Problem 14.2: Let K be a collection of polynomial-like expressions, and let $\gamma^n = 2$.

Let m be a positive integer. Consider γ^m. Using the division theorem, $m = nq + r$ for positive integers q and r such that $r < n$. Then, $\gamma^m = \gamma^{nq+r} = \gamma^{nq}\gamma^r$. Using the rule that $\gamma^n = 2$, we see that $\gamma^m = 2^q\gamma^r$. Let $f(a) = a_{n-1}y^{n-1}+...+a_2y^2+a_1\gamma+a_0$ and $f(b) = b_{n-1}y^{n-1}+...+b_2y^2+b_1\gamma+b_0$ be two non-zero elements of K. If we multiply the two polynomials together

$$(a_{n-1}y^{n-1} + ... + a_2y^2 + a_1\gamma + a_0)(b_{n-1}y^{n-1} + ... + b_2y^2 + b_1\gamma + b_0)$$
$$c_d\gamma^d + c_e\gamma^e + c_f\gamma^f ... + c_x\gamma^2 + c_y\gamma + c_z$$

for positive integers d, e, f, x, y, z where $d = 2n-2$ is the degree of the leading term, (e, f, x, y, z) are degrees less than d, and the c is a constant term that is representative of the summand of the collection of coefficients $\sum_{i,j=1}^{n-1} a_ib_j$. Using the information from above, we can apply the rule that $\gamma^n = 2$ to find that

$$2^{d_0}c_d\gamma^{d_1} + 2^{e_0}c_e\gamma^{e_1} + 2^{f_0}c_f\gamma^{f_1} + ...c_x\gamma^2 + c_y\gamma + c_z$$

for all positive integers so that we can write the product of the two polynomials as a sum of powers of 2 and their coefficients. Suppose that $f(b)$ is the inverse of $f(a)$ such that $f(b) = f(a)^{-1}$ and $f(a)f(b) = 1$. Then

$$2^{d_0}c_d\gamma^{d_1} + 2^{e_0}c_e\gamma^{e_1} + 2^{f_0}c_f\gamma^{f_1} + ...c_x\gamma^2 + c_y\gamma + c_z = 1$$

To find the values that make this true, one would have to set all the coefficients of the left and right side together in a massive n by n matrix, which for large values of n could take even a computer many hours or days to solve. In theory, it is possible, but not practical. If one were to find such values, for at least one the coefficients non-zero, then we would have proved that K is a field since both $f(a)$ and $f(b)$ are nonzero.

Problem 14.6: Let F be a field and let $m(x)$ be a polynomial of positive degree n in $F[x]$. Prove that every polynomials $a(x)$ is congruent mod $m(x)$ to exactly one polynomial of degree less than n.

To prove this, we will use a proof by contradiction. Suppose that $a(x)$ is congruent to two polynomials mod $m(x)$. $a(x) \equiv h(x) \mod m(x)$ and $a(x) \equiv g(x) \mod m(x)$ where both $h(x)$ and $g(x)$ are of degree less than n. By the definition of congruence,

$$a(x) - h(x) = q(x)m(x)$$
$$a(x) - g(x) = s(x)m(x)$$

Where $g(x) \neq h(x)$ and $s(x) \neq q(x)$. Observe that

$$a(x) = q(x)m(x) + h(x)$$
$$a(x) = s(x)m(x) + g(x)$$
Hence,
$$q(x)m(x) + h(x) = s(x)m(x) + g(x)$$
$$h(x) - g(x) = m(x)[(s(x) - q(x)]$$

Notice that for this equation to be true, $deg(h(x) - g(x)) = deg(m(x)[(s(x) - t(x)])$. We cannot say exactly what the degrees of $s(x)$ and $q(x)$ are, but at a minimum, $deg(s(x) - t(x)) = 0$. So, $m(x)[(s(x) - t(x)]$ has degree at least n since $deg(m(x)[(s(x) - t(x)]) = deg(m(x)) + deg(s(x) - q(x)) = n + 0$. Similarly, we cannot say what the degrees of $g(x)$ and $h(x)$ are, but at a minimum, $h(x) - g(x)$ has degree zero. However, since $h(x) - g(x) = m(x)[(s(x) - t(x)]$, $h(x) - g(x)$ should have degree at least n, which we have shown it does not. By this contradiction, $g(x) = h(x)$ and $s(x) = q(x)$. Therefore, we have proven that it is impossible for two different polynomials of deree less than n to be congruent to $a(x)$ mod $m(x)$, and so we have proven that every polynomial is congruent to exactly one polynomial of degree less than the degree of the modulus. $\square$

Problem 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

The congruence class of $x^5 + 3$ mod x is representative of polynomials satisfying $p(x) \equiv x^5 + 3 \bmod x$. In other words, the difference $p(x) - x^5 - 3$ is divisible by x. Thus, $p(x) - x^5 - 3$ must be a polynomial multiple of x, and so this congruence class takes the form:

$$\{xq(x) + (x^5 + 3), q(x) \in \mathbb{R}[x]\}$$

for any polynomial $q(x) \in \mathbb{R}[x]$.

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

Similarly, we can think of the congruence class of $x^3 + x^2 + 1$ in $\mathbb{F}_2[x]$ mod $x + 1$ as the collection of polynomials satisfying $b(x) \equiv x^3 + x^2 + 1 \bmod x + 1$, meaning that $x + 1$ divides the difference of $b(x) - x^3 - x^2 - 1$. This means that $b(x)$ must be a polynomial multiple of the modulus and take the form $q(x)(x + 1) + (x^3 + x^2 + 1)$ for any polynomial $q(x) \in \mathbb{F}_2[x]$. Thus, the congruence class is given by

$$\{q(x)(x + 1) + (x^3 + x^2 + 1) | q(x) \in \mathbb{F}_2[x]\}$$

Problem 14.14:

There are four congruence classes in $\mathbb{F}_2[x]$ of x^2: 0, 1, x, and $x+1$ since there are 4 elements of degree less than 2 in $\mathbb{F}_2[x]$. Below are their addition and multiplication tables.

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

×	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	0	x
x+1	0	x+1	x	1

Observe that the units of $\mathbb{F}_2[x]_{x^2}$ are 1 and $x+1$. Because not every non-zero element has a multiplicative inverse, $\mathbb{F}_2[x]_{x^2}$ is not a field.

Consider the ring $\mathbb{F}[x]_x$. By definition, elements in this congruence class are given by:

$$[\mathbb{F}[x]]_x = \{[f(x)]|deg(f(x)) < 1\}$$

Thus, the elements in the congruence class mod x have degree less than 1, so the elements of this congruence class are 0 and the constants α, $\forall \alpha \in \mathbb{F}$. Hence, $\mathbb{F}[x]_x = \mathbb{F}$.

Similarly, consider the ring $\mathbb{F}[x]_{m(x)}$ where $m(x)$ is a first degree polynomial. By definition, elements in this congruence class are given by:

$$[\mathbb{F}[x]]_{m(x)} = \{[g(x)]|deg(g(x)) < 1\}$$

Thus, the elements in the congruence class mod $m(x)$ have dregree less than 1, so the elements of this congruence class are 0 and the constants α, $\forall \alpha \in \mathbb{F}$. Hence, $\mathbb{F}[x]_{m(x)} = \mathbb{F}$. $\square$

Problem 14.18: Let $\mathbb{F}$ be a field and let $a(x)$ and $b(x)$ be elements of $\mathbb{F}[x]$ with greatest common divisor $d(x)$. Then, the equation $a(x)U + b(x)V = 1$ has a polynomial solution if and only if $a(x)$ and $b(x)$ are relatively prime.

Suppose $a(x)U+b(x)V = 1$ has a polynomial solution and $d(x)$ is the greatest common divisor of $a(x)$ and $b(x)$. By Bezout's Theorem, there exist polynomials such that $a(x)S+b(x)T = d(x)$. Since $d(x)$ divides both $a(x)$ and $b(x)$ as well as $a(x) + b(x)$, $d(x)$ certainly divides any combination of polynomial multiples of $a(x)+b(x)$. Therefore, $d(x)$ would also divide $a(x)U+b(x)V = 1$ because U, V are polynomails. If $d(x)$ divides the left side of the equation, it must also divide the right side as well. This means that $d(x)$ divides 1. This is only possible if $d(x)$ is the constant polynomial 1, because any polynomial of degree greater than 1 does not divide 1, and any polynomial of degree 1 that is not the constant polynomial 1 also does not divide 1. Therefore, $d(x)$=1 and we have shown that $a(x)$ and $b(x)$ are relatively prime.

Now, suppose that $a(x)$ and $b(x)$ are relatively prime. By Bezout's Theorem, there exist polynomials such that $a(x)U + b(x)V = 1$. Therefore, the equation $a(x)U + b(x)V = 1$ has a polynomial solution and we have proven the theorem. $\square$

Problem 14.22: Let $\mathbb{F}$ be a field. Let $a(x)$ and $m(x)$ be polynomials in $\mathbb{F}[x]$ of positive degree. The congruence class $[a(x)]_{m(x)}$ is a unit in $\mathbb{F}[x]_{m(x)}$ if and only if $(a(x), m(x)) = 1$.

Suppose that $a(x)$ is a unit in $\mathbb{F}[x]$. Then, by definition, there exists $U \in \mathbb{F}[x]$ such that $[a(x)U] = [1]$. Since $m(x)$ is a polynomial of positive degree, it is certainly true that if we were to apply the division theorem of $m(x)$ on $[a(x)U]$, the remainder would be 1. By definition of polynomial congruence, this implies that $a(x)U \equiv 1 \bmod m(x)$. By theorem 14.8 in the textbook, the equation $a(x)U \equiv 1 \bmod m(x)$ has a solution if and only if $(a(x), m(x)) = 1$. Therefore, $a(x)$ and $m(x)$ must be relatively prime.

Now, suppose that $(a(x), m(x)) = 1$. By Bezout's Theorem, there exists integers $U, V \in \mathbb{F}[x]$ such that $a(x)U + m(x)V = 1$. Then $a(x) - 1 = m(x)(-V) = m(x)V'$. Observe that $m(x)$ divides $a(x) - 1$. By definition of polynomial congruence, $a(x)U \equiv 1 \bmod m(x)$ which we know is solveable since $(a(x), m(x)) = 1$. This implies that $[a(x)U] = [1]$ in $\mathbb{F}[x]$. Hence, $[a(x)][U] = [1]$ so $[U] = [a(x)]^{-1}$ and thus $a(x)$ is a unit. $\square$

Problem 15.4: Let m be a square-free integer and let N be the norm function on $\mathbb{Z}[\sqrt{-m}]$.

Let a be an element of $\mathbb{Z}[\sqrt{-m}]$, and let $a = 0 + 0\sqrt{-m}$. Then the norm of a is given by $(0+0\sqrt{-m})(0-0\sqrt{-m}) = 0$. So a has size zero. Observe that a is the unique element of smallest size because if $a = r + s\sqrt{-m}$, then the norm of a is given by $r^2 + s^2m > 0$ if $r > 0$ and $s > 0$.

Suppose $r + s\sqrt{-m}$ is a unit. Then if we multiply by its multiplicative inverse, $(r+s\sqrt{-m})(x+y\sqrt{-m})$=1. Expanding, we see that $(r+s\sqrt{-m})(x+y\sqrt{-m}) = (rx - sy) + (sx + ry)\sqrt{-m} = 1 + 0\sqrt{-m}$. Equating coefficients on both sides of the equation, we can see that $rx - sy = 1$ and $sx + ry = 0$. Observe: $(r - s\sqrt{-m})(x - y\sqrt{-m}) = (rx - sy) + (-1)(sx + ry)\sqrt{-m}$. Using the knowledge found previously: $(r - s\sqrt{-m})(x - y\sqrt{-m}) = 1 + 0\sqrt{-m} = 1$, so if $r + s\sqrt{-m}$ is a unit, $r - s\sqrt{-m}$ is also a unit with multiplicative inverse $x - y\sqrt{-m}$. Next, notice that $(r + s\sqrt{-m})(r - s\sqrt{-m})(x + y\sqrt{-m})(x - y\sqrt{-m}) = 1(1) = 1$. Multiplying through: $(r^2 + s^2m)(x^2 + y^2m) = 1$. Since r, s, x, y are all integers and the square of an integer is never zero, it is safe to assume that both $r^2 + s^2m = 1$ and $x^2 + y^2m = 1$. This means that $r + s\sqrt{-m}$ is a unit if and only if $r^2 + s^2m = 1$. We will consider the cases next:

Suppose $m = 1$. Then $r^2 + s^2m = r^2 + s^2 = 1$. This equality is only possible in four scenarios: $(r, s) = (1, 0), (-1, 0), (0, 1)$ and $(0, -1)$. Now that we know the coefficients of r and s, the units of $\mathbb{Z}[\sqrt{-m}]$ are as follows: $\pm 1, \pm\sqrt{-1}$.

Suppose $m > 1$. Then $r + s\sqrt{-m}$ is a unit if and only if $r^2 + s^2m = 1$. Since $m > 1$, the product s^2m will never be equal to 1 since s is an integer. Then the only possible solution to the equation is if $r = 1$ and $r = -1$. Therefore, if $m > 0$, the only units of $\mathbb{Z}[\sqrt{-m}]$ are ± 1.

If $m = 1$, then the irreducibles of $\mathbb{Z}[\sqrt{-m}]$ have third smallest size 2. If $N(a) = 2$ then $a = \pm 1 \pm i$ because the norm of a is given by $r^2 + s^2 = 2$ and no integer is the square of 2, so $r = s = \pm 1$. If $m = 2$, then the third smallest size is also 2. The norm is given by $r^2 + 2s^2 = 2$, which tells us that $r = 0$ since $2s^2 \geq 2$ if $s^2 \neq 0$. So $r = 0$ and $s = 1$ in order for the norm to be true. Thus, the irredicubles when $m = 2$ are $\pm\sqrt{-2}$. Similarly, if $m = 3$, the

irreducibles have size 3 and are $\pm\sqrt{-3}$ because $(0, \pm 1)$ is the only integer solution to $r^2 + 3s^2 = 3$.

Next, assume that $N(a) = N(ab)$, and assume that $N(a) > 1$. By exercise 15.3, we have verified that $N(ab) = N(a)N(b)$. It is certainly true that $N(a) = N(a)$, but if $N(a) = N(a)N(b)$ as well, then the only way this is possible is if $N(b) = 1$, since the norm can only take positive integer values. Thus, $N(b) = 1$ so b is a unit because the only elements of $\mathbb{Z}[\sqrt{-m}]$ with norm 1 are precisely the units. Now, suppose that b is a unit. Then b has norm 1 because all units of $\mathbb{Z}[\sqrt{-m}]$ have norm 1. Then for any $a \in \mathbb{Z}[\sqrt{-m}]$, $N(a)N(b) = N(a)(1) = N(a)$. Thus we have achieved the equality $N(a) = N(a)N(b)$ if and only if b is a unit.

Problem 15.8

To show that $\mathbb{Z}[i]$ is a Gaussian Ring, we will walk through each of the properties of a Gaussian Ring and verify them. The norm function of and element a on $\mathbb{Z}[i]$ is given by: $N(a) = (b+ci)(b-ci) = b^2+c^2$. Let $a = 0 = 0i$ be the zero element of $\mathbb{Z}[i]$. Then $N(0) = 0^2 + 0^2 = 0$, so a has zero norm. Next, suppose that $a = b + ci > 0$. Then the norm of a is given by $b^2 + c^2$. Since b and c are integers and the square of an integer is never negative, $b^2 + c^2 > 0$ since either b or c or both are greater than zero. Thus, the norm of 0 is unique and the smallest norm of $\mathbb{Z}[i]$.

Suppose a and b are two non-zero elements of $\mathbb{Z}[i]$. Then by the above results, we kow that $N(a) > 0$ and $N(b) > 0$. Suppose $N(b) = 1$. Then $N(a) = N(a)(1) = N(a)N(b)$, so the equality $N(a) \leq N(a)N(b)$ holds. Suppose that $N(a) = q > 0$ and $N(b) = p > 1$. Then $N(a)N(b) = pq > p = N(a)$, so the equality $N(a) \leq N(a)N(b)$ still holds. Therefore we have verified that $N(a) \leq N(a)N(b)$ is always true if $N(a) > 0$ and $N(b) > 0$.

Lastly, in order to prove that $\mathbb{Z}[i]$ is a Gaussian Ring, we must show that the division theorem is true and that if a, b are both non zero, there exists an integer q such that $b = aq + r$ where $N(r) < N(a)$. In the previous exercise, execise 15.7, we verified that in $\mathbb{Z}[i]$, this result is true. Therefore, all conditions have been met and thus $\mathbb{Z}[i]$ is a Gaussian Ring. $\square$

Problem 2: Let $p(x) = x^2 + 2x + 2$. Form the polynomial congruence ring $\mathbb{Z}_3[x]_{x^2+2x+2}$. Below is the multiplication table for elements in the congruence ring:

$\times$	1	2	x	$2x$	$x+1$	$x+2$	$2x+1$	$2x+2$
1	$\boxed{1}$	2	x	$2x$	$x+1$	$x+2$	$2x+1$	$2x+2$
2	2	$\boxed{1}$	$2x$	x	$2x+2$	$2x+1$	$x+2$	$x+1$
x	x	$2x$	$x+1$	$2x+2$	$2x+1$	$\boxed{1}$	2	$x+2$
$2x$	$2x$	x	$2x+2$	$x+1$	$x+2$	2	$\boxed{1}$	$2x+1$
$x+1$	$x+1$	$2x+2$	$2x+1$	$x+2$	2	x	$2x$	$\boxed{1}$
$x+2$	$x+2$	$2x+1$	$\boxed{1}$	2	x	$2x+2$	$x+1$	$2x$
$2x+1$	$2x+1$	$x+2$	2	$\boxed{1}$	$2x$	$x+1$	$2x+2$	x
$2x+2$	$2x+2$	$x+1$	$x+2$	$2x+1$	$\boxed{1}$	$2x$	x	2

Observe that every non-zero element has a multiplicative inverse. By brute force, we have shown that $\mathbb{Z}_3[x]_{x^2+2x+2}$ is a field. Alternatively, Theorem 14.11 in the textbook states that a polynomial congruence ring is a field if and only if the modulus $m(x)$ is irreducible. Observe that in the field $\mathbb{F}_3$, x^2+2x+2 has no roots and is thus irreducible. Our calculations have verified the theorem in the textbook.

Problem 2 Let $p(x) = x^2 + x + 1$. Form the polynomial congruence ring $\mathbb{Z}_3[x]_{x^2+x+1}$. Below is the multiplication table for elements in the congruence ring:

$\times$	1	2	x	$2x$	$x+1$	$x+2$	$2x+1$	$2x+2$
1	$\boxed{1}$	2	x	$2x$	$x+1$	$x+2$	$2x+1$	$2x+2$
2	2	$\boxed{1}$	$2x$	x	$2x+2$	$2x+1$	$x+2$	$x+1$
x	x	$2x$	$2x+2$	$x+1$	2	$x+2$	$2x+1$	$\boxed{1}$
$2x$	$2x$	x	$x+1$	$2x+2$	$\boxed{1}$	$2x+1$	$x+2$	2
$x+1$	$x+1$	$2x+2$	2	$\boxed{1}$	x	$2x+1$	$x+2$	$2x$
$x+2$	$x+2$	$2x+1$	$x+2$	$2x+1$	$2x+1$	0	0	$x+2$
$2x+1$	$2x+1$	$x+2$	$2x+1$	$x+2$	$x+2$	0	0	$2x+1$
$2x+2$	$2x+2$	$x+1$	$\boxed{1}$	2	$2x$	$x+2$	$2x+1$	x

Observe that not every non-zero element has a multiplicative inverse. Therefore, $\mathbb{Z}_3[x]_{x^2+x+1}$ is not a field. Notice that $x = 1$ is a root of $x^2 + x + 1$ in $\mathbb{F}_3[x]$, so x^2+x+1 is reducible. Again, our findings have verified the theorem from the textbook.

Problem 4 Working in $\mathbb{Q}$, prove that if a, b and c are non-zero, then $a^3 + 2b^3 - 6abc + 4c^3 \neq 0$.

In chapter 11, we proved that every polynomial with rational coefficients could be rewritten with integer coefficients by factoring or multiplying constants out, so we will consider the same problem with integer coefficients. If we have a polynomial $a+b\gamma+c\gamma^2$, then it is possible to rewrite the polynomial as $s(a' + b'\gamma + c'\gamma^2)$ where (a', b', c') are integers. Without loss of generality, we will consider the problem $a + b\gamma + c\gamma^2$ with (a, b, c) non-zero integers.

Suppose that $a^3 + 2b^3 - 6abc + 4c^3 = 0$ with (a, b, c) non-zero integers. If we rearrange the equation, we see that $a^3 = 2(-b^3 + 3abc - 2c^3)$ which tells us that a^3 is divisible by 2, hence, a^3 is even. Since a^3 is even, a is also even and we can write it as a product of 2 and an integer a'. Then, $a^3 = (2a')^3 = 8a'^3$. Substituting into the original equation: $8a'^3 + 2b^3 - 12a'bc + 4c^3 = 0 = 2(4a'^3 + b^3 - 6a'bc + 2c^3)$. From this equation, we can see that $4a'^3 + b^3 - 6a'bc + 2c^3 = 0$. Again, we can rearrange the equation: $b^3 = 2(-2a'^3+3a'bc+c^3)$ and we may observe that b^3 is divisible by 2 as well. If b^3 is even, then so is b, and we can write it as such, $b = 2b'$. Substituting into the original equation, $4a'^3+8b'^3-12a'b'c+2c^3 = 0 = 2(2a'^3+4b'^3-6a'b'c+c^3)$. From this equation, we can see that $2a'^3 + 4b'^3 - 6a'b'c + c^3 = 0$ hence, $c^3 = 2(-a'^3 - 2b'^3 - 3a'b'c)$ and again we can observe that c^3 is divisible by 2 and we can write $c = 2c'$. In conclusion, we have shown that if (a, b, c) is a solution to $a^3+2b^3-6abc+4c^3 = 0$, then (a, b, c) are all even and $(\frac{a}{2}, \frac{b}{2}, \frac{c}{2})$ is also an integer solution. But if $(\frac{a}{2}, \frac{b}{2}, \frac{c}{2})$ is an integer solution, then its half, $(\frac{a}{4}, \frac{b}{4}, \frac{c}{4})$ is an integer solution and its half $(\frac{a}{8}, \frac{b}{8}, \frac{c}{8})$ is also an integer solution and so forth. But if (a, b, c) are all integers and we need $(\frac{a}{2^k}, \frac{b}{2^k}, \frac{c}{2^k})$ to be a solution with k infinitely large, then for no choice of (a, b, c) will $(\frac{a}{2^k}, \frac{b}{2^k}, \frac{c}{2^k})$ yield an integer solution since the donominator 2^k is arbitrarily large and (a, b, c) must be divisible by 2^k for each $k \in \mathbb{Z}$. Thus, by contradiction, we have shown that if (a, b, c) are non-zero integers, then $a^3 + 2b^3 - 6abc + 4c^3 \neq 0$. It follows from the observation above that $a^3 + 2b^3 - 6abc + 4c^3 \neq 0$ for $(a, b, c) \in \mathbb{Q}$. $\square$