MATH97036 MATH97144

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May-June 2021

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

Number Theory

Date: Thursday, 20 May 2021

Time: 09:00 to 11:30

Time Allowed: 2.5 hours

Upload Time Allowed: 30 minutes

This paper has 5 Questions.

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

Each sheet of paper should have your CID, Question Number and Page Number on the top.

Only use 1 side of the paper.

Allow margins for marking.

Any required additional material(s) will be provided.

Credit will be given for all questions attempted.

Each question carries equal weight.

SUBMIT YOUR ANSWERS ONE PDF TO THE RELEVANT DROPBOX ON BLACKBOARD INCLUDING A COMPLETED COVERSHEET WITH YOUR CID NUMBER, QUESTION NUMBERS ANSWERED AND PAGE NUMBERS PER QUESTION.

As this is an online exam, please show your work for each question, as we cannot give full marks for an answer without some indication of how it was obtained.

1. (a) Give the continued fraction expansion of $\sqrt{37}$. (6 marks)

   (b) Find the first two solutions (x, y) to $x^2 - 37y^2 = 1$, where x, y are both positive and the solutions are ordered in increasing order of y-value. (7 marks)

   (c) Find the first two solutions (x, y) to $x^2 - 37y^2 = -1$, where the solutions are ordered as in part b. (7 marks)

(Total: 20 marks)

2. (a) Find all positive integers x such that $x^7 \equiv 3 \pmod{17}$. (4 marks)

   (b) Find all integers n such that $n \equiv 3 \pmod{4}$, $n \equiv 2 \pmod{5}$, and $n \equiv 3 \pmod{7}$. (4 marks)

   (c) Find the value of the Legendre symbol $\left(\frac{259}{733}\right)$. (Note that 733 is prime, and $259 = 7 \cdot 37$.) (4 marks)

   (d) For which primes p is 14 a quadratic residue modulo p? (4 marks)

   (e) Let n be a squarefree integer. How many roots does the polynomial $x^2 - 1$ have modulo n? Prove your answer. (4 marks)

(Total: 20 marks)

3. (a) Find a quadratic imaginary algebraic integer α such that $N(a+b\alpha) = a^2 + 5ab + 7b^2$. (Here as usual $N(z) = z\overline{z}$ for any complex z.) (3 marks)

(b) For α as in part a, what are the units of the ring $\mathbb{Z}[\alpha]$? (5 marks)

(c) Given positive integers n, m, and representations $n = a^2 + 5ab + 7b^2$, $m = c^2 + 5ab + 7d^2$ (for a, b, c, d integers), find integers e, f such that $nm = e^2 + 5ef + 7f^2$. (4 marks)

(d) Show that if n is congruent to 2 mod 3, then n cannot be expressed as $a^2 + 5ab + 7b^2$. (3 marks)

(e) How many pairs of integers (a, b) (positive or otherwise) are there such that $a^2 + 5ab + 7b^2 = 481$? (Note that $481 = 13 \cdot 37$.) (5 marks)

(Total: 20 marks)

4. Let $p \in \mathbb{Z}$ be a prime, and d a positive integer.

(a) Show that the polynomial $x^d - 1$ has $(d, p-1)$ distinct roots in $\mathbb{Z}/p\mathbb{Z}$. (4 marks)

(b) Show that for any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, the polynomial $x^d - a$ has a root in $\mathbb{Z}/p\mathbb{Z}$ if, and only if, $a^{\frac{p-1}{(d,p-1)}} \equiv 1 \pmod{p}$. (4 marks)

(c) Show that under the equivalent conditions of part b, the polynomial $x^d - a$ has exactly $(d, p-1)$ distinct roots in $\mathbb{Z}/p\mathbb{Z}$. (4 marks)

(d) Give (with proof) an example of a composite $n > 1$ such that for any $d > 0$, the polynomial $x^d - 1$ has exactly $(d, \Phi(n))$ distinct roots in $\mathbb{Z}/n\mathbb{Z}$. (4 marks)

(e) Give an example of a composite n, and a $d > 0$, such that the polynomial $x^d - 1$ does NOT have exactly $(d, \Phi(n))$ distinct roots in $\mathbb{Z}/n\mathbb{Z}$. (4 marks)

(Total: 20 marks)

5. (a) Show that if $(x, y) \in \mathbb{Z}^2$ satisfy $y^2 = x^3 - 1$, then $y + i$, $y - i$ have no common factor in $\mathbb{Z}[i]$. (2 marks)

(b) Show that for (x, y) as in part a, $y + i$ is a perfect cube in $\mathbb{Z}[i]$. (3 marks)

(c) Conclude that the only integral solution to $y^2 = x^3 - 1$ is $x = 1, y = 0$. (5 marks)

(d) By modifying the approach of parts a-c, or otherwise, find, with proof, all pairs of integers (x, y) such that $y^2 = x^3 - 4$. (10 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2021

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

XXX

Number Theory (Solutions)

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

1. (a) The continued fraction expansion is $[6; 12, 12, 12, \dots]$. $\boxed{6, \text{A}}$

   (b) The second convergent $\frac{73}{12}$ of the continued fraction from part a gives the fundamental solution $(73, 12)$ of $x^2 - 37y^2 = 1$. (Alternatively, one could note that $(6, 1)$ satisfies $x^2 - 37y^2 = -1$, and then square the corresponding element of $\mathbb{Z}[\sqrt{37}]$ to obtain an element of norm 1.) The next smallest solution is obtained from $(73 + 12\sqrt{37})^2$, and equals $(10657, 1752)$. $\boxed{7, \text{A}}$

   (c) The solutions here correspond to $(6 + \sqrt{37})$, and $(6 + \sqrt{37})(73 + 12\sqrt{37})$, and are: $(6, 1)$ and $(882, 145)$. $\boxed{7, \text{A}}$

2. (a) Raising both sides to the seventh power, we get $x^{49} \equiv 3^7 \equiv 11 \pmod{17}$. Since x must be prime to 17, we must have $x^{16} \equiv 1$ mod 17, so $x \equiv x^{49} \equiv 11 \pmod{17}$.

$\boxed{4, \text{A}}$

(b) These are the integers congruent to 87 mod 140. $\boxed{4, \text{A}}$

(c) We have:

$$\left(\frac{259}{733}\right) = \left(\frac{7}{733}\right)\left(\frac{37}{733}\right) = \left(\frac{733}{7}\right)\left(\frac{733}{37}\right).$$

We have $\left(\frac{733}{7}\right) = \left(\frac{5}{7}\right) = -1$. Similarly, $\left(\frac{733}{37}\right) = \left(\frac{-7}{37}\right) = 1$, as -1 and 7 are congruent to 6^2 and 9^2 mod 37. So $\left(\frac{259}{733}\right) = -1$. $\boxed{4, \text{A}}$

(d) Since zero is never a quadratic residue we must have $p \neq 2, 7$. For such a prime we have

$$\left(\frac{14}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{7}{p}\right).$$

Note that if $p \equiv 1 \pmod{4}$, then $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$ is 1 if p is $1, 2, 4 \pmod{7}$ and -1 if p is $3, 5, 6 \pmod{7}$. If $p \equiv 3 \pmod{4}$, then $\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$ is -1 if p is $1, 2, 4 \pmod{7}$ and 1 if p is $3, 5, 6 \pmod{7}$. Thus $\left(\frac{7}{p}\right) = 1$ if p is $1, 3, 9, 19, 25$, or 27 mod 28 and -1 otherwise (i.e., when p is $5, 11, 13, 15, 17$, or 23 mod 28. Now $\left(\frac{2}{p}\right) = 1$ if p is 1 or 7 mod 8, and -1 otherwise. We thus obtain that $\left(\frac{p}{14}\right) = 1$ if p is $1, 31, 8, 47, 25$, or 55 mod 56, as well as when p is $5, 11, 13, 43, 45$, or 51 mod 56, and -1 otherwise. $\boxed{4, \text{B}}$

(e) Note that modulo any odd prime p, $x^2 - 1$ has two roots ± 1 mod p. Modulo 2, $x^2 - 1$ has a unique root. Modulo a squarefree integer n, specifying a root of $x^2 - 1$ amounts to specifying a root mod p for each prime p dividing n, by the Chinese remainder theorem. Thus there are 2^r roots, where r is the number of odd primes dividing n. $\boxed{4, \text{B}}$

3. (a) Let α be a root of the polynomial $x^2 - 5x + 7$. The discriminant of this polynomial is -3, so α is imaginary. Moreover, we have $\alpha + \overline{\alpha} = 5$ and $\alpha\overline{\alpha} = 7$. Thus $(a + b\alpha)(a + b\overline{\alpha}) = a^2 + 5ab + 7b^2$. $\boxed{3,\ \mathrm{B}}$

(b) Any unit has norm 1 and is thus of the form $a+b\alpha$, where $a^2+5ab+7b^2 = 1$. This equation has six solutions (a, b): $(1, 0),(-1, 0),(-2, 1),(-3, 1),(2, -1),(3, -1)$. Alternatively, we can note that $\alpha - 3 = e^{\frac{2\pi i}{3}}$, so that $\mathbb{Z}[\alpha]$ is the ring of Eisenstein integers, and use the known description of the units of the Eisenstein integers. $\boxed{5,\ \mathrm{C}}$

(c) We have $n = N(a + b\alpha), m = N(c + d\alpha)$, so $nm = N((a + b\alpha)(c + d\alpha))$ by multiplicativity of the norm. Since

$$(a + b\alpha)(c + d\alpha) = ac + (ad + bc)\alpha + bd\alpha^2 = (ac - 7bd) + (ad + bc + 5bd)\alpha$$

we can take $e = ac - 7bd, f = ad + bc + 5bd$. $\boxed{4,\ \mathrm{B}}$

(d) We have $a^2 + 5ab + 7b^2 \equiv a^2 - ab + b^2 \pmod 3$; by considering all possibilities for a, b mod 3 we see that this is always zero or one mod 3. $\boxed{3,\ \mathrm{B}}$

(e) We note that since $\mathbb{Z}[\alpha]$ is equal to the ring of Eisenstein integers, unique factorization holds in $\mathbb{Z}[\alpha]$. In $\mathbb{Z}[\alpha]$ the integer 13 factors as $(1 + \alpha)(1 + \overline{\alpha}) = \mathfrak{p}\overline{\mathfrak{p}}$ and 37 factors as $(-2 + 3\alpha)(-2 + 3\overline{\alpha}) = \mathfrak{q}\overline{\mathfrak{q}}$. Note that both $\mathfrak{p}$ and $\mathfrak{q}$ are prime (as their norms are 13 and 37, respectively.)

A solution (a, b) to $a^2 + 5ab + 7b^2 = 13 \cdot 37$ corresponds to an element $z = a + b\alpha$ of $\mathbb{Z}[\alpha]$ such that $z\overline{z} = 13 \cdot 37 = \mathfrak{p}\overline{\mathfrak{p}}\mathfrak{q}\overline{\mathfrak{q}}$. The possibilities are: $z = u\mathfrak{p}\mathfrak{q}$, where u is a unit, $z = u\overline{\mathfrak{p}}\mathfrak{q}$, $z = u\mathfrak{p}\overline{\mathfrak{q}}$, and $z = u\overline{\mathfrak{p}\mathfrak{q}}$. Each of these four possibilities has six choices for u, for a total of 24 solutions. (Note that $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ do not differ by a unit, as can be easily checked by verifying that $\frac{\mathfrak{p}}{\overline{\mathfrak{p}}}$ does not lie in $\mathbb{Z}[\alpha]$. Similarly $\mathfrak{q}$ and $\overline{\mathfrak{q}}$ do not differ by a unit. $\boxed{5,\ \mathrm{D}}$

4. (a) Any root of $x^d - 1$ has order dividing d in $(\mathbb{Z}/p\mathbb{Z})^\times$; since the order of this root must also divide $p-1$ by Fermat's little theorem we find that the order of such a root divides $(d, p-1)$. Thus any root of $x^d - 1$ is a root of $x^e - 1$, where $e = (d, p-1)$. Conversely, since $x^e - 1$ divides $x^d - 1$, we find that the roots of $x^d - 1$ are precisely the roots of $x^e - 1$. These roots are the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order dividing e. But since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, and e divides $p-1$, there are precisely e elements of order dividing e in $(\mathbb{Z}/p\mathbb{Z})^\times$, so we are done. $\boxed{4, \mathrm{D}}$

(b) Consider the homomorphism $x \mapsto x^d$ from $(\mathbb{Z}/p\mathbb{Z})^\times$ to $(\mathbb{Z}/p\mathbb{Z})^\times$. By part a, its kernel consists of $(d, p-1)$ elements. The image is therefore a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order $\frac{p-1}{(d,p-1)}$, so certainly anything in that image satisfies $a^{\frac{p-1}{(d,p-1)}} \equiv 1 \pmod{p}$. Conversely, since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, there are exactly $\frac{p-1}{(d,p-1)}$ elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ that satisfy $a^{\frac{p-1}{(d,p-1)}} \equiv 1 \pmod{p}$, so every one of them must be in the image of the homomorphism $x \mapsto x^d$. But the image of this homomorphism is the set of dth powers; that is, the set of a such that $x^d - a$ has a root in $(\mathbb{Z}/p\mathbb{Z})^\times$. $\boxed{4, \mathrm{D}}$

(c) If y is a root of $x^d - a$, then so is yz, for any z such that $z^d = 1$. Conversely, if y' is another rood of $x^d - a$, then $y'y^{-1}$ is a root of $x^d - 1$, so every root of $x^d - a$ is of the form yz for some root z of $x^d - 1$. Since there are $(d, p-1)$ such roots the result follows. $\boxed{4, \mathrm{C}}$

(d) We have seen in the problem sheets that for p an odd prime, $(\mathbb{Z}/2p\mathbb{Z})^\times$ is cyclic of order $\Phi(2p)$. Thus, by the same argument as in part a, $x^d - 1$ has $(d, \Phi(2p))$ roots mod $2p$ for any odd prime p. $\boxed{4, \mathrm{D}}$

(e) The polynomial $x^2 - 1$ has four distinct roots $\{\pm 1, \pm 4\}$ mod 15. $\boxed{4, \mathrm{C}}$

5. (a) Any common divisor of $y + i$ and $y - i$ also divides their difference $2i$. Thus the only possible prime of $\mathbb{Z}[i]$ (up to units) that divides both $y + i$ and $y - i$ is $1 + i$. If this is the case then y is odd (the elements of $\mathbb{Z}[i]$ divisible by $1 + i$ are those of the form $a + bi$ where a and b have the same parity.) Then y^3 is 1 mod 8, but $x^2 - 1$ is -1 or 3 mod 8, so this is impossible. Thus $y + i$ and $y - i$ are relatively prime. $\boxed{2, \mathrm{M}}$

(b) Since $x^3 = y^2 + 1 = (y + i)(y - i)$, and $y + i$ and $y - i$ have no common factors, any prime dividing $y + i$ in $\mathbb{Z}[i]$ must divide it to an order that is a multiple of 3. Thus $y + i = uz^3$ for u a unit in $\mathbb{Z}[i]$ and $z \in \mathbb{Z}[i]$. Since every unit $\pm 1, \pm i$ in $\mathbb{Z}[i]$ is a cube, we can write $y + i = z^3$ for some $z \in \mathbb{Z}[i]$. $\boxed{3, \mathrm{M}}$

(c) Write $z = a + bi$, for z as in part b. Then $z^3 = a^3 - 3ab^2 + (3a^2b - b^3)i = y + i$. We thus have $y = a^3 - 3ab^2$, and $1 = 3a^2b - b^3$. In particular b divides 1, so $b = \pm 1$. Since $b^3 \equiv -1 \pmod{3}$ we must have $b = -1$, so $a = 0$, and hence $y = 0$. Thus $x^3 = 1$ and hence $x = 1$, so the only solution is $(1, 0)$. $\boxed{5, \mathrm{M}}$

(d) We write $x^3 = (y+2i)(y-2i)$. Any common divisor of $y+2i$ and $y-2i$ divides $4i$, so either $y+2i$ and $y-2i$ have no common factor or y is even.

If y is odd, then $y+2i$ and $y-2i$ have no common divisor, so, as above, $y+2i$ is a perfect cube in $\mathbb{Z}[i]$. On the other hand, if y is even, then x is even as well, and we can write $y = 2y'$, $x = 2x'$, where x' and y' are related by $(2x')^3 = (2y')^2 + 4$. In particular we obtain $2(x')^3 = (y')^2 + 1$. We deduce that y' is odd and therefore x' must be as well (as the right hand side is $2 \bmod 4$). In particular $y+i$ and $y-i$ are divisible by $1+i$, but not by $(1+i)^2 i = 2i$; thus (considering their difference) the greatest common divisor of $y'+i$ and $y'-i$ is $1+i$. Set $z = \frac{y'+i}{1+i}$ and $z' = \frac{y'-i}{1+i}$; then $zz' = (-x')^3$. Since z and z' have no common factor, each of z and z' is a perfect cube in $\mathbb{Z}[i]$. But then $y + 2i = 2(y'+i) = 2(1+i)z = -(1+i)^3 z$ is also a perfect cube.

We thus have that $y+2i$ is a perfect cube in $\mathbb{Z}[i]$. In particular we have $y = a^3 - 3ab^2$, and $2 = 3a^2b - b^3$. In particular b divides 2, and b^3 is $1 \bmod 3$. The possibilities are $b = 1$, in which case $a = \pm 1$, $y = \pm 2$, $x = 2$, or $b = -2$, in which case $a = \pm 1$ and we obtain $y = \pm 11$, $x = 5$. $\boxed{10, \mathrm{M}}$

If your module is taught across multiple year levels, you might have received this form for each level of the module. You are only required to fill this out once for each question.

Please record below, some brief but non-trivial comments for students about how well (or otherwise) the questions were answered. For example, you may wish to comment on common errors and misconceptions, or areas where students have done well. These comments should note any errors in and corrections to the paper. These comments will be made available to students via the MathsCentral Blackboard site and should not contain any information which identifies individual candidates. Any comments which should be kept confidential should be included as confidential comments for the Exam Board and Externals. If you would like to add formulas, please include a sperate pdf file with your email.

ExamModuleCode	QuestionNumber	Comments for Students
MATH96027 MATH97036 MATH97144	1	Almost nobody had trouble with this question.
MATH96027 MATH97036 MATH97144	2	The first three parts of this were straightforward; many peole had difficulty correctly integrating the congruence conditions in part d. Full marks were given if you gave separate congruence conditions mod 7 and mod 8, but you needed to correctly combine the conditions mod 4 and mod 8.
MATH96027 MATH97036 MATH97144	3	The most difficult part of this question was accounting for units- first noticing that there were six, and then understanding how this affects the answer in part e. (Note that the number of representations of nm is not the product of the numbers of representations of n and m- this "counts the units twice!")
MATH96027 MATH97036 MATH97144	4	This question was basically about reasoning in a cyclic group (except for part e, where the point was to find an n such that Z/nZ is not cyclic!) Astute students noticed that a correct answer to 2e gave an answer to part e of this question as well.
MATH96027 MATH97036 MATH97144	5	The point of this question was to show how unique factorization in an appropriate quadratic ring lets you solve simple diophantine equations. It is quite important in these questions to keep careful track of when you are working with integers, and when you are working with elements of the larger ring!