

Name: Scott Armstrong

Quiz 6

Math 74

November 15, 2006

1. Define what it means for two integers to be congruent modulo n .

Let $a, b \in \mathbb{Z}$, $n \in \mathbb{N}^*$. We say that a is congruent to b modulo n if $a \bmod n = b \bmod n$.

We write $a \equiv b \pmod{n}$ if a is congruent to b modulo n .

2. State the Fundamental Theorem of Modular Arithmetic.

FTMA.

Suppose that $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N}^*$ such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $a + c \equiv b + d \pmod{n}$ and $a \cdot c \equiv b \cdot d \pmod{n}$.

3. Show that if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for every positive integer k .

We proceed by induction. Clearly $a^1 \equiv b^1 \pmod{n}$.

Suppose that $a^m \equiv b^m \pmod{n}$ for some $m \geq 1$.

Then by FTMA, $a^{m+1} \equiv a \cdot a^m \equiv b \cdot b^m \equiv b^{m+1} \pmod{n}$.

The result now follows by induction.