Main Examination period 2017

MTH6128 / MTH6128P: Number Theory

Duration: 2 hours

You should attempt ALL questions. Marks available are shown next to the questions.

Calculators are not permitted in this examination. The unauthorised use of a calculator constitutes an examination offence.

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

Possession of unauthorised material at any time when under examination conditions is an assessment offence and can lead to expulsion from QMUL. Check now to ensure you do not have any notes, mobile phones, smartwatches or unauthorised electronic devices on your person. If you do, raise your hand and give them to an invigilator immediately.

It is also an offence to have any writing of any kind on your person, including on your body. If you are found to have hidden unauthorised material elsewhere, including toilets and cloakrooms, it shall be treated as being found in your possession. Unauthorised material found on your mobile phone or other electronic device will be considered the same as being in possession of paper notes. A mobile phone that causes a disruption in the exam is also an assessment offence.

Exam papers must not be removed from the examination room.

Examiners: X. Li and J. Bray

Question 1. [20 marks]

(a) Define the terms

(i) **algebraic number**;
(ii) **algebraic integer**; [**4**]
(iii) **transcendental number**.

(b) Which of the following numbers are algebraic integers? Explain, stating explicitly which theorems you use.

(i) $\frac{1+\sqrt{11}}{2}$; [**6**]
(ii) $\frac{2}{3+\sqrt{7}}$;
(iii) $\frac{3+\sqrt{45}}{6}$.

(c) Let a be an algebraic number, and suppose that $a \neq 0$. Show that $\frac{1}{a}$ is an algebraic number. [**5**]

(d) Give an example of an algebraic integer which is not approximable by rationals up to order 6. Explain why the example you gave has the desired properties. [**5**]

Question 2. [20 marks]

(a) Calculate the value of the infinite continued fraction $[3; 4, \overline{2, 1}]$. [**6**]

(b) You are given that

$$[10; \overline{1, 1, 1, 2, 2, 1, 1, 1, 20}]$$

is the continued fraction for $\sqrt{113}$. Using this, find positive integers x and y such that $x^2 + y^2 = 113$. [**6**]

(c) You are given that

$$[9; \overline{1, 2, 1, 18}]$$

is the continued fraction for $\sqrt{95}$. Using this, find all the integer solutions of the equation $x^2 - 95y^2 = \pm 1$. [**8**]

Question 3. [20 marks]

(a) Let p be a prime. What is a **primitive root** (mod p)? What is the **order** (mod p) of an integer x with $1 \leq x \leq p - 1$? [**4**]

(b) Find a primitive root (mod 13). [**5**]

(c) What are the possible orders (mod 13) of an integer x with $1 \leq x \leq 12$? For each possible order, find a natural number x with $1 \leq x \leq 12$ which has exactly that order (mod 13). [**5**]

(d) Let p be a prime and g a primitive root (mod p). Show that for every integer x with $1 \leq x \leq p - 1$, there is a natural number i with $x \equiv g^i \pmod{p}$. [**6**]

Question 4. [20 marks]

(a) Let p be an odd prime, and let a be an integer. Define the **Legendre symbol** $\left(\dfrac{a}{p}\right)$. [**3**]

(b) Calculate the value of $\left(\dfrac{21}{67}\right)$. You should state clearly any rules for computing Legendre symbols that you use, but are not required to prove them. [**6**]

(c) Let p be an odd prime. Show that we have $\left(\dfrac{5}{p}\right) = -1$ if and only if $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$. You should state clearly any rules for computing Legendre symbols that you use, but are not required to prove them. [**5**]

(d) Show that there are infinitely many primes congruent to 1 modulo 4. [**6**]

Question 5. [20 marks]

(a) What is a **quadratic form** over the integers? [**2**]

(b) In each of the following cases, state whether the quadratic form is positive definite, negative definite, indefinite, or degenerate:

(i) $7x^2 + 3xy + 4y^2$;
(ii) $5x^2 + 4xy - 3y^2$. [**4**]

(c) Find the reduced positive definite quadratic form which is equivalent to [**4**]

$$5x^2 + 2xy + y^2.$$

(d) Show that equivalent quadratic forms have the same discriminant. [**4**]

(e) Write down two positive definite quadratic forms with the same discriminant, which are not equivalent. Explain why the examples you gave have the desired properties. [**6**]

End of Paper.