Imperial College
London

MATH70041

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May 2023

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

Number Theory

Date: 2 June 2023

Time: 10:00 – 12:30 (BST)

Time Allowed: 2.5hrs

This paper has 5 Questions.

Please Answer All Questions in 1 Answer Booklet

Candidates should start their answers 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

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

1. (a) Find all positive integers $n \leq 100$ such that $3n \equiv 1 \mod 5$, $4n \equiv 1 \mod 7$, and $7n \equiv 1 \mod 13$. (6 marks)

   (b) Compute $(\frac{437}{493})$. (4 marks)

   (c) Show that 5 is a primitive root modulo 23. (3 marks)

   (d) For which integers x does there exist an integer y such that $2x^2 \equiv y^{11} \mod 23$? Justify your answer. (7 marks)

   (Total: 20 marks)

2. (a) Find the continued fraction expansion of $\sqrt{13}$. (8 marks)

   (b) Find a solution to each of the following Diophantine equations:

   $$x^2 - 13y^2 = -1, \quad x^2 - 13y^2 = -3, \quad x^2 - 13y^2 = 3.$$

   [*Hint: compute the first few convergents of the continued fraction expansion of* $\sqrt{13}$ *and look at the associated approximate solutions to Pell's equation* $x^2 - 13y^2 = 1$.] (6 marks)

   (c) Find a solution to Pell's equation $x^2 - 13y^2 = 1$. (6 marks)

   (Total: 20 marks)

3. Let p be an odd prime. Let $f(x) = ax + b$ be a polynomial with coefficients in $\mathbb{Z}/p\mathbb{Z}$ such that $a \neq 0$.

(a) Show that $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ takes p values. (3 marks)

(b) Show that

$$\prod_{n \in \mathbb{Z}/p\mathbb{Z}} f(n) \equiv 0 \mod p \text{ and } \prod_{\substack{n \in \mathbb{Z}/p\mathbb{Z} \\ n \neq -b/a}} f(n) \equiv -1 \mod p.$$

(4 marks)

(c) Now let $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbb{Z}/p\mathbb{Z}$ be such that $a_1, a_2 \neq 0$. Show that the congruence:

$$a_1x^2 + b_1x + c_1 \equiv a_2y^2 + b_2y + c_2 \mod p$$

has a solution in x, y.

[*Hint: count the image of polynomials of degree* 2.] (7 marks)

(d) Show that for every $c \in \mathbb{Z}/p\mathbb{Z}$ we have:

$$\prod_{n \in \mathbb{Z}/p\mathbb{Z}} (n^2 - c)^{\frac{p-1}{2}} \equiv 0 \text{ or } (-1)^{\frac{p+1}{2}} \mod p.$$

Is it true that both values are taken? Justify your answer. (6 marks)

(Total: 20 marks)

4. For every positive integer n let $Q(n)$ denote the number of solutions of the congruence:

$$x^2 + y^2 \equiv 1 \mod n.$$

(a) Show that Q is a multiplicative function. (4 marks)

(b) Show that $Q(n) \geq 4$ when n is odd. (1 mark)

(c) Show that if p is an odd prime then $Q(p^2) = p \cdot Q(p)$. (6 marks)

(d) Show that $Q(7) = 8$. (3 marks)

(e) Show that if p is a prime congruent to $1 \mod 4$ then $Q(p) = p - 1$. (6 marks)

(Total: 20 marks)

5. In this question you may use, without proof, Dirichlet's theorem on primes in arithmetic progressions: there are infinitely many primes p congruent to a mod n for any positive integer n, and any a with $(a, n) = 1$. Let $f(x) = ax^2 + bx + c$ be a polynomial with integer coefficients.

(a) Assume that for all but finitely many primes p there are $d_p, e_p \in \mathbb{Z}/p\mathbb{Z}$ such that

$$ax^2 + bx + c \equiv (d_p x + e_p)^2 \mod p.$$

Show that $f(x) = (dx + e)^2$ for some integers d, e. (15 marks)

(b) Assume that for infinitely many primes p there are $d_p, e_p \in \mathbb{Z}/p\mathbb{Z}$ such that

$$ax^2 + bx + c \equiv (d_p x + e_p)^2 \mod p.$$

Is true that $f(x) = \pm(dx + e)^2$ for some integers d, e? Justify your answer. (5 marks)

(Total: 20 marks)

Module:	MATH60041/MATH70041/MATH97036
Setter:	Pál
Checker:	Helm
Editor:	Pál
External:	Lotay
Date:	June 4, 2023
Version:	Draft version for checking

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)

May – June 2022

MATH60041/MATH70041/MATH97036 Number Theory Solutions

The following information must be completed:

Is the paper suitable for resitting students from previous years:

Category A marks: available for basic, routine material (excluding any mastery question) (40 percent = 32/80 for 4 questions):
1(a),(b),(c) 13 marks; 2(a),(b) 14 marks; 4(b),(d) 4 marks.

Category B marks: Further 25 percent of marks (20/ 80 for 4 questions) for demonstration of a sound knowledge of a good part of the material and the solution of straightforward problems and examples with reasonable accuracy (excluding mastery question):
1(d) 7 marks; 2(c) 6 marks; 3(a),(b) 7 marks; 4(a) 4 marks.

Category C marks: the next 15 percent of the marks (= 12/80 for 4 questions) for parts of questions at the high 2:1 or 1st class level (excluding mastery question):
3(c),(d) 13 marks.

Category D marks: Most challenging 20 percent (16/80 marks for 4 questions) of the paper (excluding mastery question):
4(c),(e) 12 marks.

Signatures are required for the final version:

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

Temporary front page

BSc, MSc and MSci EXAMINATIONS (MATHEMATICS)

May – June 2022

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

Number Theory Solutions

Date: ??

Time: ??

Time Allowed: 2 Hours for MATH96 paper; 2.5 Hours for MATH97 papers

This paper has *4 Questions (MATH96 version); 5 Questions (MATH97 versions)*.

Candidates should start their solutions to each question in a new main answer book.

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

Statistical tables will not be provided.

- DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO.
- Affix one of the labels provided to each answer book that you use, but DO NOT USE THE LABEL WITH YOUR NAME ON IT.
- Credit will be given for all questions attempted.
- Each question carries equal weight.
- Calculators may not be used.

1. (a) Solving the linear equations we find that x is $2 \mod 5$, $\mod 7$, and $\mod 13$, too. Note that 2 satisfies these conditions, and any other integer satisfying them differs from 2 by a multiple of 455 by the Chinese remainder theorem. Thus 2 is the only solution ≤ 100. **A**, similar seen

(6 marks)

(b) Note that the prime factorisation of 493 is $17 \cdot 29$. So $(\frac{437}{493}) = (\frac{437}{17}) \cdot (\frac{437}{29})$. By taking residues and using quadratic reciprocity we get that $(\frac{437}{17}) = (\frac{12}{17}) = (\frac{4 \cdot 3}{17}) = (\frac{3}{17}) = (\frac{17}{3}) = (\frac{2}{3}) = -1$, while $(\frac{437}{29}) = (\frac{2}{29}) = -1$ using the Gauss lemma. So $(\frac{437}{493}) = 1$. **A**, similar seen (4 marks)

(c)The order of 5 mod 23 must divide $22 = 2 \cdot 11$, so if 5 is not a primitive root then either $5^2 \equiv 1 \mod 23$ or $5^{11} \equiv 1 \mod 23$, but we have $5^2 \equiv 25 \equiv 2 \mod 23$ and $5^{11} \equiv (\frac{5}{23}) \equiv (\frac{23}{5}) \equiv (\frac{3}{5}) \equiv -1 \mod 23$ using quadratic reciprocity. **A**, similar seen (3 marks)

(d) If either of x or y is zero mod 23 then so is the other; this gives one solution. For the others, we may write $x = 5^a$ and $y = 5^b$, where a and b are well-defined mod 22, since 5 is a primitive root mod 19. The equation becomes $2a + 2 = 11b \mod 22$. This has solutions only for b even, in which case $11b$ is congruent to 0 mod 22 and a is thus either 10 or 21 mod 22. The solutions other than $(0, 0)$ are thus $(\pm 14, b)$ for b any quadratic residue mod 23. **B**, unseen (7 marks)

(Total: 20 marks)

2. (a) The continued fraction of $\sqrt{13}$ is given by $[3;1,1,1,1,6,1,1,1,1,6,\ldots]$. Details of the computation:

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

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. **A**, similar seen (8 marks)

(b) The first four convergents are: $\frac{4}{1}, \frac{7}{2}, \frac{11}{3}$ and $\frac{18}{5}$, giving rise to the following 3 approximate solutions:

$$4^2 - 13 \cdot 1^2 = 3, \quad 7^2 - 13 \cdot 2^2 = -3, \quad 18^2 - 13 \cdot 5^2 = -1. \ \mathbf{A}, \text{ similar seen } \ (6 \text{ marks})$$

(c) Note that $(18 + 5 \cdot \sqrt{13})^2 = 649 + 180 \cdot \sqrt{13}$ has norm one, since by part (b) the element $18 + 5 \cdot \sqrt{13}$ has norm -1. So $(649, 180)$ is a solution to $x^2 - 13y^2 = 1$. **B**, similar seen

(6 marks)

(Total: 20 marks)

3. (a) Note that f is the composition of the map $x \mapsto bx$ and $x \mapsto x + c$. Since $b \neq 0$ the former is a non-zero linear map, and hence a bijection. The latter is also a bijection, as $x \mapsto x - c$ is an inverse, so f is bijective, too. **B**, unseen (3 marks)

(b) By part (a) the image of f contains 0 so we have $\prod_{n\in\mathbb{Z}/p\mathbb{Z}} f(n) \equiv 0 \mod p$, and similarly

$$\prod_{\substack{n\in\mathbb{Z}/p\mathbb{Z}\\ n\neq -b/a}} f(n) \equiv \prod_{\substack{n\in\mathbb{Z}/p\mathbb{Z}\\ n\neq 0}} n \equiv -1 \mod p$$

also using Wilson's theorem in the second equation. **B**, similar seen (4 marks)

(c) Let $f(x) = ax^2+bx+c$ be a polynomial with coefficients in $\mathbb{Z}/p\mathbb{Z}$ such that $a \neq 0$. First we show that $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ takes $\frac{p+1}{2}$ values. Since $a \neq 0$ we may write $f(x) = a(x+\frac{b}{2a})^2 + (c-\frac{b^2}{4a^2})$. Since both $x \mapsto x + \frac{b}{2a}$ and $x \mapsto x + (c - \frac{b^2}{4a^2})$ are bijections, it will be enough to count the values of ax^2. The latter is the union of 0 and all quadratic residues, when a is a quadratic residue, and the union of 0 and all non-quadratic residues, otherwise. So in both cases its cardinality is $\frac{p+1}{2}$.

By the pigeon hole principle and the above the intersection of the images of $a_1x^2 + b_1x + c_1$ and $a_2x^2 + b_2x + c_2$ is non-zero. The claim is now clear. **C**, unseen (7 marks)

(d) When c is a square there is an n such that $n^2 - c = 0$, so

$$\prod_{n\in\mathbb{Z}/p\mathbb{Z}} (n^2 - c)^{\frac{p-1}{2}} \equiv 0 \mod p.$$

Otherwise c is nonquadratic residue, and hence:

$$\prod_{n\in\mathbb{Z}/p\mathbb{Z}} (n^2 - c)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} c^{\frac{p-1}{2}} \prod_{0<n<\frac{p+1}{2}} (n^2 - c)^{p-1} \equiv (-1)^{\frac{p+1}{2}} \mod p.$$

As there are both quadratic and nonquadratic residues mod p, both values are taken. **C**, similar seen

(6 marks)

(Total: 20 marks)

4. (a) By the Chinese Remainder Theorem when m and n are relatively prime the ring $\mathbb{Z}/mn\mathbb{Z}$ is isomorphic to the product of $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ as rings. This gives a bijection between solutions to $x^2+y^2 \equiv 1 \mod mn$ and pairs of solutions to $x^2+y^2 \equiv 1 \mod m$ and solutions to $x^2+y^2 \equiv 1 \mod n$. The claim follows. **B**, similar seen (4 marks)

(b) We have the obvious pairwise different solutions $x = \pm 1, y = 0$ and $x = 0, y = \pm 1$. **A**, unseen (1 mark)

(c) Fix $x_0, y_0 \mod p^2$ such that $x_0, y_0 \mod p$ is a solution. We will count the number of solutions of the form $x_0 + px_1, y_0 + py_1$. Since

$$(x_0 + px_1)^2 + (y_0 + py_1)^2 \equiv x_0^2 + y_0^2 + 2px_0x_1 + 2py_0y_1 \mod p^2,$$

this congruence is equivalent to

$$2x_0x_1 + 2y_0y_1 \equiv \frac{1 - x_0^2 - y_0^2}{p} \mod p.$$

Since not both of x_0, y_0 are congruent to $0 \mod p$, this congruence is a non-degenerate inhomogenous linear equation in two variables so it has p solutions. So every solution mod p has p different lifts, and hence $Q(p^2) = p \cdot Q(p)$. **D**, similar seen (6 marks)

(d) There are 4 solutions when either x or y is zero by part (b). Otherwise $x = 2, 3, 4, 5$, when $1 - x^2 = 4, 6, 6, 4$, respectively. Since the squares mod 7 are $0, 1, 2, 4$, the former are squares exactly when $x = 2, 5$, giving two possible values for y each, so we have 4 such solutions. **A**, similar seen (3 marks)

(e) Since $p \equiv 1 \mod 4$ there is an $\alpha \in \mathbb{Z}/p\mathbb{Z}$ such that $\alpha^2 = -1$, so we can write the equation in the form:

$$(x + \alpha y) \cdot (x - \alpha y) = 1.$$

Set $\beta = x + \alpha y$, then β is invertible and $\beta^{-1} = x - \alpha y$. This is a system of linear equations for every β with a unique solution $x = \frac{\beta+\beta^{-1}}{2}$ and $y = \frac{\beta-\beta^{-1}}{2\alpha}$, and conversely every such pair is a solution to the original equation. Since $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$ we get that $Q(p) = p - 1$. **D**, similar seen (6 marks)

(Total: 20 marks)

5. (a) By assumption both a and c are squares mod p for all but finitely many primes p. We first show that this implies that these values are squares. Write $a = n^2 m$ where m is squarefree. First assume that $m \neq \pm 1, \pm 2$. Then there exists an odd prime p dividing m; write $m = pm'$. By Dirichlet's theorem there exist infinitely many primes q that are congruent to 1 modulo $4m'$ and congruent to a quadratic nonresidue mod p; in particular there exist infinitely many such that $(\frac{a}{q}) = 1$. But

$$\left(\frac{a}{q}\right) = \left(\frac{m}{q}\right) = \left(\frac{\pm 1}{q}\right)\left(\frac{p}{q}\right)\left(\frac{m'}{q}\right).$$

(5 marks)

We have $(\frac{\pm 1}{q}) = 1$ since $q \equiv 1 \mod 4$, and $(\frac{p}{q}) = -1$ since $q \equiv 1 \mod 4$ and a nonresidue mod p. Finally $(\frac{m'}{q})$ is a product of $(\frac{p_i}{q})$ for the primes p_i dividing m'; each term is equal to $(\frac{q}{p_i}) = (\frac{1}{q_i}) = 1$. So $(\frac{a}{q}) = -1$ contradicting our hypothesis. Suppose now that $m = \pm 2$. Then $(\frac{a}{p}) = -1$ for any prime p congruent to 5 mod 8, again contradicting our hypothesis. If $m = -1$ then $(\frac{a}{p}) = -1$ for any prime p congruent to 3 mod 4, a contradiction, too. Hence the claim follows. (5 marks)

Since $(d_p x + e_p)^2 \equiv d_p^2 x^2 + 2 d_p e_p x + e_p^2 \mod p$ we get that $4ac \equiv b^2 \mod p$ for all but finitely many primes p. Therefore $4ac = b^2$. Now choose integers e, f such that $e^2 = a, f^2 = c$. Then $4e^2 f^2 = b^2$, so $2ef = \pm b$. By changing the sign of e if it is necessary we get that $2ef = b$, and the claim is now clear. (5 marks)

(b) Set $f(x) = 5x^2 + 10x + 5$. By Dirichlet's theorem there are infinitely many primes p such that $p \equiv 1 \mod 5$. By quadratic reciprocity

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1,$$

so there is an $e_p \in \mathbb{Z}/p\mathbb{Z}$ such that $e_p^2 \equiv 5 \mod p$. Then $(e_p x + e_p)^2 \equiv f(x) \mod p$. On the other hand ± 5 is not a square, and hence $f(x) \neq \pm(dx + e)^2$ for any pair of integers d, e.

(5 marks)

(Total: 20 marks)

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.		
ExamModuleCode	**QuestionNumber**	**Comments for Students**
MATH60041/70041	1	Q1: Part (a) was a routine application of the Chinese remainder theorem. Part (b) was a simple computation using quadratic reciprocity, however some students applied it before verifying that the numerator or the denominator is a prime. We never stated quadratic reciprocity for pairs of odd numbers, only for pairs of odd primes, so you have to justify why what is done is valid. Part (c) was again easy, computing two powers of 5 mod 23. Part (d) was using using (c) and solving the resulting simple linear congruence.
MATH60041/70041	2	Q2: This problem largely consisted of routine computations, which most of the students did well. Only part (c) needed an idea; that is instead of continuing the approximation, just simply square the unit corresponding to the solution in part (b) to avoid heavy computations. Most students figured this out. Well done!
MATH60041/70041	3	Q3: Although I thought that this question will be more challenging, students did well in general. In part (a) a common error was to assume that this map is a homomorphism, but it is not, so one cannot talk about its kernel and cannot deduce anything immediately. Part (b) was done well by most. In part (c) several students did not realise that they have to complete the square to be able to use the result in (a) directly. There was also a different way to show the bound on the image of these polynomials discovered by several students, which I was very pleased to see. Part (d) was the most challenging, but several students did realise that the terms have to paired similarly to our proof of Wilson's theorem. An attempted strategy to directly count the number of terms which are 1 is not so easy, and it was not carried out correctly by anyone.
MATH60041/70041	4	Q4: Part (a) was an easy application of the Chinese remainder theorem, while parts (b) and (d) were simple computations. Part (c) required to show that solutions mod p can be lifted exactly p ways to solutions mod p^2; this required to write out the resulting congruence and realise that it is linear with non-zero coefficients. Part (d) used a trick which we saw while we solved Diophantine equations: because that p is congruent to 1 mod 4 the left hand side factorises, after which it is easy to solve. The argument needs to use this assumption, since for primes which are congruent to 3 mod 4 the answer is p+1. So all naive attempts to directly count the solutions is doomed to failure.
MATH70041	5	Q5: Students struggled with this question although part (a) was not very different from a question in the exam last year, but instead of numbers, it looked at the same problem for quadratic polynomials. One gets that the leading and the constant terms are squares mod almost all primes, after which it is routine to conclude these are squares. One also gets a relation between these coefficients and the remaining one, which can be solved by flipping the sign, if it is needed. Part (b) was easy, once one noticed that any square polynomial times any prime which is a square mod infinitely many primes will give an example.