London Academy of Maths

Number Theory

Question Paper

*

1. (i) Use Fermat's Little Theorem to find the least positive residue of 6^{542} modulo 13

(5)

*

2. **In this question you must show detailed reasoning.**

Use Fermat's Little Theorem to determine the least positive residue of

$$21^{80} \pmod{23}$$

(4)

 **

3 **(a)** Solve $7x \equiv 6 \pmod{19}$. **[2]**

(b) Show that the following simultaneous linear congruences have no solution.

$x \equiv 3 \pmod{4}$, $x \equiv 4 \pmod{6}$. **[2]**

4) Solve the simultaneous linear congruences

$$5x \equiv 3 \pmod{8} \quad \text{and} \quad x \equiv 4 \pmod{5}.$$

(3)

5) Prove that $30n + 4$ and $20n + 3$ are always coprime, where $n \in \mathbb{N}$. (3)

6) Solve the simultaneous linear congruences

$$7x \equiv 2 \pmod{25} \quad \text{and} \quad x \equiv 4 \pmod{19}.$$

(3)

7) Solve the simultaneous linear congruences

$$x \equiv a \pmod{4} \quad \text{and} \quad x \equiv b \pmod{5},$$

giving your answer in the form

$$x \equiv ha + kb \pmod{20},$$

where $h, k \in \mathbb{Z}$, $0 \leq h < 20$, and $0 \leq k < 20$. (4)

***

8 Let N be the number 15 824 578.

(a) (i) Use a standard divisibility test to show that N is a multiple of 11. **[2]**

(ii) A student uses the following test for divisibility by 7.

> 'Throw away' multiples of 7 that appear either individually or within a pair of consecutive digits of the test number.
> Stop when the number obtained is 0, 1, 2, 3, 4, 5 or 6.
> The test number is only divisible by 7 if that obtained number is 0.

For example, for the number N, they first 'throw away' the "7" in the tens column, leaving the number $N_1 = 15824508$. At the second stage, they 'throw away' the "14" from the left-hand pair of digits of N_1, leaving $N_2 = 01824508$; and so on, until a number is obtained which is 0, 1, 2, 3, 4, 5 or 6.

- Justify the validity of this process.
- Continue the student's test to show that $7 \mid N$. **[2]**

(iii) Given that $N = 11 \times 1\,438\,598$, explain why $7 \mid 1\,438\,598$. **[1]**

(b) Let $M = N^2$.

(i) Express N in the unique form $101a + b$ for positive integers a and b, with $0 \leqslant b < 101$. **[2]**

(ii) Hence write M in the form $M \equiv r \pmod{101}$, where $0 < r < 101$. **[1]**

(iii) Deduce the order of N modulo 101. **[1]**

9) Suppose

$$x \equiv 3 \pmod 7 \quad \text{and} \quad x \equiv 11 \pmod{17}.$$

Show that

$$x^2 \equiv 2 \pmod{119}.$$

(3)

***

10 Solve the simultaneous linear congruences $x \equiv 1 \pmod{3}$, $x \equiv 5 \pmod{11}$, $2x \equiv 5 \pmod{17}$. **[6]**

 ***

11 Determine all integers x for which $x \equiv 1 \pmod{7}$ and $x \equiv 22 \pmod{37}$ and $x \equiv 7 \pmod{67}$.
Give your answer in the form $x = qn + r$ for integers n, q, r with $q > 0$ and $0 \leqslant r < q$. **[6]**

12) Suppose

$$x^{109} \equiv 53 \pmod 7 \quad \text{and} \quad x^{131} \equiv 59 \pmod{11}.$$

Show that

$$x \equiv 4 \pmod{77}.$$

(3)

13) Solve the simultaneous linear congruences

$$x \equiv 2 \pmod{3}, \qquad x \equiv 3 \pmod{5}, \qquad x \equiv 4 \pmod{7}.$$

(4)

***

14. Let G be a group of order $46^{46} + 47^{47}$

Using Fermat's Little Theorem and explaining your reasoning, determine which of the following are possible orders for a subgroup of G

(i) 11

(ii) 21

(7)

15) Solve the simultaneous linear congruences

$$x \equiv 3 \pmod{6}, \qquad x \equiv 5 \pmod{8}, \qquad x \equiv 9 \pmod{14}.$$

(4)

16) Let $m, n \in \mathbb{N}$, and suppose $x, a, b \in \mathbb{Z}$ satisfy

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}.$$

Prove that

$$a \equiv b \pmod{\gcd(m, n)}.$$

(4)

****

17 **(a)** The group G consists of the set $S = \{1, 9, 17, 25\}$ under $\times_{32}$, the operation of multiplication modulo 32.

(i) Complete the Cayley table for G given in the Printed Answer Booklet. **[2]**

(ii) Up to isomorphisms, there are only two groups of order 4.

- C_4, the cyclic group of order 4
- K_4, the non-cyclic (Klein) group of order 4

State, with justification, to which of these two groups G is isomorphic. **[2]**

(b) **(i)** List the odd quadratic residues modulo 32. **[2]**

(ii) Given that n is an odd integer, prove that $n^6 + 3n^4 + 7n^2 \equiv 11 \pmod{32}$. **[4]**

****

18 Throughout this question, n is a positive integer.

(a) Explain why $n^5 \equiv n \pmod 5$. **[1]**

(b) By proving that $n^5 \equiv n \pmod 2$, show that $n^5 \equiv n \pmod{10}$. **[3]**

(c) **(i)** Prove that $n^5 - n$ is divisible by 30 for all positive integers n. **[5]**

(ii) Is there an integer N, greater than 30, such that $n^5 - n$ is divisible by N for all positive integers n? Justify your answer. **[1]**

19) Prove that

$$\gcd(12n+3,\ 20n+1) = \begin{cases} a, & \text{when } n \equiv b \pmod{c}, \\ d, & \text{otherwise,} \end{cases}$$

where $a, b, c, d \in \mathbb{Z}$ are to be found. (5)

20) Solve

$$x^9 \equiv 6 \pmod{77}.$$

(5)

21) Solve the congruence

$$x^{1351} \equiv 2024 \pmod{2027}.$$

(5)

22 **(i)** **(a)** Prove that $p \equiv \pm 1 \pmod 6$ for all primes $p > 3$. **[2]**

(b) Hence or otherwise prove that $p^2 - 1 \equiv 0 \pmod{24}$ for all primes $p > 3$. **[3]**

(ii) Given that p is an odd prime, determine the residue of 2^{p^2-1} modulo p. **[4]**

(iii) Let p and q be distinct primes greater than 3. Prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$. **[5]**