DEFINITION OF MODULAR EQUIVALENCE AND DIRECT PROOFS

FEBRUARY 13, 2018

Let a, b, c, d and m and n be integers and assume that $m, n > 0$. 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 two. Give a proof for all the ones that are true and give a counterexample for the two that is false.

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

(2) if $gcd(a, m) = 1$, then there is an integer x such that $ax = b \ (mod\ m)$.

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

(4) if $ab \equiv ac \ (mod\ m)$ and $a \not\equiv 0 \ (mod\ m)$, then $b \equiv c \ (mod\ m)$

(5) if $ab \equiv c \ (mod\ m)$ and $ad \equiv 1 \ (mod\ m)$, then $b \equiv cd \ (mod\ m)$.

(6) 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.

$5x \equiv 2 \ (mod\ 7)$ $\quad 5x \equiv 1 \ (mod\ 34)$ $\quad 5x \equiv 1 \ (mod\ 26)$ $\quad 5x \equiv 6 \ (mod\ 786)$

$7x \equiv 19 \ (mod\ 84)$ $\quad 7x \equiv 21 \ (mod\ 84)$ $\quad 139x \equiv 11 \ (mod\ 1027)$ $\quad 1197x \equiv 4 \ (mod\ 1199)$