OPTIONAL PURE / NUMBER THEORY

Modular Arithmetic and Quadratic Residues

Worked solutions 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*	5
Question 4	*6 marks*	7
Question 5	*10 marks*	8
Question 6	*5 marks*	10
Question 7	*7 marks*	11
Question 8	*7 marks*	12
Question 9	*12 marks*	14
Question 10	*16 marks*	15

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]**

Solution

(a) Since $3^4 = 81$, the congruence $81 \equiv 9 \pmod{a}$ holds exactly when a divides $81 - 9 = 72$. Writing 72 as a product of primes:

$$72 = 2^3 \times 3^2$$

The positive divisors of 72 are $1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72$. The ones with $a > 9$ are

$$a = 12, \quad 18, \quad 24, \quad 36, \quad 72$$

(b) Rearranging the congruence and factorising:

$$x^3 - x \equiv 0 \pmod{p}$$
$$x(x-1)(x+1) \equiv 0 \pmod{p}$$

So p divides the product $x(x-1)(x+1)$. Since p is prime, if p divides a product of integers then p divides at least one of the factors. Hence p divides x, $x-1$ or $x+1$, which gives

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

as required.

Now replace p by 8, and take $x = 3$:

$$3^3 - 3 = 24 = 3 \times 8 \equiv 0 \pmod{8}$$

so $3^3 \equiv 3 \pmod{8}$. However, $-1 \equiv 7 \pmod{8}$, and $3 \not\equiv 0$, $3 \not\equiv 1$ and $3 \not\equiv 7 \pmod{8}$, so the conclusion fails for $x = 3$. This happens because 8 is not prime: in $x(x-1)(x+1) = 3 \times 2 \times 4$, the factor 2 of 8 divides $x - 1$ and the factor 4 divides $x + 1$, so 8 divides the product without dividing any single factor.

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]**

Solution

(a) Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, there are integers p and q with $a - b = pn$ and $c - d = qn$. Then

$$\begin{aligned} ac - bd &= ac - ad + ad - bd \\ &= a(c - d) + d(a - b) \\ &= aqn + dpn \\ &= n(aq + dp) \end{aligned}$$

Since $aq + dp$ is an integer, n divides $ac - bd$, so $ac \equiv bd \pmod{n}$.

Now suppose $a \equiv b \pmod{n}$, and use induction on k.

Base case: When $k = 1$, $a^1 = a \equiv b = b^1 \pmod{n}$, so the statement holds.

Inductive hypothesis: Assume the statement is true for $k = m$, so

$$a^m \equiv b^m \pmod{n}$$

Inductive step: Applying the product result with $a^m \equiv b^m \pmod{n}$ as the first congruence and $a \equiv b \pmod{n}$ as the second gives

$$a^{m+1} = a^m \times a \equiv b^m \times b = b^{m+1} \pmod{n}$$

so the statement is true for $k = m + 1$.

Conclusion: If the statement is true for $k = m$, then it is true for $k = m + 1$. Since it is true for $k = 1$, by the principle of mathematical induction the statement is true for all positive integers k.

(b) The congruence $6x \equiv 6 \pmod{15}$ means that 15 divides $6x - 6 = 6(x - 1)$, so $6(x - 1) = 15t$ for some integer t. Dividing by 3:

$$2(x - 1) = 5t$$

So 5 divides $2(x - 1)$. Since 5 is prime and does not divide 2, 5 divides $x - 1$, that is, $x \equiv 1 \pmod{5}$. Each step reverses, so these are exactly the solutions, and with $0 \leq x < 15$ they are

$$x = 1, \qquad x = 6, \qquad x = 11$$

In particular $6 \times 6 \equiv 6 \times 1 \pmod{15}$, but $6 \not\equiv 1 \pmod{15}$, since 15 does not divide $6 - 1 = 5$. Cancelling the common factor 6 from $6 \times 6 \equiv 6 \times 1$ would give the false statement $6 \equiv 1 \pmod{15}$, so a common factor cannot always be cancelled from both sides of a congruence.

(c) Let $f(x) = x^3 + 5x + 4$. Every integer x leaves a remainder r on division by 11, with $0 \leq r \leq 10$, and then $x \equiv r \pmod{11}$. By part (a) with $k = 3$, $x^3 \equiv r^3 \pmod{11}$. By the product result in part (a) with $5 \equiv 5 \pmod{11}$, $5x \equiv 5r \pmod{11}$. Also $4 \equiv 4 \pmod{11}$. Adding these congruences:

$$x^3 + 5x + 4 \equiv r^3 + 5r + 4 \pmod{11}$$

So $f(x) \equiv f(r) \pmod{11}$, and $f(x) \equiv 0 \pmod{11}$ exactly when $f(r) \equiv 0 \pmod{11}$. Hence only the residues $r = 0, 1, 2, \ldots, 10$ need checking.

Evaluating $f(r)$ and reducing modulo 11:

r	0	1	2	3	4	5	6	7	8	9	10
$f(r)$	4	10	22	46	88	154	250	382	556	778	1054
$f(r) \bmod 11$	4	10	0	2	0	0	8	8	6	8	9

The residues giving 0 are $r = 2$, 4 and 5, so the solutions are

$$x \equiv 2 \pmod{11}, \qquad x \equiv 4 \pmod{11}, \qquad x \equiv 5 \pmod{11}$$

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]**

Solution

(a) (i) By the division algorithm, $n = 5k + r$ with k a non-negative integer and $0 \leq r \leq 4$. Since n is not a multiple of 5, $r \neq 0$, so

$$n = 5k + 1, \qquad n = 5k + 2, \qquad n = 5k + 3 \qquad \text{or} \qquad n = 5k + 4$$

(ii) Now $2^5 = 32 = 31 + 1$, so

$$2^5 \equiv 1 \pmod{31}$$

Writing each term of $f(n)$ as a power of 2:

$$f(n) = 1 + 2^n + 2^{2n} + 2^{3n} + 2^{4n}$$

Using part (a)(i), let $n = 5k + r$ with $r \in \{1, 2, 3, 4\}$. Then

$$2^n = \left(2^5\right)^k \times 2^r \equiv 1^k \times 2^r \equiv 2^r \pmod{31}$$

so $2^{2n} = (2^n)^2 \equiv 2^{2r}$, $2^{3n} \equiv 2^{3r}$ and $2^{4n} \equiv 2^{4r}$, giving

$$f(n) \equiv 1 + 2^r + 2^{2r} + 2^{3r} + 2^{4r} \pmod{31}$$

By the same reasoning, $2^{5q+s} \equiv 2^s \pmod{31}$ for non-negative integers q and s, so each power of 2 reduces to one of $1, 2, 4, 8, 16$. In particular

$$2^6 \equiv 2, \qquad 2^8 \equiv 2^3 = 8, \qquad 2^9 \equiv 2^4 = 16, \qquad 2^{12} \equiv 2^2 = 4, \qquad 2^{16} \equiv 2^1 = 2$$

Now consider each case.

$r = 1$:

$$f(n) \equiv 1 + 2 + 4 + 8 + 16 = 31 \equiv 0 \pmod{31}$$

$r = 2$:

$$f(n) \equiv 1 + 2^2 + 2^4 + 2^6 + 2^8 \equiv 1 + 4 + 16 + 2 + 8 = 31 \equiv 0 \pmod{31}$$

$r = 3$:

$$f(n) \equiv 1 + 2^3 + 2^6 + 2^9 + 2^{12} \equiv 1 + 8 + 2 + 16 + 4 = 31 \equiv 0 \pmod{31}$$

$r = 4$:

$$f(n) \equiv 1 + 2^4 + 2^8 + 2^{12} + 2^{16} \equiv 1 + 16 + 8 + 4 + 2 = 31 \equiv 0 \pmod{31}$$

In every case $f(n) \equiv 0 \pmod{31}$, so when n is not a multiple of 5, $f(n)$ is a multiple of 31, as required.

(b) If $n = 5k$, then

$$2^n = \left(2^5\right)^k \equiv 1^k = 1 \pmod{31}$$

so 2^{2n}, 2^{3n} and 2^{4n} are also congruent to 1, and

$$f(n) \equiv 1 + 1 + 1 + 1 + 1 = 5 \pmod{31}$$

Among $1, 2, \ldots, 40$ there are 8 multiples of 5, namely $5, 10, \ldots, 40$. By part (a)(ii), every other term $f(n)$ is congruent to 0, so

$$f(1) + f(2) + \cdots + f(40) \equiv 8 \times 5 = 40 \equiv 9 \pmod{31}$$

The remainder is 9.

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]**

Solution

Odd squares modulo 8. Any odd integer n can be written as $n = 2k + 1$ for some integer k. Then

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 4k(k+1) + 1 \end{aligned}$$

The integers k and $k+1$ are consecutive, so one of them is even and $k(k+1)$ is even. Writing $k(k+1) = 2m$ for some integer m gives $4k(k+1) = 8m$, so

$$n^2 = 8m + 1 \equiv 1 \pmod 8$$

The left-hand side. Since $p \geq 3$ is prime, p is not divisible by 2, so p is odd. A product of odd integers is odd, so p^x is odd. Applying the result above with $n = p^x$:

$$p^{2x} = (p^x)^2 \equiv 1 \pmod 8$$

Hence

$$p^{2x} + 5 \equiv 1 + 5 \equiv 6 \pmod 8$$

The right-hand side. Consider the possible values of y:

$$\begin{aligned} y = 1: &\quad 2^y = 2 \equiv 2 \pmod 8 \\ y = 2: &\quad 2^y = 4 \equiv 4 \pmod 8 \\ y \geq 3: &\quad 2^y = 8 \times 2^{y-3} \equiv 0 \pmod 8 \end{aligned}$$

So for every positive integer y, 2^y is congruent to 0, 2 or 4 modulo 8, and never to 6.

Conclusion. If $p^{2x} + 5 = 2^y$, the two sides would have the same remainder on division by 8. The left-hand side is always congruent to 6 modulo 8, while the right-hand side never is. This is a contradiction, so there are no values of p, x and y satisfying $p^{2x} + 5 = 2^y$.

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]**

Solution

(a) Every integer is congruent to one of $0, 1, \ldots, 6$ modulo 7. Since $2^3 = 8$, $3^3 = 27$, $4^3 = 64$, $5^3 = 125$ and $6^3 = 216$, reducing modulo 7 gives

$n \bmod 7$	0	1	2	3	4	5	6
$n^3 \bmod 7$	0	1	1	6	1	6	6

Since $6 \equiv -1 \pmod 7$, this shows that $n^3 \equiv 0$, 1 or $-1 \pmod 7$.

If $n^3 \equiv 0 \pmod 7$, then the table shows $n \equiv 0 \pmod 7$, so $n^7 \equiv 0 \equiv n \pmod 7$.

Otherwise $n^3 \equiv \pm 1 \pmod 7$, so $n^6 = \left(n^3\right)^2 \equiv 1 \pmod 7$ and

$$n^7 = n \times n^6 \equiv n \times 1 = n \pmod 7$$

So in every case $n^7 \equiv n \pmod 7$.

(b) Every integer is congruent to one of $0, 1, 2$ modulo 3. Since $2^3 = 8 \equiv 2 \pmod 3$, reducing modulo 3 gives

$n \bmod 3$	0	1	2
$n^3 \bmod 3$	0	1	2

So $n^3 \equiv n \pmod 3$ for every n. Using this twice:

$$\begin{aligned} n^7 &= n^3 \times n^3 \times n \\ &\equiv n \times n \times n \pmod 3 \\ &= n^3 \\ &\equiv n \pmod 3 \end{aligned}$$

Hence 3 divides $n^7 - n$. By part (a), 7 divides $n^7 - n$, so $n^7 - n = 7k$ for some integer k. Then 3 divides $7k$, and since 3 is prime and does not divide 7, 3 divides k. Writing $k = 3m$ for an integer m:

$$n^7 - n = 21m$$

so $n^7 \equiv n \pmod{21}$, as required.

(c) (i) Every integer is congruent to 0 or 1 modulo 2, and $0^7 = 0$, $1^7 = 1$, so

$$n^7 \equiv n \pmod 2$$

Hence $n^7 - n$ is even.

By part (b), $n^7 - n = 21m$ for some integer m. Since $21m$ is even and 21 is odd, 2 divides m, because 2 is prime and does not divide 21. Writing $m = 2q$ for an integer q:

$$n^7 - n = 21 \times 2q = 42q$$

so $n^7 - n$ is divisible by 42 for all positive integers n.

(ii) By part (c)(i), $N = 42$ has the property, so the largest such N is at least 42. Any such N must divide the values of $n^7 - n$ at $n = 2$ and $n = 3$:

$$2^7 - 2 = 126 = 2 \times 3^2 \times 7$$

$$3^7 - 3 = 2184 = 2^3 \times 3 \times 7 \times 13$$

The largest integer dividing both is $2 \times 3 \times 7 = 42$, so no integer larger than 42 works, and the largest such integer is $N = 42$.

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]**

Solution

Work modulo 17. Now $3^4 = 81 = 4 \times 17 + 13$, so

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

Write each term of $f(n)$ using a power that reduces neatly:

$$3^{4n+2} = 3^2 \times \left(3^4\right)^n \equiv 9 \times (-4)^n = 9(-1)^n \times 4^n \pmod{17}$$

$$2^{2n+3} = 2^3 \times \left(2^2\right)^n = 8 \times 4^n$$

Adding these gives

$$f(n) \equiv 9(-1)^n \times 4^n + 8 \times 4^n = 4^n(9(-1)^n + 8) \pmod{17}$$

Case 1: n even. Then $(-1)^n = 1$, so

$$f(n) \equiv 4^n(9 + 8) = 17 \times 4^n \equiv 0 \pmod{17}$$

Hence $f(n)$ is divisible by 17 whenever n is even.

Case 2: n odd. Then $(-1)^n = -1$, so

$$f(n) \equiv 4^n(-9 + 8) = -4^n \pmod{17}$$

Now $4^n = 2^{2n}$ has 2 as its only prime factor, so the prime 17 does not divide 4^n. Therefore $-4^n \not\equiv 0 \pmod{17}$, and $f(n)$ is not divisible by 17 whenever n is odd.

Every integer $n \geq 0$ is either even or odd. Case 1 shows that if n is even then 17 divides $f(n)$. Conversely, if 17 divides $f(n)$, Case 2 shows that n cannot be odd, so n is even. Hence $f(n)$ is divisible by 17 if and only if n is even, as required.

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 $\pmod 9$. **[4]**

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

Solution

(a) Every integer k is congruent to one of $0, \pm1, \pm2, \pm3, \pm4$ modulo 9. Since $(-r)^2 = r^2$, squaring each residue gives

$$\begin{aligned} k \equiv 0 &\implies k^2 \equiv 0 \pmod 9 \\ k \equiv \pm1 &\implies k^2 \equiv 1 \pmod 9 \\ k \equiv \pm2 &\implies k^2 \equiv 4 \pmod 9 \\ k \equiv \pm3 &\implies k^2 \equiv 9 \equiv 0 \pmod 9 \\ k \equiv \pm4 &\implies k^2 \equiv 16 \equiv 7 \pmod 9 \end{aligned}$$

So the possible residues of k^2 modulo 9 are 0, 1, 4 and 7.

Every integer n can be written as $3q$, $3q+1$ or $3q-1$ for some integer q. Expanding each cube:

$$\begin{aligned} (3q)^3 &= 27q^3 = 9\big(3q^3\big) \equiv 0 \pmod 9 \\ (3q+1)^3 &= 27q^3 + 27q^2 + 9q + 1 = 9\big(3q^3 + 3q^2 + q\big) + 1 \equiv 1 \pmod 9 \\ (3q-1)^3 &= 27q^3 - 27q^2 + 9q - 1 = 9\big(3q^3 - 3q^2 + q\big) - 1 \equiv -1 \equiv 8 \pmod 9 \end{aligned}$$

Hence $n^3 \equiv 0$, 1 or 8 $\pmod 9$, as required.

(b) Write $n^6 + n^3 + 3 = \big(n^3\big)^2 + n^3 + 3$. Using part (a), consider each possible residue of n^3 modulo 9, with $8 \equiv -1$:

$$\begin{aligned} n^3 \equiv 0 &\implies n^6 + n^3 + 3 \equiv 0 + 0 + 3 = 3 \pmod 9 \\ n^3 \equiv 1 &\implies n^6 + n^3 + 3 \equiv 1 + 1 + 3 = 5 \pmod 9 \\ n^3 \equiv -1 &\implies n^6 + n^3 + 3 \equiv 1 - 1 + 3 = 3 \pmod 9 \end{aligned}$$

So $n^6 + n^3 + 3 \equiv 3$ or 5 $\pmod 9$ for every integer n. By part (a), every perfect square k^2 is congruent to 0, 1, 4 or 7 modulo 9, and neither 3 nor 5 is among these. Therefore $n^6 + n^3 + 3$ is not a perfect square for any integer n.

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]**

Solution

(a) Since n is odd and not a multiple of 3, its remainder on division by 48 is one of

$$1,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 25,\ 29,\ 31,\ 35,\ 37,\ 41,\ 43,\ 47$$

These remainders pair up as r and $48 - r$, and

$$(48 - r)^2 = 48^2 - 96r + r^2 \equiv r^2 \pmod{48}$$

so it is enough to square $r = 1, 5, 7, 11, 13, 17, 19, 23$. Working modulo 48:

$$\begin{aligned}
1^2 &= 1 \\
5^2 &= 25 \\
7^2 &= 49 = 48 + 1 \equiv 1 \\
11^2 &= 121 = 2 \times 48 + 25 \equiv 25 \\
13^2 &= 169 = 3 \times 48 + 25 \equiv 25 \\
17^2 &= 289 = 6 \times 48 + 1 \equiv 1 \\
19^2 &= 361 = 7 \times 48 + 25 \equiv 25 \\
23^2 &= 529 = 11 \times 48 + 1 \equiv 1
\end{aligned}$$

Hence $n^2 \equiv 1$ or $n^2 \equiv 25 \pmod{48}$, and both values occur.

(b) Using part (a), there are two cases.

If $n^2 \equiv 1 \pmod{48}$, then

$$\begin{aligned}
n^8 + 4n^6 + 6n^2 &= \left(n^2\right)^4 + 4\left(n^2\right)^3 + 6n^2 \\
&\equiv 1 + 4 + 6 \\
&= 11 \pmod{48}
\end{aligned}$$

If $n^2 \equiv 25 \pmod{48}$, then first

$$n^4 = \left(n^2\right)^2 \equiv 625 = 13 \times 48 + 1 \equiv 1 \pmod{48}$$

so $n^8 = \left(n^4\right)^2 \equiv 1$ and $n^6 = n^4 \times n^2 \equiv 25 \pmod{48}$. Therefore

$$\begin{aligned}
n^8 + 4n^6 + 6n^2 &\equiv 1 + 4 \times 25 + 6 \times 25 \\
&= 251 \\
&= 5 \times 48 + 11 \\
&\equiv 11 \pmod{48}
\end{aligned}$$

In both cases $n^8 + 4n^6 + 6n^2 \equiv 11 \pmod{48}$, as required.

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]**

Solution

(a) The product $3p_1p_2 \cdots p_n$ is a multiple of 3, so

$$M = 3p_1p_2 \cdots p_n - 1 \equiv 0 - 1 \equiv -1 \equiv 2 \pmod 3$$

(b) The list contains $p_1 = 2$ and $p_2 = 5$, and every $p_i \geq 2$, so

$$M \geq 3 \times 2 \times 5 - 1 = 29 > 1$$

Since M is an integer greater than 1, the fundamental theorem of arithmetic shows that it can be written as a product of primes, $M = q_1q_2 \cdots q_r$, where the q_j need not be distinct.

Suppose that $q_j = 3$ for some j. Then 3 divides M, so $M \equiv 0 \pmod 3$. This contradicts part (a), which gives $M \equiv 2 \pmod 3$. Hence none of $q_1, \ldots, q_r$ is equal to 3.

(c) Each q_j is a prime other than 3, so 3 does not divide q_j. Therefore $q_j \not\equiv 0 \pmod 3$, and each q_j is congruent to either 1 or 2 modulo 3.

Suppose, for contradiction, that $q_j \equiv 1 \pmod 3$ for every j with $1 \leq j \leq r$. Congruences modulo 3 can be multiplied, so

$$M = q_1q_2 \cdots q_r \equiv 1 \times 1 \times \cdots \times 1 = 1^r = 1 \pmod 3$$

This contradicts part (a), which gives $M \equiv 2 \pmod 3$. So not every q_j is congruent to 1 modulo 3, and since each is congruent to 1 or 2, $q_j \equiv 2 \pmod 3$ for at least one integer j with $1 \leq j \leq r$.

(d) By part (c), there is a prime q_j dividing M with $q_j \equiv 2 \pmod 3$. The primes congruent to 2 modulo 3 are assumed to be exactly $p_1, p_2, \ldots, p_n$, so $q_j = p_k$ for some k with $1 \leq k \leq n$.

Now p_k divides $3p_1p_2 \cdots p_n$, since it is one of the factors, and $p_k = q_j$ divides M. Hence p_k divides their difference:

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

But $p_k \geq 2$, and no integer greater than 1 divides 1. This is a contradiction, so the assumption that there are only finitely many primes congruent to 2 (mod 3) is false. Therefore there are infinitely many prime numbers congruent to 2 (mod 3).

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]**

Solution

(a) Since $100 = 4 \times 25$, and 4 and 25 have no common factor, 100 divides $x^2 - 41$ exactly when 4 and 25 both divide $x^2 - 41$.

Modulo 4, $41 \equiv 1$. An even $x = 2k$ has $x^2 = 4k^2 \equiv 0 \pmod{4}$, and an odd $x = 2k + 1$ has $x^2 = 4k^2 + 4k + 1 \equiv 1 \pmod{4}$. So x must be odd.

Modulo 25, $41 \equiv 16$, so

$$x^2 - 16 \equiv 0 \pmod{25} \implies (x-4)(x+4) \equiv 0 \pmod{25}$$

If 5 divided both $x - 4$ and $x + 4$, it would divide their difference, 8, which it does not. So both factors of 5 in 25 lie in the same bracket: 25 divides $x - 4$ or $x + 4$, that is

$$x \equiv 4 \pmod{25} \quad \text{or} \quad x \equiv 21 \pmod{25}$$

For $0 \leq x < 100$ this gives $x = 4, 29, 54, 79$ or $x = 21, 46, 71, 96$. Keeping only the odd values:

$$x = 21, \quad x = 29, \quad x = 71, \quad x = 79$$

(b) If 42 were a quadratic residue modulo 100, there would be an integer x such that 100 divides $x^2 - 42$. Then 4 divides $x^2 - 42$, so $x^2 \equiv 42 \equiv 2 \pmod{4}$. But, as shown in part (a), every square is congruent to 0 or 1 modulo 4, so no such x exists and 42 is not a quadratic residue modulo 100.

(c) Every integer is congruent to one of $0, 1, \ldots, 16$ modulo 17, and x^2 modulo 17 depends only on x modulo 17. Also $0^2 = 0$, which is not a quadratic residue, and

$$(17 - x)^2 = 289 - 34x + x^2 \equiv x^2 \pmod{17}$$

so the squares of $9, \ldots, 16$ repeat those of $8, \ldots, 1$. Squaring $1, \ldots, 8$ modulo 17:

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9, \quad 4^2 \equiv 16$$

$$5^2 = 25 \equiv 8, \quad 6^2 = 36 \equiv 2, \quad 7^2 = 49 \equiv 15, \quad 8^2 = 64 \equiv 13$$

The quadratic residues modulo 17 are $1, 2, 4, 8, 9, 13, 15, 16$.

(d) In the same way, every integer is congruent to one of $0, 1, \ldots, 14$ modulo 15, $0^2 = 0$, and

$$(15 - x)^2 = 225 - 30x + x^2 \equiv x^2 \pmod{15}$$

so it is enough to square $1, \ldots, 7$ modulo 15:

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9, \quad 4^2 = 16 \equiv 1$$

$$5^2 = 25 \equiv 10, \quad 6^2 = 36 \equiv 6, \quad 7^2 = 49 \equiv 4$$

None of these is 0, so the quadratic residues modulo 15 are $1, 4, 6, 9, 10$.

(e) If $a^2 \equiv b^2 \pmod{p}$, then p divides

$$a^2 - b^2 = (a - b)(a + b)$$

Since p is prime, if it divides a product of two integers it divides at least one of them. So p divides $a - b$ or $a + b$, that is, $a \equiv b \pmod{p}$ or $a \equiv -b \pmod{p}$.

From part (d), $1^2 \equiv 1$ and $4^2 \equiv 1 \pmod{15}$, so $4^2 \equiv 1^2 \pmod{15}$. But $4 \not\equiv 1 \pmod{15}$, and $-1 \equiv 14 \pmod{15}$, so $4 \not\equiv -1 \pmod{15}$. So the result fails for the modulus 15, which is not prime.

(f) Every integer is congruent to one of $0, 1, \ldots, p - 1$ modulo p, and x^2 modulo p depends only on x modulo p. The value $x = 0$ gives 0, which is not a quadratic residue. For $1 \leq x \leq p - 1$, p does not divide x, and since p is prime, p does not divide $x \times x = x^2$, so $x^2 \not\equiv 0 \pmod{p}$. So the quadratic residues modulo p are exactly the remainders of $1^2, 2^2, \ldots, (p - 1)^2$ on division by p.

For each x, expanding gives

$$(p - x)^2 = p^2 - 2px + x^2 \equiv x^2 \pmod{p}$$

Since p is odd, $x \neq p - x$ (otherwise $p = 2x$ would be even). So the numbers $1, 2, \ldots, p - 1$ split into the $\frac{p-1}{2}$ pairs $\{x, p - x\}$ with $1 \leq x \leq \frac{p-1}{2}$, and both numbers in a pair have the same square modulo p. Hence every quadratic residue is the square of one of $1, 2, \ldots, \frac{p-1}{2}$ modulo p.

These $\frac{p-1}{2}$ squares are all different modulo p. Suppose $x^2 \equiv y^2 \pmod{p}$ with $1 \leq x, y \leq \frac{p-1}{2}$. By part (e), $x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$.

- If $x \equiv y \pmod{p}$, then p divides $x - y$, where $|x - y| < p$, so $x = y$.
- If $x \equiv -y \pmod{p}$, then p divides $x + y$, but $2 \leq x + y \leq p - 1$, which is impossible.

So distinct pairs give distinct quadratic residues, and each pair gives exactly one. Therefore, for a prime $p > 2$, the number of quadratic residues modulo p is $\frac{p-1}{2}$.