Math 430 Algebra II Homework 2 Solution based on that of Liam Bench

17.2. Answer: If $f(x) = g(x)h(x) \in D[x]$ and $f(x) \in F[x]$ is irreducible, then one of $g(x)$ or $h(x)$ must be of zero degree in $F[x]$, and thus, is a constant polynomial in $D[x]$ such that the constant is non-unit.

17.8. By Corollary 1 of Theorem 17.5 $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field. Every element in the field can be written as $g(x) + \langle f(x)\rangle : g(x)$, where $g(x) = a_{n-1}x^{n-1} + \cdots + a_0$ has degree as most $n-1$. Every a_i has p choices in $\mathbb{Z}_p$. So, there are p^n such polynomials. Moreover, if $g_1(x)$ and $g_2(x)$ in $\mathbb{Z}_p[x]$ has degree at most $n-1$, then $g_1(x) - g_2(x)$ is not a multiple of $f(x)$ so that $g_1(x) + \langle f(x)\rangle \neq g_2(x) + \langle f(x)\rangle$. So, there are exactly p^n elements in $\mathbb{Z}_p[x]/\langle f(x)\rangle$.

Remark My hint meant to push you to show that every non-zero elements in the quotient ring has an inverse and then conclude that it is a field.

17.12. They are all irreducible.
a. $3 \nmid 1$, $3|9, 3|12, 3|6$ and $9 \nmid 6$ so by Theorem 17.4 it is irreducible over $\mathbb{Q}$.
b. Looking at $x^4 + x + 1$ over $\mathbb{Z}_2$ it does not have any degree 1 factors because $f(0) = 1$ and $f(1) = 1$ and application of the Factor Theorem. Dividing $x^4 + x + 1$ by $x^2 + x + 1$ gives a nonzero remainder. This exhausts all possible factors because if we had a degree 3 factor we would have to have a degree 1 factor and the fact that $x^2 + x + 1$ is the only irreducible degree 2 polynomial over $\mathbb{Z}_2$ ($x^2 + 1 = (x + 1)(x + 1)$).
c. $3 \nmid 1, 3|3, 3|3$, and $9 \nmid 3$. By Theorem 17.4 it is irreducible over $\mathbb{Q}$.
d. If we reduce the coefficients of $x^5 + 5x^2 + 1$ over $\mathbb{Z}_2$ we get $x^5 + x^2 + 1$. For this polynomial $f(0) = f(1) = 1$ so it does not have any linear factors. Dividing $x^5 + x^2 + 1$ by $x^2 + x + 1$ we get a nonzero remainder. This exhausts all possible factors because if there was a degree 3 or 4 factor then there would be a degree 1 or 2 factor.
e. First we factor out a 14, which we can do because $\frac{1}{14} \in \mathbb{Q}$. So the polynomial can be written as $14(35x^5 + 7 \cdot 9x^4 + 14 \cdot 15x^3 + 2 \cdot 3x^2 + 14 \cdot 6x + 3)$. Using Theorem 17.4, 3 divides all coefficients except the leading coefficient and 9 does not divide the last term, 3, and we know the polynomial is irreducible.

17.16. $x^3 + x^2 + x + 1 = (x + 1)^3$.

17.26. Here is a general fact we can prove. Let $\mathbb{F}$ be a field. Define $\sqrt{a} = x$ if $x^2 - a = 0$ and note that there are at most two elements for the equation of the form $\pm c$. Then $ax^2 + bx + c \in \mathbb{F}[x]$ with $a \neq 0$ has zeros in $\mathbb{F}$ if and only if $\sqrt{b^2 - 4ac}$ exists in $\mathbb{F}$ so that the solution has the form $(2a)^{-1}(-b \pm \sqrt{b^2 - 4ac})$.

Proof. The element $x \in \mathbb{F}$ is a solution of the quadratic equation $ax^2 + bx + c = 0$ if and only if $x^2 + a^{-1}bx + a^{-1}c = 0$ so that $(x + (2a)^{-1}b)^2 = (4a)^{-1}b^2 - a^{-1}c = (4a)^{-2}(b^2 - 4ac)$, i.e., $x^2 + (2a)^{-1}b = (2a)^{-1}\sqrt{b^2 - 4ac}$. The conclusion follows.

Applying this results to $\mathbb{F} = \mathbb{Z}_p$, we see that the two methods of solving quadratics are consistent. Here are two illustrations.

By substitution the zeros for $3x^2 + x + 4$ in $\mathbb{Z}_7[x]$ are 4 and 5. The quadratic formula also yields these zeros. There are no zeros for $2x^2 + x + 3$ in $\mathbb{Z}_5[x]$. The quadratic formula does not yield zeros because $b^2 - 4ac = 2$ does not have a square root in $\mathbb{Z}_5$. The zeros to a quadratic are the solutions to the equation $ax^2 + bx + c = 0$.

$$ax^2 + bx + c = 0 \tag{1}$$
$$a(x^2 + a^{-1}bx + a^{-1}c) = 0 \tag{2}$$
$$a((x + 2^{-1}a^{-1}b)^2 - (2^{-1}a^{-1}b)^2 + a^{-1}c) = 0 \tag{3}$$
$$(x + 2^{-1}a^{-1}b)^2 = ((2^{-1}a^{-1}b)^2 - a^{-1}c) \tag{4}$$

17.28. Suppose $k = 2$ and $p(x)|a_1(x)a_2(x)$. By Corollary 2 of Theorem 17.5 $p(x)$ divides $a_1(x)$ or $a_2(x)$ and the statement is true for $k = 2$. Suppose the statement is true for some k and $p(x)|a_1(x)a_2(x)\dots a_{k+1}(x)$. Set $g(x) = a_1(x)\dots a_k(x)$. So $p(x)|g(x)a_{k+1}(x)$ and as shown either $p(x)|g(x)$ or $p(x)|a_{k+1}(x)$. If $p(x)|a_{k+1}(x)$ we are done. If $p(x)|g(x)$ then $p(x)|a_1(x)\dots a_k(x)$. Since the statement is true for k $p(x)$ divides some $a_i(x)$. So by induction the theorem is true for all $k \in \mathbb{N}$.

17.30. By the substitution $y = -x$, we see that $p(y) = \sum_{k=0}^{p-1} y^k$ is irreducible. Then $p(x)$ is irreducible.

Remark Here we use the fact that $p(x)$ is irreducible if and only if $p(\pm x + a)$ is irreducible of any $a \in \mathbb{Z}$.

17.32. If $\langle x^2 + 1\rangle$ is not prime, then $g(x), h(x) \notin \langle x^2 + 1\rangle$ and $g(x)h(x) \in \langle x^2 + 1\rangle$ so that $x^2 + 1$ is a factor of $g(x)h(x) \in \mathbb{Q}[x] \subseteq \mathbb{R}[x]$, which is impossible.

The ideal $\langle x^2 + 1\rangle$ is not maximal. Let $\langle x^2 + 1, 2\rangle = \{(x^2 + 1)f(x) + 2g(x) : f(x), g(x) \in \mathbb{Z}[x]\}$. Then it is an ideal containing $\langle x^2 + 1\rangle$ but not containing 1.

Remark One can also use results in Chapter 14 to get the conclusion. Namely, an ideal of a commutative ring with unity is prime (maximal) if and only if the quotient ring is an integral domain (field).

17.40. The polynomial that yields the same probabilities as an ordinary pair of dice factors into $x^2(x+1)^2(x^2+x+1)^2(x^2-x+1)^2$. This is $(x(x+1)(x^2-x+1))^2(x^2+x+1)^2) = (x+x^4)^2(x^2+x+1)^2 = (x + x^4)^2(x^4 + 2x^3 + 3x^2 + 2x + 1) = (x + x^4)(x^8 + 2x^7 + 3x^6 + 3x^5 + 3x^4 + 3x^3 + 2x^2 + x)$. These last two polynomials correspond to the two described dice.

17.18. a. I show that there are $p(p+1)/2$ reducible polynomials over $\mathbb{Z}_p$ of the form x^2+ax+b. If a polynomial of the form is reducible it can be written as $(x+r)(x+s)$ for some $p, q \in \mathbb{Z}_p$. If $r = s$ there are p possibilities; if $r \neq s$, there are $p(p-1)/2$ possibilities. Of course, any two such polynomials are different as they will not share more than one zero. Because there are p^2 monic polynomials of degree 2, the number of monic irreducible polynomials of degree 2 is $p^2 - p(p+1)/2 = p(p-1)/2$.

b. All quadratic irreducible polynomials can be written as $a(x^2 + bx + c)$ with $a \neq 0$ so that $x^2 + bx + c$ is irreducible. So, there are $(p-1)^2p/2$ irreducible polynomial of degree 2.