31. Prove that if $m$ is an integer, then $m^2 \equiv 0 \pmod{4}$ or $m^2 \equiv 1 \pmod{4}$.

**Proof.** Let $m \in \mathbb{Z}$. Then either $m$ is even or $m$ is odd.

**Case I:** Assume $m$ is even
If $m$ is even, then there exists $k \in \mathbb{Z}$ such that $m = 2k$. Then $m^2 = 4k^2$, so $4|m^2$ and hence $m^2 \equiv 0 \pmod{4}$.

**Case II:** Assume $m$ is odd
If $m$ is odd, then there exists $k \in \mathbb{Z}$ such that $m = 2k + 1$. Then $m^2 = 4k^2 + 4k + 1$, so $m^2 - 1 = 4(k^2 + k)$. Thus $m^2 \equiv 1 \pmod{4}$.

Thus if $m$ is an integer, then $m^2 \equiv 0 \pmod{4}$ or $m^2 \equiv 1 \pmod{4}$.

32. Prove or disprove that if $n$ is odd, then $n^2 \equiv 1 \pmod{8}$.

**Proof.** Let $n$ be odd. Then there exists an integer $k \in \mathbb{Z}$ such that $n = 2k + 1$. Thus we have the following:
\[
\begin{align*}
    n^2 - 1 &= (2k + 1)^2 - 1 \\
          &= 4k^2 + 4k + 1 - 1 \\
          &= 4k(k + 1)
\end{align*}
\]
Now consider the product $k(k + 1)$. If $k$ is even, then $k(k + 1)$ is even. If $k$ is odd, then $k + 1$ is even and hence $k(k + 1)$ is even. Hence in either case $k(k + 1)$ is even. So there exists $l \in \mathbb{Z}$ such that $k(k + 1) = 2l$. Therefore we have $n^2 - 1 = 4k(k + 1) = 4(2l) = 8l$. Thus $8|n^2 - 1$, so $n^2 \equiv 1 \pmod{8}$.

33. If $m$ is an integer, show that $m^2$ is congruent modulo 8 to one of the integers 0, 1 or 4.

**Proof.** If $m$ is odd, then we proved above that $m^2$ is congruent to 1 modulo 8.

Assume $m$ is even, so $m = 2k$. Thus $m^2 = 4k^2$. If $k$ is even, then $k^2$ is even so $k^2 = 2l$ for some $l \in \mathbb{Z}$. So $m^2 = 4(2l) = 8l$. Thus $8|m^2$. Hence $m^2$ is congruent to 0 modulo 8. If $k$ is odd, then $k^2$ is odd so $k^2 = 2j + 1$ for some $j \in \mathbb{Z}$. So $m^2 = 4(2j + 1) = 8j + 4$. Thus $m^2 - 4 = 8j$. Hence $8|m^2 - 4$, so $m^2$ is congruent to 4 modulo 8.

34. Prove that $n^3 \equiv n \pmod{6}$ for every positive integer $n$.

**Proof.** Let $n$ be a positive integer. Then $n^3 - n = n(n^2 - 1) = n(n + 1)(n - 1)$. If $n$ is odd, then $n + 1$ is even, hence $n(n + 1)(n - 1)$ is even. If $n$ is even, then $n(n + 1)(n - 1)$ is even. Thus in either case $n(n + 1)(n - 1)$ is even. In other words, $2|n(n + 1)(n - 1)$, so $2|n^3 - n$.

Dividing $n$ by 3, using the division algorithm we have $n = 3q + r$ where $r = 0, 1$ or 2. Then we have the following:
\[
    n^3 - n = n(n + 1)(n - 1) = (3q + r)(3q + r + 1)(3q + r - 1)
\]
If $r = 0$, then $n^3 - n = 3q(3q + 1)(3q - 1)$.
If $r = 1$, then $n^3 - n = (3q + 1)(3q + 2)(3q) = 3q(3q + 1)(3q + 2)$.
If $r = 2$, then $n^3 - n = (3q + 2)(3q + 3)(3q + 1) = 3(3a + 2)(q + 1)(3q + 1)$.

Thus in all cases $3|n^3 - n$.

Therefore we have that $2|n^3 - n$ and $3|n^3 - n$. Since 2 and 3 are relatively prime, then by problem #10 in section 2.4 we have that $2 \cdot 3|n^3 - n$. In other words, $6|n^3 - n$. So $n^3 \equiv n \pmod{6}$.
35. Let $x$ and $y$ be integers. Prove that if there is an equivalence class $[a]$ modulo $n$ such that $x \in [a]$ and $y \in [a]$, then $(x, n) = (y, n)$.

**Proof.** Let $x, y, a \in \mathbb{Z}$ such that $x \in [a]$ and $y \in [a]$. Thus $x \equiv a \pmod{n}$ and $y \equiv a \pmod{n}$, so by transitivity and symmetry $x \equiv y \pmod{n}$. Thus $x - y = nk$ for some $k \in \mathbb{Z}$. Therefore we have $y = x - nk$ and $x = y + nk$.

Let $d_1 = (x, n)$ and $d_2 = (y, n)$. Since $d_1|n$ and $d_1|n$, then $d_1$ divides any linear combination of $x$ and $n$. In particular, $d_1|x - nk$. In other words, $d_1|y$. Thus $d_1$ is a common divisor of $y$ and $n$. Since $d_2$ is the greatest common divisor of $y$ and $n$, it must be the case that $d_1|d_2$.

Similarly, since $d_2|y$ and $d_2|n$, then $d_2$ divides any linear combination of $y$ and $n$. In particular, $d_2|y + nk$. In other words, $d_2|x$. Thus $d_2$ is a common divisor of $x$ and $n$. Since $d_1$ is the greatest common divisor of $x$ and $n$, it must be the case that $d_2|d_1$.

Thus $d_1|d_2$ and $d_2|d_1$ implies $d_1 = \pm d_2$. However, $d_1$ and $d_2$ are both positive, so $d_1 = d_2$. 

□