OPTIONAL PURE / NUMBER THEORY

Linear and Simultaneous Congruences

Worked solutions 10 questions · 75 marks

EXAM BOARDS Edexcel FP2 9FM0/4A · OCR A Y545

Questions

Question 1	*5 marks*	2
Question 2	*7 marks*	3
Question 3	*5 marks*	4
Question 4	*9 marks*	5
Question 5	*9 marks*	7
Question 6	*7 marks*	9
Question 7	*7 marks*	11
Question 8	*8 marks*	12
Question 9	*11 marks*	13
Question 10	*7 marks*	14

1. **(a)** Evaluate 17×11 modulo 37. **[1]**

(b) Hence solve the linear congruence $17x \equiv 5 \pmod{37}$, giving your answer in the form $x \equiv a \pmod{37}$, where $0 \leq a < 37$. **[4]**

Solution

(a)

$$\begin{aligned} 17 \times 11 &= 187 \\ &= 5 \times 37 + 2 \end{aligned}$$

so

$$17 \times 11 \equiv 2 \pmod{37}$$

(b) Multiply both sides of the congruence by 11. Since $\text{hcf}(11, 37) = 1$, the new congruence is equivalent to the original one.

Using part (a):

$$\begin{aligned} 11 \times 17x &\equiv 11 \times 5 \pmod{37} \\ 2x &\equiv 55 \pmod{37} \\ 2x &\equiv 18 \pmod{37} \end{aligned}$$

The last line uses $55 = 37 + 18$. Since $\text{hcf}(2, 37) = 1$, dividing both sides by 2 is valid, so

$$x \equiv 9 \pmod{37}$$

This is in the form $x \equiv a \pmod{37}$ with $a = 9$, and $0 \leq 9 < 37$.

2. **(a)** Explain why the congruence equation

$$24x \equiv 20 \pmod{54}$$

has no solutions. **[2]**

(b) The integer k satisfies $1 \leq k \leq 30$. Consider the congruence equation

$$15y \equiv 2k + 1 \pmod{40}$$

(i) Find every value of k for which this congruence equation has solutions. **[3]**

(ii) For each of these values of k, state how many solutions the congruence equation has modulo 40, giving a reason for your answer. **[2]**

Solution

(a) The congruence $24x \equiv 20 \pmod{54}$ means that $24x - 20$ is a multiple of 54. So there is an integer m such that

$$24x - 54m = 20$$

Since $24 = 6 \times 4$ and $54 = 6 \times 9$, we have $\text{hcf}(24, 54) = 6$. The left-hand side is $6(4x - 9m)$, which is a multiple of 6 for all integers x and m. However, 20 is not a multiple of 6, so the two sides can never be equal. Hence the congruence equation has no solutions.

(b) (i) Since $15 = 5 \times 3$ and $40 = 5 \times 8$, we have $\text{hcf}(15, 40) = 5$. The congruence has a solution exactly when there are integers y and n with

$$15y - 40n = 2k + 1$$

The left-hand side is $5(3y - 8n)$, so a solution can exist only if 5 divides $2k + 1$. Conversely, if $2k + 1 = 5q$ for an integer q, dividing the equation above by 5 gives

$$3y - 8n = q \implies 3y \equiv q \pmod{8}$$

Since $3 \times 3 = 9 \equiv 1 \pmod{8}$, multiplying by 3 gives $y \equiv 3q \pmod{8}$, so solutions do exist. Hence the congruence has solutions exactly when

$$2k + 1 \equiv 0 \pmod{5}$$

$$2k \equiv -1 \equiv 4 \pmod{5}$$

$$k \equiv 2 \pmod{5}$$

The step dividing by 2 is valid because $\text{hcf}(2, 5) = 1$. With $1 \leq k \leq 30$, the values are

$$k = 2,\ 7,\ 12,\ 17,\ 22,\ 27$$

(ii) For each of these values, write $2k + 1 = 5q$. From part (b)(i), the congruence reduces to $3y \equiv q \pmod{8}$, which has the single solution $y \equiv 3q \pmod{8}$. So $y = 3q + 8t$ for an integer t, and modulo 40 this gives

$$y \equiv 3q,\ 3q + 8,\ 3q + 16,\ 3q + 24,\ 3q + 32 \pmod{40}$$

These five values are different modulo 40, since they differ by multiples of 8 less than 40. So for each value of k there are 5 solutions modulo 40, equal to $\text{hcf}(15, 40) = 5$.

3. **(a)** Solve $13x \equiv 6 \pmod{31}$. **[2]**

(b) Show that the simultaneous congruences

$$6x \equiv 4 \pmod{16}, \qquad x \equiv 7 \pmod{12}$$

have no solution. **[3]**

Solution

(a) Find the inverse of 13 modulo 31 using the Euclidean algorithm:

$$31 = 2 \times 13 + 5$$
$$13 = 2 \times 5 + 3$$
$$5 = 1 \times 3 + 2$$
$$3 = 1 \times 2 + 1$$

Working backwards:

$$\begin{aligned} 1 &= 3 - 2 = 3 - (5 - 3) = 2 \times 3 - 5 \\ &= 2(13 - 2 \times 5) - 5 = 2 \times 13 - 5 \times 5 \\ &= 2 \times 13 - 5(31 - 2 \times 13) = 12 \times 13 - 5 \times 31 \end{aligned}$$

So $12 \times 13 \equiv 1 \pmod{31}$, and the inverse of 13 modulo 31 is 12. Multiplying both sides of the congruence by 12:

$$x \equiv 12 \times 6 = 72 \equiv 10 \pmod{31}$$

(b) The first congruence means that $6x - 4 = 16k$ for some integer k. Dividing by 2 gives

$$3x - 2 = 8k$$

so $3x \equiv 2 \pmod{8}$. Since $3 \times 3 = 9 \equiv 1 \pmod{8}$, the inverse of 3 modulo 8 is 3. Multiplying both sides by 3:

$$x \equiv 6 \pmod{8}$$

Hence $x = 8m + 6 = 2(4m + 3)$ for some integer m, so any solution of the first congruence is even.

The second congruence gives $x = 12n + 7 = 2(6n + 3) + 1$ for some integer n, so any solution of the second congruence is odd.

No integer is both even and odd, so the simultaneous congruences have no solution.

4. **(a)** Use the Euclidean algorithm to show that the highest common factor of 83 and 30 is 1. **[2]**

(b) Hence find integers p and q such that

$$30p + 83q = 1$$ **[3]**

(c) Hence solve the linear congruence $30x \equiv 11 \pmod{83}$, giving your answer in the form $x \equiv a \pmod{83}$, where $0 \leq a < 83$. **[2]**

(d) Use your answer to part (b) to solve the linear congruence $83y \equiv 4 \pmod{30}$, giving your answer in the form $y \equiv c \pmod{30}$, where $0 \leq c < 30$. **[2]**

Solution

(a) Applying the Euclidean algorithm:

$$\begin{aligned} 83 &= 2 \times 30 + 23 \\ 30 &= 1 \times 23 + 7 \\ 23 &= 3 \times 7 + 2 \\ 7 &= 3 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

The last non-zero remainder is 1, so the highest common factor of 83 and 30 is 1.

(b) Working back up the algorithm, starting from the line with remainder 1:

$$\begin{aligned} 1 &= 7 - 3 \times 2 \\ &= 7 - 3 \times (23 - 3 \times 7) = 10 \times 7 - 3 \times 23 \\ &= 10 \times (30 - 23) - 3 \times 23 = 10 \times 30 - 13 \times 23 \\ &= 10 \times 30 - 13 \times (83 - 2 \times 30) = 36 \times 30 - 13 \times 83 \end{aligned}$$

So $30 \times 36 + 83 \times (-13) = 1$, giving $p = 36$ and $q = -13$.

(c) From part (b), $30 \times 36 = 1 + 13 \times 83$, so

$$30 \times 36 \equiv 1 \pmod{83}$$

Hence 36 is the multiplicative inverse of 30 modulo 83. Multiplying both sides of $30x \equiv 11 \pmod{83}$ by 36:

$$\begin{aligned} 36 \times 30x &\equiv 36 \times 11 \pmod{83} \\ x &\equiv 396 \pmod{83} \\ x &\equiv 396 - 4 \times 83 \pmod{83} \\ x &\equiv 64 \pmod{83} \end{aligned}$$

This is in the form $x \equiv a \pmod{83}$ with $a = 64$, and $0 \leq 64 < 83$.

(d) From part (b), $83 \times (-13) = 1 - 36 \times 30$, so

$$83 \times (-13) \equiv 1 \pmod{30}$$

Hence -13 is the multiplicative inverse of 83 modulo 30. Multiplying both sides of $83y \equiv 4 \pmod{30}$ by -13:

$$\begin{aligned}(-13) \times 83y &\equiv (-13) \times 4 \pmod{30} \\ y &\equiv -52 \pmod{30} \\ y &\equiv -52 + 2 \times 30 \pmod{30} \\ y &\equiv 8 \pmod{30}\end{aligned}$$

This is in the form $y \equiv c \pmod{30}$ with $c = 8$, and $0 \leq 8 < 30$.

5. **(a)** Find all integers x such that $21x \equiv 4 \pmod{89}$. **[4]**

(b) Hence, or otherwise, solve

(i) $68x \equiv 8 \pmod{89}$ **[2]**

(ii) $21x \equiv 9 \pmod{178}$ **[3]**

Solution

(a) Apply the Euclidean algorithm to 89 and 21:

$$89 = 4 \times 21 + 5$$

$$21 = 4 \times 5 + 1$$

Working backwards to write 1 in terms of 21 and 89:

$$\begin{aligned} 1 &= 21 - 4 \times 5 \\ &= 21 - 4 \times (89 - 4 \times 21) \\ &= 17 \times 21 - 4 \times 89 \end{aligned}$$

Hence $17 \times 21 \equiv 1 \pmod{89}$, so 17 is the inverse of 21 modulo 89. Multiplying both sides of $21x \equiv 4 \pmod{89}$ by 17 gives

$$x \equiv 17 \times 21x \equiv 17 \times 4 \equiv 68 \pmod{89}$$

So the integers are $x = 68 + 89k$, where k is any integer.

(b) (i) Since $68 = 89 - 21$, $68 \equiv -21 \pmod{89}$, so the congruence becomes

$$-21x \equiv 8 \pmod{89} \implies 21x \equiv -8 \pmod{89}$$

Multiplying by 17, the inverse of 21 modulo 89 from part (a):

$$x \equiv 17 \times (-8) \equiv -136 \pmod{89}$$

Adding $2 \times 89 = 178$ gives $-136 + 178 = 42$, so

$$x \equiv 42 \pmod{89}$$

(ii) Since $178 = 2 \times 89$, with 2 and 89 coprime, 178 divides $21x - 9$ exactly when both 2 and 89 divide it. So x must satisfy the simultaneous congruences

$$21x \equiv 9 \pmod{89}, \qquad 21x \equiv 9 \pmod{2}$$

Modulo 89, multiplying by 17 as in part (a) gives

$$x \equiv 17 \times 9 = 153 \equiv 64 \pmod{89}$$

Modulo 2, $21 \equiv 1$ and $9 \equiv 1$, so $x \equiv 1 \pmod{2}$, that is, x is odd.

Write $x = 64 + 89k$ for an integer k. Since 64 is even and 89 is odd, x is odd exactly when k is odd. Putting $k = 2m + 1$, where m is an integer:

$$x = 64 + 89(2m + 1) = 153 + 178m$$

Hence

$$x \equiv 153 \pmod{178}$$

6. **(a)** Solve the linear congruence $5x \equiv 8 \pmod{17}$, giving your answer in the form $x \equiv a \pmod{17}$, where $0 \leq a < 17$. **[2]**

(b) Hence, or otherwise, find all integers x with $1000 < x < 2000$ that satisfy the simultaneous linear congruences

$$5x \equiv 8 \pmod{17}, \qquad 9x \equiv 4 \pmod{23}$$ **[5]**

Solution

(a) First find the inverse of 5 modulo 17. Since

$$5 \times 7 = 35 = 2 \times 17 + 1 \equiv 1 \pmod{17}$$

the inverse of 5 modulo 17 is 7. Multiplying both sides of the congruence by 7:

$$\begin{aligned} 35x &\equiv 56 \pmod{17} \\ x &\equiv 56 - 3 \times 17 \pmod{17} \\ x &\equiv 5 \pmod{17} \end{aligned}$$

This is in the form $x \equiv a \pmod{17}$ with $a = 5$, and $0 \leq 5 < 17$.

(b) Using part (a), the first congruence is equivalent to $x \equiv 5 \pmod{17}$.

For the second congruence, find the inverse of 9 modulo 23. Since

$$9 \times 18 = 162 = 7 \times 23 + 1 \equiv 1 \pmod{23}$$

the inverse of 9 modulo 23 is 18. Multiplying both sides of $9x \equiv 4 \pmod{23}$ by 18:

$$\begin{aligned} x &\equiv 72 \pmod{23} \\ x &\equiv 72 - 3 \times 23 \pmod{23} \\ x &\equiv 3 \pmod{23} \end{aligned}$$

From the first congruence, $x = 5 + 17k$ for some integer k. Substituting into the second:

$$\begin{aligned} 5 + 17k &\equiv 3 \pmod{23} \\ 17k &\equiv -2 \equiv 21 \pmod{23} \end{aligned}$$

The inverse of 17 modulo 23 is 19, since

$$17 \times 19 = 323 = 14 \times 23 + 1 \equiv 1 \pmod{23}$$

Multiplying both sides by 19:

$$\begin{aligned} k &\equiv 21 \times 19 \pmod{23} \\ k &\equiv 399 - 17 \times 23 \pmod{23} \\ k &\equiv 8 \pmod{23} \end{aligned}$$

So $k = 8 + 23m$ for some integer m, which gives

$$x = 5 + 17(8 + 23m) = 141 + 391m$$

Since 17 and 23 are coprime, the solutions are exactly $x \equiv 141 \pmod{391}$, where $391 = 17 \times 23$.

Now require $1000 < 141 + 391m < 2000$:

$$859 < 391m < 1859 \quad \Longrightarrow \quad \frac{859}{391} < m < \frac{1859}{391}$$

Since $\frac{859}{391} \approx 2.20$ and $\frac{1859}{391} \approx 4.75$, $m = 3$ or $m = 4$. These give

$$x = 141 + 3 \times 391 = 1314, \qquad x = 141 + 4 \times 391 = 1705$$

The integers are $x = 1314$ and $x = 1705$.

7. A circular track has 17 marker posts, equally spaced and numbered 0 to 16 in order clockwise. A robot starts at post 0 and travels clockwise around the track. It makes x short moves, each taking it forward 3 posts, and y long moves, each taking it forward 8 posts, in some order. When it has made all of its moves, the robot is at post n, where $0 \leq n \leq 16$.

(a) Write down a congruence for n in the form $n \equiv ax + by \pmod{c}$, where a, b and c are integers. **[1]**

It is now given that the robot makes exactly 45 moves in total and finishes at post 5.

(b) Use your congruence to find all the possible values of the number of long moves made by the robot. **[6]**

Solution

(a) Each short move takes the robot forward 3 posts and each long move takes it forward 8 posts, so altogether it moves forward $3x + 8y$ posts. The track has 17 posts, so the post number repeats every 17 posts. This gives

$$n \equiv 3x + 8y \pmod{17}$$

This is in the required form with $a = 3$, $b = 8$ and $c = 17$.

(b) The robot makes 45 moves, so $x + y = 45$, giving $x = 45 - y$. Substituting this and $n = 5$ into the congruence from part (a):

$$3(45 - y) + 8y \equiv 5 \pmod{17}$$

$$135 + 5y \equiv 5 \pmod{17}$$

Since $135 = 7 \times 17 + 16$, we have $135 \equiv 16 \pmod{17}$, so

$$16 + 5y \equiv 5 \pmod{17}$$

$$5y \equiv -11 \pmod{17}$$

$$5y \equiv 6 \pmod{17}$$

To solve this, find the inverse of 5 modulo 17. Since

$$5 \times 7 = 35 = 2 \times 17 + 1 \equiv 1 \pmod{17}$$

the inverse of 5 modulo 17 is 7. Multiplying both sides of the congruence by 7:

$$35y \equiv 42 \pmod{17}$$

$$y \equiv 8 \pmod{17}$$

So $y = 8 + 17k$ for some integer k. The number of long moves satisfies $0 \leq y \leq 45$, so $y = 8$, 25 or 42 (the next value, 59, is too large). These give $x = 37$, 20 and 3 respectively, all non-negative, so the possible numbers of long moves are 8, 25 and 42.

8. Consider the simultaneous linear congruences

$$4x \equiv 6 \pmod{14}, \qquad 5x \equiv 2 \pmod{12}$$

(a) The first congruence, including its modulus, is divided through by the highest common factor of 4 and 14. Explain why the resulting pair of congruences has exactly one solution modulo 84. **[2]**

(b) Hence find all integers x with $0 < x < 500$ that satisfy both of the original congruences. **[6]**

Solution

(a) The highest common factor of 4 and 14 is 2, and 2 divides 6. Dividing the first congruence through by 2 gives

$$2x \equiv 3 \pmod{7}$$

This has the same solutions as $4x \equiv 6 \pmod{14}$, because 14 divides $4x - 6 = 2(2x - 3)$ exactly when 7 divides $2x - 3$.

Since $\text{hcf}(2, 7) = 1$, 2 has an inverse modulo 7, so $2x \equiv 3 \pmod{7}$ has exactly one solution modulo 7. Similarly, since $\text{hcf}(5, 12) = 1$, $5x \equiv 2 \pmod{12}$ has exactly one solution modulo 12.

The moduli satisfy $\text{hcf}(7, 12) = 1$, so by the Chinese remainder theorem the pair of congruences has exactly one solution modulo $7 \times 12 = 84$.

(b) Using part (a), solve $2x \equiv 3 \pmod{7}$. Since $2 \times 4 = 8 \equiv 1 \pmod{7}$, the inverse of 2 modulo 7 is 4. Multiplying both sides by 4:

$$x \equiv 4 \times 3 = 12 \equiv 5 \pmod{7}$$

Since $5 \times 5 = 25 \equiv 1 \pmod{12}$, the inverse of 5 modulo 12 is 5. Multiplying both sides of $5x \equiv 2 \pmod{12}$ by 5:

$$x \equiv 5 \times 2 = 10 \pmod{12}$$

So $x = 10 + 12k$ for some integer k. Substituting into $x \equiv 5 \pmod{7}$, and using $10 \equiv 3$ and $12 \equiv 5 \pmod{7}$:

$$\begin{aligned} 10 + 12k &\equiv 5 \pmod{7} \\ 3 + 5k &\equiv 5 \pmod{7} \\ 5k &\equiv 2 \pmod{7} \end{aligned}$$

Since $5 \times 3 = 15 \equiv 1 \pmod{7}$, the inverse of 5 modulo 7 is 3, so

$$k \equiv 3 \times 2 = 6 \pmod{7}$$

Writing $k = 6 + 7m$ for an integer m:

$$x = 10 + 12(6 + 7m) = 82 + 84m$$

So the solutions are exactly the integers with $x \equiv 82 \pmod{84}$, in agreement with part (a). For $0 < x < 500$, $m = 0, 1, 2, 3, 4$, since $m = 5$ gives $82 + 84 \times 5 = 502 > 500$ and $m = -1$ gives $-2 < 0$. The integers are

$$x = 82,\ 166,\ 250,\ 334,\ 418$$

9. **(a)** Use the Euclidean algorithm to find the highest common factor h of 270 and 114. **[3]**

(b) Hence find integers a and b such that

$$270a + 114b = h$$ **[3]**

(c) Hence find all integers x with $0 \leq x < 114$ that satisfy

$$270x \equiv 24 \pmod{114}$$ **[5]**

Solution

(a) Apply the Euclidean algorithm, dividing each divisor by the remainder:

$$\begin{aligned} 270 &= 2 \times 114 + 42 \\ 114 &= 2 \times 42 + 30 \\ 42 &= 1 \times 30 + 12 \\ 30 &= 2 \times 12 + 6 \\ 12 &= 2 \times 6 + 0 \end{aligned}$$

The last non-zero remainder is the highest common factor, so $h = 6$.

(b) Work back up the algorithm, starting from the line with remainder 6 and substituting for each earlier remainder in turn:

$$\begin{aligned} 6 &= 30 - 2 \times 12 \\ &= 30 - 2 \times (42 - 30) = 3 \times 30 - 2 \times 42 \\ &= 3 \times (114 - 2 \times 42) - 2 \times 42 = 3 \times 114 - 8 \times 42 \\ &= 3 \times 114 - 8 \times (270 - 2 \times 114) = 19 \times 114 - 8 \times 270 \end{aligned}$$

So $270 \times (-8) + 114 \times 19 = 6$, giving $a = -8$ and $b = 19$.

(c) Since $h = 6$ divides 24, the congruence has solutions. The congruence means $270x - 24 = 114k$ for some integer k, and dividing through by 6 gives $45x - 4 = 19k$. So the congruence is equivalent to

$$45x \equiv 4 \pmod{19}$$

Dividing the result of part (b) by 6:

$$45 \times (-8) + 19 \times 19 = 1 \implies 45 \times (-8) \equiv 1 \pmod{19}$$

So -8 is the inverse of 45 modulo 19. Multiplying both sides of $45x \equiv 4 \pmod{19}$ by -8:

$$\begin{aligned} x &\equiv -32 \pmod{19} \\ x &\equiv 6 \pmod{19} \end{aligned}$$

The values with $0 \leq x < 114$ are $6 + 19m$ for $m = 0, 1, \ldots, 5$, which gives the $6 = h$ solutions

$$x = 6,\ 25,\ 44,\ 63,\ 82,\ 101$$

10. Determine all integers x that satisfy the simultaneous congruences

$$4x \equiv 3 \pmod 9, \qquad x \equiv 7 \pmod{11}, \qquad 3x \equiv 2 \pmod{13}$$

Give your answer in the form $x = qn + r$, where n is any integer and q, r are integers with $q > 0$ and $0 \leq r < q$. **[7]**

Solution

First write each congruence in the form $x \equiv a$ by multiplying by an inverse.

Since $4 \times 7 = 28 = 3 \times 9 + 1$, the inverse of 4 modulo 9 is 7. Multiplying $4x \equiv 3 \pmod 9$ by 7 gives

$$x \equiv 21 \equiv 3 \pmod 9$$

Since $3 \times 9 = 27 = 2 \times 13 + 1$, the inverse of 3 modulo 13 is 9. Multiplying $3x \equiv 2 \pmod{13}$ by 9 gives

$$x \equiv 18 \equiv 5 \pmod{13}$$

So x must satisfy

$$x \equiv 3 \pmod 9, \qquad x \equiv 7 \pmod{11}, \qquad x \equiv 5 \pmod{13}$$

From the second congruence, $x = 7 + 11k$ for some integer k. Substituting into $x \equiv 3 \pmod 9$, and using $11 \equiv 2 \pmod 9$:

$$7 + 11k \equiv 3 \pmod 9$$

$$2k \equiv -4 \equiv 5 \pmod 9$$

The inverse of 2 modulo 9 is 5, since $2 \times 5 = 10 = 9 + 1$. Multiplying by 5 gives

$$k \equiv 25 \equiv 7 \pmod 9$$

so $k = 7 + 9j$ for some integer j, and

$$x = 7 + 11(7 + 9j) = 84 + 99j$$

Substituting into $x \equiv 5 \pmod{13}$, and using $84 = 6 \times 13 + 6$ and $99 = 7 \times 13 + 8$:

$$84 + 99j \equiv 5 \pmod{13}$$

$$6 + 8j \equiv 5 \pmod{13}$$

$$8j \equiv -1 \equiv 12 \pmod{13}$$

The inverse of 8 modulo 13 is 5, since $8 \times 5 = 40 = 3 \times 13 + 1$. Multiplying by 5 gives

$$j \equiv 60 \equiv 8 \pmod{13}$$

so $j = 8 + 13n$ for any integer n. Hence

$$\begin{aligned} x &= 84 + 99(8 + 13n) \\ &= 84 + 792 + 1287n \\ &= 1287n + 876 \end{aligned}$$

So all the integers satisfying the three congruences are $x = 1287n + 876$, where n is any integer, which is in the required form with $q = 1287$ and $r = 876$.