MATHEMATICS 271 L01 FALL 2003
ASSIGNMENT 4 SOLUTION

1. Let a, b, c be integers.
(a) Prove that if $c \mid a$ and $c \mid b$ then $c \mid (xa + yb)$ for any integers x and y.
(b) Prove that if a and b are relatively prime and, $a \mid c$ and $b \mid c$ then $(ab) \mid c$.
(c) Prove that if a and b are relatively prime and $a \mid bc$ then $a \mid c$.
Solution:
(a) Suppose that $c \mid a$ and $c \mid b$. This means there are $m, n \in \mathbb{Z}$, so that $a = cm$ and $b = cn$. Now, for any $x, y \in \mathbb{Z}$, $xa + yb = xcm + ycn = c(xm + yn)$ which implies that $c \mid (xa + yb)$ (Note that $xa + yb \in \mathbb{Z}$ because $m, n, x, y \in \mathbb{Z}$).
(a) Suppose that a and b are relatively prime and, $a \mid c$ and $b \mid c$. Since a and b are relatively prime, there are $x, y \in \mathbb{Z}$, so that $xa + yb = 1$. Since $a \mid c$ and $b \mid c$, there are $m, n \in \mathbb{Z}$, so that $c = am$ and $c = bn$. Now, $c = c \times 1 = c(xa + yb) = cxa + cyb = bnxa + amyb = ab(xn + ym)$ which implies that $(ab) \mid c$. Note that $xn + ym \in \mathbb{Z}$ because $m, n, x, y \in \mathbb{Z}$).
(c) Suppose that a and b are relatively prime and $a \mid bc$. Since a and b are relatively prime, there are $x, y \in \mathbb{Z}$, so that $xa + yb = 1$. Since $a \mid bc$, there is $m \in \mathbb{Z}$, so that $bc = am$. Thus, $c = c \times 1 = c(xa + yb) = xca + ybc = xca + am = a(xc + m)$ which implies that $a \mid c$. Note that $xc + m \in \mathbb{Z}$ because $m, x, c \in \mathbb{Z}$).

2. Let $A = \{1, 2, 3, 4\}$ and let $\mathcal{F}$ be the set of all functions from A to A. Choose an elements f of $\mathcal{F}$ and assume that all elements of $\mathcal{F}$ are equally likely.

(a) What is the probability that f is one-to-one?

(b) What is the probability that $f(1) \leq f(2)$?

(c) Given that f is one-to-one, what is the probability that $f(1) \leq f(2)$?

(d) Are the event that f is one-to-one and the event that $f(1) \leq f(2)$ independent? Explain.
Solution:
(a) Let $E = \{f \in \mathcal{F} : f \text{ is one-to-one}\}$. We want to find $P(E)$. Note that $|\mathcal{F}| = 4^4$ (this is because for each $f \in \mathcal{F}$ there are 4 choices of $f(i)$ for each of the four $i \in A$). Now, $|E|$ is the number of one-to-one functions f from A to A, which is 4!, this is because there are 4 choices for $f(1)$, there are 3 choices for $f(2)$, there are 2 choices for $f(3)$ and there is 1 choice for $f(4)$. Thus, the answer to part (a) is $P(E) = \dfrac{|E|}{|\mathcal{F}|} = \dfrac{4!}{4^4} = \dfrac{3}{32}$.
(b) Let $F = \{f \in \mathcal{F} : f(1) \leq f(2)\}$. We want to find $P(F)$.

Note that $\overline{F} = \{f \in \mathcal{F} : f(1) > f(2)\}$ and $\left|\overline{F}\right| = \binom{4}{2} \times 4 \times 4 = 6 \times 4^2$ (this is because there are $\binom{4}{2}$ choices for the images of 1 and 2 under f and there 4 choices of for each of $f(3)$ and $f(4)$). Thus, the answer to part (b) is $P(F) = 1 - P\left(\overline{F}\right) = 1 - \dfrac{\left|\overline{F}\right|}{|\mathcal{F}|} = \dfrac{4^4 - 6 \times 4^2}{4^4} = \dfrac{10 \times 4^2}{4^4} = \dfrac{5}{8}$.

(c) We want to find $P(F \mid E)$. Now, $(E \cap F)$ is the number of one-to-one functions from A to A so that $f(1) < f(2)$, which is $\binom{4}{2} \times 2 \times 2 = 6 \times 2 = 12$ (this is because there are $\binom{4}{2}$ choices for the images of 1 and 2 under f,and there 2 choices of for each of $f(3)$ and there is 1 choice for $f(4)$). Thus, $P(E \cap F) = \dfrac{|E \cap F|}{|\mathcal{F}|} = \dfrac{12}{4^4}$ and the answer to part (c) is $P(F \mid E) = \dfrac{P(E \cap F)}{P(E)} = \dfrac{12}{4!} = \dfrac{1}{2}$.
(d) The event that f is one-to-one and the event that $f(1) \leq f(2)$ are not independent because $P(E \cap F) = \dfrac{12}{4^4} = \dfrac{3}{64} = \dfrac{12}{256} \neq \dfrac{15}{256} = \dfrac{3}{32} \times \dfrac{5}{8} = P(E) \times P(F)$.

3. Let $f : A \to B$ and $g : B \to C$ be functions. Prove or disprove each of the following.
(a) If f and g are one-to-one then $g \circ f$ is also one-to-one.
(b) If $g \circ f$ is one-to-one then f must be one-to-one.
(c) If $g \circ f$ is one-to-one then g must be one-to-one.
(d) If $g \circ f$ is one-to-one and f is onto then g is one-to-one.
Solution:
(a) The statement is true and here is a proof. Let $f : A \to B$ and $g : B \to C$ be one-to-one functions. We show that $g \circ f$ is one-to-one. Let $x, y \in A$ so that $g \circ f(x) = g \circ f(y)$. Since $g \circ f(x) = g \circ f(y)$, we have $g(f(x)) = g(f(y))$ and so $f(x) = f(y)$ because g is one-to-one. Now, from $f(x) = f(y)$ and f is one-to-one, we get $x = y$. Thus, $g \circ f$ is also one-to-one.
(b) The statement is true and here is a proof. Let $f : A \to B$ and $g : B \to C$ be functions so that $g \circ f$ is one-to-one. We show that f is one-to-one. Let $x, y \in A$ so that $f(x) = f(y)$. Then $g(f(x)) = g(f(y))$, that is, $g \circ f(x) = g \circ f(y)$ which implies $x = y$ because $g \circ f$ is one-to-one. Thus, f is one-to-one.
(c) The statement is false. For example, let $A = C = \{1\}$ and $B = \{1, 2\}$. Consider the functions $f : A \to B$ and $g : B \to C$ defined by $f = \{(1, 1)\}$ and $g = \{(1, 1), (2, 1)\}$ then $g \circ f = \{(1, 1)\}$ is a one-to-one function from A to C, but g is not one-to-one because $g(1) = 1 = g(2)$ but $1 \neq 2$.
(d) The statement is true and here is a proof. Let $f : A \to B$ and $g : B \to C$ be functions so that $g \circ f$ is one-to-one and f is onto. We show that g is one-to-one. Let $x, y \in B$ so that $g(x) = g(y)$. Since $x, y \in B$ and f is onto, there are $s, t \in A$ so that $f(a) = x$ and $f(b) = y$. Thus, $g \circ f(a) = g(f(a)) = g(x) = g(y) = g(f(b)) = g \circ f(a)$ and therefore $a = b$ (because $g \circ f$ is one-to-one). Hence, $x = f(a) = f(b) = y$ and so g is one-to-one.