Practice problems for Test 3 - Solutions

1. First of all, let's list all the elements of the given set so that we see what we are working with. Since each coefficient (a and b) can be either 0 or 1, we have 4 elements: $0+0i$, $0+1i$, $1+0i$, and $1+1i$, or, for simplicity, just 0, i, 1, and $1+i$. Addition and multiplication are defined as for complex numbers, but the results are reduced modulo 2.
   It is a commutative ring with a multiplicative identity: it is easy to check that associativity, commutativity, and distributivity hold, the additive identity is 0, the multiplicative identity is 1, the additive inverse of each element is that element itself.
   Notice also that for the ring $\mathbb{Z}(i) = \{a+bi \mid a, b \in \mathbb{Z}\}$ and the ideal $I =< 2 >= \{a+bi \mid a, b \in 2\mathbb{Z}\}$, the factor ring is $\mathbb{Z}(i)/I \cong \mathbb{Z}_2(i)$.
   $\mathbb{Z}_2(i)$ is not an integral domain because e.g. $(1+i)(1+i) = 0$ while $1+i \neq 0$. It is not a field because every field is an integral domain.

2.
$$
\begin{array}{r|l}
 & \quad x^3 - 2x \\
\hline
x^2+2 & x^5 \qquad\quad + 3x + 1 \\
 & \underline{x^5 + 2x^3} \\
 & \quad -2x^3 + 3x \\
 & \quad \underline{-2x^2 - 4x} \\
 & \qquad\qquad 7x + 1
\end{array}
$$
   So the quotient is $q(x) = x^3 - 2x$ and the remainder is $r(x) = 7x + 1$.

3. $f(x) = x^5 + 4x^4 + 6x^3 + 6x^2 + 5x + 2$, $g(x) = x^4 + 3x^2 + 3x + 6$.
   (a) Using the Euclidean algorithm (modulo 7!), we have:
   $x^5 + 4x^4 + 6x^3 + 6x^2 + 5x + 2 = (x^4 + 3x^2 + 3x + 6)(x+4) + (3x^3 + 5x^2 + x + 6)$
   $x^4 + 3x^2 + 3x + 6 = (3x^3 + 5x^2 + x + 6)(5x + 1)$
   Therefore the monic polynomial that is a multiple of $3x^3 + 5x^2 + x + 6$ is the gcd of f and g. To get a monic polynomial, multiply $3x^3 + 5x^2 + x + 6$ by 5 (the multiplicative inverse of 3 modulo 7):
   $d(x) = x^3 + 4x^2 + 5x + 2$.
   (b) $3x^3 + 5x^2 + x + 6 = (x^5 + 4x^4 + 6x^3 + 6x^2 + 5x + 2) - (x^4 + 3x^2 + 3x + 6)(x+4)$
   Rewrite with a plus:
   $3x^3 + 5x^2 + x + 6 = (x^5 + 4x^4 + 6x^3 + 6x^2 + 5x + 2) + (x^4 + 3x^2 + 3x + 6)(6x+3)$
   Multiply both sides by 5:
   $x^3 + 4x^2 + 5x + 2 = (x^5 + 4x^4 + 6x^3 + 6x^2 + 5x + 2) \cdot 5 + (x^4 + 3x^2 + 3x + 6)(2x+1)$
   Therefore $a(x) = 5$ and $b(x) = 2x + 1$.

4. Using the Euclidean algorithm (modulo 5!), we have:
   $x^3 + x + 1 = (x + 4)(x^2 + x + 2) + 3$
   $3 = (x^3 + x + 1) - (x + 4)(x^2 + x + 2)$
   $3 = (x^3 + x + 1) + (x + 4)(-x^2 - x - 2)$
   $3 = (x^3 + x + 1) + (x + 4)(4x^2 + 4x + 3)$
   Now multiply both sides by 2 (the multiplicative inverse of 3 modulo 5, so that to get 1 on the left): $1 = (x^3 + x + 1)2 + (x + 4)(3x^2 + 3x + 1)$
   Thus we have $(x+4)(3x^2+3x+1) \equiv 1 \pmod{x^3+x+1}$, so $[x+4]^{-1} = 3x^2+3x+1$.

5. Since a rational root of $x^4+4x^3+8x+32 = 0$ must be of the form $\frac{r}{s}$ where $r|32$ and $s|1$, the possible roots are ±1, ±2, ±4, ±8, ±16, and ±32. But notice that since all the coefficients are positive, a root cannot be positive. An easy check gives that -1 is not a root, but -2 is a root $(16-4\cdot8-8\cdot2+32 = 0)$. Therefore the polynomial is divisible by $x+2$. Long division gives: $x^4+4x^3+8x+32 = (x+2)(x^3+2x^2-4x+16)$. Now we have to find all roots of $x^3+2x^2-4x+16$. Possible roots are -2, -4, -8, and -16. -2 is not a root, but -4 is a root $(-64 + 32 + 16 + 16 = 0)$. Therefore we can divide by $x + 4$: $x^3 + 2x^2 - 4x + 16 = (x + 4)(x^2 - 2x + 4)$. Finally, since $x^2 - 2x + 4$ has no rational roots, the original polynomial has no other roots.

6. over $\mathbb{Z}$: $x^3 - 2$ is irreducible because it has no integer roots
   over $\mathbb{Q}$: still irreducible because it has no rational roots either
   over $\mathbb{R}$: $\left(x - \sqrt[3]{2}\right)\left(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}\right)$
   Now use the quadratic formula to find the roots of $x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$:
   over $\mathbb{C}$: $\left(x - \sqrt[3]{2}\right)\left(x + \dfrac{\sqrt[3]{2} + \sqrt[3]{2}\sqrt{3}i}{2}\right)\left(x + \dfrac{\sqrt[3]{2} - \sqrt[3]{2}\sqrt{3}i}{2}\right)$
   over $\mathbb{Z}_3$: 0 is not a root; 1 is not a root; 2 is a root, so divide by $x - 2$ (or equivalently, $x+1$) over $\mathbb{Z}_3$: $x^3 - 2 = (x+1)(x^2 - x + 1)$. Now, $x^2 - x + 1$ also has a root, namely, 2 again. So divide by $x - 2 = x+1$ again, get $x^2+2x+1 = (x+1)^2$. Therefore $x^3 - 2 = (x + 1)^3$ over $\mathbb{Z}_3$.
   Another way: $x^3 - 2 \equiv x^3+1 = (x+1)(x^2-x+1) \equiv (x+1)(x^2+2x+1) = (x+1)^3 \pmod 3$.

7. First list all the polynomials of degree 3 over $\mathbb{Z}_2$. Since a polynomial of degree 3 is irreducible if and only if it has no roots, we check whether or not each of our polynomials has a root:
   x^3 has a root, $x = 0$
   $x^3 + 1$ has a root, $x = 1$
   $x^3 + x$ has a root, $x = 0$ (moreover, $x = 1$ is also a root, but we don't need that)
   $x^3 + x + 1$ has no roots
   $x^3 + x^2$ has a root, $x = 0$ (also $x = 1$)
   $x^3 + x^2 + 1$ has no roots
   $x^3 + x^2 + x$ has a root, $x = 0$
   $x^3 + x^2 + x + 1$ has a root, $x = 1$
   So only $x^3 + x + 1$ and $x^3 + x^2 + 1$ have no roots and therefore are irreducible.

8. The prime $p = 5$ divides all the coefficients of $3x^4 + 30x - 60$ except the leading coefficient, and p^2 does not divide the free term. Therefore by Eisenstein's criterion, this polynomial is irreducible over $\mathbb{Q}$.

9. (a) $R = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, $e = 1$ is obviously a multiplicative identity.
   $S = 2\mathbb{Z}_6 = \{0, 2, 4\}$, $e' = 4$. Check: $0 \cdot 4 = 0$, $2 \cdot 4 = 2$ (modulo 6!), $4 \cdot 4 = 4$.

   (b) Since e is an identity in R, $ee' = e'$, $e \neq 0$.
   Since e' is an identity in S, $e'e' = e'$, $e' \neq 0$.
   So we have $ee' = e'e'$, or $ee' - e'e' = 0$, or $(e - e')e' = 0$.
   In an integral domain, $ab = 0$ implies that either $a = 0$ or $b = 0$.
   Since $e' \neq 0$, we have $e - e' = 0$. Thus $e = e'$.

10. An element (r, s) of $R \oplus S$ is a unit (i.e. an invertible element) if and only if r is a unit in R and s is a unit in S.
    $\mathbb{Z}_6$ has 2 units: 1 and 5.
    $\mathbb{Z}_8$ has 4 units: 1, 3, 5, and 7.
    Therefore $\mathbb{Z}_6 \oplus \mathbb{Z}_8$ has 8 units: $(1, 1)$, $(1, 3)$, $(1, 5)$, $(1, 7)$, $(5, 1)$, $(5, 3)$, $(5, 5)$, $(5, 7)$.

11. We have to show that $I + J = \{x \in R \mid x = a + b \text{ for some } a \in I, b \in J\}$ is closed under addition and subtraction, and is closed under mulitplication by any element of R.
    Let $x_1, x_2 \in I + J$, so $x_1 = a_1 + b_1$ and $x_2 = a_2 + b_2$ for some $a_1, a_2 \in I$ and $b_1, b_2 \in J$. Then $x_1 \pm x_2 = (a_1 + b_1) \pm (a_2 + b_2) = (a_1 \pm a_2) + (b_1 \pm b_2) \in I + J$ because both I and J are closed under addition and subtraction.
    Let $x = a + b \in I + J$ and $r \in R$. Then $rx = r(a + b) = ra + rb \in I + J$ because both I and J are closed under multiplication by any element of R.