Math 326  Exam 3 Solutions  Fall 2014

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 \( \leq 4 \).)

\[ f = x^8 + x^5 + x^4 + x + 1. \]

**Solution:** \( f(0) = f(1) = 1 \), so \( f \) has no roots, and hence no degree 1 factors. The only irreducible in degree 2 is \( x^2 + x + 1 \). Using the division algorithm, we see that \( x^2 + x + 1 \) does not divide \( f \). So we test for irreducible factors of degree 3. \( x^3 + x + 1 \) does divide \( f \), with quotient \( x^5 + x^3 + 1 \). Since \( f \) has no irreducible factors of degree 1 or 2, neither does \( x^5 + x^3 + 1 \). But \( x^5 + x^3 + 1 \) has degree 5, and it has no irreducible factors of degree \( \leq \frac{5}{2} \), so it is irreducible. Thus,

\[ f = (x^3 + x + 1)(x^5 + x^3 + 1) \]

is a prime decomposition.

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

(a) What are the possible orders of the elements of \( \mathbb{F}^\times \)? **Solution:** 

\[ |F| = |\mathbb{Z}_2|^{\deg f} = 2^4 = 16. \]

So \( |\mathbb{F}^\times| = 16 - 1 = 15 \). The possible orders are the divisors of 15: 1, 3, 5 and 15.

(b) What is the order of \( \alpha \) in \( \mathbb{F}^\times \)? **Solution:** The fundamental equation is \( \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0 \). Since \( -1 = 1 \) in \( \mathbb{Z}_2 \), we get 

\[ \alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1. \]

Every element of \( F \) may be written uniquely in the standard form 

\[ a_3 \alpha^3 + a + 2a_2 + a_1 \alpha + a_0 \]

with \( a_0, \ldots, a_3 \in \mathbb{Z}_2 \), so \( \alpha^3 \neq 1 \) and \( |\alpha| \neq 3 \). Now 

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

\[ = \alpha^4 + \alpha^3 + \alpha^2 + \alpha \]

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

So \( |\alpha| = 5 \).
(c) What is the inverse of $\alpha + 1$? Solution: The division algorithm gives
\[ f = (x + 1)(x^3 + x) + 1. \]
So $0 = f(\alpha) = (\alpha + 1)(\alpha^3 + \alpha) + 1$. Since $-1 = 1$ in $\mathbb{Z}_2$,
\[ (\alpha + 1)(\alpha^3 + \alpha) = 1, \]
and hence the inverse of $\alpha + 1$ is $\alpha^3 + \alpha$.

3. Let $f = x^2 - 5 \in \mathbb{Z}_{13}[x]$, and let $\mathbb{F} = \mathbb{Z}_{13}[x]/(f)$, a field. Let $\alpha = [x]_f$. 
(a) What are the possible orders of the elements of $\mathbb{F}^\times$? Solution:
\[ |F| = |\mathbb{Z}_{13}|^{\deg f} = 13^2 = 169. \]
So $|\mathbb{F}^\times| = 168 = 8 \cdot 3 \cdot 7$. The possible orders are the divisors of 168.

(b) What is the order of $\alpha$ in $\mathbb{F}^\times$? Solution: The fundamental equation is $\alpha^2 - 5 = 0$, so $\alpha^2 = 5$. So $\alpha^4 = 5^2 = -1$, and $\alpha^8 = 1$. So the order of $\alpha$ divides 8. We’ve tested all the divisors of 8, so $|\alpha| = 8$.

(c) What is the order of $3\alpha$ in $\mathbb{F}^\times$? Solution: $3^3 = 27 = 1$, so the order of 3 divides 3. Since it’s order is not 1, its order must be 3. Thus $(3, |\alpha|) = (3, 8) = 1$. So $|3\alpha| = |3| \cdot |\alpha| = 24$. This can also be shown directly: $(3\alpha)^k = 3^k \alpha^k$ and do the math. :D

(d) What is the order of $\alpha + 1$ in $\mathbb{F}^\times$? Solution:
\[ (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha + 6 \]
\[ (\alpha + 1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1 = 8\alpha + 3 \]
\[ (\alpha + 1)^4 = (2\alpha + 6)^2 = 11\alpha + 4 \]
\[ (\alpha + 1)^6 = (8\alpha + 3)^2 = 9\alpha + 4 \]
\[ (\alpha + 1)^7 = (9\alpha + 4)(\alpha + 1) = 10. \]
Since 10 is in the ground field, $\mathbb{Z}_{13}$, its order divides 12. We can compute the order quickly: $10^2 = 9$. $10^3 = (-3)9 = -27 = -1$. So 10 has order 6. We get
\[ 6 = |(\alpha + 1)^7| = \frac{|\alpha + 1|}{|\alpha + 1|, 7}. \]
So $|\alpha + 1| = 6(|\alpha + 1|, 7)$, which is either 6 or 42. Since we’ve tested 6 already, the order is 42.

(e) Find a generator of $\mathbb{F}^\times$. Solution: We have
\[ |(\alpha + 1)^6| = \frac{|\alpha + 1|}{|\alpha + 1|, 6} = \frac{42}{42, 6} = 7. \]
So $(|(\alpha + 1)^6|, |3\alpha|) = (7, 24) = 1$, so $|(\alpha + 1)^6 \cdot 3\alpha| = 7 \cdot 24 = 168$. So $(\alpha + 1)^6 \cdot 3\alpha$ is a generator of $\mathbb{F}^\times$. 