Homework 12: Due Friday, April 17

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

Problem 2: 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 3: 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 4: Use the Euclidean Algorithm to find an $x \in \mathbb{Z}$ with $153x \equiv 1 \pmod{385}$.

Problem 5: Find, with full explanation, the remainder when dividing 18^{1796} by 23.

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: Let $p \in \mathbb{N}^+$ be prime. Define a function $ord_p \colon \mathbb{N}^+ \to \mathbb{N}$ as follows. Given $a \in \mathbb{N}^+$, let $ord_p(a)$ be the largest $k \in \mathbb{N}$ such that $p^k \mid a$. For example, we have $ord_3(45) = 2$ and $ord_3(10) = 0$. Without using the Fundamental Theorem of Arithmetic, prove that for all $p, a, b \in \mathbb{N}^+$ with p prime, we have $ord_p(ab) = ord_p(a) + ord_p(b)$.
Note: Think carefully about what you need to do in order to prove that $ord_p(c) = k$. You need to show that $p^k \mid c$, but you also need to show that $p^\ell \nmid c$ whenever $\ell > k$.