Solutions to Attendance Quiz # 10 for Dr. Z.'s Number Theory Course for Oct. 7, 2013

1. Without actually solving, find out how many solutions there are in $\{0, 1, \ldots n-1\}$ where n is the modulo.

i. $21x \equiv 12 \pmod{33}$

ii. $5^{10}x \equiv 2^{10} \pmod{13^{30}}$

Sol. to 1.

(i) $d = gcd(21, 33) = gcd(7 \cdot 3, 11 \cdot 3) = 3$. Since 12/3 is an integer, there are solutions, and there are 3 of them.

(ii) $d = gcd(5^{10}, 13^{30}) = 1$ (since they do not have common prime factors). Of course $2^{10}/1$ is an integer, so there are (at least one) solutions, and there is only one solution (since $d = 1$).

2. Find, or explain why it does not exist $4^{-1} \pmod{21}$.

Sol. of 2. since $gcd(21, 4) = 1$ there are solutions. Let's apply the Extended Euclidean algorithm to $gcd(21, 4)$

$21 = 5 \cdot 4 + 1$ so $gcd(21, 4) = gcd(1, 4) = 1$ and $1 = 1 \cdot \mathbf{21} - 5 \cdot \mathbf{4}$.

So

$$(-5) \cdot 4 \equiv 1 \pmod{21} \quad .$$

So $4^{-1} \equiv -5 \pmod{21} \equiv 16 \pmod{21}$, (since $-5 + 21 = 16$).

Ans. to 2.: $4^{-1} \equiv 16 \pmod{21}$.

Check: $4 \cdot 16 = 64 = 21 \cdot 3 + 1$, so indeed $4 \cdot 16 \equiv 1 \pmod{21}$.