Homework 10: Due Monday, April 11

Problem 1: Let $a, b, c \in \mathbb{Z}$. Show that if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

Problem 2: Show that for all $a \in \mathbb{Z}$, either $a^2 \equiv 0 \pmod 4$ or $a^2 \equiv 1 \pmod 4$.
Note: This problem is equivalent to Problem 2 on Homework 4. However, you should *not* just appeal to that solution. Instead, use properties of congruences and the fact that every integer is congruent to one of 0, 1, 2, or 3 modulo 4.

Problem 3: Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}^+$ be such that $a \equiv b \pmod m$. Show that $\gcd(a, m) = \gcd(b, m)$.

Problem 4: Suppose that $m, k \in \mathbb{N}^+$ and $a, b \in \mathbb{Z}$ are such that $ka \equiv kb \pmod m$. Let $d = \gcd(k, m)$, and fix $n \in \mathbb{N}^+$ with $m = dn$. Show that $a \equiv b \pmod n$.

Problem 5: For each part, determine (with explanation) whether or not there exists $x \in \mathbb{Z}$ with the given property. If so, find such an x by making use of the Euclidean algorithm.
a. $12x \equiv 9 \pmod{21}$.
b. $28x \equiv 43 \pmod{91}$.
c. $153x \equiv 1 \pmod{385}$.

Problem 6: Let $p \in \mathbb{N}^+$ be prime and let $a \in \mathbb{Z}$. Show that $a^2 \equiv 1 \pmod p$ if and only if either $a \equiv 1 \pmod p$ or $a \equiv -1 \pmod p$.

Problem 7: Find, with full explanation, the remainder when dividing 18^{1796} by 23.