IMPERIAL

MATH70041

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May 2024

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

Number Theory

Date: Thursday, May 30, 2024

Time: 14:00 – 16:30 (BST)

Time Allowed: 2.5 hours

This paper has 5 Questions.

Please Answer All Questions in 1 Answer Booklet

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.

Allow margins for marking.

Credit will be given for all questions attempted.

Each question carries equal weight.

DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO

1. (a) Find all integer solutions to the linear Diophantine equation $36x + 78y = 12$. (5 marks)

(b) Let $m, n \in \mathbb{Z}$. Find the kernel and image of the natural homomorphism of abelian groups

$$\pi : \mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n$$

given by

$$x \text{ mod } mn \to (x \text{ mod } m, x \text{ mod } n).$$

(5 marks)

(c) Show that 2 is a primitive root modulo 13. (3 marks)

(d) For which integers x, y does 21 divide the expression $8 \cdot x^3 - y^2 + 18$? (7 marks)

(Total: 20 marks)

2. (a) Find the continued fraction expansion of $\sqrt{13}$.

(6 marks)

(b) Find **all** solutions to the equation $x^2 - 13 \cdot y^2 = 1$ with x, y integers.

(6 marks)

(c) Find, with proof, infinitely many solutions $(x, y) \in \mathbb{Z}^2$ to each of the equations

$$x^2 - 13y^2 = 3$$

$$x^2 - 13y^2 = -3.$$

(8 marks)

(Total: 20 marks)

3. (a) (i) State Gauss's law of quadratic reciprocity. You need not provide a proof, nor do you need to state the supplemental laws concerning the values of $\left(\frac{2}{p}\right), \left(\frac{-1}{p}\right)$. (3 marks)

(ii) Calculate $\left(\frac{1415}{887}\right)$. (4 marks)

(b) Let p be a prime number with $p \equiv 1 \bmod 4$. Show that $\sum_{r \in R} r = \frac{p(p-1)}{4}$, where R is the set of integers $1 \leq r < p$ which are quadratic residues mod p. (5 marks)

(c) Let p be a prime number larger than 5. Let X be the set of quadratic *non-residues* mod p. Show that $\sum_{x \in X} x^2 \equiv 0 \bmod p$. (8 marks)

(Total: 20 marks)

4. In this question you may use without proof that $\mathbb{Z}[\sqrt{3}]$ is a Euclidean domain, and thus elements of this ring admit unique factorizations. Note that this ring has norm form $N(x + \sqrt{3}y) = x^2 - 3y^2$. Let p be a prime number which is $1 \bmod 12$.

(a) Show that there exists a solution to the equation $x^2 - 3y^2 \equiv 0 \bmod p$ with $x, y \in \mathbb{Z}$ and $p \nmid x, y$. (4 marks)

(b) Show that 2 factors as $-z\bar{z}$ for some $z \in \mathbb{Z}[\sqrt{3}]$ irreducible, where here $\bar{z} = a - b\sqrt{3}$ if $z = a + b\sqrt{3}$. Show that $\sqrt{3}$ is irreducible. (3 marks)

(c) Let $x^2 - 3y^2 = np$ with $x, y \in \mathbb{Z}$ as obtained from part (a) and $n \in \mathbb{Z}$. Show we may choose $(x, y) \in \mathbb{Z}^2$ as above such that $(x, y) = 1$ and $n = 1$. [Hint: use a descent argument on $|n|$ to get rid of unwanted prime factors.] (8 marks)

(d) Show that if $x^2 - 3y^2 = p$, with x, y coprime in $\mathbb{Z}$, then $x + y\sqrt{3}, x - y\sqrt{3}$ are coprime in $\mathbb{Z}[\sqrt{3}]$. (5 marks)

(Total: 20 marks)

5. (a) Find all integer solutions to the cubic equation $y^3 = x^3 + 8$. (6 marks)

(b) Show that the cubic equation $y^2 = x^3 + 16$ has only 2 solutions (x, y) with $x, y \in \mathbb{Z}$. (14 marks).

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2024

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

Math 70041

70041 (Solutions)

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

1. (a) We note that $(36, 78) = 6|12$, whence this equation reduces to $6x+13y = 2$, which has infinitely many solutions. Using Euclid's algorithm or brute observation we see that $13-2\cdot 6 = 1$, whence $(-4, 2)$ is a solution. As this equation is linear any other solution can be obtained from this one by setting $x' = -4 + 13 \cdot n, y' = 2 - 6 \cdot n$, with $n \in \mathbb{Z}$.

meth seen ⇓

5, A

(b) First we calculate the kernel of this map. We note that if x is an integer which is 0 mod n and 0 mod m, then by definition the $lcm(m, n)|x$, and vice versa. Whence we see that ker$(\pi) = (lcm(m, n))$, considered as an ideal in $\mathbb{Z}/mn\mathbb{Z}$.

seen ⇓

2, A

To calculate the image, we note that if the system $x \equiv a$ mod m, $x \equiv b$ mod n is soluble, then necessarily $a = b$ mod (n, m). Counting and using the first isomorphism theorem shows that this is also a sufficient condition for (a, b) to lie in the image of π.

3, B

(c) Indeed, $13 - 1 = 12 = 4 \cdot 3$ so we simply check that we have neither $13|(2^4 - 1)$ nor $13|(2^6 - 1)$. Because $2^4 \equiv 3, 2^6 \equiv 12$ modulo 13 this is obvious.

meth seen ⇓

3, A

unseen ⇓

(d) We know that $21|(8 \cdot x^3 + 18 - y^2)$ if and only if x, y simultaneously solve $8 \cdot x^3 + 18 - y^2 \equiv 0$ mod $3, 7$ as $3, 7$ are coprime, using the Chinese remainder theorem.

2, A

We know, computing quadratic residues mod 3, that $8 \cdot x^3 + 18 - y^2 \equiv 0$ mod 3 if and only if either $x = y = 0$ or $x = 2, y = 1$ mod 3. Modulo 7 we wish to solve $x^3 + 4 \equiv y^2$. But we note that only $-1, 0, 1$ are cubes mod 7, whereas only $0, 1, 2, 4$ are squares, thus we see that $x^3 = 0, y^2 = 4$ whence we see that $x = 0$ and $y = \pm 2$.

3, B

So finish up, we apply the Chinese remainder theorem. We see that $7 - 2 \cdot 3 = 1$. So the solutions we are looking for are $(x, y) \equiv (0, 9), (0, 12), (14, 16), (14, 19), (14, 2), (14, 5)$ mod 21. All other integer solutions are obtained by shifting these by $(21 \cdot n_1, 21 \cdot n_2)$.

2, B

2. (a) We have that

meth seen ⇓

$$\begin{aligned}
\sqrt{13} &= 3 + (\sqrt{13} - 3) \\
\frac{1}{\sqrt{13}-3} &= \frac{3+\sqrt{13}}{4} = 1 + \frac{\sqrt{13}-1}{4} \\
\frac{4}{\sqrt{13}-1} &= \frac{4(1+\sqrt{13})}{12} = \frac{1+\sqrt{13}}{3} = 1 + \frac{\sqrt{13}-2}{3} \\
\frac{3}{\sqrt{13}-2} &= \frac{3(2+\sqrt{13})}{9} = \frac{2+\sqrt{13}}{3} = 1 + \frac{\sqrt{13}-1}{3} \\
\frac{3}{\sqrt{13}-1} &= \frac{3(\sqrt{13}+1)}{12} = \frac{\sqrt{13}+1}{4} = 1 + \frac{\sqrt{13}-3}{4} \\
\frac{4}{\sqrt{13}-3} &= \frac{4(\sqrt{13}+3)}{4} = 6 + (\sqrt{13} - 3),
\end{aligned}$$

so we see that $\sqrt{13} = [3; \overline{1, 1, 1, 1, 6}, ...]$.

6, A

(b) We have from class that, as $\mathbb{Z}[\sqrt{13}]$ is a real quadratic ring, all units of norm 1 are of the form $(-1)^m(a + b\sqrt{13})^n$ for a unique $m \in \{0, 1\}, n \in \mathbb{Z}$. We further know that a, b are the first convergents of $\sqrt{13}$ satisfying $a^2 - 13 \cdot b^2 = 1$.

meth seen ⇓

$$\begin{aligned}
p_0 = 3, q_0 = 1; p_0^2 - 13q_0^2 &= -4 \\
p_1 = 4, q_1 = 1; p_1^2 - 13q_1^2 &= 3 \\
p_2 = 7, q_2 = 2; p_2^2 - 13q_2^2 &= -3 \\
p_3 = 11, q_3 = 3; p_3^2 - 13q_3^2 &= 4 \\
p_4 = 18, q_4 = 5; p_4^2 - 13q_4^2 &= -1 \\
&\vdots \\
p_9 = 649, q_9 = 180; p_9^2 - 13q_9^2 &= 1
\end{aligned}$$

so we see that $u_1 = 649 + 180 \cdot \sqrt{13}$ is a fundamental norm 1 unit, and thus all norm 1 units of $\mathbb{Z}[\sqrt{13}]$ are of the form $\pm(649 + 180 \cdot \sqrt{13})^n$ for some n.

6, B

(c) We note here that since $p_4^2 - 13q_4^2 = -1$, we actually have that $u = 18 + 5 \cdot \sqrt{13}$ is a unit of norm -1 which squares to u_1.

unseen ⇓

2, B

Trial and error with the first positive integer x such that $x^2 > 13$ gives the solution $(x, y) = (4, 1)$ to the equation $x^2 - 13 \cdot y^2 = 3$.

2, A

We now obtain infinitely many tuples (x, y) with $(x, y) \in \mathbb{Z}^2$ as follows: because the map $N(x+y\cdot\sqrt{13}) = x^2-13\cdot y^2$ is multiplicative, we see that if $u_1^2-13\cdot u_2^2 = \pm 1$ then $N\left((u_1 + u_2 \cdot \sqrt{13}) \cdot (4 + \sqrt{13})\right) = \pm 3$. Thus the integers x_n, y_n such that $x_n + y_n \cdot \sqrt{13} = (4+\sqrt{13}) \cdot (18+5\cdot\sqrt{13})^n$ give solutions $x_n^2 - 13 \cdot y_n^2 = (-1)^n \cdot 3$.

3, C

These x_n, y_n are all distinct because $18 + 5 \cdot \sqrt{13}$ is a positive real number which is not equal to 1, thus we have produced infinitely many solutions.

1, A

3. (a) (i) Let p, q be odd primes. Then $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$, where $q^* = (-1)^{\frac{q-1}{2}} q$.

seen ⇓

3, A

(ii) We see that $1415 = 5 \cdot 283$, whence

meth seen ⇓

$$\begin{aligned}\left(\frac{1415}{887}\right) &= \left(\frac{5}{887}\right) \cdot \left(\frac{283}{887}\right) \\ &= -\left(\frac{887}{5}\right) \cdot \left(\frac{887}{283}\right) \\ &= \left(\frac{38}{283}\right) = \left(\frac{2}{283}\right) \cdot \left(\frac{19}{283}\right) \\ &= \left(\frac{283}{19}\right) = \left(\frac{17}{19}\right) = \left(\frac{-2}{19}\right) = 1\end{aligned}$$

where between lines 1 and 2 we have used quadratic reciprocity, between lines 3 and 4 quadratic reciprocity combined with the supplemental law that $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \bmod 8$ for p an odd prime.

4, A

(b) We note that because $p \equiv 1 \bmod 4$ we have that -1 is a quadratic residue mod p.

meth seen ⇓

Thus if $0 < r < p$ is a quadratic residue, so is $p - r \equiv -r \bmod p$. Thus we may group and obtain $\frac{p-1}{4}$ pairs $(r, p-r)$ of the $\frac{p-1}{2}$ quadratic residues, and each pair has sum p, so the sum of all quadratic residues is $\frac{p(p-1)}{4}$

2, B

3, C

(c) We take a to be a primitive element of $\mathbb{Z}/p\mathbb{Z}$. We note that a^n is a quadratic residue if and only if n is even.

unseen ⇓

2, B

So the sum of the squares of the non-residues is $\sum_{n=1}^{\frac{p-1}{2}} a^{2\cdot(2n-1)}$. Using geometric series, we can write this as $a^2 \cdot \frac{(1-a^{2(p-1)})}{1-a^4}$.

4, D

By Euler's theorem (in this case just Fermat's little theorem) the numerator of this fraction is divisible by p, whereas the denominator is not divisible by p as $p > 5$. So we have the result.

2, C

4. (a) We see that, as $p \equiv 1 \bmod 12$, by quadratic reciprocity $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1$. Thus $x^2 - 3y^2$ has a solution mod p if and only if $x^2 - z^2$ does where $z^2 = 3y^2$, but of course we may just take $x = z$ with $(z, p) = 1$.

meth seen ⇓

4, B

(b) First we see that $x^2 - 3y^2 = -2$ has the trivial solution $x = 1, y = 1$, which shows that $z = 1 + \sqrt{3}$ has norm 2. We note that z must be irreducible as it has prime norm, as we saw in class. Namely if $z = xy$ then $N(x) = \pm 1$ or $N(y) = \pm 1$.

meth seen ⇓

2, A

We see that $\sqrt{3}$ has prime norm, so the argument above applies to show that it is irreducible.

1, A

(c) We take $x^2 - 3y^2 = np$ for some $x, y, n \in \mathbb{Z}$, $(x, y) = 1$. We are guaranteed such integers by the solution to part (a). We write this as $(x + y\sqrt{3})(x - y\sqrt{3}) = np$. Now, partially factoring n into irreducibles, we have that $n = \prod_{i=1}^{m} \pi_i^{n_i}$.

meth seen ⇓

2, D

Suppose π is one of the π_i and $\pi | n$, then so does $\bar{\pi}$ (where $\bar{\pi}$ is the conjugate of π) as n is an integer and thus fixed by the multiplicative function $a + b\sqrt{3} \to a - b\sqrt{3}$.

1, D

Without loss of generality then $\pi | (x + y\sqrt{3})$. If $\bar{\pi} | (x + y\sqrt{3})$ then $N(\pi) | (x + y\sqrt{3})$. This implies that $N(\pi) | x, y$ contradicting $(x, y) = 1$, as $N(\pi)$ cannot be ± 1 as π is prime and thus not a unit. So we see that for every prime $\pi | n$, π divides exactly one of $(x + y\sqrt{3}), (x - y\sqrt{3})$, and $\bar{\pi}$ divides the other. We also see that $\pi \notin \mathbb{Z}$ for all such π by the same argument.

2, D

Now take some $\pi | n$, then without loss of generality $\pi | (x + y\sqrt{3}), \bar{\pi} | (x - y\sqrt{3})$ dividing $(x + y\sqrt{3})$ by π, $(x - y\sqrt{3})$ by $\bar{\pi}$, we obtain a pair of integers x_0, y_0 such that $x_0 + \sqrt{3} y_0 = (x + y\sqrt{3})/\pi$, whence $(x_0, y_0) = 1 = (x, y)$. Further $x_0^2 - 3y_0^2 = (\frac{n}{N(\pi)})p$. As $N(\pi) | n$ and $N(\pi) \neq \pm 1$, continuing this process inductively we obtain a new pair $(x_0, y_0) \in \mathbb{Z}^2$ with x_0, y_0 coprime, and an equation $x_0^2 - 3y_0^2 = \pm p$. Reducing mod 3 we see that we must have $x_0^2 - 3y_0^2 = p$.

3, D

meth seen ⇓

(d) We note that $(x + y\sqrt{3}) + (x - y\sqrt{3}) = 2x$ and $(x + y\sqrt{3}) - (x - y\sqrt{3}) = 2y\sqrt{3}$. Thus if π is a prime in $\mathbb{Z}[\sqrt{3}]$ with $\pi | (x + y\sqrt{3}), (x - y\sqrt{3})$, we see that we must have $\pi | p$ whence $(\pi, 6) = 1$. Thus such a $\pi | 2x$ and thus $\pi | x, (x + y\sqrt{3})$ which implies that $\pi | y$ as well. As we assume $(x, y) = 1$, this means that such a π does not exist, thus $(x + y\sqrt{3}), (x - y\sqrt{3})$ are coprime.

5, C

5. (a) First suppose x, y are odd. We write $y = 2n+1, x = 2m+1$, then $y^3 - x^3 = 8n^3 - 8m^3 + 12n^2 - 12m^2 + 6n - 6m = 8$ if and only if $4(n^3 - m^3) + 6(n^2 - m^2) + 3(n-m) = 4$. Without loss of generality $y > x \geq 0$ and thus we have that $n > m$, and we obtain $4(n^2 + nm + m^2) + 6(n+m) + 3 = \frac{4}{n-m} < 4$, which is impossible, so there are no odd solutions. [meth seen ⇓] [3, M]

Now suppose $x = 2m, y = 2n$ are both even. Then $8n^3 - 8m^3 = 8$ and we are reduced to solving $n^3 - m^3 = (n-m) \cdot (n^2 + nm + m^2) = 1$. Once again without loss of generality $n > m \geq 0$, then $n = m+1$ and we have $3m^2 + 3m + 1 = 1$ whence $m = 0$. So the only solutions to our original diophantine equation are $x = -2, y = 0$ or $x = 0, y = 2$ [3, M]

(b) We wish to solve $y^2 - 16 = (y-4)(y+4) = x^3$, and we approach this as we have approached finding integer points on similar elliptic curves in the past. Note that we have the two obvious solutions $y = \pm 4, x = 0$, and we wish to show that indeed these are the only solutions. [meth seen ⇓] [2, M]

Now first we suppose that x is odd. Then $(y-4), (y+4)$ are coprime integers, as otherwise if $p|(y-4), (y+4)$ then $p|2y$ and $p|x$ whence $p|(x, y)$ and p is odd, which is absurd as this would force $p|16$. So we obtain that $(y-4), (y+4)$ are coprime. But then $(y-4)$ and $(y+4)$ are both cubes since their product is a cube, but as y is odd this implies that there exist $z, t \in \mathbb{Z}$ odd such that $z^3 - t^3 = 8$, contradicting part (a). [6, M]

So we may assume that both x, y are even. Then $(2n)^2 = (2m)^3 + 16$. Looking at 2-adic valuations of both sides, we see that in fact we must have that $4|y$. Thus $16y_0^2 = 8m^3 + 16$, this shows that we must have $4|x$ and thus $2|m$. Using this, we can divide our equation by 16 and we obtain $y_0^2 = 4x_0^3 + 1$. We now observe that y_0 must be odd, whence writing out $y_0 = 2k+1$ and expanding, we obtain $(2k+1)^2 = 4k^2 + 4k + 1 = 4x_0^3 + 1$ or $k^2 + k = x_0^3$. Once again, since $k, k+1$ are both coprime, they must both be cubes. However, the only pairs of consecutive cubes are those in the sequence $-1, 0, 1$. So we see that $k = 0$ or $k = -1$. In either case, we see that $x_0 = 0$. Tracing back through our descent, we see this is only possible if $x = 0$, so we see that the solutions we proposed are indeed the only solutions. [6, M]

Review of mark distribution:
Total A marks: 31 of 30 marks
Total B marks: 24 of 21 marks
Total C marks: 13 of 13 marks
Total D marks: 12 of 16 marks
Total marks: 100 of 100 marks
Total Mastery marks: 20 of 20 marks

MATH60041 Number Theory

Question	Marker's comment
1	Question 1 generally went well, many students struggled with part (d) however some students solved it quite easily, and I think it is a calculation that looks more difficult than it is.
2	Generally there were no issues with this questions. Some students forgot that (-1) times a unit has the same norm, but otherwise it went very well and there were many perfect answers.
3	Generally part (a) was 7 free marks. I took off very few points for miscalculating quadratic residues (after all, its only off by a sign :)). (b) and (c) were surprisingly problematic, there were not many correct answers.nbsp;
4	Question 4 was by far the hardest question. Many students understood how to cover part (a) as we did it in class. Similarly part (b) was relatively elementary, and many students got at least partial credit for part (d). Part (c) seemed like one of the hardest questions on the exam, and only around a fifth of all students gave complete solutions.nbsp;

MATH70041 Number Theory

Question	Marker's comment
5	Question 5 was quite difficult, as expected from a mastery question. Surprisingly many students struggled with the fact that, unlike the similar elliptic curves we had covered in class, this elliptic curve had its integral solutions controlled by the ring \mathbb{Z} of integers! Rather than the integers in some quadratic imaginary field. Very few students noticed the relevance of part (a) to part (b), which was also surprising.nbsp;