Name: Solutions

Directions: Show all work. No credit for answers without work.

1. [**5 points**] Solve the following system of congruences; your solution should identify the set of all possible solutions.

$$x \equiv 23 \pmod{31} \qquad 2x \equiv 43 \pmod{53} \qquad x \equiv 6 \pmod{25}$$

prime prime 5^2

$(27)(2)x \equiv (27)(43)$

$x \equiv 23 \pmod{31}$ $\quad x \equiv 48 \pmod{53}$ $\quad x \equiv 6 \pmod{25}$

Moduli are pairwise relatively prime $\Rightarrow$ CRT applies directly. Let $M = 31 \cdot 53 \cdot 25 = 41{,}075$

i	m_i	M/m_i	$M/m_i \pmod{m_i}$	$(M/m_i)^{-1} \pmod{m_i}$	target
1	31	1325	23	−4	23
2	53	775	33	−8	48
3	25	1643	18	7	6

$(23)^{-1}$ in $\mathbb{Z}_{31}$: -4

$31 = (1)(23) + 8$
$23 = (2)(8) + 7$
$8 = (1)(7) + 1$

$1 = 8 - (1)(7)$
$= 8 - (1)[23 - (2)(8)]$
$= (3)(8) - (1)(23)$
$= 3[31 - (1)(23)] - (1)(23)$
$= (3)(31) - (4)(23)$

$(33)^{-1}$ in $\mathbb{Z}_{53}$: -8

$53 = (1)(33) + 20$
$33 = (1)(20) + 13$
$20 = (1)(13) + 7$
$13 = (1)(7) + 6$
$7 = (1)(6) + 1$

$1 = 7 - (1)(6)$
$= (-1)(13) + (2)(7)$
$= (-3)(13) + (2)(20)$
$= (-3)(33) + (5)(20)$
$= (5)(53) - (8)(33)$

$(18)^{-1}$ in $\mathbb{Z}_{25}$: 7

$25 = (1)(18) + 7$
$18 = (2)(7) + 4$
$7 = (1)(4) + 3$
$4 = (1)(3) + 1$

$1 = 4 - (1)(3)$
$= (-1)(7) + (2)(4)$
$= (2)(18) - (5)(7)$
$= (-5)(25) + (7)(18)$

So $x = (1325)(-4)(23) + (775)(-8)(48) + (1643)(7)(6)$
$= (-121{,}900) + (-297{,}600) + 69{,}006$
$= -350{,}494$
$\equiv \boxed{19181 \bmod 41075}$

2. [**4 points**] Convert the following system of coungruences to an equivalent system of congruences with prime power moduli. (Do not solve.)

$$x \equiv 58 \pmod{98} \qquad x \equiv 16 \pmod{21} \qquad x \equiv 16 \pmod{36}$$

$98 = 2 \cdot 49 = 2 \cdot 7^2$

$x \equiv 58 \pmod 2$
$x \equiv 0 \pmod 2$

$x \equiv 58 \pmod{49}$
$x \equiv 9 \pmod{49}$

$21 = 3 \cdot 7$

$x \equiv 16 \pmod 3$
$x \equiv 1 \pmod 3$
$x \equiv 16 \pmod 7$
$x \equiv 2 \pmod 7$

$36 = 2^2 \cdot 3^2$

$x \equiv 16 \pmod 4$
$x \equiv 0 \pmod 4$
$x \equiv 16 \pmod 9$
$x \equiv 7 \pmod 9$

$p = 2$

~~$x \equiv 0 \pmod 2$~~

implies $x \equiv 0 \pmod 4$

$p = 3$

~~$x \equiv 1 \pmod 3$~~

$x \equiv 7 \pmod 9$

$p = 7$

$x \equiv 9 \bmod 49$

~~$x \equiv 2 \pmod 7$~~

So our equivalent system is

$x \equiv 0 \pmod 4$
$x \equiv 7 \pmod 9$
$x \equiv 9 \pmod{49}$

3. [**1 point**] Without using CRT, show that if $x = 9r + 5$ and $x = 7s + 3$ for $r, s \in \mathbb{Z}$, then $x = 63n + 59$ for some $n \in \mathbb{Z}$.

We have $x = 9r + 5$ and $x = 7s + 3$. Multiplying by 7 and 9 respectively gives

$$7x = 63r + 35 \qquad (Eq\ 1)$$
$$9x = 63s + 27. \qquad (Eq\ 2)$$

Next we use that $\gcd(7, 9) = 1$, so that $7u + 9v = 1$ for some $u, v \in \mathbb{Z}$. We find u, v with EEA:

$$9 = (1)(7) + 2 \qquad 1 = 7 - (3)(2)$$
$$7 = (3)(2) + 1 \qquad = 7 - (3)[9 - (1)(7)]$$
$$= (-3)(9) + (4)(7).$$

Mult. (Eq 1) by 4 and (Eq 2) by -3 and add to get:

$$(4 \cdot 7)x = 63 \cdot (4r) + 140$$
$$(-3 \cdot 9)x = 63 \cdot (-3s) - 81$$
$$x = 63(4r - 3s) + 59.$$

So $x = 63n + 59$ where n is the integer $4r - 3s$. $\boxtimes$