Imperial College
London

MATH97036 MATH70041

BSc, MSci and MSc 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

Date: 18 May 2022

Time: 09:00 – 11:30 (BST)

Time Allowed: 2:30 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 AS ONE PDF TO THE RELEVANT DROPBOX ON BLACKBOARD WITH COMPLETED COVERSHEETS WITH YOUR CID NUMBER, QUESTION NUMBERS ANSWERED AND PAGE NUMBERS PER QUESTION.

In this exam you may use, without proof, any result proved in the lectures or problem sheets as long as you state it clearly.

1. (a) Find the smallest positive integer n such that $2n \equiv 1 \pmod 3$, $3n \equiv 1 \pmod 5$, and $5n \equiv 1 \pmod 7$. (6 marks)

   (b) Compute $\left(\frac{331}{823}\right)$. (4 marks)

   (c) Show that 2 is a primitive root modulo 19. (3 marks)

   (d) For which integers x does there exist an integer y such that $2x^2 \equiv y^9 \pmod{19}$? (7 marks)

(Total: 20 marks)

2. (a) Find the continued fraction expansion of $\sqrt{7}$. (6 marks)

   (b) Find the two smallest solutions to $x^2 - 7y^2 = 1$, where x and y are both strictly positive and solutions are ordered by the value of y. (7 marks)

   (c) Find the two smallest solutions to $x^2 - 7y^2 = 2$, where x and y are both strictly positive and solutions are ordered by the value of y. (7 marks)

(Total: 20 marks)

3. Let $\Phi(n)$ denote the Euler Φ function.

(a) Show that if d divides n, then $\Phi(d)$ divides $\Phi(n)$. (4 marks)

(b) Let $P(X)$ be a nonconstant monic polynomial in X with integral coefficients, and for each positive integer n, let $f(n)$ denote the number of roots of $P(X)$ in $\mathbb{Z}/n\mathbb{Z}$. Show that the function $n \mapsto f(n)$ is multiplicative. (4 marks)

(c) Let $f(n)$ be the function defined by $f(n) = \frac{1}{n} \sum_{1 \le a \le n; (a,n)=1} a$. Show that $\sum_{d|n} f(d) = \frac{n+1}{2}$. [HINT: mimic the proof that $\sum_{d|n} \Phi(n) = n$.] (6 marks)

(d) Let $f(n)$ be as in part (c), and use the result of part (c) to show that $f(n) = \frac{1}{2}\Phi(n)$ for $n \ge 2$. [HINT: first verify this for n prime; then use induction.] (6 marks)

(Total: 20 marks)

4. As in Question 3, $\Phi(n)$ denotes the Euler Φ function.

(a) Let n be a positive integer and a an integer with $(a, n) = 1$. Show that a is a primitive root modulo n if, and only if, $a^{\frac{\Phi(n)}{p}} \not\equiv 1 \pmod{n}$ for all primes p dividing $\Phi(n)$. (6 marks)

(b) Let $\lambda(n)$ denote the exponent of $(\mathbb{Z}/n\mathbb{Z})^\times$; that is, the smallest positive integer m such that $a^m \equiv 1 \pmod{n}$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Show that if m and n are relatively prime, then $\lambda(mn)$ is the least common multiple of $\lambda(m)$ and $\lambda(n)$. (4 marks)

(c) Show that $\lambda(n) \le \frac{\Phi(n)}{2^{r-1}}$, where r is the number of odd primes dividing n. (4 marks)

(d) Show that if m divides n, then $\lambda(m)$ divides $\lambda(n)$. (6 marks)

(Total: 20 marks)

5. In this question you may use, without proof, Dirichlet's theorem that there are infinitely many primes p congruent to a mod n for any positive integer n, and any a with $(a, n) = 1$.

(a) Let a be a nonzero integer, and suppose that $\left(\frac{a}{p}\right) = 1$ for all but finitely many primes p congruent to 1 mod 4. Show that $a = \pm b^2$ for some integer b. (15 marks)

(b) Use part (a) to show that if a and b are nonzero integers such that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ for all but finitely many primes p, then ab is a perfect square. (5 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2022

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, 2 mod 5, and 3 mod 7. Note that 17 satisfies these conditions, and any other integer satisfying them differs from 17 by a multiple of 105. Thus x is 17.

meth seen ⇓

6, A

(b) We have $\left(\frac{331}{823}\right) = -\left(\frac{823}{331}\right) = -\left(\frac{161}{331}\right)$. Now $161 = 7 \cdot 23$, and $\left(\frac{7}{331}\right) = -\left(\frac{331}{7}\right) = -\left(\frac{2}{7}\right) = -1$. Similarly $\left(\frac{23}{331}\right) = -\left(\frac{331}{23}\right) = -(923) = -1$. Thus $\left(\frac{331}{823}\right) = -1$.

meth seen ⇓

4, A

(c) The order of 2 mod 19 must divide 18, so if 2 is not a primitive root the either $2^6 \equiv 1$ mod 19 or $2^9 \equiv 1$ mod 19, but we have $2^6 \equiv 7$ mod 19 and $2^9 = -1$ mod 19.

meth seen ⇓

3, A

(d) If either of x or y is zero mod 19 then so is the other; this gives one solution. For the others, we may write $x = 2^a$ and $y = 2^b$, where a and b are well-defined mod 18, since 2 is a primitive root mod 19. The equation becomes $2a + 1 = 9b$ (mod 18). This has solutions only for b odd, in which case $9b$ is congruent to 9 mod 18 and a is thus either 4 or 13 mod 19. The solutions other than $(0, 0)$ are thus $(\pm 16, b)$ for b any quadratic nonresidue mod 19.

unseen ⇓

7, B

2. (a) The continued fraction of $\sqrt{7}$ is given by $[2; 1, 1, 4, 1, 1, 4, \dots]$.

meth seen ⇓

(b) The first convergent of the continued fraction that gives a solution is $\frac{8}{3}$, so the first solution is $(8, 3)$. We have $(8 + 3\sqrt{7})^2 = 127 + 48\sqrt{7}$, so the second solution is $(127, 48)$.

6, A

(c) The smallest solution is clearly $(3, 1)$, by inspection. We have $(3+\sqrt{7})(8+3\sqrt{7}) = 45 + 17\sqrt{7}$, so the second solution is $(45, 17)$.

meth seen ⇓

7, A

meth seen ⇓

7, A

3. (a) Write $n = p_1^{r_1} \dots p_n^{r_n}$ for distinct primes $p_1, \dots, p_n$. Then $d = p_1^{s_1} \dots p_n^{s_n}$, with $s_i \leq r_i$ for all i. Since $\Phi(n)$ is the product of $\Phi(p_i^{r_i})$ for all i, and $\Phi(d)$ is the product of $\Phi(p_i^{s_i})$, it suffices to show that $\Phi(p^s)$ divides $\Phi(p^r)$ whenever $s \leq r$. But $\Phi(p^s) = (p-1)p^{s-1}$ and $\Phi(p^r) = (p-1)p^{r-1}$ so this is clear.

sim. seen ⇓

4, B

(b) 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 $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$ as rings. This gives a bijection between solutions a to $f(x) = 0$ modulo mn and pairs (b, c) of a solution to $f(x) = 0$ modulo n and a solution to $f(x) = 0$ modulo m. The claim follows.

sim. seen ⇓

4, B

(c) We have:

unseen ⇓

$$\sum_{d|n} f(d) = \sum_{d|n} \frac{1}{d} \sum_{1 \leq a \leq d, (a,d)=1} a = \frac{1}{n} \sum_{d|n} \sum 1 \leq a \leq d, (a,d) = 1 \frac{n}{d} a.$$

6, D

Rewriting the inner sum on the left as a sum over $b = \frac{n}{d}a$, we find that the right hand side is equal to

$$\frac{1}{n} \sum_{d|n} \sum_{1 \leq b \leq n, (b,n) = \frac{n}{d}} b.$$

As d varies over the divisors of n, each integer b between 1 and n appears in the sum exactly once. The sum is thus equal to $\frac{1}{n} \sum_{b=1}^{n} b = \frac{n+1}{2}$.

unseen ⇓

(d) For p prime this is easy to verify directly. We then proceed by induction. Fix $n > 2$ and suppose the claim is true for all d dividing n. Then

$$f(n) = \frac{n+1}{2} - \sum_{d|n, d<n} f(d).$$

By the induction hypothesis, and the fact that $f(1) = 1$ whereas $\frac{\Phi(1)}{2} = \frac{1}{2}$, we find that the right hand side is equal to $\frac{n}{2} - \sum_{d|n, d<n} \frac{\Phi(d)}{2}$ which is indeed equal to $\frac{\Phi(n)}{2}$.

6, D

4. (a) The order of a modulo n divides $\Phi(n)$, and thus the order of a is strictly less then $\Phi(n)$ if, and only if, the order of a divides $\frac{\Phi(n)}{p}$ for some p dividing $\Phi(n)$. The latter occurs if, and only if, $a^{\frac{\Phi(n)}{p}} \equiv 1 \bmod n$ for some p dividing $\Phi(n)$.

sim. seen ⇓

6, B

(b) When $(m,n)=1$, the group $(\mathbb{Z}/mn\mathbb{Z})^\times$ is isomorphic to the product $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Note that the order of an element (a,b) in a product of abelian groups $A \times B$ is the least common multiple of the orders of a and b; since the exponent is the least common multiple of the orders of all the elements, it follows that the exponent of $A \times B$ is the least common multiple of the exponents of A and B.

sim. seen ⇓

4, C

(c) If $m = 2^s \prod_i p_i^{r_i}$ for distinct odd primes p_i, then $\Phi(m)$ is the product of $\Phi(2^s)$ with all of the $\Phi(p_i^{r_i})$, whereas $\lambda(m)$ is the least common multiple of the $\lambda(p_i^{r_i})$. Since $\Phi(p_i^{r_i})$ is even, for each i either $\lambda(p_i^{r_i})$ is either even or at most $\frac{\Phi(p_i^{r_i})}{2}$. Since the least common multiple of s even integers is at most their product dividing by 2^{s-1} the claim follows.

unseen ⇓

4, C

(d) When m divides n we have a surjection of $(\mathbb{Z}/n\mathbb{Z})^\times$ to $(\mathbb{Z}/m\mathbb{Z})^\times$; in particular the order of any element a modulo m the order of any invertible lift modulo n. It follows that the least common multiple of these orders modulo m divides that modulo n.

unseen ⇓

6, D

5. (a) Write $a = n^2 m$ where m is squarefree, and suppose that $m \notin \{\pm 1, \pm 2\}$. 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; by assumption for such q we have $\left(\frac{a}{q}\right) = 1$. [5, M]

But

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

[3, M]

We have $\left(\frac{\pm 1}{q}\right) = 1$ since q is 1 mod 4, and $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = -1$ since q is 1 mod 4 and a nonresidue mod p. Finally $\left(\frac{m'}{q}\right)$ is a product of $\left(\frac{p_i}{q}\right)$ for p_i the primes dividing m'; each term is equal to $\left(\frac{q}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1$. So $\left(\frac{a}{q}\right) = -1$ contradicting our hypothesis. [4, M]

Suppose now that $m = \pm 2$. Then $\left(\frac{a}{p}\right) = -1$ for any prime p congruent to 5 mod 8, again contradicting our hypothesis. So $m = \pm 1$ and the claim follows. [3, M]

(b) Suppose a and b are integers such that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ for all but finitely many p. Then $\left(\frac{ab}{p}\right) = 1$ for all but finitely many primes p. By part (a) we have $ab = \pm n^2$ for some n. But if $ab = -n^2$ then $\left(\frac{ab}{p}\right) = -1$ for any prime p congruent to 3 mod 4 and not dividing ab; since there are infinitely many such p this is impossible. [5, M]

Review of mark distribution:
Total A marks: 33 of 32 marks
Total B marks: 21 of 20 marks
Total C marks: 8 of 12 marks
Total D marks: 18 of 16 marks
Total Mastery marks: 20 of 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.

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 separate pdf file with your email.

ExamModuleCode	QuestionNumber	Comments for Students
MATH60041MATH97036 MAT	1	This was mostly routine although many people missed solutions to part d. There was a small penalty for overlooking the trivial solution (0,0), and a larger one for missing some of the solutions in the multiplicative group.
	2	Everyone did quite well on this question.
	3	Lots of people tried to argue that both sides of the sum in part c were multiplicative, which is false. Some people found it easier to prove part d first and then deduce part c from part d.
	4	Many students had some trouble with the quantifiers in arguing that the exponent of a product is the lcm of the exponents of the factors.
	5	This was a quite challenging question and it was an achievement to come up with even a partial solution. Congratulations to those who did so!