1. Let R be a ring. Recall that an element a of R is called *nilpotent* if there exists a positive integer n such that $a^n = 0_R$.

(a) Explain what it would mean to say that the property of being a nilpotent element of R is "preserved by homomorphisms".

For any ring homomorphism $f: R \longrightarrow S$, if a is nilpotent in R, then $f(a)$ is nilpotent in S.

(b) Prove the statement you made in part (a). (In other words, prove that being a nilpotent element of R is preserved by homomorphisms.)

Let $f: R \longrightarrow S$ be a ring homomorphism, and let $a \in R$ be nilpotent. Then $a^n = 0_R$ for some positive integer n.

So $f(a)^n = \underbrace{f(a) \cdot f(a) \cdots f(a)}_{n \text{ times}} = f(\underbrace{a \cdot a \cdots a}_{n \text{ times}}) = f(a^n) = f(0_R) = 0_S$.

Thus $f(a)$ is nilpotent in S.

2. Let R be an integral domain, and let $a, b \in R$. Show that a and b are associates if and only if $a \mid b$ and $b \mid a$.

($\Rightarrow$) Assume a is an associate of b. Then $a = bu$ for some unit $u \in R$. Thus $b \mid a$.
Also $b = au^{-1}$, so $a \mid b$.

($\Leftarrow$) Assume $a \mid b$ and $b \mid a$. Then $b = au$ for some $u \in R$ and $a = bv$ for some $v \in R$. From this it is clear that if $a = 0$ then $b = 0$, and if $b = 0$ then $a = 0$. If both a and b are 0, then clearly they are associates. So assume both are nonzero.
Now $a \cdot 1_R = a = bv = (au)v = a(uv)$, and $a \neq 0$. Since R is an integral domain, we can use the multiplicative cancellation law to conclude

$$uv = 1_R.$$

Since R is commutative, of course we have $vu = 1_R$ also, so both u and v are units. So now $a = bv$, and v is a unit in R, so a is an associate of b.

3. Let $p = X^4 - 3X^3 - 4X^2 + 19X - 7$ and $q = X^3 - 4X^2 + 2X + 7$ in $\mathbb{Q}[X]$.

(a) Use the Euclidean algorithm to compute the greatest common divisor of p and q. (You may want to use the back of this page for scratch work.)

$$p = q\,\underline{(X+1)} + \underline{(-2X^2+10X-14)}$$

$$q = (-2X^2+10X-14)\,\underline{(-\tfrac{1}{2}X - \tfrac{1}{2})} + \underline{0}$$

So (p,q) is an associate of $-2X^2+10X-14$, but must be monic.

Thus (p,q) is

$$\boxed{X^2 - 5X + 7}$$

$$\begin{array}{r}
X+1 \\
X^3-4X^2+2X+7 \,\big)\, X^4-3X^3-4X^2+19X-7 \\
X^4-4X^3+2X^2+7X \\
\hline
X^3-6X^2+12X-7 \\
X^3-4X^2+2X+7 \\
\hline
-2X^2+10X-14
\end{array}$$

$$\begin{array}{r}
-\tfrac{1}{2}X-\tfrac{1}{2} \\
-2X^2+10X-14 \,\big)\, X^3-4X^2+2X+7 \\
X^3-5X^2+7X \\
\hline
X^2-5X+7 \\
X^2-5X+7 \\
\hline
0
\end{array}$$

(b) Using your answer from part (a), show that p is reducible in $\mathbb{Q}[X]$ but does not have any roots in $\mathbb{Q}$.

$$\begin{array}{r}
X^2+2X-1 \\
X^2-5X+7 \,\big)\, X^4-3X^3-4X^2+19X-7 \\
X^4-5X^3+7X^2 \\
\hline
2X^3-11X^2+19X-7 \\
2X^3-10X^2+14X \\
\hline
-X^2+5X-7 \\
-X^2+5X-7 \\
\hline
0
\end{array}$$

So $p = (X^2-5X+7)(X^2+2X-1)$.

By the quadratic formula, the roots of X^2-5X+7 in $\mathbb{C}$ are $\dfrac{5 \pm \sqrt{-3}}{2}$

and the roots of X^2+2X-1 are $\dfrac{-2 \pm \sqrt{8}}{2} = -1 \pm \sqrt{2}$.

Thus p is reducible, but has no roots in $\mathbb{Q}$.

4. Factor the polynomial $X^3 + 3X^2 + 3X + 4$ into irreducibles in $\mathbb{Z}_5[X]$. Show your work, and justify your answer. (In particular, be sure to explain briefly why each factor is irreducible.)

Look for a root... plug in $X = 0, 1, 2, 3, 4$.

$X=0$: $0+0+0+4 = 4 \neq 0$

$X=1$: $1+3+3+4 = 11 \neq 0$

$X=2$: $8+12+6+4 = 30 = 0$ ✓

Factor out $X-2$:

$$
\begin{array}{r|l}
 & X^2 + 3 \\
\hline
X-2 & X^3 + 3X^2 + 3X + 4 \\
 & X^3 - 2X^2 \\
\hline
 & \quad 3X + 4 \\
 & \quad 3X - 6 \\
\hline
 & \quad\quad 0
\end{array}
$$

Find roots of X^2+3... 0 and 1 can't be, so plug in $X = 2, 3, 4$.

$X=2$: $4+3 = 7 \neq 0$

$X=3$: $9+3 = 12 \neq 0$

$X=4$: $16+3 = 19 \neq 0$

X^2+3 has no roots in $\mathbb{Z}_5[X]$, and since its degree is only 2, it is therefore irreducible.

Of course $X-2$ is also irreducible, because a polynomial of degree 1 is always irreducible.

Thus $X^3+3X^2+3X+4 = (X-2)(X^2+3)$

or $\boxed{X^3+3X^2+3X+4 = (X+3)(X^2+3)}$