Homework 11: Due Friday, April 15

Problem 1: Let $n \in \mathbb{Z}$ with $n \equiv 3 \pmod 4$. Show that there does not exist $a, b \in \mathbb{Z}$ with $n = a^2 + b^2$.
Hint: Use Problem 2 on Homework 10.

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: Show that if $p \in \mathbb{N}^+$ is prime, then $(p-2)! \equiv 1 \pmod p$.

Problem 6: Recall that Wilson's Theorem says that $(p-1)! \equiv -1 \pmod p$ whenever p is prime. Notice that $(4-1)! = 6$, so $(4-1)! \equiv 2 \pmod 4$. Show that if $n \in \mathbb{N}$ is composite and $n > 4$, then $(n-1)! \equiv 0 \pmod n$.
Note: In particular, it follows that $(n-1)! \not\equiv -1 \pmod n$ whenever n is composite, giving a converse to Wilson's Theorem.