Day 12  Homework

1. (From the midterm exam)
   a. Prove that $b \mod n = (b+nk) \mod n$.

2. Suppose $a \equiv b \pmod{n}$. Prove that $a \mod n = b \mod n$. (You may use 1)

3. Suppose $a \mod n = b \mod n$. Prove that $a \equiv b \pmod{n}$.

Note: 2 and 3 show that $a \equiv b \pmod{n}$ if and only if $a \mod n = b \mod n$. 
(b) Let $m$ be a positive integer, and suppose $a^m \equiv 1 \pmod{n}$.

1. Prove that $a^{km} \equiv 1 \pmod{n}$ for any positive integer $k$. (If this is difficult, you may prove this for $k = 3$).

2. Prove that $a^{km+1} \equiv a \pmod{n}$ for any positive integer $k$.

(c) (Modular exponentiation) Let $b$ be a positive integer. The notation $a^b$ means to multiply $a$ by itself repeatedly, with a total of $b$ factors of $a$, i.e.,

$$a^b = \underbrace{a \times a \times a \times \ldots \times a}_{b \text{ times}}$$

The notation for $\mathbb{Z}_n$ is the same. If $a \in \mathbb{Z}_n$, in the context of $\mathbb{Z}_n$, we have

$$a^b = \underbrace{a \circ a \circ a \circ \ldots \circ a}_{b \text{ times}}$$

Without the aid of a calculator, find, in $\mathbb{Z}_{100}$, the value of $36^4$. 