OPTIONAL PURE / NUMBER THEORY

Fermat's Little Theorem

Mark scheme 7 questions · 52 marks

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

Questions

Question	Marks by part	Marks	Page
Question 1		5	4
Question 2	(a) 1 (b) 3 (c) 1	5	5
Question 3		6	6
Question 4	(a) 4 (b) 1 (c) 1 (d)(i) 4 (d)(ii) 1	11	7
Question 5		8	9
Question 6	(a) 2 (b)(i) 2 (b)(ii) 3 (c) 1	8	10
Question 7	(a) 4 (b) 5	9	11
	Total	**52**	

Reading the mark scheme

These rules apply throughout, unless a note says otherwise.

Marks

Every mark is worth one, so **M1 A1** on a row is two marks. Only marks coded ft follow through.

Code	Meaning
M1	Method: a correct method, applied to this question. A slip doesn't cost it if the method is clear. A formula must be used, not just quoted.
dM1	Dependent method: as M1, but only if the method mark before it was earned, unless its note names another.
A1	Accuracy: a correct answer or step. It needs the method mark it follows.
A1ft	As A1, following through from an earlier answer that the note names.
A1 AG	The last accuracy mark of the working that reaches a printed result: complete working, with no errors.
B1	A correct value, fact or statement. It needs no method mark.
B1ft	As B1, following through from an earlier answer that the note names.
E1	A written explanation, interpretation or conclusion. Concluding a proof by induction needs every earlier mark.

Abbreviations

ft and AG qualify a code in the Marks column. The others appear in the notes. A grey line gives the rule where the name alone doesn't.

ft	follow through Correct work from the student's own earlier wrong value earns the mark.	**AG**	answer given The answer is printed in the question, so every step to it must be shown.
cao	correct answer only No follow-through from an earlier error.	**cso**	correct solution only No error anywhere in the part, not just in its answer.
oe	or equivalent	**awrt**	answers which round to
soi	seen or implied Earned if written, or if later working shows it was used.	**isw**	ignore subsequent working A correct answer, once reached, isn't spoiled by later working.
SC	special case Credit, as the note says, for work outside the main method.	**their**	the student's own earlier value
condone	a slip that doesn't cost the mark	[ ]	working the mark doesn't need
s.f.	significant figures	**d.p.**	decimal places

Reading the scheme

- Each row is a line of working, with the marks it earns beside it. Where a row carries two marks, each note starts with its code.
- [$\boldsymbol{n}$] ends each part with its total.
- A shaded *Alternative* is a second method for the same total. Mark an answer by the method it follows.
- Any other valid method earns the equivalent marks, unless the question names a method or says *hence*.
- A sketch earns one B1 for each feature named below its figure.

Accuracy and answers

- Unless a question says otherwise, give answers to 3 significant figures, and angles in degrees to 1 decimal place. Angles in radians take 3 significant figures.
- A final answer with more figures is accepted if it rounds to the scheme's value; one with fewer is not. An answer spoiled by rounding too early loses its accuracy mark.
- Where a question asks for an exact answer, a decimal loses the final accuracy mark. Otherwise either is accepted.
- Wrong or missing units cost nothing unless the question asks for them.
- An omitted $\mathrm{d}\theta$, $\mathrm{d}x$ or $\mathrm{d}u$ in an integral is not penalised where the variable of integration is clear from the integrand and the limits. It is penalised where it is genuinely ambiguous: a substitution part-way through, two variables in play, or limits in the wrong variable.
- A correct answer with no working earns full marks, unless the question needs the working: show that, prove, hence, a method it names, or an exact answer. A wrong answer with no working earns nothing. Calculator answers are treated the same way.
- A correct answer, once reached, isn't spoiled by later working (isw).

Value of g

- Take $g = 9.8\,\mathrm{m\,s^{-2}}$ unless a question states a value, which is then the only one accepted. Answers that use $g = 9.8$ may be given to 2 or 3 significant figures.
- Where a question doesn't state g, an answer worked with $g = 10$ throughout earns the same marks, keeping any value printed in the question. The worked solutions list the final answers with $g = 10$.

Question	Scheme	Marks	Notes
1	$37 \equiv 3,\ 56 \equiv 5 \pmod{17}$ $3^{16} \equiv 5^{16} \equiv 1 \pmod{17}$ $200 = 12 \times 16 + 8 \Rightarrow 3^{200} + 5^{200} \equiv \ldots$	**M1**	Uses $a^{16} \equiv 1 \pmod{17}$ to reduce the exponent 200 modulo 16 for at least one term; bases may be reduced modulo 17 before or after. Not for quoting the theorem alone.
	$37^{200} + 56^{200} \equiv 3^8 + 5^8 \pmod{17}$	**A1**	oe, such as $37^8 + 56^8$.
	$3^4 = 81 \equiv -4,\ 5^2 = 25 \equiv 8,\ 5^4 \equiv \ldots$	**M1**	Evaluates their reduced power of 3 or 5 modulo 17 by any valid method, such as repeated squaring. Condone arithmetic slips.
	$3^8 \equiv -1,\ 5^8 \equiv -1 \pmod{17}$	**A1**	Both, each as -1 or 16.
	$37^{200} + 56^{200} \equiv -2 \equiv 15 \pmod{17}$	**A1**	15 only; -2 alone does not score.
	Total for Question 1	**5**	

Question	Scheme	Marks	Notes
2(a)	$3^{40} \equiv 1 \pmod{41} \Rightarrow$ order divides 40 6 does not divide 40	**E1**	States that the order divides 40, from Fermat's little theorem, $3^{40} \equiv 1$ or Lagrange's theorem, and that 6 does not divide 40.
		[1]	
2(b)	$3^1 = 3,\ 3^2 = 9$ $3^4 = 81 \equiv \ldots \pmod{41}$	**M1**	Evaluates powers of 3 modulo 41 at two or more divisors of 40 other than 1, by any method. Condone arithmetic slips.
	$3^4 \equiv -1,\ 3^5 \equiv -3 \pmod{41}$ $3^1, 3^2, 3^4, 3^5 \not\equiv 1$	**A1**	$3^4 \equiv -1$ or 40, with 3^1, 3^2, 3^4 and 3^5 not 1; 3^5 may be omitted if the order is deduced to divide 8.
	$3^8 = \left(3^4\right)^2 \equiv (-1)^2 = 1$ $\Rightarrow$ order 8	**A1**	Order 8, with $3^8 \equiv 1$ shown. cso.
		[3]	
2(c)	$3^{2026} = \left(3^8\right)^{253} \times 3^2 \equiv 9 \pmod{41}$	**B1**	9, using $3^8 \equiv 1$ or $2026 \equiv 2 \pmod{8}$.
		[1]	
	Total for Question 2	**5**	

Question	Scheme	Marks	Notes
3	$x \equiv 0 \pmod{19}$	**B1**	Stated as a solution or listed among the final answers.
	$x^{18} \equiv 1 \pmod{19}$ $x^{201} \equiv x^3,\ x^{110} \equiv x^2,\ x^{91} \equiv x$	**M1**	Uses $x^{18} \equiv 1$ to reduce at least two of the powers. Condone a slip in one remainder.
	$x^3 + 4x^2 \equiv 7x$ $x^2 + 4x - 7 \equiv 0 \pmod{19}$	**A1**	Or $x(x^2 + 4x - 7) \equiv 0$ oe.
	$(x+2)^2 \equiv 11 \equiv 49 \pmod{19}$ $\Rightarrow x + 2 \equiv \ldots$	**M1**	Completes the square or factorises their quadratic modulo 19, adding multiples of 19, or tests residues systematically. Condone arithmetic slips.
	$(x-5)(x+9) \equiv 0 \pmod{19}$	**A1**	One correct non-zero solution, or $(x-5)(x+9) \equiv 0$ or $x + 2 \equiv \pm 7$ oe.
	$x \equiv 5, \quad x \equiv 10 \pmod{19}$	**A1**	Both, with $0 \leq a \leq 18$, and no values other than these and $x \equiv 0$.
	Total for Question 3	**6**	

Question	Scheme	Marks	Notes
4(a)	$2^{10} \equiv 1 \pmod{11}$ $2^{340} = \left(2^{10}\right)^{34} \equiv \ldots$	**M1**	Uses Fermat's little theorem with $p = 11$ to give $2^{10} \equiv 1$ and writes 2^{340} as a power of 2^{10}.
	$\equiv 1^{34} \equiv 1 \pmod{11}$	**A1**	
	$2^{30} \equiv 1 \pmod{31}$ $2^{340} = \left(2^{30}\right)^{11} \times 2^{10} \equiv 2^{10} \pmod{31}$	**M1**	Uses Fermat's little theorem with $p = 31$ and reduces 2^{340} to 2^{10} or another power below 2^{30}. Condone a slip in the quotient.
	$2^{10} = 1024 = 33 \times 31 + 1$ $\Rightarrow 2^{340} \equiv 1 \pmod{31}$	**A1 AG**	$2^{10} \equiv 1 \pmod{31}$ shown correctly, as by $1024 = 33 \times 31 + 1$ or $2^5 \equiv 1$, and the printed result concluded without error.
		[4]	
4(b)	11 and 31 are distinct primes dividing $2^{340} - 1$ $\Rightarrow 341 \mid 2^{340} - 1 \Rightarrow 2^{340} \equiv 1 \pmod{341}$	**B1**	Needs 11 and 31 stated coprime or distinct primes. Not for multiplying the two congruences.
		[1]	
4(c)	$n = 341 > 1$ and $2^{340} \equiv 1 \pmod{341}$ but $341 = 11 \times 31$ is not prime: a counterexample	**E1**	States that 341 satisfies the condition, by part (b), but is not prime, so is a counterexample. Condone $n > 1$ not stated.
		[1]	
4(d)(i)	$3^{30} \equiv 1 \pmod{31}$ $3^{340} = \left(3^{30}\right)^{11} \times 3^{10}$	**M1**	Uses Fermat's little theorem modulo 31 to reduce 3^{340} to a power below 3^{30}.
	$\equiv 3^{10} \pmod{31}$	**A1**	oe, such as $\left(3^5\right)^2$.
	$3^5 = 243 \equiv -5 \pmod{31} \Rightarrow 3^{10} \equiv \ldots$	**M1**	Evaluates their power of 3 modulo 31 by any valid method, such as reducing 3^5 or 3^3, or dividing $3^{10} = 59\,049$ by 31. Condone arithmetic slips.
	$3^{340} \equiv 25 \not\equiv 1 \pmod{31}$ $31 \mid 341 \Rightarrow 3^{340} \not\equiv 1 \pmod{341}$	**A1 AG**	$3^{340} \equiv 25 \pmod{31}$ oe, such as -6, then a conclusion using $31 \mid 341$ that $3^{340} \not\equiv 1 \pmod{341}$.
		[4]	

Question 4 continued

Question	Scheme	Marks	Notes
4(d)(ii)	If 341 were prime, $3^{340} \equiv 1 \pmod{341}$, contradicting (d)(i)	**E1**	States that Fermat's little theorem with $p = 341$, $a = 3$ would give $3^{340} \equiv 1 \pmod{341}$, contradicting (d)(i). Not for using $341 = 11 \times 31$.
		[1]	
	Total for Question 4	**11**	

Question	Scheme	Marks	Notes
5	$N \equiv (-1)^{27} + 0^{26} \equiv 2 \pmod 3$ $\Rightarrow 3 \nmid N \Rightarrow 15 \nmid N$	**B1**	Needs $N \equiv 2$ (or -1) and the conclusion that 15 does not divide N.
	$27^{26} \equiv 2^{26} = \left(2^4\right)^6 \times 2^2 \equiv \ldots \pmod 5$	**M1**	Uses $a^{p-1} \equiv 1$ to reduce an exponent modulo $p-1$, working modulo 5, 7 or 17, as $2^{26} \equiv 2^2 \pmod 5$. Condone arithmetic slips.
	$N \equiv 1 + 4 \equiv 0 \pmod 5$	**A1**	
	$26^{27} \equiv 5^{27} \equiv 5^3 \equiv -1,\ 27^{26} \equiv 1 \pmod 7$ $N \equiv 0 \pmod 7$	**A1**	$N \equiv 0 \pmod 7$.
	$26^{27} \equiv 9^{11},\ 27^{26} \equiv 10^{10} \pmod{17}$ $9^2 \equiv -4,\ 10^2 \equiv -2 \Rightarrow \ldots$	**M1**	Evaluates powers of their residues of 26 and 27 modulo 17 by any valid method, such as repeated squaring. Condone arithmetic slips.
	$9^{11} \equiv 15,\ 10^{10} \equiv 2 \pmod{17}$	**A1**	Both residues, oe such as -2 for 15.
	$N \equiv 15 + 2 \equiv 0 \pmod{17}$	**A1**	cso.
	$5 \mid N,\ 7 \mid N \Rightarrow 35 \mid N$ Subgroup orders divide N (Lagrange): 15 not possible; 17 and 35 possible	**E1**	States that a subgroup's order divides $\lvert G \rvert$, rejecting 15, accepting 17, and 35 from 5 and 7 both dividing N. No example of such a subgroup is needed.
	Total for Question 5	**8**	

Question	Scheme	Marks	Notes
6(a)	$n^2 \equiv -1 \pmod{p}$ $p \mid n \Rightarrow p \mid (n^2+1) - n^2 = 1$	**M1**	Uses $n^2 \equiv -1 \pmod{p}$ and argues that $p \mid n$ leads to $p \mid 1$, or $0 \equiv -1 \pmod{p}$.
	$p \nmid n$ $n^4 = \left(n^2\right)^2 \equiv (-1)^2 = 1 \pmod{p}$	**A1 AG**	Both results: a contradiction stated for $p \mid n$, and $n^2 \equiv -1$ squared to give $n^4 \equiv 1 \pmod{p}$.
		[2]	
6(b)(i)	$d \leq 4$; $d = 1$ or 2: $n^2 \equiv 1 \pmod{p}$ $d = 3$: $n^4 \equiv n \Rightarrow n \equiv 1 \Rightarrow n^2 \equiv 1$	**M1**	Shows each of $d = 1, 2, 3$ gives $n^2 \equiv 1 \pmod{p}$, or uses the order dividing 4 to leave $d = 1, 2$.
	$n^2 \equiv -1 \Rightarrow 1 \equiv -1 \pmod{p} \Rightarrow p \mid 2$ Impossible as p is odd, so order is 4	**A1 AG**	Contradiction from p odd for every case, with $d \leq 4$ from (a), concluding the order is 4.
		[2]	
6(b)(ii)	$p \nmid n \Rightarrow n^{p-1} \equiv 1 \pmod{p}$	**B1**	Needs $p \nmid n$ cited. Not for quoting the theorem alone.
	$p - 1 = 4q + r,\ 0 \leq r \leq 3$ $n^{p-1} = \left(n^4\right)^q n^r \equiv n^r \Rightarrow n^r \equiv 1$	**M1**	Writes $p - 1 = 4q + r$ and uses $n^4 \equiv 1$ to reach $n^r \equiv 1$, or uses the order dividing every k with $n^k \equiv 1$, or writes $n^{p-1} = \left(n^2\right)^{(p-1)/2} \equiv (-1)^{(p-1)/2}$.
	$r = 1, 2, 3$ contradicts order $4 \Rightarrow r = 0$ $4 \mid p - 1 \Rightarrow p \equiv 1 \pmod{4}$	**A1 AG**	Rules out $r = 1, 2, 3$ by the order 4 from (b)(i), or deduces $4 \mid p - 1$ from it, or $(p-1)/2$ even from $-1 \not\equiv 1$; concludes $p \equiv 1 \pmod{4}$.
		[3]	
6(c)	$2027 = 4 \times 506 + 3 \Rightarrow 2027 \equiv 3 \pmod{4}$ Contradicts (b)(ii), so no such n	**B1**	Needs $2027 \equiv 3 \pmod{4}$ and a conclusion citing (b)(ii).
		[1]	
	Total for Question 6	**8**	

Question	Scheme	Marks	Notes
7(a)	$6\left(2^{p-2}+3^{p-2}+6^{p-2}\right)$ $=6\times 2^{p-2}+6\times 3^{p-2}+6\times 6^{p-2}$	**M1**	Multiplies the sum by 6, or each term by its base, to obtain powers $p-1$.
	$=3\times 2^{p-1}+2\times 3^{p-1}+6^{p-1}$	**A1**	oe.
	$\equiv 3\times 1+2\times 1+1\equiv 6 \pmod p$	**M1**	Uses $a^{p-1}\equiv 1 \pmod p$ for each of $a=2,3,6$ in their expression. Condone arithmetic slips.
	p does not divide 6 $\Rightarrow 2^{p-2}+3^{p-2}+6^{p-2}\equiv 1 \pmod p$	**A1 AG**	Correct $\equiv 6$, or $2^{-1}+3^{-1}+6^{-1}\equiv 1$, leading without error to the printed result, citing p prime, $p\geq 5$, so p does not divide 2, 3 or 6.
		[4]	
7(b)	$a^{p-1}\equiv 1 \pmod p$, so $a^{29}\equiv a^{p-2}$ if $29=k(p-1)+(p-2)$	**M1**	Uses Fermat's little theorem to relate a^{29} to a^{p-2}, giving a condition equivalent to $29\equiv p-2$ modulo $p-1$.
	$30=(k+1)(p-1)\Rightarrow (p-1)$ divides 30	**A1**	oe, such as $p-1$ a factor of 30, or $29\equiv p-2$ modulo $p-1$ checked for each of three primes found by trial.
	$p=7,\ 11,\ 31$	**A1**	All three, with no other primes greater than 5.
	Applies part (a) for $p=7,\ 11,\ 31$: $a^{29}\equiv a^{p-2} \pmod p$ $\Rightarrow N\equiv 2^{p-2}+3^{p-2}+6^{p-2}-1\equiv 0 \pmod p$	**M1**	Applies part (a) to deduce $N\equiv 0$ modulo at least one of 7, 11, 31, with $a^{29}\equiv a^{p-2}$ shown generally or for that prime.
	$N\equiv 1-1\equiv 0$ modulo 7, 11 and 31	**A1**	cso. Divisibility shown for all three primes using part (a); $p=31$ directly. Not for direct evaluation of N alone.
		[5]	
	Total for Question 7	**9**	