QUIZ #2 – MATH 311W

SEPTEMBER 24TH, 2012

1. Compute the inverses of the following equivalence classes or say that the inverse does not exist. Show your work and write clearly. (3 points)

(a) $[2]_7$
(b) $[6]_{10}$
(c) $[1]_2$

Solution: I just eye-balled these.
(a) $([2]_7)^{-1} = [4]_7$ since $2 \cdot 4 = 8 \equiv_7 = 1$.
(b) $([6]_10)^{-1}$ does not exist, this is because $\gcd(6, 10) = 2 \neq 1$.
(c) $([1]_2)^{-1} = [1]_2$ since $1 \cdot 1 = 1$.

3. Give an example of equation $ax \equiv_n b$ which has no solution. I want explicit values of a, b and n. (1 point)

Solution: There are many solutions, but consider $n = 2$, $a = 2$, $b = 1$. Then $2 \cdot x \equiv_2 1$ has no solutions since $\gcd(2, 2) = 2$ does not divide $b = 1$. Alternately, $2 \cdot x$ is always even, so is equivalent to 0 modulo 2, but 1 is not.

2. Suppose that $x \equiv_m 0$ and $y \equiv_m 0$. Prove that $m | \gcd(x, y)$. (2 points)

Solution: Since $x \equiv_m 0$ we know that $m|(x-0)$ and so $m|x$. Likewise $m|y$. But then $m| \gcd(x, y)$ since $\gcd(x, y)$ is a multiple of every divisor dividing x and y also divides $\gcd(x, y)$ (see the original definition of gcd in the text).