Number theory 1E

1 a $20 \equiv 2 \pmod 9$, so least residue is 2

b $7 \equiv 1 \pmod 2$, so least residue is 1

c $120 \equiv 0 \pmod{15}$, so least residue is 0

d $91 \equiv 11 \pmod{20}$, so least residue is 11

2 a $30 = 4 \times 7 + 2 \Rightarrow x \equiv 2 \pmod 7$

b $69 = 7 \times 9 + 6 \Rightarrow x \equiv 6 \pmod 9$

c $-60 = -10 \times 6 \Rightarrow x \equiv 0 \pmod 6$

d $-63 = -6 \times 11 + 3 \Rightarrow x \equiv 3 \pmod{11}$

e $-38 = -3 \times 17 + 13 \Rightarrow x \equiv 13 \pmod{17}$

f $x \equiv 3 - 2 \equiv 1 \pmod 9$

g $x \equiv 21 - 5 \equiv 16 \equiv 7 \pmod 9$

h $x \equiv 50 + 3 \equiv 4 \times 11 + 9 \equiv 9 \pmod{11}$

3 Using $ka \equiv kb \pmod m$ and $\gcd(k,m) = d$, then $a \equiv b\left(\bmod \frac{m}{d}\right)$

$27n \equiv 81 \pmod{15} \Rightarrow 27n \equiv 27 \times 3 \pmod{15}$ and $\gcd(27,15) = 3$

So $n \equiv 3\left(\bmod \frac{15}{3}\right) \equiv 3 \pmod 5$

4 a $91 = 4 \times 20 + 11$

$20 = 1 \times 11 + 9$

$11 = 1 \times 9 + 2$

$9 = 4 \times 2 + 1$

$2 = 2 \times 1 + 0$

So $\gcd(91,20) = 1$

b $91n \equiv 455 \pmod{20} \Rightarrow 91n \equiv 91 \times 5 \pmod{20}$

As $\gcd(91,20) = 1$, using the division (cancelling) laws $n \equiv 5 \pmod{20}$

5 a $10x \equiv 20 \pmod 7 \Rightarrow 10x \equiv 10 \times 2 \pmod 7$

As $\gcd(10,7) = 1$, using the division (cancelling) laws $n \equiv 2 \pmod 7$

b $3x \equiv 9 \pmod 8 \Rightarrow 3x \equiv 3 \times 3 \pmod 8$

As $\gcd(3,8) = 1$, using the division (cancelling) laws $n \equiv 3 \pmod 8$

5 c $5x \equiv 15 \pmod 3 \Rightarrow 5x \equiv 5 \times 3 \pmod 3$

As $\gcd(5,3) = 1$, using the division (cancelling) laws $x \equiv 3 \equiv 0 \pmod 3$

d $3x \equiv 12 \pmod 9 \Rightarrow 3x \equiv 3 \times 4 \pmod 9$

As $\gcd(3,9) = 3$, using the division (cancelling) laws $x \equiv 4\left(\text{mod } \frac{9}{3}\right)$,

i.e. $x \equiv 4 \pmod 3 \Rightarrow x \equiv 1 \pmod 3$

The solution can also be written as $x \equiv 1, 4 \text{ or } 7 \pmod 9$

e $6x \equiv 18 \pmod{15} \Rightarrow 6x \equiv 6 \times 3 \pmod{15}$

As $\gcd(6,15) = 3$, using the division (cancelling) laws $x \equiv 3\left(\text{mod } \frac{15}{3}\right)$, i.e. $x \equiv 3 \pmod 5$

The solution can also be written as $x \equiv 3, 8 \text{ or } 13 \pmod{15}$

f $20x \equiv 200 \pmod{30} \Rightarrow 20x \equiv 20 \times 10 \pmod{30}$

As $\gcd(20,30) = 10$, using the division (cancelling) laws $x \equiv 10\left(\text{mod } \frac{30}{10}\right)$,

i.e. $x \equiv 10 \pmod 3 \Rightarrow x \equiv 1 \pmod 3$

The solution can also be written as $x \equiv 1, 4, 7, 10, 13, 16, 19, 22, 25 \text{ or } 28 \pmod{30}$

6 a $\{0,1,2,3,4,5,6,7,8,9,10,11\}$

b $4x \equiv 8 \pmod{12} \Rightarrow 4x \equiv 4 \times 2 \pmod{12}$

As $\gcd(4,12) = 4$, using the division (cancelling) laws $x \equiv 2\left(\text{mod } \frac{12}{4}\right)$, i.e. $x \equiv 2 \pmod 3$

The solutions of $x \equiv 2 \pmod 3$ in the set given in part **a** are $x = 2, 5, 8, 11$

7 a $733 = 6 \times 120 + 13$

$120 = 9 \times 13 + 3$

$13 = 4 \times 3 + 1$

$3 = 3 \times 1 + 0$

So $\gcd(733,120) = 1$

Working backwards through the steps of the Euclidean algorithm gives:

$1 = 13 - 4(3)$

$= 13 - 4(120 - 9(13))$

$= 37(13) - 4(120)$

$= 37(733 - 6(120)) - 4(120)$

$= 37(733) - 226(120)$

So $a = -226$, $b = 37$

b From part **a**, $-226 \times 120 = -37 \times 733 + 1 \Rightarrow -226 \times 120 \equiv 1 \pmod{733}$

So $120x \equiv 1 \pmod{733} \Rightarrow 120x \equiv 120 \times (-226) \pmod{733}$

As $\gcd(120,733) = 1$, using the division (cancelling) laws $x \equiv -226 \pmod{733}$

$\Rightarrow x \equiv 733 - 226 \equiv 507 \pmod{733}$

8 **a** $571 = 11 \times 50 + 21$
$50 = 2 \times 21 + 8$
$21 = 2 \times 8 + 5$
$8 = 1 \times 5 + 3$
$5 = 1 \times 3 + 2$
$3 = 1 \times 2 + 1$
$2 = 2 \times 1 + 0$
So $\gcd(571, 50) = 1$

Working backwards through the steps of the Euclidean algorithm gives:
$1 = 3 - 2$
$= 2(3) - 5$
$= 2(8) - 3(5)$
$= 2(8) - 3(21 - 2(8))$
$= 8(50 - 2(21)) - 3(21)$
$= 8(50) - 19(571 - 11(50)$
$= -19(571) + 217(50)$
So $a = -19$, $b = 217$

b From part **a**, $217 \times 50 = 19 \times 571 + 1 \Rightarrow 217 \times 50 \equiv 1 \pmod{571}$
So a multiplicative inverse of 50 modulo 571 is 217.

c $50x \equiv 3 \pmod{571} \Rightarrow 217 \times 50x \equiv 217 \times 3 \equiv 651 \pmod{571}$
As $217 \times 50 \equiv 1 \pmod{571}$, therefore $x \equiv 651 \pmod{571}$
$\Rightarrow x \equiv 651 - 571 \pmod{571} \Rightarrow x \equiv 80 \pmod{571}$

9 **a** $10 = 1 \times 7 + 3$
$7 = 2 \times 3 + 1$
So $\gcd(7, 10) = 1$

Working backwards:
$1 = 7 - 2(3)$
$= 7 - 2(10 - 7)$
$= 3(7) - 2(10)$
$\Rightarrow 3(7) = 2(10) + 1$
Hence $3 \times 7 \equiv 1 \pmod{10}$, so 3 is a multiplicative inverse of 7 modulo 10

b $4 = 1 \times 3 + 1$
So $\gcd(3, 4) = 1$
$1 = 4 - 1(3)$
$\Rightarrow -1(3) = -1(4) + 1$
Hence $-1 \times 3 \equiv 1 \pmod{4}$, so -1 is a multiplicative inverse of 3 modulo 4
So $x = 4 - 1$, i.e. $x = 3$ is also a solution $[3 \times 3 \equiv 9 \equiv 1 \pmod{4}]$

9 c $37 = 3\times 12 + 1$

So $\gcd(12,37) = 1$

$1 = 37 - 3(12)$

$\Rightarrow -3(12) = -1(37) + 1$

Hence $-3\times 12 \equiv 1 \pmod{10}$, so -3 is a multiplicative inverse of 12 modulo 37

So $x = 37 - 3$, i.e. $x = 34$ is also a solution

d $99 = 1\times 70 + 29$

$70 = 2\times 29 + 12$

$29 = 2\times 12 + 5$

$12 = 2\times 5 + 2$

$5 = 2\times 2 + 1$

So $\gcd(70,99) = 1$

Working backwards:

$1 = 5 - 2(2)$

$= 5 - 2(12 - 2(5))$

$= 5(29 - 2(12)) - 2(12)$

$= 5(29) - 12(70 - 2(29))$

$= 29(99 - 70) - 12(70)$

$= 29(99) - 41(70)$

$\Rightarrow -41(70) = -29(99) + 1$

Hence $-41\times 70 \equiv 1 \pmod{99}$, so -41 is a multiplicative inverse of 70 modulo 99

So $x = 99 - 41$, i.e. $x = 58$ is also a solution

10 a $7 = 1\times 5 + 2$

$5 = 2\times 2 + 1$

So $\gcd(5,7) = 1$, there is a unique solution

Working backwards:

$1 = 5 - 2(2)$

$= 5 - 2(7 - 5)$

$= 3(5) - 2(7)$

$\Rightarrow 3(5) \equiv 2(7) + 1$

Hence $3\times 5 \equiv 1 \pmod 7$

$5x \equiv 2 \pmod 7$, so $3\times 5x \equiv 6 \pmod 7$, so $x \equiv 6 \pmod 7$

10 b $49 = 9 \times 5 + 4$
$5 = 1 \times 4 + 1$
So $\gcd(5,49) = 1$, there is a unique solution

Working backwards:
$1 = 5 - 4$
$= 5 - (49 - 9(5))$
$= 10(5) - 49$
$\Rightarrow 10(5) \equiv 49 + 1$
Hence $10 \times 5 \equiv 1 \pmod{49}$
$5x \equiv 9 \pmod{49}$, so $10 \times 5x \equiv 90 \pmod{49}$
This gives $x \equiv 90 \pmod{49} \Rightarrow x \equiv 41 \pmod{49}$

c $\gcd(3, 78) = 3$, but 3 does not divide 2, so $3x \equiv 2 \pmod{78}$ has no solutions

d $13 = 1 \times 8 + 5$
$8 = 1 \times 5 + 3$
$5 = 1 \times 3 + 2$
$3 = 1 \times 2 + 1$
So $\gcd(8,13) = 1$, there is a unique solution

Working backwards:
$1 = 3 - (5 - 3)$
$= 2(8 - 5) - 5$
$= 2(8) - 3(13 - 8)$
$= 5(8) - 3(13)$
$\Rightarrow 5(8) \equiv 3(13) + 1$
Hence $5 \times 8 \equiv 1 \pmod{13}$
$8x \equiv 7 \pmod{13}$, so $5 \times 8x \equiv 35 \pmod{13}$
This gives $x \equiv 35 \pmod{13} \Rightarrow x \equiv 9 \pmod{13}$

e $91 = 6 \times 15 + 1$
So $\gcd(15,91) = 1$, there is a unique solution
$-6 \times 15 \equiv -91 + 1$, hence $-6 \times 15 \equiv 1 \pmod{91}$
$15x \equiv 7 \pmod{91}$, so $-6 \times 15x \equiv -42 \pmod{91}$
This gives $x \equiv -42 \pmod{91} \Rightarrow x \equiv 49 \pmod{91}$

10 f $27 = 2 \times 10 + 7$

$10 = 1 \times 7 + 3$

$7 = 2 \times 3 + 1$

So $\gcd(10, 27) = 1$, there is a unique solution

Working backwards:

$1 = 7 - 2(3)$

$= 7 - 2(10 - 7)$

$= 3(27 - 2(10)) - 2(10)$

$= 3(27) - 8(10)$

$\Rightarrow -8(10) \equiv -3(27) + 1$

Hence $-8 \times 10 \equiv 1 \pmod{27}$

$10x \equiv 9 \pmod{27}$, so $-8 \times 10x \equiv -72 \pmod{27}$

This gives $x \equiv -72 \pmod{27} \Rightarrow x \equiv 9 \pmod{27}$

11 a $\gcd(9, 21) = 3$, so simplify equation by dividing everything by 3, which gives:

$3x \equiv 5 \pmod 7$

Applying the Euclidean algorithm:

$7 = 2 \times 3 + 1$, so $-2 \times 3 \equiv 1 \pmod 7$

$3x \equiv 5 \pmod 7$, so $-2 \times 3x \equiv -10 \pmod 7$

This gives $x \equiv -10 \pmod 7 \Rightarrow x \equiv 4 \pmod 7$

b $\gcd(14, 21) = 7$, so $14x \equiv 13 \pmod{21}$ has no solutions.

c $\gcd(9, 15) = 3$, so simplify equation by dividing everything by 3, which gives:

$3x \equiv 4 \pmod 5$

Applying the Euclidean algorithm:

$5 = 1 \times 3 + 2$

$3 = 1 \times 2 + 1$

This gives:

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

So $2 \times 3 = 5 + 1$, thus $2 \times 3 \equiv 1 \pmod 5$

$3x \equiv 4 \pmod 5$, so $2 \times 3x \equiv 8 \pmod 5$

This gives $x \equiv 8 \pmod 5 \Rightarrow x \equiv 3 \pmod 5$

11 d $\gcd(490,750)=10$, so simplify equation by dividing everything by 10, which gives:
$49x \equiv 75 \pmod{80}$
Applying the Euclidean algorithm:
$80 = 1\times 49 + 31$
$49 = 1\times 31 + 18$
$31 = 1\times 18 + 13$
$18 = 1\times 13 + 5$
$13 = 2\times 5 + 3$
$5 = 1\times 3 + 2$
$3 = 2\times 1 + 1$
Working backwards this gives:
$1 = 3 - 2 = 2(3) - 5 = 2(13) - 5(5)$
$= 7(13) - 5(18) = 7(31) - 12(18)$
$= 19(31) - 12(49)$
$= 19(80) - 31(49)$
$\Rightarrow -31(49) \equiv -19(80) + 1$
Hence $-31\times 49 \equiv 1 \pmod{80}$
$49x \equiv 75 \pmod{80}$, so $-31\times 49x \equiv -2325 \pmod{80}$
This gives $x \equiv -2325 \pmod{80} \Rightarrow x \equiv 75 \pmod{80}$

e $\gcd(12,18)=6$ does not divide 9, so $12x \equiv 9 \pmod{18}$ has no solutions.

f $\gcd(15,25)=5$ does not divide 9, so $15x \equiv 9 \pmod{25}$ has no solutions.

12 Suppose $\gcd(a,m)=d$, then $a = pd$, $m = qd$ for some integers p and q.
If $ax \equiv b \pmod{m}$, then $ax = km + b$ for some integer k, and hence
$pdx = kqd + b \Rightarrow b = d(px - qd)$
So if there is a solution x to $ax \equiv b \pmod{m}$, then $d \mid b$
Since b is not divisible by d, then there can be no solutions to the equation

13 a Applying the Euclidean algorithm:
$702 = 8\times 80 + 62$
$80 = 1\times 62 + 18$
$62 = 3\times 18 + 8$
$18 = 2\times 8 + 2$
$8 = 4\times 2 + 0$
So $\gcd(702,80) = 2$.

b As $\gcd(702,80)=2$, the number of distinct solutions of $80x \equiv 20 \pmod{702}$ is 2.

13 c $\gcd(80,702)=2$, so simplify equation by dividing everything by 2, which gives:
$40x \equiv 10 \pmod{351}$
Applying the Euclidean algorithm:
$351 = 8 \times 40 + 31$
$40 = 1 \times 31 + 9$
$31 = 3 \times 9 + 4$
$9 = 2 \times 4 + 1$
Working backwards this gives:
$1 = 9 - 2(4) = 9 - 2(31 - 3(9))$
$= 7(9) - 2(31) = 7(40 - 31) - 2(31)$
$= 7(40) - 9(31) = 7(40) - 9(351 - 8(40))$
$= 79(40) - 9(351)$
$\Rightarrow 79(40) \equiv 9(351) + 1$
Hence $79 \times 40 \equiv 1 \pmod{351}$
$40x \equiv 10 \pmod{351}$, so $79 \times 40x \equiv 790 \pmod{351}$
This gives $x \equiv 790 \pmod{351} \Rightarrow x \equiv 88 \pmod{351}$
So solutions in the set of least residuals modulo 702 are 88 and $88 + 351 = 439$

14 a Applying the Euclidean algorithm to 39 and 216:
$216 = 5 \times 39 + 21$
$39 = 1 \times 21 + 18$
$21 = 1 \times 18 + 3$
$18 = 6 \times 3 + 0$
so $\gcd(39,216) = 3$ and 3 does not divide 10, so $39x \equiv 10 \pmod{216}$ has no solutions.

b $\gcd(39,216)=3$, so simplify equation by dividing everything by 3, which gives:
$13x \equiv 3 \pmod{72}$
Applying the Euclidean algorithm:
$72 = 5 \times 13 + 7$
$13 = 1 \times 7 + 6$
$7 = 1 \times 6 + 1$
Working backwards this gives:
$1 = 7 - 6 = 2(7) - 13$
$= 2(72 - 5(13)) - 13$
$= 2(72) - 11(13)$
$\Rightarrow -11(13) \equiv -2(72) + 1$
Hence $-11 \times 13 \equiv 1 \pmod{72}$
$13x \equiv 3 \pmod{72}$, so $-11 \times 13x \equiv -33 \pmod{72}$
This gives $x \equiv -33 \pmod{72} \Rightarrow x \equiv 39 \pmod{72}$
So solutions in the set of least residuals modulo 216 are 39, 111 and 183

15 $\gcd(21,30)=3$, so simplify equation by dividing everything by 3, which gives:

$7n \equiv 4 \pmod{10}$

Applying the Euclidean algorithm:

$10 = 1\times 7+3$

$7 = 2\times 3+1$

Working backwards this gives:

$1 = 7-2(3) = 3(7)-2(10)$

$\Rightarrow 3(7) \equiv 2(10)+1$

Hence $3\times 7 \equiv 1 \pmod{10}$

$7n \equiv 4 \pmod{10}$, so $3\times 7n \equiv 12 \pmod{10}$

This gives $n \equiv 12 \pmod{10} \Rightarrow n \equiv 2 \pmod{10}$

So solutions in the range $0 \leqslant n < 29$ are 2, 12 and 22

16 Applying the Euclidean algorithm:

$277 = 11\times 25+2$

$25 = 12\times 2+1$

So $\gcd(25,277)=1$, there is a unique solution.

Working backwards this gives:

$1 = 25-12(2)$

$= 25-12(277-11(25))$

$= 133(25)-12(277)$

$\Rightarrow 133(25) \equiv 12(277)+1$

Hence $133\times 25 \equiv 1 \pmod{277}$

$25x \equiv 6 \pmod{277}$, so $133\times 25x \equiv 798 \pmod{277}$

This gives $x \equiv 798 \pmod{277} \Rightarrow x \equiv 798-277-277 \equiv 244 \pmod{277}$

17 $\gcd(28,100)=4$, so simplify equation by dividing everything by 4, which gives:

$7x \equiv 5 \pmod{25}$

Applying the Euclidean algorithm:

$25 = 3\times 7+4$

$7 = 1\times 4+3$

$4 = 1\times 3+1$

Working backwards this gives:

$1 = 4-3 = 2(4)-7 = 2(25-3(7))-7$

$= 2(25)-7(7)$

$\Rightarrow -7(7) \equiv -2(25)+1$

Hence $-7\times 7 \equiv 1 \pmod{25}$

$7x \equiv 5 \pmod{25}$, so $-7\times 7x \equiv -35 \pmod{25}$

This gives $x \equiv -35 \pmod{25} \Rightarrow x \equiv 15 \pmod{25}$

So solutions in the range $0 \leqslant x < 100$ are 15, 40, 65 and 90

18 $\gcd(70, 925) = 5,$ so simplify equation by dividing everything by 5, which gives:

$14x \equiv 4 \pmod{185}$

Applying the Euclidean algorithm:

$185 = 13 \times 14 + 3$

$14 = 4 \times 3 + 2$

$3 = 1 \times 2 + 1$

Working backwards this gives:

$1 = 3 - 2 = 3 - (14 - 4(3))$

$= 5(3) - (14) = 5(185 - 13(14)) - (14)$

$= 5(185) - 66(14)$

$\Rightarrow -66(14) \equiv -5(185) + 1$

Hence $-66 \times 14 \equiv 1 \pmod{185}$

$14x \equiv 4 \pmod{185}$, so $-66 \times 14x \equiv -264 \pmod{185}$

This gives $x \equiv -264 \pmod{185} \Rightarrow x \equiv 106 \pmod{185}$