OPTIONAL PURE / NUMBER THEORY

Modular Arithmetic and Quadratic Residues

Mark scheme 10 questions · 88 marks

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

Questions

Question	Marks by part	Marks	Page
Question 1	(a) 2 (b) 4	6	4
Question 2	(a) 3 (b) 2 (c) 3	8	5
Question 3	(a)(i) 1 (a)(ii) 7 (b) 3	11	6
Question 4		6	7
Question 5	(a) 2 (b) 3 (c)(i) 3 (c)(ii) 2	10	8
Question 6		5	9
Question 7	(a) 4 (b) 3	7	10
Question 8	(a) 3 (b) 4	7	11
Question 9	(a) 1 (b) 3 (c) 4 (d) 4	12	12
Question 10	(a) 4 (b) 1 (c) 2 (d) 2 (e) 3 (f) 4	16	13
	Total	**88**	

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(a)	a divides $81 - 9 = 72$ $72 = 2^3 \times 3^2 \Rightarrow$ divisors ...	**M1**	Uses a divides $3^4 - 9$ and attempts its divisors, or tests values of a above 9 systematically.
	$a = 12,\ 18,\ 24,\ 36,\ 72$	**A1**	All five values and no others.
		[2]	
1(b)	$x^3 - x \equiv 0 \pmod{p}$ $x(x-1)(x+1) \equiv 0 \pmod{p}$	**M1**	Rearranges and factorises fully to $x(x-1)(x+1)$, divisible by p or congruent to 0.
	p prime, so p divides x, $x-1$ or $x+1$ $\Rightarrow x \equiv 0,\ 1$ or $-1 \pmod{p}$	**A1 AG**	Uses that a prime dividing a product divides one of its factors, reaching all three congruences. A0 if primality is not used.
	$x = 3$: $3^3 - 3 = 24 \equiv 0 \pmod{8}$	**B1**	Any $x \equiv 3$ or $5 \pmod{8}$, with $x^3 - x$ shown divisible by 8 or $x^3 \equiv x$ verified.
	$3 \not\equiv 0,\ 1,\ 7 \pmod{8}$	**B1**	States their suitable value is not congruent to 0, 1 or -1 (or 7) modulo 8.
		[4]	
Total for Question 1		**6**	

Question	Scheme	Marks	Notes
2(a)	$a-b=pn, \quad c-d=qn$ $ac-bd=a(c-d)+d(a-b)$	**M1**	Writes $a-b$ and $c-d$ as integer multiples of n and expresses $ac-bd$ using them, by adding and subtracting a term or substituting $a=b+pn$, $c=d+qn$.
	$ac-bd=aqn+dpn=n(aq+dp)$ n divides $ac-bd$, so $ac\equiv bd \pmod{n}$	**A1 AG**	$ac-bd$ reached without error as n times an expression stated to be an integer, with the conclusion $ac\equiv bd \pmod{n}$.
	$k=1$: $a\equiv b$; $a^m\equiv b^m$ and $a\equiv b$ $\Rightarrow a^{m+1}\equiv b^{m+1} \pmod{n}$ True for all positive integers k	**E1**	Uses the product result with $a^m\equiv b^m$ and $a\equiv b$, or applies it repeatedly, and concludes for all positive integers k. Available without the earlier marks.
		[3]	
2(b)	$x=1,\ 6,\ 11$	**B1**	All three and no others.
	$6\times 6\equiv 6\times 1 \pmod{15}$ but $6\not\equiv 1 \pmod{15}$, so cancelling fails	**E1**	Uses two solutions, such as 6 and 1, whose products with 6 are congruent though they are not, and concludes that cancelling 6 fails.
		[2]	
2(c)	$x\equiv r \Rightarrow x^3\equiv r^3,\ 5x\equiv 5r$ $\Rightarrow f(x)\equiv f(r) \pmod{11}$, $0\le r\le 10$	**E1**	Explains, citing part (a) for x^3 and $5x$, that $f(x)\equiv f(r)$ where r is the remainder on division by 11, so only 0 to 10 need checking.
	$f(r)$ mod 11 for $r=0,1,\ldots,10$ $[4,10,0,2,0,0,8,8,6,8,9]$	**M1**	Evaluates $f(r)$ modulo 11 for every residue in 0 to 10, or another complete set such as -5 to 5. Condone arithmetic slips.
	$x\equiv 2,\ 4,\ 5 \pmod{11}$	**A1**	All three as congruences modulo 11, and no others.
		[3]	
Total for Question 2		**8**	

Question	Scheme	Marks	Notes
3(a)(i)	$n = 5k+1,\ 5k+2,\ 5k+3,\ 5k+4$	**B1**	All four forms. Equivalents such as $5k \pm 1$, $5k \pm 2$ accepted; condone no condition on k.
		[1]	
3(a)(ii)	$2^5 = 32 = 31+1 \Rightarrow 2^5 \equiv 1 \pmod{31}$	**B1**	Needs 32 written as $31+1$, or 31 divides $32-1$, not the congruence alone.
	$f(n) = 1 + 2^n + 2^{2n} + 2^{3n} + 2^{4n}$ $n = 5k+r \Rightarrow 2^n = \left(2^5\right)^k \times 2^r \equiv 2^r$	**M1**	Uses $n = 5k+r$ and $2^5 \equiv 1$ to reduce 2^n to 2^r, or each term of $f(n)$ to its value at r. Condone slips.
	$f(n) \equiv 1 + 2^r + 2^{2r} + 2^{3r} + 2^{4r} \pmod{31}$	**A1**	
	$2^6 \equiv 2,\ 2^8 \equiv 8,\ 2^9 \equiv 16,\ 2^{12} \equiv 4,\ 2^{16} \equiv 2$	**M1**	Uses $2^5 \equiv 1$ to reduce at least one power of 2 above 2^4, or works each case numerically modulo 31.
	$r=1:\ 1+2+4+8+16 = 31 \equiv 0$ $r=2:\ 1+4+16+2+8 = 31 \equiv 0$	**A1**	Both cases reduced correctly and summing to $31 \equiv 0$.
	$r=3:\ 1+8+2+16+4 = 31 \equiv 0$	**A1**	
	$r=4:\ 1+16+8+4+2 = 31 \equiv 0$ So $f(n)$ is a multiple of 31 when 5 does not divide n	**A1 AG**	Case $r=4$ correct, all four cases without error, and a conclusion covering every n not a multiple of 5.
		[7]	
3(b)	$n = 5k \Rightarrow 2^n \equiv 1 \Rightarrow f(n) \equiv 5 \pmod{31}$	**B1**	
	Eight multiples of 5, other terms $\equiv 0$: $f(1) + \cdots + f(40) \equiv 8 \times$ "5" $= \ldots$	**M1**	Uses eight multiples of 5 in 1 to 40, with all other terms $\equiv 0$, and forms $8\times$ their value. Need not be reduced.
	Remainder 9	**A1**	9 only; 40 unreduced scores A0.
		[3]	
	Total for Question 3	**11**	

Question	Scheme	Marks	Notes
4	$(2k+1)^2 = 4k^2 + 4k + 1$	**M1**	Writes an odd integer as $2k+1$ oe and expands its square, or squares each odd residue modulo 8. Condone expansion slips.
	$= 4k(k+1) + 1$	**A1**	Or all four odd residues squared correctly.
	$k(k+1)$ even $\Rightarrow (2k+1)^2 = 8m + 1$ $\equiv 1 \pmod 8$	**A1**	Concludes $n^2 \equiv 1 \pmod 8$ for every odd n; where $k(k+1)$ is used, needs a reason it is even, such as consecutive integers or parity cases. Not for an assertion alone.
	p odd $\Rightarrow p^{2x} = (p^x)^2 \equiv 1 \pmod 8$ $\Rightarrow p^{2x} + 5 \equiv 6 \pmod 8$	**B1**	Needs p, or p^x, stated odd.
	$y = 1 : 2^y \equiv 2, \quad y = 2 : 2^y \equiv 4$ $y \geq 3 : 2^y = 8 \times 2^{y-3} \equiv 0 \pmod 8$	**M1**	Considers 2^y modulo 8 for every positive y, or shows $y \geq 3$ since $2^y \geq 14$.
	$2^y \not\equiv 6 \pmod 8$, contradiction No values of p, x, y	**A1 AG**	cso. All cases of y correct and a conclusion in words that the residues differ, so no solutions.
	Total for Question 4	**6**	

Question	Scheme	Marks	Notes
5(a)	$n \bmod 7: \ 0,1,2,3,4,5,6$ $n^3 \bmod 7: \ 0,1,1,6,1,6,6$	**M1**	Lists n^3 modulo 7 for every residue 0 to 6, or for 0 to 3 using $(-n)^3 = -n^3$. Condone one arithmetic slip.
	$n \equiv 0 \Rightarrow n^7 \equiv 0 \equiv n \pmod 7$ $n^3 \equiv \pm 1 \Rightarrow n^6 \equiv 1 \Rightarrow n^7 \equiv n \pmod 7$	**A1 AG**	Correct table; both cases, $n \equiv 0$ and $n^3 \equiv \pm 1$, reaching $n^7 \equiv n$ without error, with a conclusion for every n.
		[2]	
5(b)	$n \bmod 3: \ 0,1,2$, $n^3 \bmod 3: \ 0,1,2$ $n^7 = n^3 \times n^3 \times n \equiv n \times n \times n$	**M1**	Finds n^3 modulo 3 for each residue, or otherwise relates n^3 to n modulo 3, and uses it to reduce n^7. Listing n^7 mod 3 for each residue is accepted.
	$n^7 \equiv n^3 \equiv n \pmod 3$	**A1**	Conclusion for every n.
	$n^7 - n = 7k$, 3 divides $7k$, not 7 $\Rightarrow k = 3m \Rightarrow n^7 - n = 21m$	**A1 AG**	Uses part (a) and that 3 and 7 are coprime, or distinct primes, to reach 21 dividing $n^7 - n$. Not for 3×7 asserted with no coprimality reason.
		[3]	
5(c)(i)	$0^7 = 0, \ 1^7 = 1 \Rightarrow n^7 \equiv n \pmod 2$ $n^7 - n$ is even	**B1**	Any valid reason, such as n^7 and n having the same parity.
	$n^7 - n = 21m$ is even, 21 is odd $\Rightarrow m = 2q$	**M1**	Combines evenness with part (b), using that 2 and 21 are coprime, or that 2, 3, 7 are distinct primes.
	$n^7 - n = 42q$	**A1 AG**	Reaches $n^7 - n = 42q$, or 42 divides $n^7 - n$, without error, with a conclusion for all positive integers n.
		[3]	
5(c)(ii)	$2^7 - 2 = 126 = 2 \times 3^2 \times 7$ $3^7 - 3 = 2184 = 2^3 \times 3 \times 7 \times 13$	**M1**	Evaluates $n^7 - n$ for at least two values of $n \geq 2$ and finds their highest common factor, by factorising or otherwise.
	Highest common factor 42, $N \geq 42$ by (c)(i) $\Rightarrow N = 42$	**A1**	Needs both the lower bound from part (c)(i) and values whose highest common factor is 42.
		[2]	
	Total for Question 5	**10**	

Question	Scheme	Marks	Notes
6	$3^4 = 81 \equiv 13 \equiv -4 \pmod{17}$	**B1**	$3^4 \equiv 13$ or $3^4 \equiv -4$ seen.
	$f(n) = 9\left(3^4\right)^n + 8\left(2^2\right)^n$ $\equiv 9\,(\text{“}-4\text{”})^n + 8 \times 4^n$	**M1**	Writes both terms as constants times nth powers and reduces modulo 17 to powers of their residue of 3^4 and of 4. Condone slips in the constants.
	$f(n) \equiv 4^n\,(9(-1)^n + 8) \pmod{17}$	**A1**	oe, such as $9(-4)^n + 8 \times 4^n$.
	n even: $f(n) \equiv 4^n(9+8)$ $= 17 \times 4^n \equiv 0 \pmod{17}$	**A1**	
	n odd: $f(n) \equiv 4^n(-9+8) = -4^n$ 17 does not divide $4^n = 2^{2n}$, so $f(n) \not\equiv 0$ 17 divides $f(n)$ if and only if n is even	**A1 AG**	cso. Needs a reason 17 does not divide 4^n, such as 2 its only prime factor, and a conclusion in words covering both directions.
	Total for Question 6	**5**	

Question	Scheme	Marks	Notes
7(a)	$k \equiv 0, \pm 1, \pm 2, \pm 3, \pm 4 \pmod 9$ $\Rightarrow k^2 \equiv 0, 1, 4, 9, 16 \pmod 9$	**M1**	Squares a complete set of residues modulo 9, such as 0 to 8 or $0, \pm 1, \ldots, \pm 4$. Condone one slip.
	$k^2 \equiv 0, 1, 4$ or $7 \pmod 9$	**A1**	All four, and no others.
	$(3q)^3 = 27q^3$ $(3q \pm 1)^3 = 27q^3 \pm 27q^2 + 9q \pm 1$	**M1**	Expands $(3q)^3$ and at least one of $(3q \pm 1)^3$, by any method. Condone one slip.
	$(3q)^3 = 9\left(3q^3\right) \equiv 0 \pmod 9$ $(3q \pm 1)^3 = 9\left(3q^3 \pm 3q^2 + q\right) \pm 1 \equiv \pm 1 \pmod 9$ $-1 \equiv 8 \Rightarrow n^3 \equiv 0, 1$ or $8 \pmod 9$	**A1 AG**	All three cases correctly reduced modulo 9 as a multiple of 9 plus a constant, with $-1 \equiv 8$, and a conclusion for n^3.
		[4]	
7(b)	$n^3 \equiv 0, 1, -1 \Rightarrow \left(n^3\right)^2 + n^3 + 3 \equiv \ldots \pmod 9$	**M1**	Evaluates $\left(n^3\right)^2 + n^3 + 3$ modulo 9 for at least two of their residues of n^3 from part (a). Condone one arithmetic slip.
	$n^6 + n^3 + 3 \equiv 3$ or $5 \pmod 9$	**A1**	Both values from all three cases, and no others.
	Squares $\equiv 0, 1, 4, 7 \pmod 9$; 3 and 5 are not among these $\Rightarrow$ not a perfect square for any integer n	**A1 AG**	cso. Compares with the square residues $0, 1, 4, 7$ and concludes in words. A0 if the conclusion is missing.
		[3]	
	Total for Question 7	**7**	

Question	Scheme	Marks	Notes
8(a)	$n \equiv \pm 1, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \pm 19, \pm 23 \pmod{48}$	**B1**	All sixteen residues, or the eight in $\pm$ form, and no others; or $n = 6k \pm 1$, or n odd with $n \equiv \pm 1 \pmod 3$.
	$(48-r)^2 \equiv r^2 \pmod{48}$ $7^2 = 49 \equiv 1,\ 11^2 = 121 \equiv 25,\ \ldots$	**M1**	Finds the squares of the residues modulo 48: all sixteen, or eight using $(48-r)^2 \equiv r^2$, or equivalent work modulo 16 and 3, or squares $6k \pm 1$. Condone arithmetic slips.
	$n^2 \equiv 1$ or $n^2 \equiv 25 \pmod{48}$	**A1**	Both values and no others.
		[3]	
8(b)	$n^2 \equiv 1$: $\left(n^2\right)^4 + 4\left(n^2\right)^3 + 6n^2$ $\equiv 1 + 4 + 6 = 11 \pmod{48}$	**M1 A1**	**M1** Substitutes $n^2 \equiv 1$ into the expression, written in powers of n^2 or reduced directly.
	$n^2 \equiv 25 \Rightarrow n^4 \equiv 625 \equiv 1$ $n^8 \equiv 1,\ n^6 \equiv 25 \pmod{48}$	**M1**	Uses $n^2 \equiv 25$ to reduce n^8 and n^6 modulo 48, by any route. Condone arithmetic slips.
	$n^8 + 4n^6 + 6n^2 \equiv 1 + 100 + 150$ $= 251 \equiv 11 \pmod{48}$	**A1 AG**	cso. Correct substitution reduced to $251 \equiv 11$, with a conclusion covering both cases.
		[4]	
Total for Question 8		**7**	

Question	Scheme	Marks	Notes
9(a)	$M \equiv -1 \equiv 2 \pmod 3$	**B1**	Accept -1 or 2.
		[1]	
9(b)	$M \geq 3 \times 2 \times 5 - 1 = 29 > 1$ $\Rightarrow M = q_1 q_2 \cdots q_r$, by the fundamental theorem	**E1**	States $M > 1$, or a lower bound above 1, and cites the fundamental theorem for the factorisation. Not for the theorem alone.
	Supposes $q_j = 3$: 3 divides M $\Rightarrow M \equiv 0 \pmod 3$	**M1**	Links a factor $q_j = 3$ to 3 dividing M, by supposition or directly from $M \equiv 2 \pmod 3$.
	Contradicts $M \equiv 2 \pmod 3$, so no q_j equals 3	**A1 AG**	Contradiction with part (a) stated, or 3 shown not to divide M using part (a), and the conclusion that no q_j is 3.
		[3]	
9(c)	$q_j \neq 3 \Rightarrow 3$ does not divide q_j $\Rightarrow q_j \equiv 1$ or $2 \pmod 3$	**B1**	Both residues 1 and 2, with 0 excluded because q_j is a prime other than 3.
	Supposes every $q_j \equiv 1 \pmod 3$: $M = q_1 q_2 \cdots q_r \equiv 1 \times 1 \times \cdots \times 1 \pmod 3$	**M1**	Assumes every $q_j \equiv 1$ and multiplies the congruences, or otherwise finds the residue of M from the residues of the q_j.
	$M \equiv 1^r = 1 \pmod 3$	**A1**	Or $M \equiv 2^k$, where k is the number of $q_j \equiv 2$.
	Contradicts $M \equiv 2 \pmod 3$ $\Rightarrow q_j \equiv 2 \pmod 3$ for at least one j	**A1 AG**	cso. Contradiction with, or direct use of, $M \equiv 2 \pmod 3$ from part (a), and the conclusion that some $q_j \equiv 2 \pmod 3$.
		[4]	
9(d)	$q_j \equiv 2 \pmod 3 \Rightarrow q_j = p_k$ for some k	**B1**	Uses the assumption that $p_1, \ldots, p_n$ are all such primes to identify q_j with some p_k.
	p_k divides $3p_1 p_2 \cdots p_n$ and M $\Rightarrow p_k$ divides $3p_1 p_2 \cdots p_n - M$	**M1**	Uses p_k dividing both $3p_1 \cdots p_n$ and M to deduce it divides their difference, or reduces M modulo p_k.
	$3p_1 p_2 \cdots p_n - M = 1$	**A1**	Or $M \equiv -1 \pmod{p_k}$.
	$p_k \geq 2$ does not divide 1: contradiction $\Rightarrow$ infinitely many primes $\equiv 2 \pmod 3$	**A1 AG**	cso. Contradiction stated, using $p_k > 1$, and the conclusion that the assumption is false.
		[4]	
	Total for Question 9	**12**	

Question	Scheme	Marks	Notes
10(a)	$x^2 \equiv 0$ or $1 \pmod 4$, $41 \equiv 1 \pmod 4$ $\Rightarrow x$ odd	**B1**	Squares are only 0 or 1 modulo 4, so x is odd.
	$x^2 \equiv 16 \pmod{25}$ $\Rightarrow (x-4)(x+4) \equiv 0 \pmod{25} \Rightarrow x \equiv \ldots$	**M1**	Takes 41 modulo 25 and attempts to solve $x^2 \equiv 16 \pmod{25}$ by any method, such as factorising or testing residues.
	$x \equiv 4$ or $x \equiv 21 \pmod{25}$	**A1**	Both, oe such as $x \equiv \pm 4 \pmod{25}$.
	$x = 21,\ 29,\ 71,\ 79$	**A1**	All four and no others.
		[4]	
10(b)	$x^2 \equiv 42 \equiv 2 \pmod 4$, but squares are 0 or 1 $\pmod 4$	**E1**	States that x^2 would be 2 modulo 4 and that squares are only 0 or 1 modulo 4, with a conclusion.
		[1]	
10(c)	$(17-x)^2 \equiv x^2 \pmod{17}$ $1^2 \equiv 1,\ 2^2 \equiv 4,\ \ldots,\ 8^2 \equiv 13$	**M1**	Squares and reduces at least 1 to 8 modulo 17, or all of 1 to 16. Condone one arithmetic slip.
	$1,\ 2,\ 4,\ 8,\ 9,\ 13,\ 15,\ 16$	**A1**	All eight and no others; 0 not included.
		[2]	
10(d)	$(15-x)^2 \equiv x^2 \pmod{15}$ $1^2 \equiv 1,\ 2^2 \equiv 4,\ \ldots,\ 7^2 \equiv 4$	**M1**	Squares and reduces at least 1 to 7 modulo 15, or all of 1 to 14. Condone one arithmetic slip.
	$1,\ 4,\ 6,\ 9,\ 10$	**A1**	All five and no others; 0 not included.
		[2]	
10(e)	p divides $a^2 - b^2 = (a-b)(a+b)$	**M1**	Factorises $a^2 - b^2$ and states that p divides the product.
	p prime, so p divides $a-b$ or $a+b$ $\Rightarrow a \equiv b$ or $a \equiv -b \pmod p$	**A1 AG**	Uses that a prime dividing a product divides a factor, reaching both cases. A0 if primality is not used.
	$4^2 \equiv 1^2 \pmod{15}$, $4 \not\equiv \pm 1 \pmod{15}$	**B1**	Any correct example from part (d), checking both $a \not\equiv b$ and $a \not\equiv -b \pmod{15}$.
		[3]	

Question 10 continued

Question	Scheme	Marks	Notes
10(f)	$(p-x)^2 = p^2 - 2px + x^2 \equiv x^2 \pmod{p}$ $1 \leq x \leq p-1 \Rightarrow x^2 \not\equiv 0 \pmod{p}$	**M1**	Shows x and $p-x$ have the same square modulo p, and that $1 \leq x \leq p-1$ gives a nonzero square.
	p odd $\Rightarrow x \neq p-x$ $\frac{p-1}{2}$ pairs $\{x, p-x\}$, $1 \leq x \leq \frac{p-1}{2}$	**A1**	Uses p odd so that $x \neq p-x$, giving $\frac{p-1}{2}$ pairs.
	$x^2 \equiv y^2$, $1 \leq x, y \leq \frac{p-1}{2}$ $\Rightarrow x \equiv y$ or $x \equiv -y \pmod{p}$	**M1**	Applies part (e) to two of $1, \ldots, p-1$ with equal squares.
	$x \equiv y \Rightarrow x = y$ $x \equiv -y$: $2 \leq x + y \leq p-1$, impossible $\Rightarrow \frac{p-1}{2}$ quadratic residues	**A1 AG**	Both cases dismissed using the bounds, or each square shown to come from exactly one pair $\{x, p-x\}$, with a conclusion. A0 if the case $x \equiv -y$ is not dealt with.
		[4]	
Total for Question 10		**16**	