DEFINITION OF MODULAR EQUIVALENCE AND DIRECT PROOFS

FEBRUARY 13, 2018

Let a, b, c, d and m be integers and assume that $m > 0$. We say that $a \equiv b \ (mod\ m)$ if m divides $a - b$. We say 'a is equivalent to b mod m' if this is true. The integer m is called the modulus. Operations which are performed "mod m" are called modular arithmetic.

WARNING: Don't use the operation of division when using modular arithmetic unless you know that the result is an integer. It doesn't make sense to say $\frac{a}{b} \equiv c \ (mod\ m)$ unless a/b is an integer. It just isn't defined and it is best to not use fractions to avoid confusion. Instead if a/b is an integer, then write $a = kb$ and use k in place of a/b.

All of the following statements are true except for one. Give a proof for all the ones that are true and give a counterexample for the one that is false.

(1) for all integers a, $a \equiv a \ (mod\ m)$

(2) if $a \equiv b \ (mod\ m)$, then $b \equiv a \ (mod\ m)$

(3) if $a \equiv b \ (mod\ m)$ and $b \equiv c \ (mod\ m)$, then $a \equiv c \ (mod\ m)$

(4) if a is even, then $a \equiv 0 \ (mod\ 2)$. If a is odd, then $a \equiv 1 \ (mod\ 2)$.

(5) if $ab \equiv ac \ (mod\ m)$ and $a \neq 0$, then $b \equiv c \ (mod\ m)$

(6) if $b \equiv c \ (mod\ m)$, then $ab \equiv ac \ (mod\ m)$

(7) if $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $a + c \equiv b + d \ (mod\ m)$

(8) if $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $ac \equiv bd \ (mod\ m)$

(9) if $ab \equiv ac \ (mod\ am)$ and $a > 0$, then $b \equiv c \ (mod\ m)$

(10) if $ab \equiv c \ (mod\ m)$ and there are integers r and s, such that $ra+sm = 1$, then $b = rc \ (mod\ m)$.

(11) if $a \equiv b \ (mod\ m)$ and k divides a and k divides m, then k divides b.

Now apply the results above to find all the values of x that solve following modular equations.

$$5x \equiv 1 \ (mod\ 24) \quad 7x \equiv 1 \ (mod\ 39) \quad 7x \equiv 29 \ (mod\ 101) \quad 33x \equiv 13 \ (mod\ 121)$$