1. Give a prime factorization in $\mathbb{Z}_2[x]$ for the following polynomial. Give proofs that the factors are prime. (You may use the results from class on the irreducibles in degrees $\leq 4$.)

$$f = x^8 + x^6 + x^2 + x + 1$$

**Solution:** We first test for roots. $f(0) = 1$ and $f(1) = 5 = 1$, so $f$ has no roots, hence no degree 1 factors.

We now test for degree 2 irreducible factors. $x^2 + x + 1$ is the only irreducible of degree 2 in $\mathbb{Z}_2[x]$. When we divide $f$ by $x^2 + x + 1$, the remainder is $x + 1$, so there are no irreducible factors of degree 2.

Now we test for irreducible factors of degree 3. There are two degree 3 irreducibles in $\mathbb{Z}_2[x]$: $x^3 + x + 1$ and $x^3 + x^2 + 1$. We see that $x^3 + x + 1$ divides evenly into $f$, giving

$$f = (x^3 + x + 1)(x^5 + x^2 + 1).$$

We must now factor $g = x^5 + x^2 + 1$. If $g$ is reducible, it must have an irreducible factor of degree $\leq \frac{5}{2}$, i.e., in degree $\leq 2$. But any factor of $g$ is a factor of $f$, and $f$ has no irreducible factors in degree $\leq 2$. Thus, $g$ is irreducible, and (1) is a prime factorization.

2. Let $f = x^3 + x^2 + 5x + 1$. In which of the following is $f$ irreducible?

a) $\mathbb{Q}[x]$ b) $\mathbb{Z}_2[x]$ c) $\mathbb{Z}_3[x]$ d) $\mathbb{Z}_5[x]$ e) $\mathbb{R}[x]$  

**Solution:** In all cases, since $f$ has degree 3, $f$ is irreducible if and only if it has no roots in the ground field.

a) The possible rational roots are $\frac{a}{b}$, where $a$ divides the constant term of $f$, which is 1, and $b$ divides the leading coefficient of $f$, which is also 1. Thus, the only possible rational roots are $\pm 1$. Since the coefficients of $f$ are all positive, any real roots must be negative, so $-1$ is the only possible rational root. But $f(-1) = -4 \neq 0$, so $f$ is irreducible in $\mathbb{Q}[x]$.

b) $f(0) = 1$ and $f(1) = 8 = 0$, so 1 is a root and $f$ is reducible in $\mathbb{Z}_2[x]$.

c) $f(0) = 1$, $f(1) = 8 = 2$, $f(2) = 23 = 2$, so $f$ has no roots in $\mathbb{Z}_3$, and hence is irreducible in $\mathbb{Z}_3[x]$.

d) $f(0) = 1$, $f(1) = 8 = 3$, $f(2) = 23 = 3$, $f(3) = 52 = 2$, $f(4) = 101 = 1$, so $f$ has no roots in $\mathbb{Z}_5$, and hence is irreducible in $\mathbb{Z}_5[x]$.
There are no irreducibles of degree $> 2$ in $\mathbb{R}[x]$, so $f$ is reducible there.

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

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

**Solution:** $|F| = |\mathbb{Z}_2|^\deg f = 16$. So $|F^\times| = 15$, and the possible orders are the divisors of 15: 1, 3, 5, 15.

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

**Solution:** Every element of $F$ may be written uniquely as a polynomial of degree $\leq 3$ in $\alpha$. Thus $\alpha^3 \neq 1$, and the order is not 3. The fundamental equation is

$$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0,$$

so $\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$, as $1 = -1$ in $\mathbb{Z}_2$. Thus,

$$\begin{align*}
\alpha^5 &= \alpha(\alpha^3 + \alpha^2 + \alpha + 1) \\
&= \alpha^4 + \alpha^3 + \alpha^2 + \alpha \\
&= (\alpha^3 + \alpha^2 + \alpha + 1) + \alpha^3 + \alpha^2 + \alpha \\
&= 2\alpha^3 + 2\alpha^2 + 2\alpha + 1 \\
&= 1.
\end{align*}$$

So the order of $\alpha$ is 5.

c) What is the order of $\alpha + 1$ in $F^\times$?

**Solution:** The binomial theorem gives

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

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

Every element of $F$ may be written uniquely as a polynomial of degree $\leq 3$ in $\alpha$, so the order is not 3. Continuing, we have

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

$$= \alpha^5 + \alpha^4 + \alpha + 1$$

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

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

Again, this isn’t 1, so the order is not 5. Since the order must be 1, 3, 5 or 15, the order is 15.

d) Find a primitive element of $F$.

**Solution:** Since the order of $\alpha + 1$ is $|F^\times|$, $\alpha + 1$ is primitive.
4. Let \( f = x^2 - 2 \in \mathbb{Z}_{11}[x] \), and let \( F = \mathbb{Z}_{11}[x]/(f) \), a field. Let \( \alpha = [x]_f \).

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

Solution: \( |F| = |\mathbb{Z}_{11}|^{\deg f} = 121 \). So \( |F^\times| = 120 \), and the possible orders are the divisors of 120. The fundamental equation is \( \alpha^2 - 2 = 0 \), so \( \alpha^2 = 2 \). We now calculate the order of 2.

Since 2 is in the ground field, \( o(2)|\mathbb{Z}_{11}^\times| = 10 \). We have \( 2^2 = 4 \) and \( 2^5 = 32 = -1 \), so 2 has order 10.

\[
10 = o(2) = o(\alpha^2) = \frac{o(\alpha)}{(o(\alpha), 2)},
\]

so

\[
o(\alpha) = 10(o(\alpha), 2).
\]

Thus \( 10 \mid o(\alpha) \), hence \( 2 \mid o(\alpha) \), so \( (o(\alpha), 2) = 2 \). Thus,

\[
o(\alpha) = 10(o(\alpha), 2) = 10 \cdot 2 = 20.
\]

b) What is the order of \( \alpha^{96} \) in \( F^\times \)?

\[
o(\alpha^{96}) = \frac{o(\alpha)}{(o(\alpha), 96)} = \frac{20}{(20, 96)} = \frac{20}{4} = 5.
\]

c) What is the order of \( 7\alpha \) in \( F^\times \)?

Solution: \( (7\alpha)^2 = 49\alpha^2 = 5 \cdot 2 = -1 \), so \( (7\alpha)^4 = 1 \). Since we’ve tested all divisors of 4, \( 7\alpha \) has order 4.

d) What is the order of \( \alpha + 1 \) in \( F^\times \)?

Solution: \( (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha + 3 \).

\[
(\alpha + 1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1
= 2\alpha + 3 \cdot 2 + 3\alpha + 1 = 5\alpha + 7.
\]

\[
(\alpha + 1)^4 = (2\alpha + 3)^2 = 4\alpha^2 + 12\alpha + 9 = \alpha + 6.
\]

\[
(\alpha + 1)^5 = (\alpha + 1)(\alpha + 6) = \alpha^2 + 7\alpha + 6 = 7\alpha + 8.
\]

\[
(\alpha + 1)^6 = (5\alpha + 7)^2 = 25\alpha^2 + 70\alpha + 49 = 4\alpha.
\]

We now calculate the order of \( 4\alpha \).

\[
(4\alpha)^2 = 32 = -1,
\]

so \( (4\alpha)^4 = 1 \), hence the order of \( 4\alpha \) is 4. So

\[
4 = o(4\alpha) = o((\alpha + 1)^6) = \frac{o(\alpha + 1)}{(o(\alpha + 1), 6)},
\]

so

\[
o(\alpha + 1) = 4(o(\alpha + 1), 6).
\]
So $4|o(\alpha + 1)$, hence $(o(\alpha + 1), 6) = 2$ or 6, making $o(\alpha + 1)$ either 8 or 24. Now,

$$(\alpha + 1)^8 = (\alpha + 6)^2 = \alpha^2 + 12\alpha + 36 = \alpha + 5,$$

so the order is not 8. Thus, the order is 24.