M5420 F15 TEST 1 SOL

9:56

1. $(276, 120)$

$276 = 2\cdot 120 + 36$

$120 = 3\cdot 36 + 12$

$36 = 3\cdot 12$ so $(276,120) = 12 = 7\cdot 120 - 3\cdot 276$

$12 = 120 - 3\cdot 36 = 120 - 3(276 - 2\cdot 120)$

$= 7\cdot 120 - 3\cdot 276$

9:57

2. $9x \equiv 3 \ (15)$ implies $3x \equiv 1 \ (5)$ so (mult. by 2), $6x \equiv 2 \ (5)$ OR $\boxed{x \equiv 2 \ (5).}$

check: $x = 5n+2 \Rightarrow 9x = 45n + 18 \equiv 3 \ (15)$.

9:59

3. $x \equiv 9 \ (10)$ and $x \equiv 10 \ (11)$

$x = 9 + 10n$

$9 + 10n \equiv 10 \ (11)$

$10n \equiv 1 \ (11)$

$-n \equiv 1 \ (11)$

$n \equiv 10 \ (11)$

$\Rightarrow x = 9 + 10(10 + 11k)$

$= 109 + 110k$

$\boxed{x \equiv -1 \ (110)}$

10:01

4. $4 \mid 2\cdot 2$ but $4 \nmid 2$

$6 \mid 2\cdot 3$ but $6 \nmid 2$ and $6 \nmid 3$

If you used $c|ab$ with c a prime, you got 0 points instantly.

10:01

5. (a) $\mathbb{Z}_{40} \xrightarrow{f} \mathbb{Z}_{40}$ is 1-1 because adding 3 is 1-1 and mult. by 7 is 1-1 (mod 40) [since $(7,40) = 1$]

(b) $|\mathbb{Z}_{40}| = 40$ is finite so f is onto since it is 1-1.

10:02

(6) $f([2x]) = [3x]$ is well-defined because every element of $\mathbb{Z}_7$ is $2[x]$ for a unique $[x] \in \mathbb{Z}_7$. $[(2,7)=1]$
on $\mathbb{Z}_7$

In $\mathbb{Z}_8$ it fails because
1. Not every element can be written as $[2x]$, only $[0], [2], [4]$ and $[6]$ can, (Not def for all of $\mathbb{Z}_8$)

and 2. There are two ways to write the elements which are "even" & they don't give the same result:

$$2[0]_8 = [0]_8 \quad \text{and} \quad 3[0]_8 = [0]_8$$
$$2[4]_8 = [0]_8 \quad \quad 3[4]_8 = [4]_8$$

10:07

(7) If $k, j \in I$ then $ka \equiv 0\ (n)$ and $ja \equiv 0\ (n)$ so $(k+j)a \equiv ka + ja \equiv 0\ (n)$. Hence $k+j \in I$.
Similarly if $k, j \in I$ then $(k-j)a \equiv 0\ (n)$ so $k-j \in I$.

10:08

(8) (b) $\phi(30) = 30\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 8$ so

(a) $k = 8$ has $[a]^k = (1)$ for every $[a] \in \mathbb{Z}_{30}^{\times}$

(c) $\mathbb{Z}_{30}^{\times} = \{1, 7, 11, 13, 17=-13, 19=-11, 23=-7, 29=-1\}$

$7^2 = 19$ $\quad 11^2 = 1$ $\quad (-13)^2 = 169 = 19$ $\quad (29)^2 = (-1)^2 = 1$

$7^3 = -77 = -17 = 13$ $\quad (-13)^3 = (-13)(-11) = 143 = -7 = 23$

$7^4 = 91 = 1$ $\quad (-13)^4 = (-13)(-7) = 91 = 1$

No element $[a]$ generates more than 4 elements of $\mathbb{Z}_{30}^{\times}$ by taking powers, so $\boxed{\text{No}}$

(d) $[a] \in \mathbb{Z}_{30}^{\times} \Rightarrow$ mult. by a is invertible mod 30, hence it is one-to-one and onto.

10:12

9 $(99,40)=1$ so ~~$d99x \equiv 0$~~ $1 = 99a + 40b$ for some integers a and b. Then

$$x = 1\cdot x = (99a+40b)x$$
$$\equiv \quad = a(99x) + b(40x)$$
$$\equiv 0 + 0 = 0 \qquad (n).$$