### 1.6.9 Solution:

**Claim:** If prime number $p \mid a_1 a_2 \cdots a_r$, then p divides one of the factors.

**Proof:** Since $p \mid a_1 a_2 \cdots a_r$, we know that $a_1 a_2 \cdots a_r = q_0 p$, $q \in \mathbb{Z}$. And without losing generality we can denote the factor as $a_i$, thus $a_i = qp$.

For base case, if $p \mid a_1$, $p \mid a_1$ is obviously true.

Suppose when $r = k$, namely, $p \mid a_1 a_2 \cdots a_k$, p divides one of the factors is true, then when $r = k + 1$, if $p \mid a_1 a_2 \cdots a_{k+1}$, so $a_1 a_2 \cdots a_{k+1} = q_1 p$. Then there're 2 cases.

If $p \mid a_{k+1}$, the statement is proved.

If $p \mid a_1 a_2 \cdots a_k$, the hypothesis gives that $p \mid a_i$.

So when $r = k + 1$, namely, $p \mid a_1 a_2 \cdots a_{k+1}$, p divides one of the factors is true.

Thus, we can conclude that if prime number $p \mid a_1 a_2 \cdots a_r$, then p divides one of the factors.$\blacksquare$

### 1.7.4 Solution:

**Claim:** $[4^{237}] = [4]$.

**Proof:** In $\mathbb{Z}_5$, $[4^2] = [1]$. Thus $[4^{2n}] = [1]$, so $[4^{236}] = [1]$. And since $[4] = [-1]$, $[4^{237}] = [4^{236}][4] = [1][-1] = [-1] = [4]$.$\blacksquare$

### 1.7.11 Solution:

**Claim:** If $a$ is relatively prime to $n$ and there are integers $s$ and $t$ so that $as + nt = 1$. The inverse of $[a]$ is $[s]$.

**Proof:** Since $a$ is relatively prime to $n$ and $as+nt = 1$, we have $as-1 = nt$. So $n \mid (as - 1)$ and as a result $as \equiv 1 \mod n$. Which means that $[as] = [1]$, so $[a][s] = [1]$.

Thus, $[s]$ is the inverse of $[a]$ in $\mathbb{Z}_n$$\blacksquare$.

### 1.7.14 Solution:

**(a) Claim:** $\forall b \in \mathbb{Z}$, $ax \equiv b \mod n$ has a solution.

**Proof:** For all integer a, b, if we want to make $ax \equiv b \mod n$ holds, $ax - b = qn, q \in \mathbb{Z} \Rightarrow ax - qn = b$ must hold. Therefore, $g.c.d(a, n) \mid b$ must be true. Since $a$ and $n$ are relatively prime, $g.c.d(a, n) = 1$, the statement above must be true.

So we can conclude that $\forall b \in \mathbb{Z}$, $ax \equiv b \mod n$ has a solution$\blacksquare$.

**(b)** Base on the logical deduction above, we need to find a pair of integer $(s, r)$ with the inverse of Euclidean Algorithm so that $sa + rn = 1$, so $(bs)a + (br)n = b$, and one $x_0 = bs$. And all the solutions become a set $\{x|x = kn + x_0, k \in \mathbb{Z}\}$.

**(c)** **Claim:** For $8x \equiv 12 \mod 125$, $x = 64$.

**Proof:** Since $8x \equiv 12 \mod 125$, $8x - 12 = 125q, q \in \mathbb{Z} \Rightarrow 8x - 125q = 12$
So apply Euclidean Algorithm to 8 and 125 first:

$$
\begin{aligned}
&125 = 8 \times 15 + 5 \\
&8 = 5 \times 1 + 3 \\
&5 = 3 \times 1 + 2 \\
&3 = 2 \times 1 + 1 \\
&2 = 1 \times 2
\end{aligned}
$$

Thus,

$$
\begin{aligned}
&125 - 8 \times 15 = 8 - 3 \\
\Rightarrow\ &125 - 8 \times 16 = -3 \\
\Rightarrow\ &8 \times 16 - 125 = 3 \\
\Rightarrow\ &8 \times 16 - 125 = 5 - 2 \\
\Rightarrow\ &8 \times 16 - 125 = (125 - 8 \times 15) - 2 \\
\Rightarrow\ &8 \times 31 - 125 \times 2 = -2 \\
\Rightarrow\ &125 \times 2 - 8 \times 31 = 3 - 1 = (8 - 5) - 1 \\
\Rightarrow\ &125 \times 2 - 8 \times 32 = -5 - 1 = -6 \\
\Rightarrow\ &125 \times 4 - 8 \times 64 = -12 \\
\Rightarrow\ &8 \times 64 - 125 \times 4 = 12
\end{aligned}
$$

As a result, $x_0 = 64$. And all solutions consist a set $\{x|x = 64 + 125k, k \in \mathbb{Z}\}\blacksquare$.