. Explain how this exercise generalizes part 3 of the previous exercise.

This generalizes part 3 of the previous exercise because $m(x)$ is arbitrary positive degree, and shows that if we can relate it back to $F$ itself, we can show that there is a ring inside $F[x]_{m(x)}$

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

$a(x), b(x) \in F[x]_{m(x)}$, with gcd $d(x)$

Let $e(x) \in F[x]_{m(x)}$

Prove forwards: If $a(x)U + b(x)V = e(x)$ has a solution, then $d(x)$ divides $e(x)$

Since $d(x)$ is gcd of $a(x), b(x)$, rewrite as

$a(x) = j(x)d(x), b(x) = k(x)d(x)$ for some $j(x), k(x) \in F[x]_{m(x)}$

Then $e(x) = d(x)[Uj(x) + Vk(x)]$

Then $d(x)$ divides $e(x)$

Prove backwards: If $d(x)$ divides $e(x)$, then $a(x)U + b(x)V = e(x)$

Prove backwards: If $a(x)U + b(x)V = e(x)$ has no solution, then $d(x)$ does not divide $e(x)$

$d(x)|e(x)$, so $e(x) = k(x)d(x)$ for some $k(x) \in F[x]_{m(x)}$

We know by Bezouts theorem that $a(x)U + b(x)V = d(x)$ has solutions

Then $a(x)Uk(x) + b(x)Vk(x) = k(x)d(x) = e(x)$ has solutions.

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 $gcd(a(x), m(x)) = 1$

Prove forwards: if $a(x)U \equiv 1 \text{ mod} m(x)$ is solvable, then $gcd(a(x), m(x)) = 1$

$a(x)U \equiv 1 \text{ mod } m(x)$ is equivalent to saying that $a(x)U - 1 = m(x)k(x)$ for some $k(x)$

Rearranging, this is $a(x)U + m(x)k(x) = 1$

And since this has a solution, we know by theorem 14.7 that the gcd of $a(x), m(x)$ must divide 1.

Then $gcd(a(x), m(x)$ must be 1.

Prove backwards: if $gcd(a(x), m(x)) = 1$ then $a(x)U \equiv 1 \text{ mod} m(x)$

$gcd(a(x), m(x)) = 1$

then by bezouts theorem, we know that there exists $U, V$ such that

$a(x)U + m(x)V = 1$

Rearranging, this is $a(x)U - 1 = m(x)V$

This means that $a(x) \equiv 1 \text{ mod } m(x)$

Prove Corollary 14.9

Let $F$ be a field. Suppose $m(x)$ is an irreducibel polynomial in $F[x]$ and $a(x)$ is a nonzero polynomial in $F[x]$ of degree less than the degree of $m(x)$. Then there exists a polynomial $r(x)$ in $F[x]$ such that $a(x)r(x) \equiv 1 \text{ mod } m(x)$

$m(x)$ irreducible, no lower degree factors

and $a(x)$ lower degree

Then $a(x), m(x)$ must have $gcd(a(x), m(x)) = 1$

Then by bezouts theorem, there exists $U, V$ such that

$a(x)U + m(x)V = 1$

Rearranging, this is $a(x)U - 1 = m(x)V$

Then $a(x)U \equiv 1 \text{ mod } m(x)$

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.

$m(x)$ irreducible, so for congruence classes in $F[x]_{m(x)}$,

They are relatively prime to $m(x)$

Then by theorem 14.10, each congruence class $[a(x)]_{m(x)}$ in $F[x]_{m(x)}$ is a unit

Then $F[x]_{m(x)}$ must be 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

1. $r = ab$ is a nontrivial factorization of $r$

$r$ is not a unit, so for $r = ab$, by theorem 15.1, $N(a) \neq N(ab)$

And $N(b) \neq N(ab)$

And by 15.1, we know that $N(a) < N(ab) = N(r)$

And $N(b) < N(ab) = N(r)$

2.

$r$ is not a unit, and is nonzero

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

1. $r$ is not a unit, so for $r = ab$, by theorem 15.3, $N(a) \neq N(ab)$

And $N(b) \neq N(ab)$

And by 15.3, we know that $N(a) < N(ab) = N(r)$

and $N(b) < N(ab) = N(r)$

2. $r$ is not a unit and is non zero

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.

It is a Euclidean Ring if it satisfies

A) There is a norm function $N$ assigning every nonzeor element $a$ of $R$ a nonnegative integer $N(a)$ and assigning 0 a value $N(0)$ less than the norm of every nonzero element of R.

Yes, for $a = x + yi$

Then $N(a) = x^2 + y^2$

And for $N(0)$, this is $N(0) = (0)(0) = 0$, which is less than the Norm of any nonzero element $a$ of $R$

B) For any two nonzero elements $a, b$ of $R$, $N(a) \leq N(ab)$

Let $a = x + yi$

$b = j + ki$

$N(ab) = (x + yi)(x - yi)(j + ki)(j - ki)$

$N(ab) = (x^2 + y^2)(j^2 + k^2)$

So $N(a) \leq N(ab)$

C) For any two nonzero elements $a, b$ of $R$, there exists elements $q, r$ such that $b = aq+r$ and $N(r) < N(a)$

We know this is true, by theorem 15.9