4.3 #14. Show that $x^2 + x$ can be factored in two ways in $\mathbb{Z}_6[x]$ as a product of non-constant polynomials that are not units.

\[ x^2 + x = (x+1)x \]
\[ x^2 + x = x^2 - 5x + 6 = (x-3)(x-2) \]

4.3 #20. If $p(x)$ and $q(x)$ are non-associate irreducibles in $\mathbb{F}[x]$, prove that they are relatively prime.

Proof: Up to multiplying by units, the only divisors of $p(x)$ are 1 and $p(x)$ and the only divisors of $q(x)$ are 1 and $q(x)$. Thus, up to units, the only possible common divisors are 1, $p(x)$, and $q(x)$.

If $p(x) \mid q(x)$, then either $p(x)$ is associate to 1 or $p(x)$ is associate to $q(x)$.

The first is not possible (definition of irreducible is that the polynomial is assumed to be non-constant) and the second is not possible either by the hypothesis.

A similar argument holds if $q(x) \mid p(x)$.

Hence, up to units, 1 is the only common divisor.

In other words, $p(x)$ and $q(x)$ are relatively prime.

4.4 #2 (a,d). Find the remainder when $f(x)$ is divided by $g(x)$.

(a) $f(x) = x^5 + x^3$, $g(x) = x - 1$ in $\mathbb{Q}[x]$.

$f(x) = q(x) \cdot g(x) + r(x)$, where $\deg(r(x)) = 0$ (since $\deg(g(x)) = 1$).

\[ r(x) = f(1) = 0 + 2(1) \]. Therefore $r(x) = 2$.

(d) $f(x) = 2x^5 - 3x^4 + x^3 + 2x + 3$, $g(x) = x - 3$ in $\mathbb{Z}_5[x]$.

As above, $f(3) = 1 - 3 + 2 + 1 + 3 = 4$; so $\lambda(x) = 4$. 

4.3 #14, 20
4.4 #2 (a, d), 4 (a, b), 8 (d, f), 12, 15, 24, 26
4.4 \# 4(a, b)

(a) For what value of \( k \) is \( x - 2 \) a factor of
\[ f(x) = x^4 - 5x^3 + 5x^2 + 3x + k \] in \( \mathbb{Q}[x] \)
\[ f(2) = 16 - 40 + 20 + 6 + k = k + 2. \] \( k = -2 \)

(b) For what value of \( k \) is \( x + 1 \) a factor of
\[ f(x) = x^4 + 2x^3 - 3x^2 + kx + 1 \] in \( \mathbb{Z}_5[x] \)
\[ f(-1) = 1 - 2 - 3 - k + 1 = 2 - k, \] \( k = 2 \)

4.4 \# 8(d,f)

(d) Is \( f(x) = 2x^3 + x^2 + 2x + 2 \) irreducible in \( \mathbb{Z}_5[x] \)?
It suffices (since \( \deg f(x) = 3 \)) to check if \( f(x) \) has a root in \( \mathbb{Z}_5 \).
\[ f(0) = 2, f(1) = 2, f(2) = 1, f(-2) = -16 + 4 - 4 + 2 = -4 = 1, f(-1) = -1 = 4. \]
So \( f(x) \) is irreducible (no roots).

(f) \( f(x) = x^4 + x^2 + 1 \) Is \( f(x) \) irreducible in \( \mathbb{Z}_5[x] \)?
No. \( f(1) = 1 + 1 + 1 = 0 \), \( \text{So, } (x-1) \) is a factor.

4.4 \# 12

If \( a \in F \) is a non-zero root of \( c_0 x^n + \ldots + c_1 x + c_0 \) in \( F[x] \), show that \( a^{-1} \) is a root of \( c_0 x^n + c_1 x^{n-1} + \ldots + c_n \).

\( \text{Proof: multiply by } (a^{-1})^n : \)
\[ c_0 a^{-n} (c_0 a^n + \ldots + c_1 a + c_0) = c_0 + \ldots + c_1 (a^{-1})^{n-1} + c_n a^{-n} \]

4.4 \# 15

Prove that \( x^2 + 1 \) is reducible in \( \mathbb{Z}_p[x] \) iff there exist integers \( a, b \) and \( a, b \equiv 1 \) (mod \( p \)).

\( \text{Proof: } x^2 + 1 \text{ reducible } \Rightarrow x^2 + 1 = (x + a)(x + b) \)
for some \( a, b \in \mathbb{Z} \Rightarrow a + b \equiv 0 \) (mod \( p \)) and \( a \cdot b \equiv 1 \) (mod \( p \)).

Factoring in \( \mathbb{Z}_p \Rightarrow 0 \leq a < p \) and \( 0 \leq b < p \). Thus \( a + b = p \).
\[ \Rightarrow \text{ If } p = a + b \text{ and } a \cdot b \equiv 1 \text{ (mod } p \text{), then } x^2 + 1 = (x + a)(x + b) \]

\( \Box \)
4.4 #24 Let $a \in F$. Define $\varphi_a : F[x] \to F$ by $\varphi_a(f(x)) = f(a)$. Prove $\varphi_a$ is a surjective homomorphism.

This was solved in class on 04/08/11.

4.4 #26 Let $Q[\sqrt{2}] = \{ c \in \overline{Q} : c = \sum_{n=0}^{\infty} r_n \sqrt{2}^n \}$ for some $r_n \in \mathbb{Z}$ and some $r_0, \ldots, r_n \in \mathbb{Q}$.

(a) Show $Q[\sqrt{2}]$ is a subring of $\overline{Q}$.

Subtracting:

$C - C' = \left( \sum_{n=0}^{\infty} r_n \sqrt{2}^n \right) - \left( \sum_{n=0}^{\infty} r'_n \sqrt{2}^n \right) = \sum_{n=0}^{\infty} (r_n - r'_n) \sqrt{2}^n \in Q[\sqrt{2}]$,

where $C = \sum_{n=0}^{\infty} r_n \sqrt{2}^n$ and $C' = \sum_{n=0}^{\infty} r'_n \sqrt{2}^n$.

When $n = \max\{n, n'\}$ and $r_{n+1}, \ldots, r_n$ and $r'_{n+1}, \ldots, r'_{n}$ may be zero (so as to match the coefficients)

(b) Show that $\Theta : Q[x] \to Q[\sqrt{2}]$ via $\Theta(f(x)) = f(\sqrt{2})$ is a surjective homomorphism, but not an isomorphism.

Proof: That $\Theta$ is a surjective homomorphism follows identically to the proof in 4.4 #24.

That $\Theta$ is not an isomorphism follows from

$\Theta(x^2 - 2) = 0 = \Theta(0)$,

but $x^2 - 2 \neq 0$ in $Q[x]$. So $\Theta$ is not injective.