IMPERIAL

MATH70041

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
Summer 2025

This paper is also taken for the relevant examination for the
Associateship of the Royal College of Science

Number Theory

Date: Friday, May 30, 2025

Time: Start time 14:00 – End time 16:30 (BST)

Time Allowed: 2.5 hours

This paper has 5 Questions.

Please Answer All Questions in 1 Answer Booklet

This is a closed book examination.

Candidates should start their solutions to each question on a new sheet of paper.

Supplementary books may only be used after the relevant main book(s) are full.

Any required additional material(s) will be provided.

Credit will be given for all questions attempted.

Allow margins for marking.

DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO DO SO

You can use, without proof, any results from the course provided you state them correctly and clearly.

1. (a) Find all positive integers $n \leq 200$ such that $2n \equiv 1 \mod 3$, $4n \equiv 4 \mod 5$, and $8n \equiv 4 \mod 7$. (5 marks)

   (b) State *Euler's theorem* on even perfect numbers. (2 marks)

   (c) For every positive integer n let $q(n)$ denote the number of solutions of the congruence $x^2 \equiv 1 \mod n$. Is $q(n)$ a multiplicative function? Justify your answer. (3 marks)

   We say that a prime p is *ample* if the number of primitive roots mod p is $\frac{p-1}{2}$.

   Recall that a number is a *Fermat prime* if it is a prime number of the form $2^{2^n}+1$ for some $n \in \mathbb{N}$.

   (d) Show that a prime p is ample if and only if it is a Fermat prime. (10 marks)

   (Total: 20 marks)

2. (a) Write the periodic continued fraction $[3; 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, \ldots]$ as a quadratic irrational. (6 marks)

   (b) Find the continued fraction expansion of $\sqrt{15}$. (6 marks)

   (c) Find a solution to the following Diophantine equation:

   $$x^2 - 15y^2 = -6$$

   using convergents, or otherwise. (4 marks)

   (d) Find all solutions to the equations:

   (i) $x^2 - 15y^2 = 1$,

   (ii) $x^2 - 15y^2 = -1$.

   (4 marks)

   (Total: 20 marks)

3. (a) Compute $(\frac{29}{31})$. (2 marks)

(b) Determine if a is a 4th power modulo the prime p when

(i) $a = -1$ and $p \equiv 1 \mod 8$,

(ii) $a = 2$ and $p = 23$,

(iii) $a = 5$ and $p = 31$.

Justify your answer. (8 marks)

(c) Let p be a prime. Show that $\sum_{i=1}^{p-1} i^4$ is not divisible by p if and only if $p = 2, 3$, or 5. (10 marks)

(Total: 20 marks)

4. (a) Is the ring $\mathbb{Z}[\sqrt{-2}]$ an Euclidean domain? (1 mark)

(b) Compute the order of $\mathbb{Z}[\sqrt{-2}]^*$. Justify your answer. (2 marks)

(c) Let p be an odd prime. Show that the congruence $x^2 + 2y^2 \equiv 0 \mod p$ has a solution such that $x, y \not\equiv 0 \mod p$ if and only if $p \equiv 1, 3 \mod 8$. (3 marks)

(d) Prove that for a prime p the Diophantine equation $x^2 + 2y^2 = p$ has a solution if and only if $p = 2$ or $p \equiv 1, 3 \mod 8$. (6 marks)

(e) Show that the only solutions of the Diophantine equation $x^2 + 2 = y^3$ are $x = \pm 5$, $y = 3$. (8 marks)

(Total: 20 marks)

5. Let $\zeta = e^{2\pi \mathbf{i}/8}$ be a primitive 8th root of unity, and set

$$\tau = \zeta + \zeta^{-1}.$$

(a) Show that $\tau^2 = 2$. (1 mark)

Let p be an odd prime, set $R = \mathbb{Z}[\zeta]$, and let $\overline{\zeta}, \overline{\tau}$ denote the reduction of ζ, τ modulo the ideal generated by p, respectively, that is, their image under the quotient map $R \to R/(p)$.

(b) Deduce that $\overline{\tau}^{p-1} = \left(\frac{2}{p}\right)$. (2 marks)

(c) Show that $\overline{\tau}^p = \overline{\zeta}^p + \overline{\zeta}^{-p}$. (3 marks)

(d) Show that $\overline{\tau}$ is invertible. (3 marks)

(e) Deduce that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{, if } p \equiv \pm 1 \mod 8, \\ -1 & \text{, if } p \equiv \pm 5 \mod 8. \end{cases}$$

(11 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2025

This paper is also taken for the relevant examination for the Associateship.

MATH60041/MATH70041/MATH97036

Number Theory (Solutions)

Setter's signature	Checker's signature	Editor's signature
.....	.....	.....

1. (a) Solving the linear equations we find that x is $2 \mod 3$, $1 \mod 5$, and $4 \mod 7$. Note that 11 satisfies these conditions, and any other integer satisfying them differs from 11 by a multiple of 105 by the Chinese remainder theorem. Thus 11 and 116 are the only solutions ≤ 200.

meth seen ⇓

5, A

(b) For an even number n we have $2n = \sum_{d|n} d$ if and only if $n = 2^k(2^{k+1} - 1)$ with $2^{k+1} - 1$ a prime.

seen ⇓

2, A

(c) Note that $q(n)$ is the order of the 2-torsion $(\mathbb{Z}/n\mathbb{Z})^*[2]$ of $(\mathbb{Z}/n\mathbb{Z})^*$. For relatively prime n, m we have $(\mathbb{Z}/nm\mathbb{Z})^*[2] \cong (\mathbb{Z}/n\mathbb{Z})^*[2] \times (\mathbb{Z}/m\mathbb{Z})^*[2]$ by the Chinese remainder theorem, so $q(nm) = q(n)q(m)$, and hence $q(n)$ is a multiplicative function.

meth seen ⇓

3, B

(d) The number of primitive roots mod p is $\phi(p-1)$. If p is Fermat, then $\phi(p-1) = \phi(2^{2^n}) = 2^{2^{n-1}} = \frac{p-1}{2}$, so p is ample. Now assume that p is ample. Clearly p is odd. Suppose that $p-1$ has an odd divisor d. Since no generator $\mathbb{Z}/(p-1)\mathbb{Z}$ is divisible by 2 or d, by the inclusion-exclusion principle $\phi(p-1)$ is at most

$$(p-1) - \frac{p-1}{2} - \frac{p-1}{d} + \frac{p-1}{2d} < \frac{p-1}{2},$$

a contradiction. So it remains to show that if a prime is of the form $2^m + 1$, then m is a 2-power. Assume that $m = rt$, where r is odd. Then

$$2^m + 1 = (2^t)^r + 1 = .(2^t + 1)(2^{t(r-1)} - \cdots + 1),$$

a contradiction, so the claim holds.

meth seen ⇓

10, D

2. (a) The continued fraction $[3;1,1,1,1,6,1,1,1,1,6,\ldots]$ is equal to $\sqrt{13}$, because the latter is the unique positive solution of the equation:

meth seen ⇓

$$x = \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\frac{1}{x}}}}}}.$$

6, A

(b) The continued fraction expansion of $\sqrt{15}$ is $[3;1,6,1,6,\ldots]$. Details of the computation:

meth seen ⇓

$$\sqrt{15} = 3 + (\sqrt{15} - 3),$$

$$\frac{1}{\sqrt{15}-3} = \frac{\sqrt{15}+3}{6} = 1 + \frac{\sqrt{15}-3}{6},$$

$$\frac{6}{\sqrt{15}-3} = \frac{6(\sqrt{15}+3)}{6} = 6 + (\sqrt{15}-3).$$

The residue on the right hand side of the last line is the same as the residue on the right hand side of the first line, so this is the point where the continued fraction starts to repeat itself.

6, A

(c) The first two convergents are: $\frac{4}{1}$ and $\frac{27}{7}$, giving rise to the following approximate solutions:

meth seen ⇓

$$4^2 - 15 \cdot 1^2 = 1, \qquad 27^2 - 15 \cdot 7^2 = -6.$$

4, A

(d) The first convergent $\frac{4}{1}$ is a solution to $x^2 - 15y^2 = 1$, so it is the fundamental solution. Therefore the solutions of this equation are $x + \sqrt{15}y = \pm(4+\sqrt{15})^n$. Every solution of $x^2 - 15y^2 = 1$ satisfies the congruence $x^2 - 15y^2 \equiv x^2 \equiv -1 \mod 3$, but the latter has no solution, as -1 is not a quadratic residue mod 3.

meth seen ⇓

4, B

3. (a) Since both 29 and 31 are primes, by the quadratic reciprocity law we have $(\frac{29}{31}) = (\frac{2}{29})$. Using Gauss's second supplement $(\frac{2}{29}) = -1$, as $29 \equiv 5 \mod 8$.

meth seen ⇓

2, A

(b) (i) Since $p \equiv 1 \mod 8$, the order of $(\mathbb{Z}/p\mathbb{Z})^*$ is divisible by 8. Since it is a cyclic group, there is an element b of order 8. Then $b^4 \not\equiv 1 \mod p$, but the square of b^4 is 1 mod p, so $b^4 \equiv -1 \mod p$.

meth seen ⇓

3, B

(ii) If a is a 4th power modulo p then it is a quadratic residue mod p, but $(\frac{2}{29}) = -1$, so 2 is not a quadratic residue mod 23.

meth seen ⇓

2, B

(iii) Since $(\frac{5}{31}) = (\frac{31}{5}) = (\frac{1}{5}) = 1$ we get that 5 is a quadratic residue mod 31. As $31 \equiv 3 \mod 4$ the subgroup of quadratic residues mod 31 has odd order, so the squaring is bijective on it. Therefore 5 is a 4th power mod 31.

meth seen ⇓

3, B

(c) Assume that $p \geq 7$ and let ζ be a primitive root mod p. Then

$$\sum_{i=1}^{p-1} i^4 \equiv \sum_{i=0}^{p-2} \zeta^{4i} \equiv \frac{\zeta^{4(p-1)} - 1}{\zeta^4 - 1} \equiv 0 \mod p$$

using Fermat's little theorem and that $\zeta^4 \not\equiv 1 \mod p$, since otherwise the order of ζ is $1, 2$, or 4, and hence $p = 2, p = 3$ or $p = 5$, respectively. When $p = 2, p = 3$ or $p = 5$ we have $\sum_{i=1}^{p-1} i^4 = 1$, $\sum_{i=1}^{p-1} i^4 = 1 + 2^4 \equiv 2 \mod 3$, and $\sum_{i=1}^{p-1} i^4 \equiv 1 + 1 + 1 + 1 \equiv 4 \mod 5$, respectively, which are not zero mod p.

unseen ⇓

10, C

4. (a) Yes.

seen ⇓

1, A

(b) For every solution of the Diophantine equation $x^2 + 2y^2 = 1$ we have $y = 0$, so $\mathbb{Z}[\sqrt{-2}]^* = \{\pm 1\}$, and hence its order is 2.

meth seen ⇓

2, A

(c) The congruence $x^2 + 2y^2 \equiv 0 \mod p$ has a solution such that $x, y \not\equiv 0 \mod p$ if and only if -2 is a quadratic residue mod p. By the multiplicativity of the Legendre symbol and the two supplementary laws

$$(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = \begin{cases} 1 & \text{, if } p \equiv 1, 3 \mod 8, \\ -1 & \text{, if } p \equiv 5, 7 \mod 8. \end{cases}.$$

meth seen ⇓

3, A

(d) Since $0^2 + 2 \cdot 1^2 = 2$, the case $p = 2$ is clear; now assume that p is odd. If the Diophantine equation $x^2 + 2y^2 = p$ has a solution, it gives rise to a solution of $x^2 + 2y^2 \equiv 0 \mod p$ such that $x, y \not\equiv 0 \mod p$, so $p \equiv 1, 3 \mod 8$.

If p is not the norm $x^2 + 2y^2$ of an $x + \sqrt{-2}y \in \mathbb{Z}[\sqrt{-2}]$ then it remains a prime in $\mathbb{Z}[\sqrt{-2}]$, a UFD. Assume that this is the case, and suppose that $p \equiv 1, 3 \mod 8$. Then the congruence $x^2 + 2 \equiv 0 \mod p$ has a solution. Let x be such a solution; then p divides one of $x + \sqrt{-2}$ or $x - \sqrt{-2}$, since it divides their product. This implies that p divides ± 1 which is a contradiction.

meth seen ⇓

6, B

(e) If (x, y) is an integer solution of $x^2 + 2 = y^3$, then x must be odd. Otherwise x is even, so the LHS is congruent to 2 mod 4. It is also congruent to the RHS mod 4, but the RHS is congruent to 0 mod 4, since y must be even. Contradiction.

meth seen ⇓

3, A

Also note that $x + \sqrt{-2}$ and $x - \sqrt{-2}$ are relatively prime in $\mathbb{Z}[\sqrt{-2}]$. Indeed if $a + \sqrt{-2}b$ is a common divisor of $x + \sqrt{-2}$ and $x - \sqrt{-2}$, it divides their difference $2\sqrt{-2}$. It also divides y^3. By taking norms we get $a^2 + 2b^2 | 4$ and $a^2 + 2b^2 | y^6$, which is odd by the above, so $a^2 + b^2$ divides 1. Hence $a + \sqrt{-2}b$ is a unit.

Since $\mathbb{Z}[\sqrt{-2}]$ is a UFD, every prime diving $x + \sqrt{-2}$ appears to a power divisible by 3 in its factorisation. So $x + \sqrt{-2}$ is a cube times a unit. Since every unit in $\mathbb{Z}[\sqrt{-2}]$ is a cube, too, we get that $x + \sqrt{-2}$ is a cube, say, $x + \sqrt{-2} = (c + d\sqrt{-2})^3$. Comparing the coefficients at $\sqrt{-2}$ one gets $1 = d(3c^2 - 2d^2)$. The claim is now immediate.

5, D

5. (a) Since $\zeta^2 = \mathbf{i}$, we have $\tau^2 = \zeta^2 + 2\zeta \cdot \zeta^{-1} + \zeta^{-2} = \mathbf{i} + 2 - \mathbf{i} = 2$.

unseen ⇓

1, M

(b) Using Euler's formula for the Legendre symbol we get that

$$\overline{\tau}^{p-1} = (\overline{\tau}^2)^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \mod p.$$

meth seen ⇓

2, M

(c) Since $R/(p)$ is a commutative ring where $p = 0$, by the binomial theorem:

$$\overline{\tau}^p = (\overline{\zeta} + \overline{\zeta}^{-1})^p = \overline{\zeta}^p + \overline{\zeta}^{-p}$$

using that reduction mod p is a ring homomorphism.

meth seen ⇓

3, M

(d) It is enough to show that some power of $\overline{\tau}$ is 1. Since $\left(\frac{2}{p}\right) = \pm 1$, we have $\overline{\tau}^{2(p-1)} = 1$ by the above.

meth seen ⇓

3, M

(e) Using that $\zeta^8 = 1$, and hence $\overline{\zeta}^8 = 1$, too, we get that when $p \equiv \pm 1 \mod 8$ the following holds:

$$\overline{\zeta}^p + \overline{\zeta}^{-p} = \zeta^{\pm 1} + \zeta^{\mp 1} = \overline{\tau},$$

and also using that $\zeta^{\pm 4} = -1$, and hence $\overline{\zeta}^{\pm 4} = -1$, too, we get that when $p \equiv \pm 5 \mod 8$ the following holds:

$$\overline{\zeta}^p + \overline{\zeta}^{-p} = \overline{\zeta}^4(\overline{\zeta}^{\pm 1} + \overline{\zeta}^{\mp 1}) = -\overline{\tau}.$$

Putting everything together we get that

$$\overline{\tau}\left(\frac{2}{p}\right) = \overline{\tau}^p = \begin{cases} \overline{\tau} & \text{, if } p \equiv \pm 1 \mod 8, \\ -\overline{\tau} & \text{, if } p \equiv \pm 5 \mod 8. \end{cases}$$

Since $\overline{\tau}$ is invertible, we may divide by it to get that the equation in the claim holds mod p. But the two sides of the equation are ± 1, so if their difference is not zero, it must be ± 2. The latter is invertible mod p, and hence the claim holds.

11, M

Review of mark distribution:
Total A marks: 34 of 32 marks
Total B marks: 21 of 20 marks
Total C marks: 10 of 12 marks
Total D marks: 15 of 16 marks
Total Mastery marks: 20 of 20 marks

MATH70041 Number Theory Markers Comments

Question 1	This problem was routine except the last part, which needed a clever, but elementary argument. The latter is quite similar to Euler's proof of the theorem on even perfect numbers, so this why I asked about the latter previously, as a form of a hint.
Question 2	This question was quite computational, but otherwise rather straightforward. Not surprisingly most students did well.
Question 3	The first half of the problem could be solved by using the theory of quadratic residues and the existence of a primitive root modulo a prime. Unfortunately, the solution of b (ii) has a computation error, coming from a typo, but luckily most students found the correct answer. Part (c) was trickier, but again there is a very quick solution using the existence of primitive roots, tying it with the rest of the question. Many students did find the solution to this part, too.
Question 4	The first half of this problem is rather standard material about doing number theory in a quadratic ring which is a UFD. There were attempts to use descent to do part (c), but this is a bit more involved to adopt. Part (e) was a rather standard example of a Diophantine equation split in a quadratic ring, but I gave hints which was ample to make the argument completely in previous parts.
Question 5	This was a Gauss sum proof of the second complimentary law of quadratic reciprocity. The problem introduced the simple Gauss sum needed, gave the main steps as separate simple problems in (a)-(d), so the students only had to put it all together in part (e). Some candidates try to completely copy the general case proof, ignoring what they just did, which is not good, since the latter has a formula for the Gauss sum which is degenerate in this case.