1. 

(a) $f(x)$ and $g(x)$ are associates if and only if $f(x) = ug(x)$ for some unit $u \in F$, if and only if $g(x) = u^{-1}f(x)$. Hence $f(x)$ and $g(x)$ are associates if and only if $g(x)|f(x)$ and $f(x)|g(x)$.

(b) Let $p(x) \in F[x]$, and $g(x) \in F[x]$. If $p(x)$ is irreducible in $F[x]$, then $\gcd(g(x), p(x)) = 1$ or $p(x)$. To show the converse, suppose that $p(x) = c(x)d(x)$ with $c(x), d(x) \in F[x]$. Then $\deg p(x) = \deg c(x) + \deg d(x)$ (⋆). If $\gcd(p(x), c(x)) = 1$, then $p(x)|d(x)$ and so $\deg p(x) \leq \deg d(x)$. So by (⋆), $\deg d(x) = \deg p(x)$ and $\deg c(x) = 0$. This says that $c(x) = c \in F, \neq 0$. So $p(x) = cd(x)$ or $d(x) = c^{-1}p(x)$ and hence $p(x)$ is irreducible in $F[x]$. If $\gcd(p(x), c(x)) = p(x)$, then $d(x) = d \in F, \neq 0$. So $p(x) = dc(x)$ or $c(x) = d^{-1}p(x)$. Therefore, $p(x)$ is irreducible in $F[x]$.

(c) Let $\phi : F[x] \to F[x]$ be a map defined, for any polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$, by

$$\Phi(f(x)) := a_0 + a_1\Phi(x) + a_2\Phi(x)^2 + \cdots + a_n\Phi(x)^n \in F[x]$$

We claim that $\Phi$ is an isomorphism. Clearly,

$$\Phi(f(x) + g(x)) = \Phi(f(x)) + \Phi(g(x))$$

and

$$\Phi(f(x)g(x)) = \Phi(f(x))\Phi(g(x))$$

$\Phi$ is one-to-one as $\Phi(f(x)) = \Phi(0(x))$ if and only if $a_i = 0 \ \forall i$. $\Phi$ is onto, as for any $f(y) = a_0 + a_1y + \cdots + a_ny^n \in F[x]$, letting $x$ so that $\Phi(x) = y$, we get $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ such that $\Phi(f(x)) = f(y)$. Therefore, $\Phi$ is an isomorphism.

This implies that $f(x)$ is irreducible in $F[x]$ if and only if $\Phi(f(x))$ is irreducible in $F[x]$.

2. 

(a) If $f(x)$ and $g(x)$ are associates, then $f(x) = ug(x)$ for some unit $u \in F$. If $\alpha \in F$ is a root of $f(x)$, then $0 = f(\alpha) = ug(\alpha)$ so $g(x)$ has a same root as $f(x)$.
(b) Let \( f(x) \in F[x] \). Then by Division Algorithm, \( f(x) = (x - 1)q(x) + r(x) \) with \( r(x) = 0 \text{ or } \deg r(x) = 0 \). So \( x - 1 | f(x) \iff f(1) = r(1) = 0 \).

(c) Let \( f(x) = x^2 + 1 \in \mathbb{Z}_p[x] \). If \( f(x) \) is reducible, it is a product of two degree 1 monic polynomials

\[
x^2 + 1 = (x + a)(x + b) \in \mathbb{Z}_p[x]
\]

so \( a + b = 0, \ ab = 1 \in \mathbb{Z}_p \). Equivalently, \( a + b = p \) and \( ab \equiv 1 (\text{mod } p) \).

3.

(a) Let \( f(x) \in F[x] \). If \( \alpha \in F \) is a multiple root of \( f(x) \), then we can factor \( f(x) \) in \( F[x] \) as follows:

\[
f(x) = c(x - \alpha)^k g(x) \quad \text{with } k > 1
\]

Then the first derivative of \( f(x) \) with respect to \( x \) is

\[
f'(x) = ak(x - \alpha)^{k-1}g(x) + a(x - \alpha)^k g'(x) = (x - \alpha)^{k-1}(ag(x) + a(x - \alpha)g'(x))
\]

Therefore, \( \gcd(f(x), f'(x)) = (x - \alpha)^{k-1} \) and hence \( \alpha \) is a root of \( f(x) \) and \( f'(x) \).

(b) Let \( \Phi : F[x] \to F[x] \) be a map that sends any polynomial \( f(x) \in F[x] \) to \( f(x + c) \) for some nonzero constant \( c \in F \), that is,

\[
\Phi(f(x)) := f(x + c)
\]

Then \( \Phi \) is a ring homomorphism. \( \Phi \) is onto as for any \( f(x) \in F[x] \), we can take \( f(x - c) \in F[x] \) so that

\[
\Phi(f(x - c)) = f(x - c + c) = f(x)
\]

Clearly, \( \Phi \) is one-to-one. Therefore, \( \Phi \) is an isomorphism.

Then \( f(x) \) is irreducible in \( F[x] \) if and only if \( \Phi(f(x)) = f(x + c) \) is irreducible in \( F[x] \).

(c) Consider \( \Phi_p(x + 1) \). Then

\[
\Phi_p(x + 1) = \frac{(x + 1)^p - 1}{x + 1 - 1} = \frac{1}{x} \{(x + 1)^p - 1\}
\]

Now

\[
(x + 1)^p = x^p + \binom{p}{1} x^{p-1} + \binom{p}{2} x^{p-2} + \cdots + \binom{p}{i} x^{p-i} + \cdots + \binom{p}{p-1} x + 1
\]

\[2\]
(b) Let $f$ form. Assume that in $\mathbb{Q}$ a $f(x)$ is irreducible in $\mathbb{Q}[x]$ and hence $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(d) A degree $k$ polynomial $f(x) \in \mathbb{Z}_n[x]$ has the form

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$$

where there are $n-1$ choices for $a_k$ and $n$ choices for each coefficient $a_i, 0 \leq i < k$. Hence there are $n^k(n-1) = n^{k+1} - n^k$ polynomials of degree $k$ in $\mathbb{Z}_n[x]$.

4.

(a) Let $f(x) \in \mathbb{Z}[x]$ be a nonconstant polynomial. We want $f(x)$ to factor modulo 2, 3, 4 and 5.

The easiest example is $f(x) = x^2 - 60 \in \mathbb{Z}[x]$. Then $f(x) \equiv x^2 \mod 2, 3$ and 5, but $f(x)$ is irreducible in $\mathbb{Q}[x]$.

A more interesting example would be $f(x) = x^3 + 30x^2 - 14x - 15 \in \mathbb{Z}[x]$. Then $f(x) \mod 2 \equiv x^3 - 1 = (x - 1)(x^2 + x + 1) \in \mathbb{Z}[2][x], f(x) \mod 3 \equiv x^3 - 2x = x(x^2 - 2) \in \mathbb{Z}_3[x], f(x) \mod 4 \equiv x^3 + x = x(x^2 + 1) \in \mathbb{Z}_4[x]$ and $f(x) \mod 4 = x^3 + 2x^2 - 2x - 3 = (x + 1)9x^2 + x - 3) \in \mathbb{Z}_4[x]$. However, $f(x)$ is irreducible in $\mathbb{Q}[x]$. In fact, if it has a linear factor, $\pm 1, \pm 3, \pm 5$ and $\pm 15$ must be roots of $f(x)$. But $f(1) = 2, f(-1) = 28, f(3) = 240, f(-3) = 270, f(5) = 690, f(-5) = 580, f(15) = 3 \cdot 15^3$ and $f(-15) = 15 \cdot 238$. Hence $f(x)$ has no linear factor in $\mathbb{Q}[x]$. Thus, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(b) In $\mathbb{Z}_5[x]$, any degree 2 polynomial is of the form $ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}_5$. Therefore, there are $5^3$ polynomials of degree $\leq 2$ in $\mathbb{Z}_5[x]$. Among them five are constant polynomials (corresponding to $a = b = 0$), and there are $5^2 - 5 = 20$ degree 1 polynomials (corresponding to $a = 0, c \neq 0, b \in \mathbb{Z}_5$) in $\mathbb{Z}_5[x]$. Now assume that $f(x) = ax^2 + bx + c$ with $a \neq 0$. We have 100 polynomials of this form. $f(x) = ax^2 + bx + c$ is reducible in $\mathbb{Z}_5[x]$ if and only if it has a root in $\mathbb{Z}_5$. If
0 is a root, then $0 = f(0) = c$. So there are 4 choices for $a$ and 5 choices for $b$, in total 20 polynomials. If 1 is a root, then $0 = f(1) = a + b + c$. So there are 4 choices for $a$, 5 choices for $b$, once $a$ and $b$ are chosen, $c$ is uniquely determined. So in total 20 polynomials. If 2 is a root, then $0 = f(2) = 4a + 2b + c = -a + 2b + c$. So there are 4 choices for $a$ and 5 choices for $b$. $c$ is then uniquely determined. So in total 20 polynomials. If 3 = −2 is a root, then $0 = f(3) = f(-2) = -a - 2b + c$. So there are 20 polynomials in total. If 4 is a root, then $0 = f(4) = f(-1) = a - b + c$. So there are again 20 polynomials in total. Summing up, all 100 polynomials are reducible.

(c) Let $f(x) = x^3 - 3x^2 - 30x - 43 \in \mathbb{Z}[x]$. We compute

$$f(x + 1) = (x + 1)^3 - 3(x + 1)^2 - 30(x + 1) - 43 = x^3 - 33x - 75$$

By Eisenstein criterion with $p = 3$, $3 | -33, -75$, but $3 \nmid 1, 3^3 \nmid 75$. Therefore, $f(x + 1)$ is irreducible and hence $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(d) Let $f(x) = 21 + 12x + 6x^2 + 4x^3 + x^4$. If $r/s \in \mathbb{Q}$ with $\gcd(r, s) = 1$ is a rational root of $f(x)$, then $r|21$ and $s|1$. So $s = 1$, and $r \in \{\pm 1, \pm 3, \pm 7, \pm 21\}$. We compute

$$f(1) = 44, f(-1) = 12, f(3) = 310, f(-3) = 22, f(7) = 4532, f(-7) = 900$$

and

$$f(21) = 234444, f(-21) = 159852.$$ 

So $f(x)$ has no degree 1 factors.

Suppose that

$$f(x) = (x^2 + ax + b)(x^2 + cx + d) \in \mathbb{Z}[x]$$

Then

$$x^4 + 4x^3 + 6x^2 + 12x + 21 = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd$$

from which we get

$$a + c = 4, b + d + ac = 6, ad + bc = 12, bd = 21 \quad (\star)$$

So $b, d \in \{\pm 1, \pm 3, \pm 7, \pm 21\}$ with $bd = 21$. By case by case checking, we see that there are no solutions satisfying $(\star)$. Therefore, $f(x)$ is irreducible in $\mathbb{Q}[x]$. 
(e) Let \( f(x) = -91 - 63x - 73x^2 + 22x^3 + 50x^4 \in \mathbb{Z}[x]. \) Take \( p = 3. \) Then
\[
\overline{f(x)} = f(x) \pmod{3} = 2x^4 + x^3 - x - 1 \in \mathbb{Z}_3[x]
\]
Check that
\[
\overline{f(0)} = -1, \quad \overline{f(1)} = 1, \quad \overline{f(2)} = \overline{f(-1)} = 2 - 1 + 1 - 1 = 1
\]
So \( f(x) \pmod{3} \) is irreducible in \( \mathbb{Z}_3[x], \) so \( f(x) \) is irreducible in \( \mathbb{Q}[x]. \)

5.

(a) Let \( f(x) = x^4 - 10x^2 + 1 \in \mathbb{Z}[x]. \) First we show that \( f(x) \) has no rational root using rational root test. If \( r/s \in \mathbb{Q} \) with \( \gcd(r, s) = 1 \) is a root of \( f(x), \) then \( r|1 \) and \( s|1. \) So \( r = s = 1, \) but \( f(1) = 1 - 10 + 1 = -8 \neq 0. \) Suppose that
\[
f(x) = (x^2 + ax + b)(x^2 - ax + c) \in \mathbb{Z}[x]
\]
Then
\[
x^4 - 10x^2 + 1 = x^4 + (c + b - a^2)x^2 + a(c - b)x + bc
\]
so that
\[
c + b - a^2 = 10, \quad a(c - b) = 0, \quad bc = 1
\]
We have either \( a = 0 \) or \( b = c. \) If \( a = 0, \) \( c + b = 0 \) so \( b^2 = -1 \) impossible. If \( b = c, \) then \( 2b = a^2, \) \( b^2 = 1 \) so that \( a^4 = 2^2 \) impossible. Therefore \( f(x) \) is irreducible in \( \mathbb{Q}[x]. \)

To find the roots of \( f(x), \) put \( y = x^2 \) and solve the quadratic equation \( y^2 - 10y + 1 = 0 \) to get \( y = 5 \pm \sqrt{24}. \) Note that \( 5 \pm \sqrt{24} = (\pm \sqrt{2} \pm \sqrt{3})^2 \) so that roots of \( f(x) \) are
\[
\sqrt{2} + \sqrt{3}, \quad \sqrt{2} - \sqrt{3}, \quad -\sqrt{2} + \sqrt{3}, \quad -\sqrt{2} - \sqrt{3}
\]

(b) \( f(x) = (x - 1)(x - 2)(x - 3) - 1 = x^3 - 6x^2 + 11x - 7 \) is irreducible by rational root test.

(c) \( f(x) = (x-1)(x-2)(x-3)(x-4)+1 = x^4-10x^3+35x^2-50x+25 = (x^2-5x+5)^2. \) So it is reducible in \( \mathbb{Q}[x]. \)

6. [1pt each]
(a) For any $n \in \mathbb{N}$,
\[ f(x) = (x - 1)(x - 2)(x - 3) \cdots (x - n) - 1 \]
is irreducible in $\mathbb{Q}[x]$.

(b) For any $n \in \mathbb{N}$ such that $n \neq 4$,
\[ g(x) = (x - 1)(x - 2)(x - 3) \cdots (x - n) + 1 \]
is irreducible in $\mathbb{Q}[x]$.

(a) Let $f(x) = (x - 1)(x - 2) \cdots (x - n) - 1 \in \mathbb{Z}[x]$. Suppose that $f(x)$ is reducible and write $f(x) = g(x)h(x)$ where both $g(x)$ and $h(x)$ are monic polynomials in $\mathbb{Z}[x]$ with degree $< n$. Now substitute $x = r$ where $r$ is any integer such that $1 \leq r \leq n$ to the factorization $f(x) = g(x)h(x)$. We get $g(r)h(r) = -1$. This means that $g(r) = 1$ and $h(r) = -1$ or $g(r) = -1$ and $h(r) = 1$. Now consider the polynomial $P(x) := g(x) + h(x) \in \mathbb{Z}[x]$. Then $P$ has degree strictly smaller than $n$. But $P(r) = g(r) + h(r) = 0$ for every $r$, $1 \leq r \leq n$. This means that $g(x) + h(x) = 0$, that is $g(x) = -h(x)$. Now we still have to eliminate the possibility that $P(x) = -g(x)^2$. But if it were, every value of $P(x)$ would be negative, and clearly if we take $x$ to be bigger than $n + 1$, then $P(x) > 0$. Therefore $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(b) Suppose that $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Z}[x]$ with degree $\geq 1$. Then $f(r) = g(r)h(r) = 1$ for any $r \in \mathbb{N}, 1 \leq r \leq n$. Hence $g(r)$ and $h(r)$ are units in $\mathbb{Z}$, that is, $g(r) = h(r) = 1$ or $g(r) = h(r) = -1$. Now suppose that $g(x) = h(x)$. Then $f(x) = g(x)^2$. In particular, look at the constant terms. We get $f(0) = (-1)^n n! + 1 = g(0)^2$. If $n$ is odd, then $f(0) = -n! + 1$ cannot be a square. If $n$ is even, $f(0) = n! + 1$ and could be a square. In fact, if $n = 4, 4! + 1 = 25 = 5^2$. Are there any other $n$ for which $n! + 1$ is a square? Actually this is still an open problem. No one knows if there are even integers $n > 4$ for which $n! + 1$ is a square!

Conclusion: We cannot determine if $f(x) = (x - 1)(x - 2) \cdots (x - n) + 1 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$ or not.