MATH 431 Written Homework 2 Solution Radford 02/05/09

1. Page 315, number 4: (**20 points**) Write $r = p/q$, where $p, q \in \mathbf{Z}$ and have no common prime factor. Since r is a root of $f(x)$ we may write $f(x) = (x - r)g(x)$ for some $g(x) \in \mathbf{Q}[x]$. Clearing denominators $ag(x) = bh(x)$ for some non-zero $a, b \in \mathbf{Z}$, where $h(x) \in \mathbf{Z}[x]$ and is primitive. Thus $aqf(x) = (qx - p)ag(x) = b(qx - p)h(x)$ (**10**). Now $(qx - p)h(x)$ is the product of primitive polynomials and is thus primitive. Therefore $aq = \pm b$ which means $f(x) = \pm(qx - p)h(x)$ (**5**).

By assumption $f(x) = a_0 + \cdots + a_n x^n \in \mathbf{Z}[x]$, where $n \geq 0$ and $a_n = 1$. Write $h(x) = b_0 + \cdots + b_m x^m \in \mathbf{Z}[x]$. Then $1 = a_n = \pm q b_m$ which means $q, b_m \in \{-1, 1\}$. Therefore $r = p/q \in \mathbf{Z}$ (**5**).

2. Page 316, number 10: (**20 points**) The polynomials of (a) and (c) are irreducible over $\mathbf{Q}$ by the Eisenstein Criterion with $p = 3$ (**7**, **7**). Let $f(x)$ be the polynomial of (c) and $u \in \mathbf{Q}$ be non-zero, that is a unit u of $\mathbf{Q}$. Then $f(x)$ is irreducible over $\mathbf{Q}$ if and only if $uf(x)$ is irreducible over $\mathbf{Q}$. Now $14f(x)$ is irreducible over $\mathbf{Q}$ by the Eisenstein criterion with $p = 3$ again. Therefore $f(x)$ is irreducible over $\mathbf{Q}$ (**6**).

Parts (b) and (d) were not graded; however here are solutions. We apply the mod 2 test in both cases.

Part (b). $x^4 + x + 1 \in \mathbf{Z}[x]$ is primitive. Thus $x^4 + x + 1 \in \mathbf{Q}[x]$ is irreducible if and only if $x^4 + x + 1 \in \mathbf{Z}[x]$ is irreducible.

The mod 2 reduction of $x^4 + x + 1 \in \mathbf{Z}[x]$ is $f(x) = x^4 + x + 1 \in \mathbf{Z}_2[x]$. Since $f(a) = 1 \neq 0$ for all $a \in \mathbf{Z}2$ it follows that $f(x)$ has no linear factors.

Suppose that $f(x)$ is reducible. Then it must be the product of quadratic factors.

There are 3 quadratic *reducible* polynomials in $\mathbf{Z}_2[x]$; see the solution of Exercise 3 below. Thus there is 1 irreducible quadratic in $\mathbf{Z}_2[x]$ which is $x^2 + x + 1$ since this polynomial has no roots in $\mathbf{Z}_2[x]$. Therefore $f(x) = (x^2 + x + 1)^2 = x^4 + x^2 + 1$ which is not the case.

We have shown $f(x) \in \mathbf{Z}_2[x]$ is irreducible. Thus $x^4 + x + 1 \in \mathbf{Z}[x]$ is irreducible which means $x^4 + x + 1 \in \mathbf{Q}[x]$ is also.

Part (d). Note $x^5 + 5x^2 + 1 \in \mathbf{Q}[x]$ as a polynomial in $\mathbf{Z}[x]$ is primitive and the mod 2 reduction is $f(x) = x^5 + x^2 + 1 \in \mathbf{Z}_2[x]$. This polynomial has no roots in $\mathbf{Z}$ which means $f(x)$ has no linear factors.

Suppose $f(x)$ is reducible. Then it is divisible by an irreducible quadratic which must be $x^2 + x + 1$ from part (b). Since $x^5 + x^2 + 1 = (x^3 + x^2)(x^2 + x + 1) + 1$, this is not possible by the Division Algorithm. Thus $f(x) \in \mathbf{Z}_2[x]$ is irreducible and therefore $x^5 + 5x^2 + 1 \in \mathbf{Q}[x]$ is as well by the argument of part (b).

3. Page 316, number 16: (**20 points**) (a) We count the number of *reducible* polynomials in $\mathbf{Z}_p[x]$ of the form $x^2 + ax + b$. These are of type $(x - d)^2$ or $(x - d)(x - e) = (x - e)(x - d)$, where $d \neq e$. There are p of the first type, $\binom{p}{2}$ of the second, and p^2 of the form

$x^2 + bx + c$. The number of *irreducible* polynomials of the form $x^2 + ax + b$ is therefore $p^2 - (p + \binom{p}{2}) = p(p-1) - \frac{p(p-1)}{2} = \frac{p(p-1)}{2}$ (**10**).

(b) Let $f(x) \in \mathbf{Z}_p[x]$ and $0 \neq u \in \mathbf{Z}_p$. Then $f(x)$ is irreducible if and only if $uf(x)$ is irreducible. Thus the number of irreducible polynomials in $\mathbf{Z}_p[x]$ of the form ax^2+bx+c, where $a \neq 0$, is $p-1$ times the answer in part (a). There are $\frac{(p-1)^2 p}{2}$ of them (**10**).

4. Page 316, number 22: (**20 points**) Suppose $\pi^2 = a\pi + b$, or equivalently $\pi^2 - a\pi - b = 0$ (**10**), for some $a, b \in \mathbf{Q}$. Then π is a zero, or root, of the polynomial $f(x) = x^2 - ax - b \in \mathbf{Q}[x]$ which contradicts the given of the problem. Therefore $\pi^2 \neq a\pi + b$ for all $a, b \in \mathbf{Q}$ (**10**).

5. Page 316, number 24: (**20 points**) $f(x) = 3x^2 + x + 4 \in \mathbf{Z}_7[x]$. By the quadratic formula the roots of $f(x)$ in $\mathbf{Z}_7$ are given by

$$((-1) \pm \sqrt{(-1)^2 - 4{\cdot}3{\cdot}4})(2{\cdot}3)^{-1} = ((-1) \pm \sqrt{2})(-1)^{-1} = (-1 \pm 3)(-1) = 4, -2 \;\; (\mathbf{5})$$

or $4, 5$ (**5**). Substitution yields $f(4) = 0 = f(5)$ (**5**). The quadratic formula holds if and only if $b^2 - 4ac$ has a square root in $\mathbf{Z}_p$ (**5**).