quiz 11.1 Solution

(1) Find the number of irreducible monic degree 18 polynomials in $F_3[x]$.
Use the theorem which asserts that, in general, for $Q$ the set of distinct prime factors of the degree $d$, and for $|Q|$ the number of elements in $Q$, the number of irreducibles of degree $d$ with coefficients in a field with $p$ elements is

\[
\frac{1}{d} \cdot \sum_{i=0}^{|Q|} (-1)^i \sum_{q_1 \ldots < q_i} p^{d/q_1 \ldots q_i},
\]

where $q_1, \ldots, q_i$ is summed over $i$-element subsets of $Q$. Here $p = 3$ and $d = 18$, and by trial division $Q = \{2, 3\}$, and $|Q| = 2$. The formula becomes

\[
\text{number irreducibles degree 18 in } F_3[x] = \frac{3^{18} - 3^{18/2} - 3^{18/3} + 3^{18/(2 \cdot 3)}}{18} = 2152228
\]

(2) Find the number of primitive monic degree 7 polynomials in $F_3[x]$.
Use the formula which says, in general, that

\[
\text{number primitives degree } d \text{ in } F_q[x] = \frac{\varphi(q^d - 1)}{d}
\]

where $\varphi(n)$ is Euler's totient function, counting the number of integers $t$ in the range $1 \leq t \leq n$ such that $\gcd(t, n) = 1$. Here $q = 3$ and $d = 7$. We use the formula for $\varphi(n)$ in terms of the prime factorization $n = p_1^{e_1} \ldots p_\ell^{e_\ell}$ of $n$, that

\[
\varphi(n) = (p_1 - 1)p_1^{e_1 - 1} \ldots (p_\ell - 1)p_\ell^{e_\ell}
\]

Here, factoring by trial division,

\[
3^7 - 1 = 2 \cdot 1093
\]

and

\[
\varphi(3^7 - 1) = (2 - 1) \cdot (1093 - 1) = 1092
\]

so, by the formula

\[
\text{number primitives degree 7 in } F_3[x] = \varphi(3^7 - 1)/d = 1092/7 = 156
\]

(3) Let $\alpha$ be a root of the cubic $x^3 + 2x^2 + x + 1 = 0$. (Yes, $x^3 + 2x^2 + x + 1$ is irreducible. Do not bother to check this.) Find coefficients $A, B, C$ in $F_3$ such that $\beta = \alpha^2 + \alpha + 2$ is a root of

\[
Y^3 - AY^2 + BY - C = 0
\]

We anticipate that the complete collection of the roots of the equation $Y^3 - AY^2 + BY - C = 0$ will consist of the given root $\beta$ and all its images under Frobenius, namely $\beta_2 = \beta^3$ and $\beta_3 = (\beta^3)^3 = \beta^9$. And we have the symmetric-function formulas

\[
A = \beta + \beta_2 + \beta_3
\]
\[
B = \beta \beta_2 + \beta_2 \beta_3 + \beta_3 \beta
\]
\[
C = \beta \cdot \beta_2 \cdot \beta_3
\]

It is wise to reduce the expressions for the second and third roots modulo $x^3 + 2x^2 + x + 1$, obtaining

\[
\beta_2 = (\alpha^2 + \alpha + 2)^3 \% (x^3 + 2x^2 + x + 1) = \alpha^2 + \alpha
\]
\[
\beta_3 = (\alpha^2 + \alpha)^3 \% (x^3 + 2x^2 + x + 1) = \alpha^2 + \alpha + 1
\]
Then the formulas for the coefficients give

\[ A = \beta + \beta_2 + \beta_3 = (\alpha^2 + \alpha + 2) + (\alpha^2 + \alpha) + (\alpha^2 + \alpha + 1) = 0 \]

\[ B = \beta\beta_2 + \beta_2\beta_3 + \beta_3\beta = (\alpha^2 + \alpha + 2)(\alpha^2 + \alpha) + (\alpha^2 + \alpha)(\alpha^2 + \alpha + 1) + (\alpha^2 + \alpha + 1)(\alpha^2 + \alpha + 2) = 2 \]

\[ C = \beta \cdot \beta_2 \cdot \beta_3 = (\alpha^2 + \alpha + 2)(\alpha^2 + \alpha)(\alpha^2 + \alpha + 1) = 1 \]

So the equation satisfied by \( \beta = \alpha^2 + \alpha + 2 \) is

\[ Y^3 - 0 \cdot Y^2 + 2 \cdot Y - 1 = 0 \]

(4) We grant ourselves that \( x^5 + x^3 + x^2 + x + 1 \in F_2[x] \) is irreducible. Let \( \alpha \) be a root of \( x^5 + x^3 + x^2 + x + 1 = 0 \). Find a reduced expression of the form \( \beta = a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 \) which is a root of \( x^5 + x^2 + 1 = 0 \).

From the theorem proven in class, with

\[ Q_1(x) = x^5 + x^2 + 1 \]
\[ Q_2(x) = x^5 + x^3 + 1 \]
\[ Q_3(x) = x^5 + x^3 + x^2 + x + 1 \]
\[ Q_4(x) = x^5 + x^4 + x^2 + x + 1 \]
\[ Q_5(x) = x^5 + x^4 + x^3 + x + 1 \]
\[ Q_6(x) = x^5 + x^4 + x^3 + x^2 + 1 \]

(the labelling is an artifact) that

for a root \( \alpha \) of \( Q_1 = 0 \), \( \alpha^3 \) is a root of \( Q_6 = 0 \), for a root \( \alpha \) of \( Q_5 = 0 \), \( \alpha^3 \) is a root of \( Q_4 = 0 \), for a root \( \alpha \) of \( Q_4 = 0 \), \( \alpha^3 \) is a root of \( Q_2 = 0 \), for a root \( \alpha \) of \( Q_2 = 0 \), \( \alpha^3 \) is a root of \( Q_3 = 0 \), for a root \( \alpha \) of \( Q_3 = 0 \), \( \alpha^3 \) is a root of \( Q_5 = 0 \), and for a root \( \alpha \) of \( Q_5 = 0 \), \( \alpha^3 \) is a root of \( Q_1 = 0 \). Our given cubics are, by this labelling, \( Q_3 \) and \( Q_1 \), respectively. Thus, by the theorem, for a root \( \alpha \) of \( Q_3 \), \( \alpha^3 \) is a root of \( Q_5 \), and then \( (\alpha^3)^3 \) is a root of \( Q_1 \). Reducing modulo \( Q_3 \) gives the expression

\[ x^9 \equiv (x^5 + x^3 + x^2 + x + 1) = x^4 + x^3 + x \]

so a root of \( x^5 + x^2 + 1 = 0 \) is \( \alpha^4 + \alpha^3 + \alpha \).