SCS 2210 - DISCRETE MATHEMATICS II

TUTORIAL I

1. Prove that for each $a, b \in \mathbb{Z} \setminus \{0\}$, $a|b$ and $b|a$ if and only if $a = \pm b$.

2. Prove that for each $a, b, c, d \in \mathbb{Z}$ such that $ac \neq 0$, if $a|b$ and $c|d$, then $ac|bd$.

3. Prove that for each $a, b, c \in \mathbb{Z}$ such that $ac \neq 0$, if $ac|bc$, then $a|b$.

4. Prove or disprove: For each $a, b, c \in \mathbb{Z}^+$, if $a|bc$, then $a|b$ or $a|c$.

5. Prove that for each $a, b \in \mathbb{Z}$, if $a|b$ and $b \neq 0$ then $|a| \leq |b|$.

6. Let $a, b \in \mathbb{Z}$. Suppose $a \equiv 11 \pmod{19}$ and $b \equiv 3 \pmod{19}$. Find the integer c with $0 \leq c \leq 18$ such that

a). $c \equiv 13a \pmod{19}$ b). $c \equiv 8b \pmod{19}$ c). $c \equiv (a-b) \pmod{19}$

d). $c \equiv (7a+3b) \pmod{19}$ e). $c \equiv (2a^2+3b^2) \pmod{19}$ f). $c \equiv (a^3+4b^3) \pmod{19}$

7. Let $m \in \mathbb{Z}^+$ and let $a, b \in \mathbb{Z}$. Prove that $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$ (equivalently $a \equiv b \pmod{m}$ if and only if a and b leave the same nonnegative remainder when divided by m).

8. Show that if a is an integer and d is an integer greater than 1, then the quotient and remainder obtained when a is divided by d are $\lfloor a/d \rfloor$ and $a - d\lfloor a/d \rfloor$, respectively, where $\lfloor \cdot \rfloor$ is the floor function (i.e., for $x \in \mathbb{R}$, $\lfloor x \rfloor$ = the largest integer less than or equal to x).

9. Find the integer a such that

a). $a \equiv 43 \pmod{23}$ and $-22 \leq a \leq 0$.

b). $a \equiv 17 \pmod{29}$ and $-14 \leq a \leq 14$.

c). $a \equiv -11 \pmod{21}$ and $90 \leq a \leq 110$.

(10). Let $a, b, c, d \in \mathbb{Z}$ and let $m \in \mathbb{Z}$ be such that $m \geq 2$. Prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $(a-c) \equiv (b-d) \pmod{m}$.

(11). Let $a, b \in \mathbb{Z}$ and let $m, n \in \mathbb{Z}$ be such that $m, n > 1$. Prove that if $n | m$ and $a \equiv b \pmod{m}$, then $a \equiv b \pmod{n}$.

(12). Let $a, b, c \in \mathbb{Z}$ be such that $c > 0$ and let $m \in \mathbb{Z}$ be such that $m \geq 2$. Prove that if $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$.

(13). Find counterexamples to each of these statements about congruences.

a). If $ac \equiv bc \pmod{m}$, where a, b, c and m are integers with $m \geq 2$, then $a \equiv b \pmod{m}$.

b). If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where $a, b, c, d, m \in \mathbb{Z}$ such that $c, d > 0$ and $m \geq 2$, then $a^c \equiv b^d \pmod{m}$.

(14). a). Show that if $n \in \mathbb{Z}$, then $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

b). Use part (a) to show that if m is a positive integer of the form $4k+3$, where $k \in \mathbb{Z}^+ \cup \{0\}$, then m is not the sum of the squares of two integers.

(15). Prove that if n is an odd positive integer, then $n^2 \equiv 1 \pmod{8}$.

(16). Show that if $a, b, k, m \in \mathbb{Z}$ such that $k \geq 1$, $m \geq 2$ and $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$.