Introduction to Mathematical Reason | MATH 300 Test #2 | March 11, 2010

Name:____________________ R. Hammack Score:______

Directions The purpose of this very brief test is to check your understanding of the three main methods of proving conditional statements. Prove the following statements. In each case, work strictly from the definitions.

---

1. If a is an odd integer, then a^2+4a+7 is even.

   Proof (Direct) Suppose a is odd.
   Then $a = 2k+1$ for some $k \in \mathbb{Z}$.
   Thus $a^2+4a+7 = (2k+1)^2+4(2k+1)+7 = 4k^2+4k+1+8k+4+7 = 4k^2+12k+12 = 2(2k^2+6k+6)$.
   Consequently $a^2+4a+7 = 2m$, where $m = 2k^2+6k+6 \in \mathbb{Z}$.
   Therefore a^2+4a+7 is even. ■

2. Suppose $a, b \in \mathbb{Z}$. If $25 \nmid ab$, then $5 \nmid a$ or $5 \nmid b$.

   Proof (Contapositive) Suppose it is not the case that $5 \nmid a$ or $5 \nmid b$.
   Then $5|a$ and $5|b$. (Using DeMorgan's Law.)
   This means $a = 5m$ and $b = 5n$ for integers m and n.
   Multiplying, $ab = (5m)(5n) = 25mn$.
   We now have $ab = 25mn$, where mn is an integer.
   Therefore, by definition of divides, we see that $25|ab$.
   Thus it is not the case that $25 \nmid ab$. ■

3. Suppose $a, b \in \mathbb{R}$. If a is rational and ab is irrational, then b is irrational.

   Proof Suppose for the sake of contradiction that a is rational, ab is irrational, but b is not irrational.
   Thus a is rational, and ab is irrational, and b is rational.
   Then $a = \frac{m}{n}$ and $b = \frac{k}{\ell}$ for some $m, n, k, \ell \in \mathbb{Z}$, by definition of a rational number.
   Consequently, $ab = \frac{m}{n}\frac{k}{\ell} = \frac{mk}{n\ell}$.
   But, as mk and $k\ell$ are integers, we deduce that $ab = \frac{mk}{n\ell}$ is rational.
   Thus ab is rational and ab is not rational. This is a contradiction. ■

4. Suppose $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$, then $a^2 \equiv bc \pmod{n}$.

   Proof (Direct) Suppose $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$.
   By definition of congruence, this means $n|(a-b)$ and $n|(a-c)$.
   In turn, the definition of divisibility yields $a-b = nk$ and $a-c = n\ell$ for some integers k and ℓ.
   Therefore $a = nk+b$ and $a = n\ell+c$.
   Multiplying, we get $a^2 = (nk+b)(n\ell+c) = n^2k\ell + nkc + bn\ell + bc$.
   From this, we get $a^2 - bc = n(nk\ell + kc + b\ell)$, where $nk\ell + kc + b\ell$ is an integer.
   The definition of divides now gives $n|(a^2-bc)$.
   Finally the definition of congruence modulo n produces $a^2 \equiv bc \pmod{n}$. ■