Notation for modular arithmetic

Math 307 - Fall 2011

We will often denote modular arithmetic slightly differently (although equivalent matematically) from the text. On the first homework, from Chapter 0, for example, Problem 11 reads as follows:

Problem 11 (text version): Let n be a fixed positive integer greater than 1. If a mod $n = a'$ and b mod $n = b'$, prove that $(a + b)$ mod $n = (a' + b')$ mod n and (ab) mod $n = (a'b')$ mod n.

Instead, we will write the same problem (as you should on your homework) as follows:

Problem 11 (our version): Let n be a fixed positive integer greater than 1. If $a \equiv a'(\text{mod } n)$ and $b \equiv b'(\text{mod } n)$, prove that $(a + b) \equiv (a' + b')(\text{mod } n)$ and $(ab) \equiv (a'b')(\text{mod } n)$.

The main difference here, as mentioned in the text and in lecture, is that in the first version, the symbol "mod n" acts like an operation, where a mod $n = a'$ means that if one applies the division algorithm to a divided by n, then a' is the unique non-negative remainder less than n. In the second version, $\equiv \cdots (\text{mod } n)$ acts as an equivalence relation, where $a \equiv a'(\text{mod } n)$ means that n divides $a - a'$. Similarly, in Chapter 0, Problem 13, you should replace "ax mod $n = 1$" with "$ax \equiv 1(\text{mod } n)$".

While these two interpretations mean the exact equivalent things mathematically, the second (our) interpretation will lend itself to proofs which are a bit more straighforward to write down, including Problems 11 and 13. To get you started on Problem 11, for example, you would start by writing down the fact that $a \equiv a'(\text{mod } n)$ and $b \equiv b'(\text{mod } n)$ translate to mean $n|a - a'$ and $n|b - b'$, so that we may write $a - a' = nk$ and $b - b' = nl$ for some integers k and l. Take it from there!

In Chapter 0, Problem 18, however, which states “Determine 8^{402} mod 5”, this means to calculate the remainder of 8^{402} when dividing by 5, as in the first interpretation above of the meaning of “mod”.