Lecture 18

Enoch Cheung

October 28, 2013

1. Show that if $a \in \mathbb{Z}$ and $b, c \in \mathbb{N}$ such that when a is divided by b the quotient is q and the remainder is r and when q is divided by c the quotient is s and the remainder is t then wehn a is divided by bc the quotient is s and the remainder is $bt + r$. (Make sure to show that $0 \leq bt + r < bc$.)

   The assumption is $a = bq + r$ and $q = cs + t$, and we wish to show that $a = bc(s) + (bt + r)$. By substitution,
   $$a = b(cs + t) + r = bcs + bt + r = bc(s) + (bt + r)$$
   as desired.

   To check that $0 \leq bt + r < bc$, note that since r, t are remainders $0 \leq r < b$ and $0 \leq t < c$. Rewritten, this is $0 \leq t \leq c - 1$, which means that $0 \leq bt \leq b(c - 1)$. Add the inequality $0 \leq r < b$ to obtain
   $$0 \leq bt + r < b(c - 1) + b = bc$$
   so $0 \leq bt + r < bc$ as desired.

2. True, false, true, true, false, true.

3. Claim:
   $$\forall a, b \in \mathbb{Z}.\ \forall m \in \mathbb{N}.\ (a \equiv b \pmod{m} \to \forall n \in \mathbb{N}.\ a^n \equiv b^n \pmod{m})$$

   Consider $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$ arbitrary such that $a \equiv b \pmod{m}$. We will prove by induction on $n \in \mathbb{N}$ that $a^n \equiv b^n \pmod{m}$. The base case is just $a \equiv b \pmod{m}$ which we already have.

   For the inductive step, suppose for some $n \in \mathbb{N}$ that $a^n \equiv b^n \pmod{m}$, then since $a \equiv b \pmod{m}$, by Lemma 6.5.10 (Modular Arithmetic Lemma p.419), $a^n a \equiv b^n b \pmod{m}$, so $a^{n+1} \equiv b^{n+1} \pmod{m}$.

   Therefore, by induction, we have shown that $\forall n \in \mathbb{N}.\ a^n \equiv b^n \pmod{m}$. Since $a, b \in \mathbb{Z}, m \in \mathbb{N}$ were arbitrary, we showed $\forall a, b \in \mathbb{Z}.\ \forall m \in \mathbb{N}.\ (a \equiv b \pmod{m} \to \forall n \in \mathbb{N}.\ a^n \equiv b^n \pmod{m})$.