OPTIONAL PURE / NUMBER THEORY

Fermat's Little Theorem

Worked solutions 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*	6
Question 5	*8 marks*	8
Question 6	*8 marks*	10
Question 7	*9 marks*	12

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

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

Solution

First reduce the bases modulo 17. Since $37 = 2 \times 17 + 3$ and $56 = 3 \times 17 + 5$, it follows that

$$37 \equiv 3 \pmod{17}, \qquad 56 \equiv 5 \pmod{17}$$

so

$$37^{200} + 56^{200} \equiv 3^{200} + 5^{200} \pmod{17}$$

Fermat's little theorem states that, if p is prime and p does not divide a, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Here $p = 17$ is prime and 17 divides neither 3 nor 5, so

$$3^{16} \equiv 1 \pmod{17}, \qquad 5^{16} \equiv 1 \pmod{17}$$

Since $200 = 12 \times 16 + 8$:

$$3^{200} = \left(3^{16}\right)^{12} \times 3^8 \equiv 1^{12} \times 3^8 \equiv 3^8 \pmod{17}$$

$$5^{200} = \left(5^{16}\right)^{12} \times 5^8 \equiv 1^{12} \times 5^8 \equiv 5^8 \pmod{17}$$

Now find 3^8 by repeated squaring, using $81 = 4 \times 17 + 13$:

$$3^2 = 9$$

$$3^4 = 81 \equiv 13 \equiv -4 \pmod{17}$$

$$3^8 \equiv (-4)^2 = 16 \equiv -1 \pmod{17}$$

Similarly for 5^8, using $25 = 17 + 8$ and $64 = 3 \times 17 + 13$:

$$5^2 = 25 \equiv 8 \pmod{17}$$

$$5^4 \equiv 8^2 = 64 \equiv 13 \equiv -4 \pmod{17}$$

$$5^8 \equiv (-4)^2 = 16 \equiv -1 \pmod{17}$$

Therefore

$$37^{200} + 56^{200} \equiv (-1) + (-1) = -2 \equiv 15 \pmod{17}$$

so the least positive residue is 15.

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]**

Solution

(a) Fermat's little theorem states that, if p is prime and p does not divide a, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Since 41 is prime and 41 does not divide 3, this gives

$$3^{40} \equiv 1 \pmod{41}$$

The order of 3 modulo 41 must therefore divide 40. Since 6 does not divide 40, the order cannot be 6, so the student's claim is incorrect.

(b) By part (a), the order divides 40, so it is one of $1, 2, 4, 5, 8, 10, 20, 40$. Working modulo 41:

$$3^1 = 3$$

$$3^2 = 9$$

$$3^4 = 81 = 2 \times 41 - 1 \equiv -1$$

$$3^5 = 3^4 \times 3 \equiv -3 \equiv 38$$

$$3^8 = \left(3^4\right)^2 \equiv (-1)^2 = 1$$

None of 3^1, 3^2, 3^4, 3^5 is congruent to 1 modulo 41, but $3^8 \equiv 1 \pmod{41}$. So 8 is the smallest possible order that works, and the order of 3 modulo 41 is 8.

(c) Since $2026 = 8 \times 253 + 2$, using $3^8 \equiv 1 \pmod{41}$ from part (b):

$$3^{2026} = \left(3^8\right)^{253} \times 3^2 \equiv 1^{253} \times 9 = 9 \pmod{41}$$

The remainder when 3^{2026} is divided by 41 is 9.

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]**

Solution

Fermat's little theorem states that, if p is prime and p does not divide b, then

$$b^{p-1} \equiv 1 \pmod{p}$$

Case 1: $19 \mid x$**.** Then $x \equiv 0 \pmod{19}$, and both sides of the congruence are $\equiv 0 \pmod{19}$. So $x \equiv 0 \pmod{19}$ is a solution.

Case 2: $19 \nmid x$**.** Since 19 is prime, Fermat's little theorem gives

$$x^{18} \equiv 1 \pmod{19}$$

Writing each exponent in terms of multiples of 18:

$$201 = 11 \times 18 + 3, \qquad 110 = 6 \times 18 + 2, \qquad 91 = 5 \times 18 + 1$$

so

$$x^{201} = \left(x^{18}\right)^{11} x^3 \equiv x^3 \pmod{19}$$

$$x^{110} = \left(x^{18}\right)^{6} x^2 \equiv x^2 \pmod{19}$$

$$x^{91} = \left(x^{18}\right)^{5} x \equiv x \pmod{19}$$

The congruence therefore becomes

$$x^3 + 4x^2 \equiv 7x \pmod{19}$$

$$x\left(x^2 + 4x - 7\right) \equiv 0 \pmod{19}$$

So 19 divides $x\left(x^2 + 4x - 7\right)$. As 19 is prime and $19 \nmid x$, it follows that $19 \mid x^2 + 4x - 7$, that is

$$x^2 + 4x - 7 \equiv 0 \pmod{19}$$

Completing the square:

$$(x+2)^2 - 11 \equiv 0 \pmod{19}$$

$$(x+2)^2 \equiv 11 \pmod{19}$$

Now $11 \equiv 11 + 2 \times 19 = 49 = 7^2 \pmod{19}$, so

$$(x+2)^2 - 7^2 \equiv 0 \pmod{19}$$

$$(x+2-7)(x+2+7) \equiv 0 \pmod{19}$$

$$(x-5)(x+9) \equiv 0 \pmod{19}$$

Since 19 is prime, it divides $x - 5$ or $x + 9$, so

$$x \equiv 5 \pmod{19} \quad \text{or} \quad x \equiv -9 \equiv 10 \pmod{19}$$

Neither of these is divisible by 19, so both belong to this case.

Combining the two cases, the solutions are

$$x \equiv 0 \pmod{19}, \qquad x \equiv 5 \pmod{19}, \qquad x \equiv 10 \pmod{19}$$

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]**

Solution

(a) Fermat's little theorem states that, if p is prime and p does not divide a, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Since 11 is prime and does not divide 2, Fermat's little theorem gives

$$2^{10} \equiv 1 \pmod{11}$$

As $340 = 34 \times 10$, this gives

$$\begin{aligned} 2^{340} &= \left(2^{10}\right)^{34} \\ &\equiv 1^{34} \\ &\equiv 1 \pmod{11} \end{aligned}$$

Since 31 is prime and does not divide 2, Fermat's little theorem gives

$$2^{30} \equiv 1 \pmod{31}$$

As $340 = 11 \times 30 + 10$, this gives

$$\begin{aligned} 2^{340} &= \left(2^{30}\right)^{11} \times 2^{10} \\ &\equiv 1^{11} \times 2^{10} \\ &\equiv 1024 \pmod{31} \end{aligned}$$

Since $1024 = 33 \times 31 + 1$, it follows that $1024 \equiv 1 \pmod{31}$, so

$$2^{340} \equiv 1 \pmod{31}$$

as required.

(b) By part (a), $2^{340} - 1$ is divisible by 11 and by 31. These are distinct primes, so their product $11 \times 31 = 341$ also divides $2^{340} - 1$. Hence

$$2^{340} \equiv 1 \pmod{341}$$

(c) Take $n = 341$. Then $n > 1$, and by part (b), $2^{n-1} = 2^{340} \equiv 1 \pmod{341}$, so n satisfies both conditions of the statement. However, $341 = 11 \times 31$ is not prime. So $n = 341$ is a counterexample, and the statement is false.

(d) (i) Work modulo 31. Since 31 is prime and does not divide 3, Fermat's little theorem gives $3^{30} \equiv 1 \pmod{31}$. As $340 = 11 \times 30 + 10$, this gives

$$\begin{aligned} 3^{340} &= \left(3^{30}\right)^{11} \times 3^{10} \\ &\equiv 1^{11} \times 3^{10} \\ &\equiv 3^{10} \pmod{31} \end{aligned}$$

Now $3^5 = 243 = 7 \times 31 + 26$, so $3^5 \equiv 26 \equiv -5 \pmod{31}$. Squaring:

$$3^{10} \equiv (-5)^2 = 25 \pmod{31}$$

So $3^{340} \equiv 25 \pmod{31}$, and therefore $3^{340} \not\equiv 1 \pmod{31}$.

If $3^{340} \equiv 1 \pmod{341}$, then 341 would divide $3^{340} - 1$. Since 31 divides 341, 31 would then divide $3^{340} - 1$, giving $3^{340} \equiv 1 \pmod{31}$, which is false. Hence

$$3^{340} \not\equiv 1 \pmod{341}$$

(ii) Suppose 341 were prime. Since 341 does not divide 3, Fermat's little theorem with $p = 341$ and $a = 3$ would give $3^{340} \equiv 1 \pmod{341}$. This contradicts part (d)(i), so 341 cannot be prime. This argument needs only the result of part (d)(i), not the factorisation $341 = 11 \times 31$.

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]**

Solution

Let $N = 26^{27} + 27^{26}$, the order of G. By Lagrange's theorem, the order of any subgroup of G divides N. So the task is to decide whether 15, 17 and 35 divide N, working modulo the primes 3, 5, 7 and 17.

Fermat's little theorem states that, if p is prime and p does not divide a, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Modulo 3: $26 \equiv -1$ and $27 \equiv 0 \pmod 3$. Since 27 is odd, $(-1)^{27} = -1$, so

$$N \equiv (-1)^{27} + 0^{26} \equiv -1 \equiv 2 \pmod 3$$

So 3 does not divide N, and therefore $15 = 3 \times 5$ does not divide N.

Modulo 5: $26 \equiv 1 \pmod 5$, so $26^{27} \equiv 1$. Also $27 \equiv 2 \pmod 5$, and by Fermat's little theorem $2^4 \equiv 1 \pmod 5$. Since $26 = 4 \times 6 + 2$:

$$27^{26} \equiv 2^{26} = \left(2^4\right)^6 \times 2^2 \equiv 1^6 \times 4 = 4 \pmod 5$$

$$N \equiv 1 + 4 = 5 \equiv 0 \pmod 5$$

So 5 divides N.

Modulo 7: $26 \equiv 5 \pmod 7$, and by Fermat's little theorem $5^6 \equiv 1 \pmod 7$. Since $27 = 6 \times 4 + 3$:

$$26^{27} \equiv 5^{27} = \left(5^6\right)^4 \times 5^3 \equiv 125 = 126 - 1 \equiv -1 \pmod 7$$

Also $27 \equiv -1 \pmod 7$, and 26 is even, so $27^{26} \equiv (-1)^{26} = 1 \pmod 7$. Hence

$$N \equiv -1 + 1 = 0 \pmod 7$$

So 7 divides N. As 5 and 7 are distinct primes that both divide N, their product 35 divides N.

Modulo 17: $26 \equiv 9$ and $27 \equiv 10 \pmod{17}$. Neither is divisible by 17, so by Fermat's little theorem $9^{16} \equiv 1$ and $10^{16} \equiv 1 \pmod{17}$. Since $27 = 16 + 11$ and $26 = 16 + 10$, $26^{27} \equiv 9^{11}$ and $27^{26} \equiv 10^{10} \pmod{17}$.

For the first term, $9^2 = 81 = 85 - 4 \equiv -4$, so $9^4 \equiv 16 \equiv -1$ and $9^8 \equiv 1 \pmod{17}$. Then

$$9^{11} = 9^8 \times 9^2 \times 9 \equiv 1 \times (-4) \times 9 = -36 \equiv 15 \pmod{17}$$

For the second term, $10^2 = 100 = 102 - 2 \equiv -2 \pmod{17}$, so

$$10^{10} = \left(10^2\right)^5 \equiv (-2)^5 = -32 \equiv 2 \pmod{17}$$

Hence

$$N \equiv 15 + 2 = 17 \equiv 0 \pmod{17}$$

So 17 divides N.

Conclusion: Since 15 does not divide N, Lagrange's theorem shows that G cannot have a subgroup of order 15.

Both 17 and 35 divide N, so Lagrange's theorem does not rule them out, and such subgroups can occur. For example, if G is cyclic with generator g, then $g^{N/17}$ has order 17 and $g^{N/35}$ has order 35. Each of these elements generates a subgroup of that order.

Therefore 17 and 35 are possible orders for a subgroup of G, but 15 is not.

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]**

Solution

(a) Suppose that p divides n. Then p divides n^2. Since p also divides $n^2 + 1$, it divides the difference

$$(n^2 + 1) - n^2 = 1$$

This is impossible, because $p \geq 3$. Hence p does not divide n.

Since p divides $n^2 + 1$, we have $n^2 \equiv -1 \pmod{p}$. Squaring both sides gives

$$n^4 = \left(n^2\right)^2 \equiv (-1)^2 = 1 \pmod{p}$$

so $n^4 \equiv 1 \pmod{p}$, as required.

(b) (i) Let d be the order of n modulo p. By part (a), $n^4 \equiv 1 \pmod{p}$, so $d \leq 4$. Also $n^2 \equiv -1 \pmod{p}$.

If $d = 1$, then $n \equiv 1 \pmod{p}$, so $n^2 \equiv 1 \pmod{p}$.

If $d = 2$, then $n^2 \equiv 1 \pmod{p}$.

If $d = 3$, then $n^3 \equiv 1 \pmod{p}$, so $n^4 = n \times n^3 \equiv n \pmod{p}$. Since $n^4 \equiv 1 \pmod{p}$, this gives $n \equiv 1 \pmod{p}$, and so $n^2 \equiv 1 \pmod{p}$.

In each of these cases $n^2 \equiv 1 \pmod{p}$. Combining this with $n^2 \equiv -1 \pmod{p}$ gives

$$1 \equiv -1 \pmod{p} \implies p \text{ divides } 2$$

This is impossible, since p is an odd prime. Hence none of $d = 1, 2, 3$ is possible, and the order of n modulo p is 4.

(ii) Fermat's little theorem states that, if p is prime and p does not divide a, then

$$a^{p-1} \equiv 1 \pmod{p}$$

By part (a), p does not divide n, and p is prime, so Fermat's little theorem gives

$$n^{p-1} \equiv 1 \pmod{p}$$

Divide $p - 1$ by 4: write $p - 1 = 4q + r$, where q and r are integers with $0 \leq r \leq 3$. Then, using $n^4 \equiv 1 \pmod{p}$:

$$n^{p-1} = n^{4q+r} = \left(n^4\right)^q \times n^r \equiv 1^q \times n^r = n^r \pmod{p}$$

so $n^r \equiv 1 \pmod{p}$.

If r were 1, 2 or 3, then r would be a positive integer less than 4 with $n^r \equiv 1 \pmod{p}$, contradicting part (b)(i), which shows that the order of n modulo p is 4. Hence $r = 0$, so $p - 1 = 4q$ and 4 divides $p - 1$, that is

$$p \equiv 1 \pmod{4}$$

as required.

(c) Dividing 2027 by 4 gives

$$2027 = 4 \times 506 + 3$$

so $2027 \equiv 3 \pmod{4}$. Suppose some integer n has $n^2 + 1$ divisible by 2027. Since 2027 is an odd prime, part (b)(ii) applies with $p = 2027$ and gives $2027 \equiv 1 \pmod{4}$, which contradicts $2027 \equiv 3 \pmod{4}$. Hence there is no integer n for which $n^2 + 1$ is divisible by 2027.

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]**

Solution

(a) Since $p \geq 5$ is prime, p does not divide 2, 3 or 6. Fermat's little theorem states that, if p is prime and p does not divide a, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Hence $2^{p-1} \equiv 1$, $3^{p-1} \equiv 1$ and $6^{p-1} \equiv 1 \pmod{p}$.

Let $S = 2^{p-2} + 3^{p-2} + 6^{p-2}$. Multiplying by 6:

$$\begin{aligned} 6S &= 6 \times 2^{p-2} + 6 \times 3^{p-2} + 6 \times 6^{p-2} \\ &= 3 \times 2^{p-1} + 2 \times 3^{p-1} + 6^{p-1} \\ &\equiv 3 \times 1 + 2 \times 1 + 1 \pmod{p} \\ &\equiv 6 \pmod{p} \end{aligned}$$

So p divides $6S - 6 = 6(S-1)$. Since p is prime and does not divide 6, p must divide $S - 1$, so

$$2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \pmod{p}$$

as required.

(b) Let $p > 5$ be prime. Using part (a):

$$2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv 0 \pmod{p}$$

so p divides N if $a^{29} \equiv a^{p-2} \pmod{p}$ for each of $a = 2, 3, 6$.

For each such a, p does not divide a, so $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem. Therefore, for any integer $k \geq 0$, the laws of indices give

$$a^{k(p-1)+(p-2)} = \left(a^{p-1}\right)^k \times a^{p-2} \equiv a^{p-2} \pmod{p}$$

So it is enough that $29 = k(p-1) + (p-2)$ for some integer $k \geq 0$. Rearranging:

$$29 + 1 = k(p-1) + (p-1) \implies 30 = (k+1)(p-1)$$

so $p-1$ must be a factor of 30. The factors of 30 are $1, 2, 3, 5, 6, 10, 15, 30$, giving $p = 2, 3, 4, 6, 7, 11, 16, 31$. The primes greater than 5 in this list are 7, 11 and 31.

$p = 7$: here $p - 2 = 5$ and $29 = 4 \times 6 + 5$. For $a = 2, 3, 6$, Fermat's little theorem gives

$$a^{29} = \left(a^6\right)^4 \times a^5 \equiv a^5 \pmod{7}$$

so part (a) with $p = 7$ gives

$$N \equiv 2^5 + 3^5 + 6^5 - 1 \equiv 1 - 1 \equiv 0 \pmod{7}$$

$p = 11$**:** here $p - 2 = 9$ and $29 = 2 \times 10 + 9$. For $a = 2, 3, 6$, Fermat's little theorem gives

$$a^{29} = \left(a^{10}\right)^2 \times a^9 \equiv a^9 \pmod{11}$$

so part (a) with $p = 11$ gives

$$N \equiv 2^9 + 3^9 + 6^9 - 1 \equiv 1 - 1 \equiv 0 \pmod{11}$$

$p = 31$**:** here $p - 2 = 29$, so part (a) with $p = 31$ gives directly

$$N = 2^{29} + 3^{29} + 6^{29} - 1 \equiv 1 - 1 \equiv 0 \pmod{31}$$

Hence 7, 11 and 31 each divide N, so three prime factors of N greater than 5 are 7, 11 and 31.