MATH 215 (WHYTE), MIDTERM EXAM NOV 2^{nd} 2018 SOLUTIONS

(1) Prove that if a, b, and c are integers and n a natural number such that $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$.

The definition of $x \equiv y \bmod z$ is that z divides $x - y$. Thus our hypotheses are that n divides both $a - b$ and $b - c$. If we write $a - b = nq_1$ and $b - c = nq_2$ then we get:

$$a - c = (a - b) + (b - c) = nq_1 + nq_2 = n(q_1 + q_2)$$

so we can conclude that $n|a-c$, which is the definition of $a \equiv c \bmod n$.

(2) Prove that if x and y are integers where $x|y$ and $y|x$ then $x = y$ or $x = -y$.

The definition of $a|b$ is that there is an integer q so that $b = aq$. Thus our hypotheses are that there are q_1 and q_2 with $y = xq_1$ and $x = yq_2$. Substituting the first of these into the second gives $x = xq_1q_2$. So we have that $x(q_1q_2 - 1) = 0$. Thus $x = 0$ or $q_1q_2 = 1$.

In the first case we have $y = 0q_2$ so $y = 0$ as well, thus both $y = x$ and $y = -x$ are true in this case.

In the second case, q_1 must be a divisor of 1, hence is either 1 or -1. The equation $y = xq_1$ then gives that $x = y$ or $x = -y$.

(3) Prove that if m and n are natural numbers with $n < m$ then $n^k < m^k$ for all $k \in \mathbb{N}$.

Let $S = \{k \in \mathbb{N} : n^k \geq m^k\}$. The claim is then that S is empty. If not, then by the well-ordering principle, there is a smallest element in S, call it k_0.

Since $n^1 = n$ and $m^1 = m$, we certainly have that $n^1 < m^1$ so that $1 \notin S$ and thus $k_0 > 1$. This means that $k_0 - 1 \in \mathbb{N}$. Since $k_0 - 1 < k_0$ we cannot have $k_0 - 1 \in S$ so we know:

$$n^{k_0-1} < m^{k_0-1}$$

If we multiply this by n, since $n > 0$ we get :

$$n^{k_0} < nm^{k_0-1}$$

Likewise, since m^{k_0-1} is positive we can multiply it by the inequality $n < m$ to get

$$nm^{k_0-1} < m_{k_0}$$

Putting together these two inequalities gives $n^{k_0} < m^{k_0}$ which contradicts $k_0 \in S$. Thus S must be empty.

(4) Show that common divisors of s and t are the same as the common divisors of s and $s - t$.

If a is a common divisor of s and t, so $a|s$ and $a|t$, then $s = aq_1$ and $t = aq_2$ so $s - t = a(q_1 - q_2)$, showing that $a|s - t$ and so a is also a common divisor of s and $s - t$.

On the other hand, if b is a common divisor of s and $s - t$, so $b|s$ and $b|s - t$, so $s = br_1$ and $s - t = br_2$. Then since $t = s - (s - t)$ we have $t = b(r_1 - r_2)$ and so b is also a common divisor of s and t.