1. Give the 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 $\leq 4$.)

$$f = x^8 + x^7 + x^6 + x^5 + x^3 + x^2 + 1.$$ 

**Solution:** $f(0) = 1$ and $f(1) = 7 = 1$ so $f$ has no roots, and hence no factors of degree 1.

We next test to see if $f$ has an irreducible factor of degree 2. There is only one irreducible of degree 2 in $\mathbb{Z}_2[x]$: $x^2 + x + 1$. Using polynomial division, we obtain

$$f = (x^2 + x + 1) \cdot g \quad \text{with} \quad g = x^6 + x^3 + x^2 + x + 1.$$ 

We must now factor $g$. Since $f$ has no roots and $g | f$, $g$ has no roots. We must test to see if the unique irreducible in degree 2 divides $g$. Polynomial division gives

$$g = (x^2 + x + 1) \cdot (x^4 + x^3 + 1).$$

$x^4 + x^3 + 1$ is known to be irreducible by our computations in class. We obtain the prime decomposition

$$f = (x^2 + x + 1)^2 \cdot (x^4 + x^3 + 1).$$

2. Let $f = x^2 - x + 1 \in \mathbb{Z}_{11}[x]$, and let $\mathbb{F} = \mathbb{Z}_{11}[x]/(f)$, a field. Let $\alpha = [x]_f$.

**Solution:** Note first that the orders of elements must divide $[\mathbb{F}^\times] = [\mathbb{Z}_{11}]^{\deg f} - 1 = 120$.

The fundamental equation is $0 = f(\alpha) = \alpha^2 - \alpha + 1$, so

$$\alpha^2 = \alpha - 1.$$ 

(a) What is the order of $\alpha$ in $\mathbb{F}^\times$?

**Solution:** we use the fundamental equation repeatedly:

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

$$\alpha^3 = \alpha(\alpha - 1) = \alpha^2 - \alpha = (\alpha - 1) - \alpha = -1.$$ 

So $\alpha^6 = (-1)^2 = 1$. Since we’ve tested all divisors of 6, the order of $\alpha$ is 6.
(b) What is the order of $2\alpha$ in $\mathbb{F}^\times$?

**Solution:** We make use of our calculations of the powers of $\alpha$.

\[
(2\alpha)^2 = 2^2\alpha^2 = 4(\alpha - 1) = 4\alpha - 4
\]
\[
(2\alpha)^3 = 8\alpha^3 = -8 = 3.
\]

$3$ lies in the ground field and it will be easy to calculate its order there, as it must divide $\phi(11) = 10$.

\[
3^2 = 9 = -2
\]
\[
3^4 = (-2)^2 = 4
\]
\[
3^5 = 3 \cdot 4 = 12 = 1,
\]

so $3$ has order $5$. Thus,

\[
5 = |(2\alpha)^3| = \frac{|2\alpha|}{(|2\alpha|, 3)}
\]
\[
|2\alpha| = 5(|2\alpha|, 3).
\]

Since $3$ is prime, $|\alpha| = 1$ or $3$, so $|2\alpha|$ is $5$ or $15$. Now

\[
(2\alpha)^5 = 2^5\alpha^5 = -\alpha^3\alpha^2 = \alpha^2 = \alpha - 1,
\]

so $|2\alpha| = 15$.

(c) What is the order of $3\alpha$ in $\mathbb{F}^\times$?

**Solution:** $|3|, |\alpha| = (5, 6) = 1$, so

\[
|3 \cdot \alpha| = |3| \cdot |\alpha| = 30.
\]

(d) What is the order of $\alpha + 1$ in $\mathbb{F}^\times$? **Solution:**

\[
(\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = (\alpha - 1) + 2\alpha + 1 = 3\alpha.
\]

From the preceding part, we see that $3\alpha$ has order $30$. Thus,

\[
30 = |(\alpha + 1)^2| = \frac{|\alpha + 1|}{(|\alpha + 1|, 2)}
\]
\[
|\alpha + 1| = 30(|\alpha + 1|, 2).
\]

Thus, $30$ divides $|\alpha + 1|$, so $2$ does also, and hence $|(\alpha + 1|, 2) = 2$.
So $|\alpha + 1| = 60$.

**Remarks:** $|2| = 10$, while $|3| = 5$. The order of $2\alpha$ is strictly less than $|(\alpha + 1|, 2) = 30$ because $2^{15} = \alpha^{15} = -1$.

Meanwhile, despite the fact that the order of $3$ is smaller than the order of $2$, the order of $3\alpha$ is greater than the order of $2\alpha$. 
3. Let \( f = x^2 + 1 \in \mathbb{Z}_{19}[x] \), and let \( F = \mathbb{Z}_{19}[x]/(f) \), a field. Let \( \alpha = [x]_f \).

**Solution:** Here,

\[
|F^\times| = |F| - 1 = |\mathbb{Z}_{19}|^{\deg f} - 1 = 168 = 2^3 \cdot 3 \cdot 7, 
\]

and the fundamental equation is \( \alpha^2 + 1 = 0 \), so \( \alpha^2 = -1 \).

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

**Solution:** \( \alpha^4 = (-1)^2 = 1 \). Since we’ve tested all divisors of 4, we see the order of \( \alpha \) is 4.

(b) What is the order of \( 2\alpha \) in \( F^\times \)?

**Solution:**

\[
(2\alpha)^2 = 4\alpha^2 = -4. 
\]

Let’s calculate the order of \(-4\). Since \(-4\) lies in the ground field, its order divides \( \phi(19) = 18 = 2 \cdot 3^2 \).

\[
(-4)^2 = 16 = -3 \\
(-4)^3 = (-3)(-4) = 12 = -7 \\
(-4)^6 = (-7)^2 = 49 = 11 = -8 \\
(-4)^9 = (-7)(-8) = 56 = -1. 
\]

Thus, \( |\alpha| = 18 \). So

\[
18 = |(2\alpha)^2| = \frac{|2\alpha|}{(2\alpha, 2)} \\
|2\alpha| = 18 \cdot (|2\alpha|, 2). 
\]

Since 18 divides \( |2\alpha| \), so does 2, hence \( (|2\alpha|, 2) = 2 \). Thus, \( |2\alpha| = 36 \).

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

**Solution:**

\[
(\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha. 
\]

By the preceding part, \( |2\alpha| = 36 \). So

\[
36 = |(\alpha + 1)^2| = \frac{|\alpha + 1|}{(|\alpha + 1|, 2)} \\
|\alpha + 1| = 36(|\alpha + 1|, 2). 
\]

As above, \( (|\alpha + 1|, 2) = 2 \), so \( |\alpha + 1| = 72 \).