Queen Mary
University of London

# B. Sc. Examination by course unit 2009

## MTH6128 Number Theory

**Duration: 2 hours**

**Date and time: 26 May 2009, 10:00–12:00**

---

**Apart from this page, you are not permitted to read the contents of this question paper until instructed to do so by an invigilator.**

**You may attempt as many questions as you wish and all questions carry equal marks. Except for the award of a bare pass, only the best 4 questions answered will be counted.**

**Calculators are NOT permitted in this examination. The unauthorized use of a calculator constitutes an examination offence.**

**Complete all rough workings in the answer book and cross through any work which is not to be assessed.**

**Candidates should note that the Examination and Assessment Regulations state that possession of unauthorized materials by any candidate who is under examination conditions is an assessment offence. Please check your pockets now for any notes that you may have forgotten that are in your possession. If you have any, then please raise your hand and give them to an invigilator now.**

**Exam papers must not be removed from the examination room.**

**Examiner(s): P. J. Cameron**

---

 

**Question 1** (a) Use the Euclidean algorithm to find the greatest common divisor of 167 and 59, and to express it in the form $167x+59y$ for integers $x$ and $y$. [5]

(b) What is meant by a finite *continued fraction* $[a_0;a_1,a_2,\ldots,a_n]$? [3]

(c) Find a continued fraction whose value is $\dfrac{167}{59}$. [5]

(d) Given two integers $a$ and $b$, show that an integer $n$ can be written in the form $ax+by$ for some $x,y\in\mathbb{Z}$ if and only if $n$ is divisible by $\gcd(a,b)$, and describe how to find the general solution of this equation in integers $x,y$. [7]

(e) Find all solutions of $167x+59y=5$. [5]

**Question 2** (a) What is meant by an infinite continued fraction $[a_0;a_1,a_2,\ldots]$, where $a_0$ is an integer and $a_1,a_2,\ldots$ are positive integers? [4]

(b) State without proof which numbers can be represented by

(i) a finite continued fraction,

(ii) an infinite continued fraction.

Are the representations unique? [4]

(c) Prove that a number which is represented by a purely periodic continued fraction is a quadratic irrational. (You should define these terms.) [7]

(d) Find a continued fraction representation for $\sqrt{5}$. [5]

(e) Find the numbers represented by the continued fractions $[\overline{1;1,2}]$ and $[1;\overline{1,1,2}]$. [5]

**Question 3** (a) What is meant by a *best rational approximation* $p/q$ to an irrational number $y$? [3]

(b) State without proof a theorem relating the best rational approximations to $y$ to the convergents to the continued fraction for $y$. [4]

(c) Given that $\sqrt{2}=[1;\overline{2}]$, show that the sequence of best rational approximations $p_n/q_n$ to $\sqrt{2}$ is given by the pair of recurrence relations

$$p_0=q_0=1,\qquad p_1=3,\,q_1=2,$$
$$p_{n+1}=2p_n+p_{n-1},\quad q_{n+1}=2q_n+q_{n-1}\quad\text{for } n\geq 1.$$

[5]

(d) Prove (by induction or otherwise) that, with $p_n$, $q_n$ as in part (c),

$$p_{n+1}=p_n+2q_n,\qquad q_{n+1}=p_n+q_n.$$

[5]

(e) State a theorem describing the solutions in positive integers to the equation $x^2-ny^2=\pm 1$ in terms of the convergents to $\sqrt{n}$. Hence describe all solutions in positive integers to $x^2-2y^2=\pm 1$, explaining which solutions correspond to each choice of sign. [8]

**Question 4** (a) What is a *quadratic residue* modulo an odd prime $p$? Define the *Legendre symbol* $\left(\frac{a}{p}\right)$. [3]

(b) State the value of $\left(\frac{-1}{p}\right)$. [3]

(c) State the *Law of Quadratic Reciprocity*. [3]

(d) Use the Law of Quadratic Reciprocity to show that, if $p$ is a prime with $p \geq 5$, then

$$\left(\frac{-3}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \bmod 3, \\ -1 & \text{if } p \equiv -1 \bmod 3 \end{cases}.$$

(Other rules for computing the Legendre symbol may be used without proof provided they are stated clearly.) [8]

(e) Suppose that $p_1, \ldots, p_r$ are primes congruent to 1 mod 3. Let $x = 2p_1 \cdots p_r$, and $N = x^2 + 3$. Show that $N$ has a prime divisor congruent to 1 mod 3. [4]

(f) Hence show that there are infinitely many primes congruent to 1 mod 3. [4]

**Question 5** (a) Define *Euler's totient function* $\phi(n)$ for positive integers $n$. [3]

(b) Show that [6]

$$\sum_{d|n} \phi(d) = n.$$

(c) Show that, if $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r$ are positive integers, then

$$\phi(n) = p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1)\cdots p_r^{a_r-1}(p_r-1).$$

[5]

(d) Prove that $\phi(n)$ is even for all integers $n > 2$. [5]

(e) Find all positive integers $n$ such that $\phi(n) = 4$. [6]

**Question 6** (a) State a theorem on the representation of prime numbers as sums of two squares. [4]

(b) Deduce that the positive integer $n$ is a sum of two squares if and only if the squarefree part of $n$ has no prime divisors congruent to $-1$ mod 4. You may use any results you require about quadratic residues, but should state them clearly. [11]

(c) Find all expressions for 130 as the sum of two squares. [4]

(d) State which positive integers can be represented as

(i) sums of three squares,

(ii) sums of four squares.

[6]

 

**Question 7** (a) What is a *quadratic form* in two variables $x$ and $y$i over the integers? What is its *discriminant*? [3]

(b) What is meant by saying that a quadratic form is

(i) *positive definite*,

(ii) *negative definite*,

(iii) *indefinite*?

Give conditions for each of these properties in terms of the coefficients and the discriminant of the form. [4]

(c) For each of the following quadratic forms, say whether it is positive definite, negative definite or indefinite:

(i) $x^2 + 2xy - y^2$,

(ii) $x^2 - 3xy + 3y^2$.

[4]

(d) What is meant by saying that a positive definite quadratic form is *reduced*? [3]

(e) Find a reduced quadratic form equivalent to each of the forms in part (c) which you found to be positive definite. [4]

(f) Find all reduced positive definite quadratic forms with discriminant $-8$. [7]

---

**End of Paper**