Problem 1 (§22.3). Find the product of \( f(x) = 2x^2 + 3x + 4 \) and \( g(x) = 3x^2 + 2x + 3 \) in \( \mathbb{Z}_6[x] \).

Solution. Simplifying the expression in \( \mathbb{Z}_6[x] \), we recover
\[
f(x)g(x) = (2x^2 + 3x + 4)(3x^2 + 2x + 3) \\
= 6x^4 + (4 + 9)x^3 + (6 + 6 + 12)x^2 + (9 + 8)x + 12 \\
= x^3 + 5x.
\]

Problem 2 (§22.5). How many polynomials are there of degree at most three in \( \mathbb{Z}_2[x] \)?

Solution. Polynomials of degree at most three in \( \mathbb{Z}_2[x] \) are of the form:
\[
a_3x^3 + a_2x^2 + a_1x + a_0
\]
where \( a_i \in \mathbb{Z}_2 \). Since each \( a_i \) for \( i \in \{0, 1, 2, 3\} \) can be 0 or 1, this gives that there are \( 2^4 = 16 \) such polynomials.

Remark. However, in \( \mathbb{Z}_2[x] \), Fermat’s little theorem gives \( x^3 = x^2 = x \) and thus we may reduce every such polynomial to one of the following four \( \{0, 1, x, x + 1\} \). However, the distinction here is between the polynomial and the function itself. This is very subtle.

Problem 3 (§22.11). Let \( F = \mathbb{Z}_7 \) and compute the evaluation homomorphism \( \phi_4(3x^{106} + 5x^{99} + 2x^{53}) \).

Solution. Fermat’s little theorem gives that \( 4^6 = 1 \) in \( \mathbb{Z}_7 \) and hence in \( \mathbb{Z}_7 \)
\[
3(4^{106}) = 3(4^{6(17)+4}) = 3(4^4) = 3(4) = 5 \\
5(4^{99}) = 5(4^{6(16)+3}) = 5(4^3) = 5(1) = 5 \\
2(4^{53}) = 2(4^{8(6)+5}) = 2(4^5) = (2)2 = 4.
\]

Using each of these equations,
\[
\phi_4(3x^{106} + 5x^{99} + 2x^{53}) = \phi_4(3x^{106}) + \phi_4(5x^{99}) + \phi_4(2x^{53}) = 5 + 5 + 4 = 0
\]
Problem 4 (§22.16). Let \( \phi_3 : \mathbb{Z}_5[x] \rightarrow \mathbb{Z}_5 \) be the evaluation homomorphism and compute \( \phi_3(x^{231} + 3x^{117} - 2x^{53} + 1) \).

Solution. By Fermat’s Little Theorem, we know that \( 3^4 \equiv 1 \pmod{5} \) as \( \gcd(3, 5) = 1 \). Then, we have that
\[
\begin{align*}
3^{231} + 3 \cdot 3^{117} - 2 \cdot 3^{53} + 1 &\equiv 3^{4(57)+3} + 3 \cdot 3^{4(29)+1} - 2 \cdot 3^{4(13)+1} + 1 \pmod{5} \\
&\equiv 3^3 + 3 \cdot 3^1 - 2 \cdot 3^1 + 1 \pmod{5} \\
&\equiv 27 + 9 - 6 + 1 \pmod{5} \\
&\equiv 1 \pmod{5}.
\end{align*}
\]

Thus, \( \phi_3(x^{231} + 3x^{117} - 2x^{53} + 1) = 1 \).

Problem 5 (§22.17). Use Fermat’s little theorem to find all zeros in \( \mathbb{Z}_5 \) of \( f(x) = 2x^{119} + 3x^{74} + 2x^{57} + 3x^{44} \).

Solution. As the constant term is zero, clearly \( 0 \in \mathbb{Z}_5 \) is zero of \( f(x) \). For the nonzero element, using Fermat’s little theorem, we get
\[
\begin{align*}
x^{119} &= x^{4(29)+3} = x^3 \\
x^{74} &= x^{4(18)+2} = x^2 \\
x^{57} &= x^{4(14)+1} = x \\
x^{44} &= x^{4(11)} = 1.
\end{align*}
\]

As a result, for each \( i \in \mathbb{Z}_5 \setminus \{0\} \),
\[
\phi_i(2x^{119} + 3x^{74} + 2x^{57} + 3x^{44}) = \phi_i(2x^3 + 3x^2 + 2x + 3).
\] (1)

We then note that factoring by grouping yields
\[
2x^3 + 3x^2 + 2x + 3 = (2x + 3)(x^2 + 1)
\]

Using the fact that \( \mathbb{Z}_5 \) is an integral domain
\[
(2x + 3)(x^2 + 1) = 0 \iff (2x + 3) = 0 \pmod{5} \text{ or } x^2 = -1 = 4 \pmod{5}
\]

The first equation \( 2x = 3 \pmod{5} \) has exactly one such solution \( x = 4 \) as \( \gcd(2, 5) = 1 \). The second equation \( x^2 = 4 \pmod{5} \) has solutions \( x = 2 \) and \( x = 3 \).

Putting everything together the zeroes in \( \mathbb{Z}_5 \) of \( f(x) = 2x^{119} + 3x^{74} + 2x^{57} + 3x^{44} \) are \( \{0, 2, 3, 4\} \).

Remark. From Equation [1], it is totally valid (and probably easier) to simply plug in the values of \( \mathbb{Z}_5 \setminus \{0\} \). However, this is the solution that uses more of the theory from this course.

Problem 6 (§22.22). Find a polynomial of positive degree which is a unit in \( \mathbb{Z}_4[x] \).

Solution. Consider \( f(x) = 2x + 1 \in \mathbb{Z}_4[x] \) and note that
\[
f(x)^2 = (2x + 1)(2x + 1) = 4x^2 + 4x + 1 = 1
\]
in \( \mathbb{Z}_4[x] \) and as such \( f(x) = 2x + 1 \) is a unit in \( \mathbb{Z}_4[x] \).