Math 42-Number Theory
Problem Set #2
Due Tuesday, February 15, 2011

For problems 4, 5 and 6, either prove the statement is true or give an example showing that it is false (a counterexample).

4. If a and b are elements of U_m, then $a+b$ is in U_m.

Solution: This statement is false. For example, 1 and 3 are in U_8, but $1+3=4$ is not in U_8.

5. If a and b are elements of U_m, then $a \cdot b$ is in U_m.

Solution: This statement is true. If a and b are elements of U_m, then they have multiplicative inverses mod m. Call these inverses a' and b' respectively. Then, we know that $a \cdot a' \equiv 1 \mod m$ and $b \cdot b' \equiv 1 \mod m$. Now, ab is an element of U_m because it has a multiplicative inverse mod m, namely $b'a'$. Mod m, we have

$$abb'a' = a \cdot 1 \cdot a' = aa' = 1 \mod m.$$

6. If a is in U_m, then $-a$ is in U_m.

Solution: This statement is also true. If a is an element of U_m, as above, a has a multiplicative inverse mod m. Call it a' so that $aa' \equiv 1 \mod m$. Then $-a$ is also an element of U_m since $-a$ has a multiplicative inverse mod m, namely $-a'$ as $(-a)(-a') = aa' \equiv 1 \mod m$.

9. How many solutions are there to the linear congruence $ax \equiv b \mod m$? Explain why your answer is correct.

Solution: If $(a,m) \nmid b$, then there are no solutions. If $(a,m) \mid b$, then there are (a,m) solutions. We can see that this is the case by realizing that the congruence $ax \equiv b \mod m$ is equivalent to the equation $ax = b + my$, where x and y are integers (by the definition of congruence). In other words, solving $ax \equiv b \mod m$ is the same as solving the linear diophantine equation $ax - my = b$. We know that this linear diophantine equation has no solutions if $(a,m) \nmid b$. If, on the other hand, $(a,m) \mid b$, we know there are solutions. If x_0 and y_0 are integers such that $ax_0 - my_0 = b$, then all integer solutions to $ax - my = b$ are given by $x = x_0 - mk/d$, $y = y_0 + ak/d$, where $d = (a,m)$. Then, there are d choices of k that make the x values incongruent mod m, namely $k = 0,\ 1,\ 2, \ldots, d-1$. In other words, the d incongruent solutions are $x = x_0,\ x_0 - m/d,\ x_0 - 2m/d, \ldots, x_0 - (d-1)m/d$.