OPTIONAL PURE / NUMBER THEORY

Fermat's Little Theorem

Questions by topic 7 questions · 52 marks

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

Questions

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

1. Use Fermat's little theorem to determine the least positive residue of

$$37^{200} + 56^{200} \pmod{17}$$ **[5]**

2. A student claims that the order of 3 modulo 41 is 6.

(a) Without calculation, explain why the student's claim must be incorrect. **[1]**

(b) Determine the order of 3 modulo 41, justifying your answer. **[3]**

(c) Hence find the remainder when 3^{2026} is divided by 41. **[1]**

3. Use Fermat's little theorem to find all the solutions of the congruence

$$x^{201} + 4x^{110} \equiv 7x^{91} \pmod{19}$$

giving each in the form $x \equiv a \pmod{19}$, where $0 \leq a \leq 18$. **[6]**

4. The integer 341 is not prime, since $341 = 11 \times 31$.

(a) Use Fermat's little theorem to show that

$$2^{340} \equiv 1 \pmod{11} \qquad \text{and} \qquad 2^{340} \equiv 1 \pmod{31}$$ **[4]**

(b) Hence show that $2^{340} \equiv 1 \pmod{341}$. **[1]**

(c) Explain why the result of part (b) shows that the following statement is false.
"If $n > 1$ is an integer and $2^{n-1} \equiv 1 \pmod{n}$, then n is prime." **[1]**

(d) (i) Show that $3^{340} \not\equiv 1 \pmod{341}$. **[4]**

(ii) Explain why the result of part (d)(i) alone shows that 341 is not prime. **[1]**

5. Let G be a group whose order is

$$26^{27} + 27^{26}$$

Using Fermat's little theorem and explaining your reasoning, determine which of 15, 17 and 35 are possible orders for a subgroup of G. **[8]**

6. Let p be an odd prime, and let n be an integer such that p divides $n^2 + 1$.

(a) Show that p does not divide n, and that $n^4 \equiv 1 \pmod{p}$. **[2]**

(b) The order of n modulo p is the least positive integer d such that $n^d \equiv 1 \pmod{p}$.

(i) Show that the order of n modulo p is 4. **[2]**

(ii) Use Fermat's little theorem to deduce that $p \equiv 1 \pmod{4}$. **[3]**

(c) Given that 2027 is prime, show that there is no integer n for which $n^2 + 1$ is divisible by 2027. **[1]**

7. **(a)** Let p be a prime with $p \geq 5$. Prove that

$$2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \pmod{p}$$ **[4]**

(b) The integer N is defined by

$$N = 2^{29} + 3^{29} + 6^{29} - 1$$

By using the result of part (a), find three prime factors of N that are greater than 5, justifying your answer. **[5]**