2513: Solutions to 3/24 homework

2a

$\gcd(11,9)$:

①	$11 = 9\cdot 1 + 2$	$(9,2)$	
②	$9 = 2\cdot 4 + 1$	$(2,1)$	
③	$2 = 1\cdot 2 + 0$	$(1,0)$	$\gcd = 1$.

② $\Rightarrow$ $1 = (1)\cdot 9 + (-4)\cdot 2$

① $\Rightarrow$ $2 = (1)\cdot 11 + (-1)\cdot 9$

$1 = (1)\cdot 9 + (-4)\big((1)\cdot 11 + (-1)\cdot 9\big)$

$\underline{1 = (5)\cdot 9 + (-4)\cdot 11}$

2b

$\gcd(44,33)$

①	$44 = 33\cdot 1 + 11$	$(33,11)$	
②	$33 = 11\cdot 3 + 0$	$(11,0)$	$\gcd = 11$

① $\Rightarrow$ $\underline{11 = (1)\cdot 44 + (-1)\cdot 33}$

2c

$\gcd(78,35)$

①	$78 = 35\cdot 2 + 8$	$(35,8)$	
②	$35 = 8\cdot 4 + 3$	$(8,3)$	
③	$8 = 3\cdot 2 + 2$	$(3,2)$	
④	$3 = 2\cdot 1 + 1$	$(2,1)$	
⑤	$2 = 1\cdot 2 + 0$	$(1,0)$	$\gcd = 1$

④ $\Rightarrow$ $1 = (1)\cdot 3 + (-1)\cdot 2$

③ $\Rightarrow$ $2 = (1)\cdot 8 + (-2)\cdot 3$

$1 = (1)\cdot 3 + (-1)\big((1)\cdot 8 + (-2)\cdot 3\big)$

$1 = (-1)\cdot 8 + (3)\cdot 3$

② $\Rightarrow$ $3 = (1)\cdot 35 + (-4)\cdot 8$

$1 = (-1)\cdot 8 + (3)\left((1)\cdot 35 + (-4)\cdot 8 \right)$

$1 = (3)\cdot 35 + (-13)\cdot 8$

① $\Rightarrow$ $8 = (1)\cdot 78 + (-2)\cdot 35$

$1 = (3)\cdot 35 + (-13)\left((1)\cdot 78 + (-2)\cdot 35 \right)$

$\underline{1 = (-13)78 + (29)35}$

$\boxed{2d}$ gcd(55, 21)

①	$55 = 21\cdot 2 + 13$	$(21, 13)$
②	$21 = 13\cdot 1 + 8$	$(13, 8)$
③	$13 = 8\cdot 1 + 5$	$(8, 5)$
④	$8 = 5\cdot 1 + 3$	$(5, 3)$
⑤	$5 = 3\cdot 1 + 2$	$(3, 2)$
⑥	$3 = 2\cdot 1 + 1$	$(2, 1)$
⑦	$2 = 1\cdot 2 + 0$	$(1, 0)$ gcd = 1

$1 = (1)\cdot 3 + (-1)\cdot 2$ by ⑥

$2 = (1)\cdot 5 + (-1)\cdot 3$ by ⑤

$1 = (1)3 + (-1)\left((1)5 + (-1)3 \right)$

$1 = (-1)5 + (2)3$

$3 = (1)\cdot 8 + (-1)\cdot 5$ by ④

$1 = (-1)5 + (2)\left((1)\cdot 8 + (-1)\cdot 5 \right)$

$1 = (2)8 + (-3)5$

$5 = (1)\cdot 13 + (-1)\cdot 8$ by ③

$1 = (2)\cdot 8 + (-3)\big((1)\cdot 13 + (-1)\cdot 8\big)$

$1 = (-3)\cdot \underline{13} + (5)\cdot \underline{8}$

$8 = (1)\cdot 21 + (-1)\cdot 13$ by ②

$1 = (-3)\cdot 13 + (5)\big((1)\cdot 21 + (-1)\cdot 13\big)$

$1 = (5)\cdot \underline{21} + (-8)\cdot \underline{13}$

$13 = (1)\cdot 55 + (-2)\cdot 21$ by ①

$1 = (5)\cdot 21 + (-8)\big((1)\cdot 55 + (-2)\cdot 21\big)$

$\underline{1 = (-8)\cdot 55 + (21)\cdot 21}$

$\boxed{2e}$ gcd(203, 101)

$203 = 101 \cdot 2 + 1$ (101, 1)

gcd = 1.

$\underline{1 = (1)\cdot 203 + (-2)\cdot 101}$

$\boxed{2f}$ gcd(323, 124)

①	323	$=$	$124\cdot 2$	$+75$	(124, 75)
②	124	$=$	$75\cdot 1$	$+49$	(75, 49)
③	75	$=$	$49\cdot 1$	$+26$	(49, 26)
④	49	$=$	$26\cdot 1$	$+23$	(26, 23)
⑤	26	$=$	$23\cdot 1$	$+3$	(23, 3)
⑥	23	$=$	$3\cdot 7$	$+2$	(3, 2)
⑦	3	$=$	$2\cdot 1$	$+1$	(2, 1)

gcd = 1

$$1 = (1)\underline{3} + (-1)\cdot\underline{2} \quad \text{by } ⑦$$

$$2 = (1)\cdot 23 + (-7)\cdot 3 \quad \text{by } ⑥$$

$$1 = (1)\cdot 3 + (-1)\big((1)\cdot 23 + (-7)\cdot 3\big)$$

$$1 = (-1)\cdot\underline{23} + (8)\cdot\underline{3}$$

$$3 = (1)\cdot 26 + (-1)\cdot 23 \quad \text{by } ⑤$$

$$1 = (-1)23 + (8)\big((1)26 + (-1)\cdot 23\big)$$

$$1 = (8)\cdot\underline{26} + (-9)\cdot\underline{23}$$

$$23 = (1)\cdot 49 + (-1)\cdot 26 \quad \text{by } ④$$

$$1 = (8)26 + (-9)\big((1)49 + (-1)26\big)$$

$$1 = (-9)\underline{49} + (17)\underline{26}$$

$$26 = (1)\cdot 75 + (-1)\cdot 49 \quad \text{by } ③$$

$$1 = (-9)49 + (17)\big((1)75 + (-1)49\big)$$

$$1 = (17)\underline{75} + (-26)\underline{49}$$

$$49 = (1)\cdot 124 + (-1)\cdot 75 \quad \text{by } ②$$

$$1 = (17)75 + (-26)\big((1)\cdot 124 + (-1)75\big)$$

$$1 = (-26)\underline{124} + (43)\underline{75}$$

$$75 = (1)323 + (-2)124 \quad \text{by } ①$$

$$1 = (-26)124 + (43)\big((1)323 + (-2)124\big)$$

$$\underline{1 = (43)323 + (-112)124}$$

$\boxed{2g}$ $\gcd(2339, 2002)$

①	$2339 = 2002 \cdot 1 + 337$		$(2002, 337)$
②	$2002 = 337 \cdot 5 + 317$		$(337, 317)$
③	$337 = 317 \cdot 1 + 20$		$(317, 20)$
④	$317 = 20 \cdot 15 + 17$		$(20, 17)$
⑤	$20 = 17 \cdot 1 + 3$		$(17, 3)$
⑥	$17 = 3 \cdot 5 + 2$		$(3, 2)$
⑦	$3 = 2 \cdot 1 + 1$		$(2, 1)$
			$\gcd = 1$

$1 = (1)\underline{3} + (-1)\underline{2}$ by ⑦

$\downarrow$

$2 = (1)17 + (-5)3$ by ⑥

$1 = (1)3 + (-1)\big((1)17 + (-5)3\big)$

$1 = (-1)\underline{17} + (6)\underline{3}$

$\downarrow$

$3 = (1)\cdot 20 + (-1)\cdot 17$ by ⑤

$1 = (-1)17 + (6)\big((1)\cdot 20 + (-1)17\big)$

$1 = (6)\cdot\underline{20} + (-7)\underline{17}$

$\downarrow$

$17 = (1)\cdot 317 + (-15)\cdot 20$ by ④

$1 = (6)20 + (-7)\big((1)\cdot 317 + (-15)\cdot 20\big)$

$1 = (-7)\underline{317} + (111)\cdot\underline{20}$

$\downarrow$

$20 = (1)\cdot 337 + (-1)\cdot 317$ by ③

$1 = (-7)317 + (111)\big((1)337 + (-1)317\big)$

$1 = (111)\cdot\underline{337} + (-118)\cdot\underline{317}$

$\downarrow$

$317 = (1)\cdot 2002 + (-5)\cdot 337$ by ④

$1 = (111)\cdot 337 + (-118)\big((1)2002 + (-5)337\big)$

$1 = (-118)\underline{2002} + (701)\underline{337}$

$$337 = (1)2339 + (-1)2002 \quad \text{by } ①$$

$$1 = (-118)2002 + (701)\big((1)2339 + (-1)2002\big)$$

$$1 = (701)2339 + (-819)2002$$

$\boxed{2h}$ gcd (4669, 3457)

① $4669 = 3457 \cdot 1 + 1212$
② $3457 = 1212 \cdot 2 + 1033$
③ $1212 = 1033 \cdot 1 + 179$
④ $1033 = 179 \cdot 5 + 138$
⑤ $179 = 138 \cdot 1 + 41$
⑥ $138 = 41 \cdot 3 + 15$
⑦ $41 = 15 \cdot 2 + 11$
⑧ $15 = 11 \cdot 1 + 4$
⑨ $11 = 4 \cdot 2 + 3$
⑩ $4 = 3 \cdot 1 + 1$ gcd $= 1$

$$1 = (1)\underline{4} + (-1)\underline{3} \quad \text{by } ⑩$$

$$3 = (1)11 + (-2)4 \quad \text{by } ⑨$$

$$1 = (1)4 + (-1)\big((1)11 + (-2)4\big)$$

$$1 = (-1)\underline{11} + (3)\underline{4}$$

$$4 = (1)15 + (-1)11 \quad \text{by } ⑧$$

$$1 = (-1)11 + (3)\big((1)15 + (-1)11\big)$$

$$1 = (3)\underline{15} + (-4)\underline{11}$$

$$11 = (1)41 + (-2)15 \quad \text{by } ⑦$$

$$1 = (3)15 + (-4)\big((1)41 + (-2)15\big)$$

$$1 = (-4)\underline{41} + (11)\underline{15}$$

$$15 = (1)138 + (-3)41 \quad \text{by } ⑥$$

$$1 = (-4)41 + (11)\big((1)138 + (-3)41\big)$$
$$1 = (11)\underline{138} + (-37)\underline{41}$$
$$41 = (1)179 + (-1)138 \quad \text{by } 5$$

$$1 = (11)138 + (-37)\big((1)179 + (-1)138\big)$$
$$1 = (-37)\underline{179} + (48)\underline{138}$$
$$138 = (1)1033 + (-5)179 \quad \text{by } 4$$

$$1 = (-37)179 + (48)\big((1)1033 + (-5)179\big)$$
$$1 = (48)\underline{1033} + (-277)\underline{179}$$
$$179 = (1)1212 + (-1)1033 \quad \text{by } 3$$

$$1 = (48)1033 + (-277)\big((1)1212 + (-1)1033\big)$$
$$1 = (-277)\underline{1212} + (325)\underline{1033}$$
$$1033 = (1)3457 + (-2)1212 \quad \text{by } 2$$

$$1 = (-277)1212 + (325)\big((1)3457 + (-2)1212\big)$$
$$1 = (325)\underline{3457} + (-927)\underline{1212}$$
$$1212 = (1)4669 + (-1)3457 \quad \text{by } 1$$

$$1 = (325)3457 + (-927)\big((1)4669 + (-1)3457\big)$$
$$\underline{1 = (-927)4669 + (1252)3457}$$

$\boxed{2i}$ $\gcd(13422, 10001)$

$$
\begin{array}{lrcll}
① & 13422 & = & 10001 \cdot 1 & + 3421 \\
② & 10001 & = & 3421 \cdot 2 & + 3159 \\
③ & 3421 & = & 3159 \cdot 1 & + 262 \\
④ & 3159 & = & 262 \cdot 12 & + 15 \\
⑤ & 262 & = & 15 \cdot 17 & + 7 \\
⑥ & 15 & = & 7 \cdot 2 & + 1 \\
⑦ & 7 & = & 1 \cdot 7 & + 0
\end{array}
$$

$\gcd = 1$

$$1 = (1)\underline{15} + (-2)\cdot\underline{7} \qquad \text{by } ⑥$$

$$7 = (1)262 + (-17)\cdot 15 \qquad \text{by } ⑤$$

$$1 = (1)15 + (-2)\big((1)262 + (-17)\cdot 15\big)$$
$$1 = (-2)\underline{262} + (35)\underline{15}$$

$$15 = (1)\,3159 + (-12)\,262 \qquad \text{by } ④$$

$$1 = (-2)262 + (35)\big((1)3159 + (-12)262\big)$$
$$1 = (35)\underline{3159} + (-422)\underline{262}$$

$$262 = (1)\,3421 + (-1)\,3159 \qquad \text{by } ③$$

$$1 = (35)3159 + (-422)\big((1)3421 + (-1)3159\big)$$
$$1 = (-422)\underline{3421} + (457)\underline{3159}$$

$$3159 = (1)\,10001 + (-2)\,3421 \qquad \text{by } ②$$

$$1 = (-422)\,3421 + (457)\big((1)\,10001 + (-2)\,3421\big)$$

$$1 = (457)\underline{10001} + (-1336)\underline{3421}$$

$$3421 = (1)\,13422 + (-1)\,10001 \qquad \text{by } ①$$

$$1 = (457)10001 + (-1336)\big((1)13422 + (-1)10001\big)$$
$$\underline{1 = (-1336)13422 + (1793)10001}$$

(6) Want x with $2x \equiv 1 \pmod{17}$.

Since $18 \equiv 1 \pmod{17}$, $x = 9$ works.

(12) Since $2 \cdot 9 \equiv 1 \pmod{17}$, multiplying by 7 gives $2 \cdot 9 \cdot 7 \equiv 7 \pmod{17}$

So $x = 9 \cdot 7 = 63$ works.

Writing $63 = 17 \cdot 3 + 12$, we get $63 \equiv 12 \pmod{17}$

So $x = 12$ also works.

(check: $2 \cdot 12 = 24 \equiv 7 \pmod{17}$. ✓)

(18) Chinese Remainder Theorem says (since 3, 4, 5 are pairwise rel. prime) that there is a unique solution modulo 60.

To find it, first find y_1, y_2, y_3 such that

$$20 y_1 \equiv 1 \pmod 3$$
$$15 y_2 \equiv 1 \pmod 4$$
$$12 y_3 \equiv 1 \pmod 5,$$

then $x = 2 \cdot 20 \cdot y_1 + 1 \cdot 15 \cdot y_2 + 3 \cdot 12 \cdot y_3$ is a solution.

Taking $y_1 = 2$, get $20 y_1 = 40 \equiv 1 \pmod 3$ ✓

Taking $y_2 = 3$, get $15 y_2 = 45 \equiv 1 \pmod 4$ ✓

Taking $y_3 = 3$, get $12 y_3 = 36 \equiv 1 \pmod 5$ ✓

(I used trial and error - only 3 possible choices for y_1, etc.)

So $x = 80 + 45 + 108 = 233$.

$233 = 60 \cdot 3 + 53$

So $x = 53$ is the unique solution between 0 and 59. All other solutions are of the form $\boxed{53 + 60n}$, $n \in \mathbb{Z}$.

(26) We are looking for solutions to the linear congruences

$$x \equiv 0 \pmod 5$$
$$x \equiv 1 \pmod 3.$$

Checking multiples of 5, one finds that $x = 10$ works. C.R.T. says that the solutions are exactly the numbers of the form $\boxed{10 + 15n}$, $n \in \mathbb{Z}$.