OPTIONAL PURE / NUMBER THEORY

Modular Arithmetic and Quadratic Residues

Questions by topic 10 questions · 88 marks

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

Questions

Question 1	*6 marks*	2
Question 2	*8 marks*	3
Question 3	*11 marks*	4
Question 4	*6 marks*	5
Question 5	*10 marks*	6
Question 6	*5 marks*	7
Question 7	*7 marks*	8
Question 8	*7 marks*	9
Question 9	*12 marks*	10
Question 10	*16 marks*	11

1. **(a)** Determine all the possible integers a, where $a > 9$, such that

$$3^4 \equiv 9 \pmod{a}$$ **[2]**

(b) Show that if p is prime, x is an integer and $x^3 \equiv x \pmod{p}$, then

$$x \equiv 0 \pmod{p}, \qquad x \equiv 1 \pmod{p} \qquad \text{or} \qquad x \equiv -1 \pmod{p}$$

Show also, by giving a suitable value of x, that this conclusion can fail when p is replaced by 8. **[4]**

2. Throughout this question, $n \geq 2$ is an integer, and $a \equiv b \pmod{n}$ means that n divides $a - b$.

(a) Prove, from the definition, that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$. Deduce that if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for every positive integer k. **[3]**

(b) Find every integer x with $0 \leq x < 15$ such that $6x \equiv 6 \pmod{15}$. Hence show that a common factor cannot always be cancelled from both sides of a congruence. **[2]**

(c) You may assume that congruences modulo n may be added. Using part (a), explain why the integer solutions of $x^3 + 5x + 4 \equiv 0 \pmod{11}$ can be found by checking only the residues $x = 0, 1, 2, \ldots, 10$. Hence find all integers x such that $x^3 + 5x + 4 \equiv 0 \pmod{11}$, giving your answers as congruences modulo 11. **[3]**

3. For positive integers n, let

$$f(n) = 1 + 2^n + 4^n + 8^n + 16^n$$

(a) (i) Given that n is **not** a multiple of 5, use the division algorithm to write down the four possible forms that n can take. **[1]**

(ii) Show that $2^5 \equiv 1 \pmod{31}$. Hence show that, when n is **not** a multiple of 5, $f(n)$ is a multiple of 31. **[7]**

(b) Determine the value of $f(n)$, modulo 31, in the case when n is a multiple of 5. Hence find the remainder when $f(1) + f(2) + f(3) + \cdots + f(40)$ is divided by 31. **[3]**

4. Let $p \geq 3$ be a prime number and let x and y be positive integers.
By first showing that the square of any odd integer is congruent to 1 modulo 8, prove that there are **no** values of p, x and y satisfying the equation

$$p^{2x} + 5 = 2^y$$

[6]

5. Throughout this question, n is a positive integer.

(a) By listing the possible values of n^3 modulo 7, prove that $n^7 \equiv n \pmod 7$. **[2]**

(b) Prove that $n^7 \equiv n \pmod 3$, and hence show that $n^7 \equiv n \pmod{21}$. **[3]**

(c) (i) Prove that $n^7 - n$ is divisible by 42 for all positive integers n. **[3]**

(ii) Find the largest integer N such that $n^7 - n$ is divisible by N for all positive integers n, justifying your answer. **[2]**

6. Let

$$f(n) = 3^{4n+2} + 2^{2n+3}$$

Use arithmetic modulo 17 to prove that, for integers $n \geq 0$, $f(n)$ is divisible by 17 if and only if n is even. **[5]**

7. In this question, k and n denote integers.

(a) By considering the residues of k modulo 9, list the possible residues of k^2 modulo 9. By writing n in the form $3q$, $3q+1$ or $3q-1$, where q is an integer, show also that $n^3 \equiv 0$, 1 or 8 (mod 9). **[4]**

(b) Hence prove that $n^6 + n^3 + 3$ is not a perfect square for any integer n. **[3]**

8. Throughout this question, n is an integer that is divisible by neither 2 nor 3.

(a) Find all the possible values of n^2 modulo 48. **[3]**

(b) Hence prove that $n^8 + 4n^6 + 6n^2 \equiv 11 \pmod{48}$. **[4]**

9. The fundamental theorem of arithmetic states that every integer greater than 1 can be written as a product of prime numbers, uniquely apart from the order of the factors.
Suppose that there are only finitely many prime numbers congruent to 2 (mod 3). Label these primes $p_1, p_2, \ldots, p_n$, where $p_1 = 2$ and $p_2 = 5$, and define the integer M by

$$M = 3p_1p_2 \cdots p_n - 1$$

(a) Write down the value of M modulo 3. **[1]**

(b) Explain why $M = q_1q_2 \cdots q_r$, where $q_1, \ldots, q_r$ are primes, not necessarily distinct, and show that none of $q_1, \ldots, q_r$ is equal to 3. **[3]**

(c) By considering the possible residues of $q_1, \ldots, q_r$ modulo 3, prove that $q_j \equiv 2 \pmod 3$ for at least one integer j with $1 \leq j \leq r$. **[4]**

(d) Hence deduce that there are infinitely many prime numbers congruent to 2 (mod 3). **[4]**

10. Throughout this question, n is an integer greater than 1.
An integer q, where $0 < q < n$, is said to be a quadratic residue modulo n if there exists an integer x such that $x^2 \equiv q \pmod{n}$.
Note that under this definition 0 is not considered to be a quadratic residue modulo n.

(a) By considering congruences modulo 4 and modulo 25, find all the integers x, where $0 \leq x < 100$, which satisfy $x^2 \equiv 41 \pmod{100}$. **[4]**

(b) By considering squares modulo 4, explain why 42 is not a quadratic residue modulo 100. **[1]**

(c) Determine the quadratic residues modulo 17. **[2]**

(d) Determine the quadratic residues modulo 15. **[2]**

(e) Let p be a prime. Prove that if a and b are integers with $a^2 \equiv b^2 \pmod{p}$, then $a \equiv b \pmod{p}$ or $a \equiv -b \pmod{p}$.
By referring to your answer to part (d), give an example to show that this result need not hold when the modulus is not prime. **[3]**

(f) Hence prove that if p is prime, where $p > 2$, then the number of quadratic residues modulo p is

$$\frac{p-1}{2}$$ **[4]**