1. Let \( f = 3x^5 + 3x^4 + 15x^2 + 4 \). List all the candidates for rational roots of \( f \), as identified by the theorem on rational roots.

**Solution:** The numerator must divide 4 and the denominator must divide 3. Thus, the solutions are \( \pm 1, \pm 2, \pm 4, \pm \frac{1}{3}, \pm \frac{2}{3} \) and \( \pm \frac{4}{3} \).

2. Determine whether the following polynomial is irreducible in \( \mathbb{Q}[x] \) or not. **Show your work.** If you use Eisenstein’s criterion, say which prime you used and what verifications you made to show the criterion is satisfied.

\[ f = 7x^4 + 42x^3 + 84 \]

**Solution:** The prime \( p \) must divide both 42 and 84, but must not divide 7. And \( p^2 \) must not divide 84. There is exactly one prime that satisfies all these conditions: \( p = 3 \). So \( f \) is irreducible by Eisenstein’s criterion.

3. Give prime factorizations in \( \mathbb{Z}_2[x] \) for the following polynomials. Give proofs that the factors are prime. (You may use the results from class on the irreducibles in degrees \( \leq 2 \).

a) \( f = x^7 + x^6 + x^5 + x^4 + x^3 + x + 1 \)

**Solution:** \( f(0) = 1 \) and \( f(1) = 1 \), so \( f \) has no roots, hence no irreducible factors of degree 1. The only irreducible polynomial of degree 2 in \( \mathbb{Z}_2[x] \) is \( x^2 + x + 1 \), we test by division to see if it divides \( f \). It does divide evenly, and we obtain

\[ f = (x^2 + x + 1)(x^5 + x^2 + 1) \]

We must now factor \( g = x^5 + x^2 + 1 \). We have \( g(0) = 1 \) and \( g(1) = 1 \), so \( g \) has no roots, and hence no factors of degree 1. Since \( g \) has degree 5, it is irreducible unless it has an irreducible factor of degree \( \leq \frac{5}{2} \), so the only other degree to test is 2: If \( g \) has no irreducible quadratic factor, then \( g \) is irreducible.

The only irreducible quadratic over \( \mathbb{Z}_2 \) is \( x^2 + x + 1 \). Dividing \( g \) by \( x^2 + x + 1 \), we get a remainder of 1. So \( g \) does not have an irreducible quadratic factor, and hence \( g \) is irreducible. The prime factorization of \( f \) is \( f = (x^2 + x + 1)(x^5 + x^2 + 1) \).
Exam 3 Solutions

4. Let \( f = x^2 - 3 \in \mathbb{Z}_7[x] \), and let \( F = \mathbb{Z}_7[x]/(f) \), a field. Let \( \alpha = [x]_f \).

a) What are the possible orders of the elements of \( F^\times \)?

Solution: \( |F| = |\mathbb{Z}_7|^{\deg f} = 7^2 = 49 \), so \( |F^\times| = 49 - 1 = 48 \). The possible orders are the divisors of 48.

b) What is the order of \( \alpha \) in \( F^\times \)?

Solution: The fundamental equation is \( \alpha^2 - 3 = 0 \), so \( \alpha^2 = 3 \). Thus,

\[
\begin{align*}
\alpha^3 &= \alpha^2 \cdot \alpha = 3\alpha \\
\alpha^4 &= (\alpha^2)^2 = 9 = 2 \\
\alpha^6 &= (\alpha^2)^3 = 27 = -1
\end{align*}
\]

Thus, \( \alpha^{12} = 1 \). Since we’ve already tested all the divisors of 12, \( o(\alpha) = 12 \).

c) What is the order of \( \alpha^{88} \) in \( F^\times \)?

Solution:

\[
o(\alpha^{88}) = \frac{o(\alpha)}{(o(\alpha), 88)} = \frac{12}{(12, 88)} = \frac{12}{4} = 3
\]

d) What is the order of \( 3\alpha \) in \( F^\times \)?

Solution:

\[
(3\alpha)^2 = 9\alpha^2 = 27 = -1
\]

Thus, \( (3\alpha)^4 = 1 \), so \( 3\alpha \) has order 4.
Exam 3 Solutions

e) What is the order of $\alpha + 1$ in $\mathbf{F}^\times$?

**Solution:**

$$(\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha + 4 = 2(\alpha + 2)$$

$$(\alpha + 1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1 = 3\alpha + 9 + 3\alpha + 1 = -\alpha + 3$$

$$(\alpha + 1)^4 = [2(\alpha + 2)]^2 = 4(\alpha^2 + 4\alpha + 4) = 4(4\alpha) = 2\alpha$$

$$(\alpha + 1)^6 = (-\alpha + 3)^2 = \alpha^2 - 6\alpha + 9 = \alpha + 5$$

$$(\alpha + 1)^8 = (2\alpha)^2 = 4\alpha^2 = 12 = 5$$

$$(\alpha + 1)^{12} = (\alpha + 1)^8(\alpha + 1)^4 = 5 \cdot 2\alpha = 3\alpha$$

$$(\alpha + 1)^{16} = 5^2 = 25 = 4$$

$$(\alpha + 1)^{24} = (\alpha + 1)^{16}(\alpha + 1)^8 = 4 \cdot 5 = -1$$

Thus, $o(\alpha + 1) = 24$.

5. Let $f = x^4 + x^3 + x^2 + x + 1 \in \mathbf{Z}_2[x]$, and let $\mathbf{F} = \mathbf{Z}_2[x]/(f)$, a field. Let $\alpha = [x]_f$.

a) What are the possible orders of the elements of $\mathbf{F}^\times$?

**Solution:** $|\mathbf{F}| = |\mathbf{Z}_2|^{\deg f} = 2^4 = 16$, so $|\mathbf{F}^\times| = 16 - 1 = 15$.

The possible orders are the divisors of 15: 1, 3, 5, 15.

b) What is the order of $\alpha$?

**Solution:** Every element of $\mathbf{F}$ may be written uniquely as a polynomial of degree $< \deg f$ in $\alpha$. Since $\alpha^3$ already has this form, that the polynomial $(x^3)$ is not the constant polynomial 1, $\alpha^3 \neq 1$, and hence $\alpha$ does not have order 3.

To write the higher powers of $\alpha$ as polynomials of degree $< 4$ in $\alpha$, we use the fundamental equation: $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$.

Thus,

$$\alpha^4 = -\alpha^3 - \alpha^2 - \alpha - 1$$

$$= \alpha^3 + \alpha^2 + \alpha + 1 \text{ since } -1 = 1 \text{ in } \mathbf{Z}_2.$$ 

Thus,

$$\alpha^5 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha$$

$$= (\alpha^3 + \alpha^2 + \alpha + 1) + \alpha^3 + \alpha^2 + \alpha$$

$$= 2\alpha^3 + 2\alpha^2 + 2\alpha + 1 = 1$$

so $o(\alpha) = 5$. 

Exam 3 Solutions

c) What is the order of $\alpha + 1$?

**SOLUTION:** We use the binomial theorem to expand the powers of $\alpha + 1$.

\[(\alpha + 1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1 = \alpha^3 + \alpha^2 + \alpha + 1\]
\[(\alpha + 1)^5 = \alpha^5 + 5\alpha^4 + 10\alpha^3 + 10\alpha^2 + 5\alpha + 1 = \alpha^5 + \alpha^4 + \alpha + 1 = 1 + (\alpha^3 + \alpha^2 + \alpha + 1) + \alpha + 1 = \alpha^3 + \alpha^2 + 1\]

Here, we used the expansions of $\alpha^5$ and $\alpha^4$ given in part b). We see that neither $(\alpha + 1)^3$ nor $(\alpha + 1)^5$ is equal to 1. Since the order of $\alpha + 1$ is 1, 3, 5, or 15, $\alpha + 1$ has order 15.

d) Find a primitive element in $F$.

**SOLUTION:** A primitive element is an element whose order is $|F^*|$. We just showed that $\alpha + 1$ has order 15, and hence $\alpha + 1$ is primitive.