Homework #6 Solutions

p 315, #4 Let \( f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x] \) and suppose that \( x - r \) divides \( f(x) \) for some \( r \in \mathbb{Q} \). Then we must have \( f(r) = 0 \). We will use this fact to prove that in fact \( r \in \mathbb{Z} \). If \( r = 0 \) then there is nothing to prove. So assume \( r \neq 0 \) and write \( r = a/b \) with \( a, b \in \mathbb{Z} \), \( b \neq 0 \) and \((a, b) = 1\). Then

\[
0 = f(r) = f(a/b) = \left(\frac{a}{b}\right)^n + a_{n-1} \left(\frac{a}{b}\right)^{n-1} + \cdots + a_1 \left(\frac{a}{b}\right) + a_0.
\]

Multiplying both sides by \( b^n \) then yields

\[
0 = a^n + a_{n-1}a^{n-1}b + a_{n-2}a^{n-2}b^2 + \cdots + a_1ab^{n-1} + a_0b^n
\]

which is equivalent to

\[
a^n = -(a_{n-1}a^{n-1}b + a_{n-2}a^{n-2}b^2 + \cdots + a_1ab^{n-1} + a_0b^n)
= -b(a_{n-1}a^{n-1} + a_{n-2}a^{n-2}b + \cdots + a_1ab^{n-2} + a_0b^{n-1}).
\]

Since \( a_{n-1}a^{n-1} + a_{n-2}a^{n-2}b + \cdots + a_1ab^{n-2} + a_0b^{n-1} \in \mathbb{Z} \), this implies that \( b \) divides \( a^n \). Since \((a, b) = 1\), this can only occur if \( b = \pm 1 \). But then \( r = a/b = \pm a \in \mathbb{Z} \), as claimed.

p 315, #6 If \( p \) is prime and \( f(x) \in \mathbb{Z}_p[x] \) is irreducible then \( \mathbb{Z}_p[x]/\langle f(x) \rangle \) is a field by Corollary 1 to Theorem 17.5, since \( \mathbb{Z}_p \) is a field. Moreover, we proved in class that since \( \deg f(x) = n \) the each element of \( \mathbb{Z}_p[x]/\langle f(x) \rangle \) can be expressed uniquely as \( a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 + \langle f(x) \rangle \) for some \( a_i \in F \). Since there are \( p \) choices for each coefficient \( a_i \) and \( n \) coefficients, there are exactly \( p^n \) such cosets. That is, \( \mathbb{Z}_p[x]/\langle f(x) \rangle \) is a field with \( p^n \) elements.

p 316, #8 Let \( f(x) = x^3 + 2x + 1 \in \mathbb{Z}_3[x] \). It is easy to show that \( f(x) \) has no roots in \( \mathbb{Z}_3 \) and as \( \deg f(x) = 3 \), this implies \( f(x) \) is irreducible in \( \mathbb{Z}_3[x] \). So according to Exercise #6, \( \mathbb{Z}_3[x]/\langle x^3 + 2x + 1 \rangle \) is a field with \( 3^3 = 27 \) elements.

p 316, #10

a. \( x^5 + 9x^4 + 12x^2 + 6 \) is irreducible according Eisenstein’s criterion with \( p = 3 \).

b. Consider \( x^4 + x + 1 \mod 2 \). It is easy to see that this polynomial has no roots in \( \mathbb{Z}_2 \), and so to prove irreducibility in \( \mathbb{Z}_2 \) it suffices to show it has no quadratic factors. The only quadratic polynomial in \( \mathbb{Z}_2[x] \) that does not have a root in \( \mathbb{Z}_2 \) is \( x^2 + x + 1 \) which does not divide \( x^4 + x + 1 \) in \( \mathbb{Z}_2[x] \), as is also easily checked. It follows that \( x^4 + x + 1 \) is irreducible in \( \mathbb{Z}_2[x] \) and so by the mod \( p \) test with \( p = 2 \) we conclude that \( x^4 + x + 1 \) is irreducible in \( \mathbb{Q}[x] \).
c. $x^4 + 3x^2 + 3$ is irreducible according to Eisenstein’s criterion with $p = 3$.

d. Consider $x^5 + 5x^2 + 1 \mod 2$, which is $x^5 + x^2 + 1$. It is easy to see that this polynomial has no roots in $\mathbb{Z}_2$, and so to prove irreducibility in $\mathbb{Z}_2$ it again suffices to show it has no quadratic factors. The only quadratic polynomial in $\mathbb{Z}_2[x]$ that does not have a root in $\mathbb{Z}_2$ is $x^2 + x + 1$ which does not divide $x^5 + x^2 + 1$ in $\mathbb{Z}_2[x]$, as is also easily checked. It follows that $x^5 + x^2 + 1$ is irreducible in $\mathbb{Z}_2[x]$ and so by the mod $p$ test with $p = 2$ we conclude that $x^5 + 5x^2 + 1$ is irreducible in $\mathbb{Q}[x]$.

e. Let $f(x) = (5/2)x^5 + (9/2)x^4 + 15x^3 + (3/7)x^2 + 6x + 3/14$ and $g(x) = 35x^5 + 63x^4 + 210x^3 + 6x^2 + 84x + 3 = 14f(x)$. Since 14 is a unit in $\mathbb{Q}[x]$, $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if $g(x)$ is, and the latter statement is true by Eisenstein’s criterion with $p = 3$.

p 316, #12 Since it has degree 2, to show that $x^2 + x + 4$ is irreducible in $\mathbb{Z}_41[x]$ it suffices to show it has no roots in $\mathbb{Z}_{11}$, as $\mathbb{Z}_{11}$ is a field. This is straightforward and is left to the reader.

p 316, #16

a. Since $\mathbb{Z}_p$ is a field, a polynomial of the form $x^2 + ax + b \in \mathbb{Z}_p[x]$ is reducible if and only if there exist $c, d \in \mathbb{Z}_{11}$ so that $x^2 + ax + b = (x + c)(x + d)$. There are $\binom{p}{2}$ such polynomials for which $c \neq d$ and $p$ for which $c = d$. Therefore, there are exactly

$$\binom{p}{2} + p = \frac{p(p - 1)}{2} + p = \frac{p(p + 1)}{2}$$

reducible monic quadratic polynomials in $\mathbb{Z}_p[x]$. Since there are $p^2$ polynomials of the form $x^2 + ax + b$ and each one is either reducible or irreducible, we conclude there are

$$p^2 - \frac{p(p + 1)}{2} = \frac{p(p - 1)}{2}$$

irreducible monic degree 2 polynomials in $\mathbb{Z}_p[x]$.

b. If $f(x) \in \mathbb{Z}_p[x]$ is irreducible of degree 2, then $f(x) = ag(x)$ for some $a \in F$, $a \neq 0$ and $g(x) \in F[x]$ irreducible, monic and of degree 2. There are $p - 1$ choices for $a$ and, by part (a), $p(p - 1)/2$ choices for $g(x)$. Therefore there are $p(p - 1)^2/2$ irreducible quadratic polynomials in $\mathbb{Z}_p[x]$.

p 316, #24 Substituting all of the elements of $\mathbb{Z}_7$ into $3x^2 + x + 4$ we find that it has two roots: 4 and 5. The quadratic formula “predicts” the roots

$$\frac{-1 \pm \sqrt{-47}}{6} = 6(-1 \pm \sqrt{2}) = 1 \pm 6\sqrt{2}$$

since $6^{-1} = 6$ in $\mathbb{Z}_7$ and $-47 = 2$ in $\mathbb{Z}_7$. Since $3^2 = 9 = 2$ in $\mathbb{Z}_7$, we can take $\sqrt{2} = 3$ and so the two predicted roots are

$$1 \pm 6 \cdot 3 = 4, 5$$
which agree with those found by substitution.

If we substitute all of the elements of \( \mathbb{Z}_5 \) into \( 2x^2 + x + 3 \) we find no roots. The quadratic formula predicts the roots are

\[
\frac{-1 \pm \sqrt{-23}}{4} = 4(4 + \sqrt{2}) = 1 + 4\sqrt{2}
\]
since \( 4^{-1} = 4 \) and \(-23 = 2 \) in \( \mathbb{Z}_5 \). However, there is no element in \( \mathbb{Z}_5 \) whose square is 2, so \( \sqrt{2} \) is not an element of \( \mathbb{Z}_5 \). Consequently the roots predicted by the quadratic formula do not belong to \( \mathbb{Z}_5 \), which is in agreement with the fact that there are no roots in \( \mathbb{Z}_5 \).

It turns out that the quadratic formula always gives the roots of \( ax^2 + bx + c \in F[x] \) for any field \( F \), as long as we agree that if \( b^2 - 4ac \) is not a square in \( F \) then we interpret the formula as yielding no roots. This is easily proven using the usual proof of the quadratic formula (i.e. completing the square).

\[\text{p 317, #28} \quad \text{Let } f(x) \in \mathbb{Q}[x] \text{ be nonzero. Choose an } n \in \mathbb{Z}^+ \text{ so that } g(x) = nf(x) \in \mathbb{Z}[x]. \text{ Since } n \neq 0 \text{ it is a unit in } \mathbb{Q}[x]. \text{ So } f(x) \text{ is irreducible in } \mathbb{Q}[x] \text{ if and only if } g(x) \text{ is, and the latter’s irreducibility can be tested using the mod } p \text{ test.}\]

\[\text{p 317, #30} \quad \text{Let } f(x) = x^{p-1} - x^{p-2} + x^{p-3} - \cdots - x + 1. \text{ If } p = 2 \text{ then the polynomial in question is } x - 1 \text{ which is obviously irreducible in } \mathbb{Q}[x]. \text{ If } p > 2 \text{ then it is odd and so } g(x) = f(-x) = x^{p-1} + x^{p-2} + x^{p-3} + \cdots + x + 1 \text{ is the } p \text{th cyclotomic polynomial, which is irreducible according to the Corollary of Theorem 17.4. It follows that } f(x) \text{ is irreducible, for if } f(x) \text{ factored so too would } g(x).\]

\[\text{p 317, #32} \quad \text{Let } f(x), g(x) \in \mathbb{Z}[x] \text{ and suppose that } f(x)g(x) \in \langle x^2 + 1 \rangle. \text{ Then there is an } h(x) \in \mathbb{Z}[x] \text{ so that } f(x)g(x) = (x^2 + 1)h(x). \text{ Since } x^2 + 1 \text{ is primitive and irreducible in } \mathbb{Q}[x], \text{ it is also irreducible in } \mathbb{Z}[x]. \text{ We apply Theorem 17.6 to write}
\]

\[
f(x) = a_1 \cdots a_k p_1(x) \cdots p_l(x)
g(x) = b_1 \cdots b_m q_1(x) \cdots q_n(x)
h(x) = c_1 \cdots c_t r_1(x) \cdots r_t(x)
\]

where the \( a_i, b_i \) and \( c_i \) are primes in \( \mathbb{Z} \) and the \( p_i(x), q_i(x) \) and \( r_i(x) \) are irreducible polynomials of positive degree in \( \mathbb{Z}[x] \). Substituting these expressions into \( f(x)g(x) = (x^2 + 1)h(x) \) and rearranging we obtain

\[
a_1 \cdots a_k b_1 \cdots b_m p_1(x) \cdots p_l(x) q_1(x) \cdots q_n(x) = c_1 \cdots c_t r_1(x) \cdots r_t(x) (x^2 + 1).
\]

Theorem 17.6 and the irreducibility of \( x^2 + 1 \) now imply that \( x^2 + 1 = \pm p_i(x) \) for some \( i \) or \( x^2 + 1 = \pm q_i(x) \) for some \( i \). In the first case \( x^2 + 1 \) divides \( f(x) \) and in the second \( x^2 + 1 \) divides \( g(x) \). That is, either \( f(x) \in \langle x^2 + 1 \rangle \) or \( g(x) \in \langle x^2 + 1 \rangle \). Therefore \( \langle x^2 + 1 \rangle \) is prime in \( \mathbb{Z}[x].\)

\[\text{1} \quad \text{Now that we know about UFD’s we can actually dramatically simplify this proof: as above, } x^2 + 1 \text{ is irreducible in } \mathbb{Z}[x]; \text{ since } \mathbb{Z}[x] \text{ is a UFD, every irreducible element is also prime, so } \langle x^2 + 1 \rangle \text{ is a prime ideal.}\]
Let \( p \in \mathbb{Z}^+ \) be any prime. We will show that \( \langle x^2 + 1 \rangle \) is properly contained in \( \langle x^2 + 1, p \rangle \) which is not equal to \( \mathbb{Z}[x] \). This will prove that \( \langle x^2 + 1 \rangle \) is not maximal. Since every nonzero element of \( \langle x^2 + 1 \rangle \) has degree at least 2, \( p \not\in \langle x^2 + 1 \rangle \). This proves that \( \langle x^2 + 1 \rangle \) is properly contained in \( \langle x^2 + 1, p \rangle \). Now suppose, for the sake of contradiction, that \( \langle x^2 + 1, p \rangle = \mathbb{Z}[x] \). Then there exist \( f(x), g(x) \in \mathbb{Z}[x] \) so that \( f(x)(x^2 + 1) + g(x)p = 1 \). If we consider this equation mod \( p \) we obtain \( f(x)(x^2 + 1) = 1 \) in \( \mathbb{Z}_p[x] \), which is impossible since \( f(x)(x^2 + 1) \) in \( \mathbb{Z}_p[x] \) is either 0 or has degree at least 2. This contradiction establishes that \( \langle x^2 + 1, p \rangle \) is not equal to \( \mathbb{Z}[x] \), which completes the proof that \( \langle x^2 + 1 \rangle \) is not maximal in \( \mathbb{Z}[x] \).