1. (0.8) Let a and b be integers and let $d = \gcd(a, b)$. If $a = da'$ and $b = db'$, show that $\gcd(a'b') = 1$.

   Proof. Let $d' = \gcd(a'b')$. Since $d = \gcd(a, b)$, there exists integers s and t such that $sa + tb = d$. Therefore by substition we have

   $$s(da') + t(db') = d \text{ and so}$$

   $$sa' + tb' = 1.$$

   Since by assumption $d' \mid a'$ and $d' \mid b'$, we have $d' \mid 1$. Hence $d' = 1$.

2. (0.19) Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

   Proof. Suppose that $\gcd(a, bc) = 1$ and let $\gcd(a, b) = d$. Thus d divides a and b. Hence d divides a and bc. Therefore $d = 1$. Similarly $\gcd(a, c) = 1$.

   Conversely, suppose that $\gcd(a, b) = 1 = \gcd(a, c)$. Now assume that $\gcd(a, bc) = d > 1$ and we will arrive at a contradiction. Let p be a prime divisor of d. Thus p divides a and p divides bc. By Euclid's Lemma, p divides either b or c. In the former case, p is a common divisor of both a and b. In the latter it is a common divisor of both a and c. In either case we have a contradiction that proves $\gcd(a, bc) = 1$.

3. (2.16) Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40. Can you see any relationship between this group and $U(8)$?

   Proof. Since this is the usual multiplication of integers, one does not have to check associativity. Next, we have to make sure that the set is closed under multiplication.

   $$5 \cdot 5 = 25, 5 \cdot 15 = 75 \equiv 35, 5 \cdot 25 = 125 \equiv 5, 5 \cdot 35 = 175 \equiv 15$$
   $$15 \cdot 15 = 225 \equiv 25, 15 \cdot 25 = 375 \equiv 15, 15 \cdot 35 = 525 \equiv 5$$
   $$25 \cdot 25 = 625 \equiv 25, 25 \cdot 35 = 875 \equiv 35 \text{ and } 35 \cdot 35 = 1225 \equiv 25.$$

   Thus the set is closed under multiplication. We also see that 25 is the identity element, and each element is its own inverse. Thus the set forms a group.

   We have that $U(8) = \{1, 3, 5, 7\}$. This group also has 4 elements and one checks each element is its own inverse, i.e., $x^2 = 1$ for all $x \in U(8)$!

4. (2.34) Prove that in a group $(ab)^2 = a^2b^2$ if and only if $ab = ba$.

Proof. First suppose that $ab = ba$. Now multiple on the left by a and on the right b, which gives

$$a^2b^2 = a(ab)b = abab \text{ or } a^2b^2 = (ab)(ab) = (ab)^2$$

Conversely, suppose that $(ab)^2 = a^2b^2$. Multiple this equation on the left by a^{-1} and on the right by b^{-1}. The left hand side is

$$a^{-1}[(ab)^2]b^{-1} = a^{-1}[(ab)(ab)]b^{-1} = ba.$$

While the right hand side is

$$a^{-1}(aabb)b^{-1)} = ab.$$

This proves this direction.