MATHEMATICS 271 L01 FALL 2004
ASSIGNMENT 2 SOLUTION

1. Two integers a and b are said to be *relatively prime* if, and only if $\gcd(a.b) = 1$. Thus, two integers a and b are relatively prime if, and only if there are integers x and y such that $xa + yb = 1$. Prove or disprove the following:

(a) For all integers a and b, if a and b are relatively prime then $a+b$ and $a-b$ are relatively prime.

(b) For all integers a and b, if $a+b$ and $a-b$ are relatively prime then a and b are relatively prime.

(c) For all integers a, b and c, if a and b are relatively prime, and $a \mid bc$ then $a \mid c$.

(d) For all integers a, b and c, if a and b are relatively prime, and $a \mid c$ and $b \mid c$ then $ab \mid c$.

Solution:

(a) This statement is false because when $a = b = 1$, we see that a and b are relatively prime (because $\gcd(a, b) = \gcd(1, 1) = 1$), but $a+b$ and $a-b$ are relatively prime (because $\gcd(a + b, a - b) = \gcd(2, 0) = 2$).

(b) This statement is true and here is a proof. Let a and b be integers so that $a + b$ and $a - b$ are relatively prime, which means $\gcd(a + b, a - b) = 1$. Let $d = \gcd(a, b)$. Since 1 is a common divisor of a and b, it is clear that $d \geq 1$. Since $d = \gcd(a, b)$, we get $d \mid a$ and $d \mid b$, that means, there are integers m and n so that $a = dm$ and $b = dn$. It follows that $a + b = dm + dn = d(m + n)$ and $a - b = dm - dn = d(m - n)$. These imply that d is common divisor of $a + b$ and $a - b$, and so $d \leq 1$ because $\gcd(a + b, a - b) = 1$.

From $d \geq 1$ and $d \leq 1$, we conclude that $d = 1$, and so $\gcd(a, b) = 1$, which means a and b are relatively prime.

(c) This statement is true and here is a proof. Let a, b and c be integers so that a and b are relatively prime, and $a \mid bc$. Since a and b are relatively prime, there are integers x and y such that $xa + yb = 1$. Since $a \mid bc$, $bc = ak$ for some integer k. Now,

$$\begin{aligned} c &= c \times 1 \\ &= c(xa + yb) && \text{because } xa + yb = 1. \\ &= cax + cyb \\ &= cax + yak && \text{because } bc = ak. \\ &= a(cx + yk) \end{aligned}$$

Thus, $a \mid c$.

(d) This statement is true and here is a proof. Let a, b and c be integers so that a and b are relatively prime, and $a \mid c$ and $b \mid c$. Since a and b are relatively prime, there are integers x and y such that $xa + yb = 1$. Since $a \mid c$ and $b \mid c$, $c = am$ and $c = bn$ for some integers m and n. Now,

$$\begin{aligned} c &= c \times 1 \\ &= c(xa + yb) && \text{because } xa + yb = 1. \\ &= cax + cyb \\ &= bnax + amyb && \text{because } c = am \text{ and } c = bn \\ &= ab(nx + ym) \end{aligned}$$

Thus, $ab \mid c$.

2. Let n be a positive integer. Prove the following statements:

(a) For all integers a and b, $(a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n$.

(b) For all integers a and b, $(ab) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$.

(c) For all integers a, if a and n are relatively prime then there is an integer b such that $1 \leq b \leq n-1$ and $(ab) \bmod n = 1$.

(d) For all integers a, x and y, if a and n are relatively prime, and $(ax) \bmod n = (ay) \bmod n$ then $x \bmod n = y \bmod n$.

Solution:
(a) Let a, b be integers. Let $r = a \bmod n$, $s = b \bmod n$ and $t = (r+s) \bmod n$. Then $0 \leq r, s, t < n$, and there are integers x, y, z so that $a = nx+r$, $b = ny+s$ and $r+s = nz+t$. Now, $a+b = nx+r+ny+s = nx+ny+nz+t = n(x+y+z)+t$, where $0 \leq t < n$, which means $(a+b) \bmod n = t = (r+s) \bmod n = (a \bmod n + b \bmod n) \bmod n$.
(b) Let a, b be integers. Let $r = a \bmod n$, $s = b \bmod n$ and $t = (rs) \bmod n$. Then $0 \leq r, s, t < n$, and there are integers x, y, z so that $a = nx+r$, $b = ny+s$ and $rs = nz+t$. Now, $ab = (nx+r)(ny+s) = n^2xy + nxs + nry + rs = n^2xy + nxs + nry + nz + t = n(nxy + xs + ry + z) + t$, where $0 \leq t < n$, which means $ab \bmod n = t = (rs) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$.
(c) This statement only makes sense when $n \geq 2$. We prove this statement in the case $n \geq 2$. Let a be an integer such that a and n are relatively prime. Since a and n are relatively prime, there.are integers x and y such that $ax + ny = 1$, and so $ax = 1 - ny$ Let $b = x \bmod n$. We prove that $(ab) \bmod n = 1$. Since $b = x \bmod n$, there is integer q such that $x = nq + b$ and note that $0 \leq b \leq n-1$. From $x = nq + b$, we get $b = x - nq$ and so $ab = ax - anq = 1 - ny - anq = n(-y - aq) = 1$ which implies that $(ab) \bmod n = 1$. It remains to show that $1 \leq b \leq n$. However, we know that $0 \leq b \leq n-1$, so we only have to show that $b \neq 0$ (by a contradiction proof). Suppose that $b = 0$. Then $x = nq$, and so from $ax + ny = 1$, we get $n(aq + y) = anq + ny = ax + ny = 1$, which means n is a divisor of 1, but this is impossible because $n \geq 2$. Thus, $1 \leq b \leq n-1$.
(d) Let a, x and y be integers so that a and n are relatively prime, and $(ax) \bmod n = (ay) \bmod n$. We prove that $x \bmod n = y \bmod n$. It is clear that when $n = 1$, $x \bmod n = y \bmod n = 0$. Now suppose that $n \geq 2$. Then by part (c), there is an integer b such that $1 \leq b \leq n-1$ and $(ab) \bmod n = 1$. Thus,

$$
\begin{array}{rcll}
x \bmod n & = & (x \bmod n) \bmod n & \text{because } 0 \le x \bmod n < n \\
& = & ((1 \times x) \bmod n) \bmod n & \\
& = & ((ab) \bmod n\,(x \bmod n)) \bmod n & \\
& = & (abx) \bmod n & \text{by part (b)} \\
& = & ((ax) \bmod n\,(b \bmod n)) \bmod n & \text{by part (b)} \\
& = & ((ay) \bmod n\,(b \bmod n)) \bmod n & \text{because } (ax) \bmod n = (ay) \bmod n. \\
& = & (aby) \bmod n & \\
& = & ((ab) \bmod n\,(y \bmod n)) \bmod n & \text{by part (b)} \\
& = & (y \bmod n) \bmod n & \text{by part (b)} \\
& = & y \bmod n & \text{because } 0 \le y \bmod n < n
\end{array}
$$

3. Prove or disprove the following statements:

(a) For real numbers x and y, $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$.

(b) For real numbers x and y, if $x + \lceil x \rceil = y + \lceil y \rceil$ then $x = y$.

(c) For real numbers y, there is a real number x such that $y = x + \lceil x \rceil$.

(d) For real numbers x and y, if $x + \lceil x \rceil = y$ then $x = y - \frac{1}{2} \lceil y \rceil$.

Solution:

(a) This statement is false. For example, $\lceil 0.5 + 0.5 \rceil = 1 \neq 2 = \lceil 0.5 \rceil + \lceil 0.5 \rceil$.

(b) This statement is true, and here is a proof. Let x and y be real numbers so that $x + \lceil x \rceil = y + \lceil y \rceil$. Put $a = \lceil x \rceil - x$ and $b = \lceil y \rceil - y$. We see that $x = \lceil x \rceil - a$ and $y = \lceil y \rceil - b$ where $0 \le a, b < 1$. Now,

$$
\begin{array}{rcll}
x + \lceil x \rceil = y + \lceil y \rceil & \Leftrightarrow & 2\lceil x \rceil - a = 2\lceil y \rceil - b & \\
& \Leftrightarrow & a - b = 2\lceil x \rceil - 2\lceil y \rceil & (*)
\end{array}
$$

Since $0 \le a, b < 1$, we have $-1 < a - b < 1$, and from $(*)$ we see that $a - b$ is an integer strictly between -1 and 1 and therefore, $a - b = 0$. It follows from $(*)$ that $2\lceil x \rceil - 2\lceil y \rceil = 0$. From $a - b = 0$ and $2\lceil x \rceil - 2\lceil y \rceil = 0$, we have that $a = b$ and $\lceil x \rceil = \lceil y \rceil$, and so $x = \lceil x \rceil - a = \lceil y \rceil - b = y$.

(c) This statement is false. In fact, we can show that $x + \lceil x \rceil \neq 1$ for all real numbers x by a contradiction proof. Suppose that there is a real number x so that $x + \lceil x \rceil = 1$. From $x + \lceil x \rceil = 1$, we get $x = 1 - \lceil x \rceil$ which is an integer and so $\lceil x \rceil = 1 - \lceil x \rceil$ or equivapently, $\lceil x \rceil = \frac{1}{2}$ which contradicts the fact that $\lceil x \rceil$ is an integer. Thus, $x + \lceil x \rceil \neq 1$ for all real numbers x.

(d) This statement is true, and here is a proof. Let x and y be real numbers so that $x + \lceil x \rceil = y$. Since $\lceil x \rceil - 1 < x \le \lceil x \rceil$. we get $2\lceil x \rceil - 1 < x + \lceil x \rceil \le \lceil x \rceil + \lceil x \rceil = 2\lceil x \rceil$, which means $2\lceil x \rceil - 1 < y \le \lceil x \rceil + \lceil x \rceil = 2\lceil x \rceil$ (because $y = x + \lceil x \rceil$) where $2\lceil x \rceil$ is an integer. It follows that $\lceil y \rceil = 2\lceil x \rceil$ and so $\lceil y \rceil = \frac{1}{2}\lceil x \rceil$, and from $x + \lceil x \rceil = y$ we see that $x = y - \lceil x \rceil = y - \frac{1}{2}\lceil y \rceil$.