Problems For Tour 9

Suppose a and b are integers. We say that a is *congruent* to b *modulo* m if a and b both give the same remainder when divided by m. We write this as $a \equiv b \pmod{m}$. For our purposes, we will say that m must be a positive integer.

For example, $17 \equiv 1 \pmod{4}$, $19 \equiv -5 \pmod{12}$, and $26 \equiv 0 \pmod{13}$.

If $a \equiv b \pmod{m}$, then $a = km + b$ for some integer k.
Note that saying $a \equiv b \pmod{m}$ is equivalent to saying that $a - b$ is a multiple of m.

Note that every integer a is congruent to *exactly* one of $\{0, 1, 2, \ldots, m-1\} \pmod{m}$.

Here are three important rules which are not too difficult to prove.

i) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.
ii) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
iii) If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$, for all non-negative integers n.

Can you see how we can use rule ii) to prove rule iii)?

For example, because $17 \equiv 2 \pmod{5}$ and $4 \equiv 14 \pmod{5}$, we have:
$17 + 4 \equiv 2 + 14 \pmod{5}$, and $17 \times 4 \equiv 2 \times 14 \pmod{5}$.

Here are some problems.

1. Determine the last digit of 3^{1999}.
2. What is the rule for divisibility by 9? Prove it! Similarly, state and prove the rule for divisibility by 11.
3. Show that $4^{3n+1} + 2^{3n+1} + 1$ is divisible by 7 for all positive integers n.
4. Pick any 55 numbers from the set $\{1, 2, 3, \ldots, 100\}$. Prove that among those 55 numbers, you can find two of them that differ by 9.
5. Prove Fermat's Little Theorem: if p is prime and a is not divisible by p, show that $a^{p-1} \equiv 1 \pmod{p}$.

   (Hint: look at the set $\{a, 2a, 3a, \ldots, (p-1)a\}$ and reduce each element modulo p. For example, if $a = 3$ and $p = 7$, the set becomes $\{3, 6, 9, 12, 15, 18\}$, which reduces to $\{3, 6, 2, 5, 1, 4\}$ in modulo 7. What do you notice?)