PMAT 315
SOLUTIONS TO ASSIGNMENT 6
WINTER 2010

1. (a) For which primes p is $x+2$ a factor of $f(x) = 5x^4 - 2x^3 + 3x^2 + 4x - 1$ in $\mathbb{Z}_p[x]$? 3 marks

   (b) Factor $f(x) = x^3 + 1$ into linear factors in $\mathbb{Z}_7[x]$. 2 marks

   (c) Find all roots in $\mathbb{Q}$ of $f(x) = 4x^4 + 4x^3 + 3x^2 - x - 1$, and factor $f(x)$ as far as possible in $\mathbb{Q}[x]$. 3 marks

   SOLUTION. (a). $f(-2) = 80 + 16 + 12 - 8 - 1 = 99$ is 0 in $\mathbb{Z}_p$ only if $p = 3$ or $p = 11$. We have $q(x) = 2x^3 + 1$ in $\mathbb{Z}_3[x]$ and $q(x) = 5x^3 - x^2 + 5x + 5$ in $\mathbb{Z}_{11}[x]$.

   (b). Since -1 is a root, $f(x) = (x+1)(x^2 - x + 1)$ in $\mathbb{Z}_7[x]$ by long division. Then -3 is a root of $x^2 - x + 1$ so finally $x^3 + 1 = (x+1)(x-3)(x-5)$ in $\mathbb{Z}_7[x]$.

   (c). By the Rational Roots Theorem, the roots in $\mathbb{Q}$ are $\frac{1}{2}$ and $-\frac{1}{2}$. Then long division (twice) gives $f(x) = (2x-1)(2x+1)(x^2 + x + 1)$.

2. §4.1, #26. If $m \geq 0$ is an integer, show that $\sqrt[n]{m}$ is not rational unless $m = k^n$ for some integer k. 8 marks

   SOLUTION. Put $f(x) = x^n - m$ in $\mathbb{Z}[x]$. If $\frac{c}{d}$ is a rational root of $f(x)$ in lowest terms then $c|m$ and $d|1$, so $\frac{c}{d} = k$ is an integer. Thus $f\left(\frac{c}{d}\right) = 0$ means $m = k^n$.

3. (a) Factor $f(x) = x^4 - x^2 + x - 1$ into irreducibles in $\mathbb{Z}_{13}[x]$. 2 marks

   (b). Factor $f(x) = x^5 + 6x^4 + 12x + 15$ into irreducibles in $\mathbb{Q}[x]$. 2 marks

   (c) Factor $f(x) = x^4 - x^3 + 2x^2 - 3x + 2$ into irreducibles in $\mathbb{Q}[x]$. 4 marks

   SOLUTION. (a). Since 1 is a root, $f(x) = (x-1)(x^3 + x^2 + 1)$. Now 2 is a root of $x^3 + x^2 + 1$, so another division gives $x^4 - x^2 + x - 1 = (x-1)(x-2)(x^2 + 3x + 6)$ in $\mathbb{Z}_{13}[x]$.

   (b) $f(x)$ is itself irreducible by the Eisenstein criterion (with $p = 3$).

   (c). There are no rational roots (candidates ± 1 , ± 2). If it factors in $\mathbb{Q}[x]$, it must factor in $\mathbb{Z}[x]$.

   So assume if possible that $f(x) = (x^2 + ax + b)(x^2 + cx + d)$; $a, b, c, d \in \mathbb{Z}$. Comparing coefficients gives

   $$a + c = -1, \quad b + ac + d = 2, \quad ad + bc = -3 \quad \text{and} \quad bd = 2.$$

   Hence $(b, d) = (1, 2)$, $(-1, -2)$, $(2, 1)$ or $(-2, -1)$. By symmetry, assume $(b, d) = (1, 2)$ or $(b, d) = (-1, -2)$.

   Case 1. $(b, d) = (1, 2)$. Then $-3 = ad + bc = 2a + c = 2a + (-1 - a) = a - 1$; $a = -2$, $c = 1$. But then $2 = b + d + ac = 1$, a contradiction.

   Case 2. $(b, d) = (-1, -2)$. Then $-3 = ad + bc = -2a - c = -2a - (-1 - a) = 1 - a$; $a = 4$, $c = -5$. With this, $2 = b + d + ac = -23$, a contradiction.

   So $f(x)$ is already irreducible in $\mathbb{Q}[x]$.

4. §4.3, #10(a). If F is any field, show that $\frac{F[x]}{\langle x^2 \rangle} \cong \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \middle| \, a, b \in F \right\}$. 8 marks

   SOLUTION. As in Theorem 2 §4.3 with $h(x) = x^2$, $R = F[x]/\langle x^2 \rangle = \{a + bt \mid a, b \in F;\ t^2 = 0\}$. Define $\theta : R \to M_2[F]$ by $\theta(a + bt) = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$. This is well defined by Lemma 3 and is clearly a one-to-one homomorphism of additive groups carrying 1 to 1. Finally

   $$\theta[(a+bt)(c+dt)] = \theta[ac + (ad+bc)t] = \begin{bmatrix} ac & ad+bc \\ 0 & ac \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} = \theta(a+bt) \cdot \theta(c+dt)$$

   so θ is a one-to-one ring homomorphism. Thus $R \cong \theta(R) = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \middle| \, a, b \in F \right\}$.

5. §4.3, #14(d). If $p(x) = x^3 - x^2 + 1$, let $E = \mathbb{Z}_3[x]/\langle p(x) \rangle$. Factor $p(x)$ into linear factors in $E[x]$. 8 marks

   SOLUTION. Here $E = \{a + bt + ct^2 \mid t^3 = t^2 - 1; a, b, c \in \mathbb{Z}_3\}$. We know that t is a root of $p(x)$ in $\mathbb{Z}_3[x]$, so $x - t$ is a factor. Long division gives

   $$p(x) = x^3 - x^2 + 1 = (x - t)[x^2 + (t-1)x + (t^2 - t)].$$

One way to find a root of $x^2 + (t-1)x + (t^2 - t)$ is to use the quadratic formula. Note that $\frac{1}{2} = -1$ in $\mathbb{Z}_3$, so the formula reads

$$x = -[-(t-1) \pm \sqrt{(1-t)}] = (t-1) \pm \sqrt{(1-t)}.$$

This turns the search into finding a square root of $1-t$ in E. One verifies that $(t^2-t)^2 = 1-t$, so

$$x = (t-1) \pm (t^2 - t).$$

Hence the roots are $t^2 - 1$ and $-(1+t+t^2)$. Finally, then

$$p(x) = [x-t][x-(t^2-1)][x+(1+t+t^2)].$$