Homework 13: Due Wednesday, April 22

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 if $n \in \mathbb{Z}$ and $7 \nmid n$, then $7 \mid n^{12} - 1$.

Problem 3: Let $p \in \mathbb{N}^+$ be prime, let $a \in \mathbb{Z}$ be such that $p \nmid a$. Let $d \in \mathbb{N}^+$ be the smallest positive power of a that is congruent to 1 modulo p. That is, let $d \in \mathbb{N}^+$ be such that $a^d \equiv 1 \pmod{p}$ and $a^k \not\equiv 1 \pmod{p}$ whenever $0 < k < d$. Show that $d \mid p - 1$.
Hint: Start by doing Division with Remainder.

Problem 4: Prove the following converse to the first version of Fermat's Little Theorem: Let $n \in \mathbb{N}$ with $n \geq 2$, and suppose that $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}$ with $n \nmid a$. Show that n is prime.
Aside: It turns out that converse of the second version is *not* true. That is, there do exist composite n such that $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$. Such numbers are called *Carmichael numbers*.

Problem 5:
a. Show that there exists $a \in \mathbb{Z}$ with $a \not\equiv 1 \pmod{8}$ and $a \not\equiv -1 \pmod{8}$ such that $a^2 \equiv 1 \pmod{8}$.
b. Let $p \in \mathbb{N}^+$ be an *odd* prime, let $k \in \mathbb{N}^+$ and let $a \in \mathbb{Z}$. Show that $a^2 \equiv 1 \pmod{p^k}$ if and only if either $a \equiv 1 \pmod{p^k}$ or $a \equiv -1 \pmod{p^k}$.
Hint: Part (b) generalizes Problem 6 on Homework 12 to odd prime powers. Problem 7 on that assignment is helpful.

Problem 6: Let $p \in \mathbb{N}^+$ be prime and let $a, b \in \mathbb{Z}$. Show that if $a \equiv b \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.