Math 236
Prof. Seelinger
Fall 2008

EXAM III – Solutions

Answer all of the following problems. Each problem is worth 20 points.
Fully justify each answer.

1. Prove that the following polynomials are irreducible.

   (a) $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.

   To show $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$, we first note that $f(x)$ has no roots in $\mathbb{Z}_2$ since $f(0) = 1$ and $f(1) = 1$. So, by the Factor Theorem, $f(x)$ has no linear factors. Also, by Theorem 4.2, $f(x)$ has no degree 3 factors. So we check the irreducible degree 2 factors. By results in class, we know x^2+x+1 is the only irreducible degree 2 polynomial in $\mathbb{Z}_2[x]$ (it is the only one without roots), hence we divide $f(x)$ by $x^2 + x + 1$ and we get a remainder of $x + 1$. Therefore $x^2 + x + 1$ is not a factor of $f(x)$, hence $f(x)$ is irreducible.

   (b) $x^4 - 7x^3 + 5x^2 - 3x - 9$ is irreducible in $\mathbb{Q}[x]$.

   We reduce $g(x) = x^4-7x^3+5x^2-3x-9$ modulo 2 to get $\bar{g}(x) = x^4+x^3+x^2+x+1$, which was shown to be irreducible in $\mathbb{Z}_2[x]$ in Part (a). Therefore, by Theorem 4.24, $g(x)$ is irreducible in $\mathbb{Q}[x]$.

   (c) $x^8 + 6x^5 - 12x^3 + 18x^2 - 24x - 60$ is irreducible in $\mathbb{Q}[x]$.

   Here we can use Eisenstein's Criterion with $p = 3$. Indeed, $3 \nmid 1$, $3|6$, $3|-12$, $3|24$, and $3|60$, but $3^2 \nmid 60$. Therefore, by Eisenstein's Criterion, $x^8 + 6x^5 - 12x^3 + 18x^2 - 24x - 60$ is irreducible in $\mathbb{Q}[x]$.

2. Find all monic irreducible polynomials of degree 2 in $\mathbb{Z}_3[x]$. Justify why each of these polynomials are irreducible and why these are the only irreducibles.

   By Corollary 4.18, a polynomial of degree 2 in $\mathbb{Z}_3[x]$ is irreducible if and only if it has no roots in $\mathbb{Z}_3$. There are 9 monic polynomials of degree 2 in $\mathbb{Z}_3[x]$ of which three have no constant, hence zero would be a root of these three. This leaves six possibilities: $x^2+1, x^2+2, x^2+x+1, x^2+x+2, x^2+2x+1, x^2+2x+2$. We test these six for roots.

$f(x)$	x^2+1	x^2+2	x^2+x+1	x^2+x+2	x^2+2x+1	x^2+2x+2
$f(1)$	2	0	0	1	1	2
$f(2)$	2	0	1	2	0	1

Therefore, there are exactly three monic degree 2 polynomials without roots, $x^2 + 1$, $x^2 + x + 2$, and $x^2 + 2x + 2$, hence by Corollary 4.18 these are the only monic degree 2 irreducible polynomials in $\mathbb{Z}_2[x]$.

3. Factor $x^6 + x^4 + 2x^2 + 2 \in \mathbb{Z}_3[x]$ into a product of irreducibles. Say why each of the factors you have are irreducible.

   Let $f(x) = x^6 + x^4 + 2x^2 + 2 \in \mathbb{Z}_3[x]$. Then $f(1) = 6 = 0$ and $f(2) = 90 = 0$, so by the Factor Theorem, $(x - 1) = (x + 2)$ and $(x - 2) = (x + 1)$ are factors of $f(x)$. After doing long division, we get that $f(x) = (x + 1)(x + 2)(x^4 + 2x^2 + 1)$. But $x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$. So we get $f(x) = (x + 1)(x + 2)(x^2 + 1)^2$. We further note each linear factor is irreducible since it is of degree 1, and $x^2 + 1$ is irreducible by Problem 2.

4. Let
$$R = \mathbb{Z}_3[x]/(x^2 + 2x + 2).$$
   Determine how many congruence classes there are in R and list a representative of each congruence class.

   By Corollary 5.5, there is one congruence class in R for each polynomial of degree 1, degree 0, and the zero polynomial. Hence there are $3^2 = 9$ of these. They are: $[0], [1], [2], [x], [x + 1], [x + 2], [2x], [2x + 1], [2x + 2]$.

5. Use the Euclidean Algorithm to find the greatest common divisor of $f(x) = x^4 + 3x^3 + 4x^2 + 2$ and $g(x) = x^3 + 4x^2 + 2$ in $\mathbb{Z}_5[x]$. Show all work.

   To use the Euclidean Algorithm, we do a series of divisions. From our first division, we get
$$q_1(x) = x + 4 \quad \text{and} \quad r_1(x) = 3x^2 + 3x + 4.$$
   Then we divide $g(x)$ by $r_1(x)$ and we get
$$q_2(x) = 2x + 1 \quad \text{and} \quad r_2(x) = 4x + 3.$$
   Now we divide $r_1(x)$ by $r_2(x)$ and we get
$$q_2(x) = 2x + 3 \quad \text{and} \quad r_3(x) = 0.$$
   Therefore, the greatest common divisor is the monic associate of $r_2(x)$, which is $4(4x + 3) = 16x + 12 = x + 2$.