7a)

RTP: $(P \implies Q) \implies ((P \implies \neg Q) \implies \neg P)$

Assume that for all statements P and Q: $(P \implies Q)$. Then assume $(P \implies \neg Q)$.

We use a proof by contradiction. Therefore, assume P. Then, by $(P \implies Q)$, Q must be true. Also, by $(P \implies \neg Q)$, Q must be false.

This is a contradiction, so P must be false, meaning $(P \implies Q) \implies ((P \implies \neg Q) \implies \neg P)$, as required.

b) (i)

RTP: $a \equiv b \pmod{p \cdot q} \iff (a \equiv b \pmod{p} \wedge a \equiv b \pmod{q})$

($\implies$) Assume that a and b are integers, and that $a \equiv b \mod p \cdot q$. Then by definition, $a = kpq + d$ and $b = lpq + d$ for some integers k, l, d, with $0 \leq d < pq$.

Let $x = kp$, and $y = lp$. Now, $a = xq$ and $b = yq$. This gives $a \equiv b \mod q$. A similar result can be acquired by letting $x = kq$, and $y = lq$, to give $a \equiv b \mod p$. Therefore we have $(a \equiv b \pmod{p} \wedge a \equiv b \pmod{q})$ as required.

($\impliedby$) Assume a and b are integers, and that $a \equiv b \pmod{p} \wedge a \equiv b \pmod{q}$. By definition, we have $a - b = ps$, and $a - b = qt$, for some integers s, t.

We then have $p \mid (a-b)$ and $q \mid (a-b)$. Since p and q are coprime, this means that $pq|(a-b)$. We then have $a \equiv b \mod p \cdot q$, as required.

(ii)

For all natural numbers i and primes p, $i^p \equiv i \mod p$. If i is not a multiple of p, then $i^{p-1} \equiv 1 \mod p$

(iii)

We can split the problem up into cases.

Case 1: If n is divisible by both p and q, clearly the two sides are equivalent (both $0 \mod pq$)

Case 2: n is divisible by neither p nor q.

Then, define k such that $ed = k(p-1)(q-1) + 1$ so that

$$n^{ed} = n^{k(p-1)(q-1)+1} = n \cdot n^{k(p-1)(q-1)}$$

Then,

$$(n^{k(p-1)})^{(q-1)} \equiv 1 \mod q$$
$$(n^{k(q-1)})^{(p-1)} \equiv 1 \mod p$$

Applying the proof from part (ii), we then have $n \cdot n^{k(p-1)(q-1)} \equiv n \mod pq$ as required.

Case 3: Suppose one of p or q divides n - say this is p.

Then

$$\begin{aligned}
(n^{k(p-1)})^{(q-1)} &\equiv 1 \mod q \\
(n^{k(q-1)})^{(p-1)} &\equiv 0 \mod p
\end{aligned}$$

and so

$$\begin{aligned}
n \cdot n^{k(p-1)(q-1)} &\equiv n \mod q \\
&\equiv 0 \mod p
\end{aligned}$$

which gives us for some a, b

$$n \cdot n^{k(p-1)(q-1)} = ap = bq + n$$

from which we can clearly see that b is divisble by p, since both other terms are divisible by p, so that $n \cdot n^{k(p-1)(q-1)} \equiv n \mod pq$ as required.