MATHEMATICS 271 L01 FALL 2003 QUIZ 5 SOLUTION

1. Let a, b and c be integers. Prove or disprove each of the following statement.
(a) If $a \mid bc$ then $a \mid b$ or $a \mid c$.
(b) If a and b are relatively prime, and $a \mid bc$ then $a \mid c$.
Solution:
(a) This statement is false. For example, when $a = 4$, and $b = c = 2$, it is clear that $a \mid bc$, but $a \nmid b$ and $a \nmid c$.
(b) 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. In this question, the three parts are related.
(a) Find $\gcd(473, 467)$ using Euclidean Algorithm and find some integers x and y so that $\gcd(473, 467) = 473x + 467y$.
(b) Is 467 invertible in $\mathbb{Z}_{473}$? Explain. If 467 is invertible in $\mathbb{Z}_{473}$, find the inverse (reciprocal) of 467 in $\mathbb{Z}_{473}$.
(c) In $\mathbb{Z}_{473}$, solve the equation $(467 \otimes x) \oplus 252 = 2$.
Solution:
(a)

$$\begin{array}{rcrcl} 473 & = & 1 \times 467 & + & 6 \\ 467 & = & 77 \times 6 & + & 5 \\ 6 & = & 1 \times 5 & + & 1 \\ 5 & = & 5 \times 1 & + & 0 \end{array} \quad \text{and} \quad \begin{array}{rrr} 473 & 1 & 0 \\ 467 & 0 & 1 \\ 6 & 1 & -1 \\ 5 & -77 & 78 \\ 1 & 78 & -79 \end{array} .$$

Thus, $\gcd(473, 467) = 1 = 78 \times 473 + (-79) \times 467$. That is, $x = 78$ and $y = -79$.
(b) 467 is invertible in $\mathbb{Z}_{473}$ because 473 and 467 are relatively prime (note that $\gcd(473, 467) = 1$ as in (a)), and the inverse (reciprocal) of 467 in $\mathbb{Z}_{473}$ is $-79 \bmod 473 = 394$.
(c) $x = 467^{-1} \otimes (2 \ominus 252) = 394 \otimes 223 = 87862 \bmod 473 = 357$.