UNIVERSITY OF BRISTOL

Examination for the Degree of B.Sc. and M.Sci. (Level 3)

NUMBER THEORY

MATH 30200

(Paper Code MATH-30200)

May-June 2015, 2 hours 30 minutes

This paper contains **five** *questions.*
A candidate's **FOUR** *best answers will be used for assessment.*
On this examination, the marking scheme is indicative and is intended only as a guide to the relative weighting of the questions.
Calculators are **not** *permitted in this examination.*

Do not turn over until instructed.

1. (a) (2+4 marks) (i) State, without proof, the Law of Quadratic Reciprocity for Legendre symbols.
   (ii) Determine the primes p for which 5 is a quadratic residue modulo p.

   (b) (3+2+3 marks) (i) Suppose that $p > 5$ is a prime number for which 5 is a quadratic residue modulo p. Show that the congruence $x^2 - x - 1 \equiv 0 \pmod{p}$ has a solution λ.
   (ii) Put $\mu = 1 - \lambda$. Show that μ is also a solution of $x^2 - x - 1 \equiv 0 \pmod{p}$, and prove that $\lambda \not\equiv \mu \pmod{p}$.
   (iii) When n is a non-negative integer, put

   $$u_n = \frac{\lambda^n - \mu^n}{\lambda - \mu}.$$

   Prove that u_n satisfies $u_0 \equiv 0 \pmod{p}$, $u_1 \equiv 1 \pmod{p}$ and

   $$u_{n+2} \equiv u_{n+1} + u_n \pmod{p} \quad (n \geq 0).$$

   (c) (2+3 marks) State and prove Fermat's Little Theorem.

   (d) (6 marks) Let (F_n) denote the sequence of Fibonacci numbers, defined by taking

   $$F_1 = 1, \quad F_2 = 1, \quad \text{and} \quad F_{n+2} = F_{n+1} + F_n \ (n \geq 1).$$

   Suppose that $p > 5$ is a prime number for which 5 is a quadratic residue modulo p. Using the conclusion of (b)(iii), prove that $F_n \equiv 0 \pmod{p}$ whenever $(p-1)|n$.

2. This question is concerned with the polynomial $f(x) = x^2 - 2x + 8$.

   (a) (2+2 marks) (i) State Lagrange's theorem concerning the number of solutions of a polynomial congruence.
   (ii) Find all of the solutions of the polynomial congruence $f(x) \equiv 0 \pmod{11}$.

   (b) (2+3+3 marks) (i) State a version of Hensel's Lemma.
   (ii) Find all of the solutions of the polynomial congruence $f(x) \equiv 0 \pmod{121}$, justifying your answer.
   (iii) Find all of the solutions of the polynomial congruence $f(x) \equiv 0 \pmod{49}$, justifying your answer.

   (c) (6 marks) Let $p > 7$ be a prime number. By examining the values of x for which $f(x) \equiv f'(x) \equiv 0 \pmod{p}$, show that for every natural number n, the number of solutions of the polynomial congruence $f(x) \equiv 0 \pmod{p^n}$ is at most 2.

   (d) (2+5 marks) (i) Determine the number of solutions of the polynomial congruence $f(x) \equiv 0 \pmod{8}$.
   (ii) Determine the number of solutions of the respective polynomial congruences

   $$f(x) \equiv 0 \pmod{560008} \quad \text{and} \quad f(x) \equiv 0 \pmod{560024},$$

   explaining your answer. [You may assume in this question that the integers 70001 and 70003 are both prime numbers].

Continued...

3. (a) (2+2 marks) Give a formula for Euler's function $\phi(n)$, and state Euler's theorem.

   (b) (2+2 marks) (i) Define what it means for a residue modulo n to be a primitive root.

   (ii) For what values of n do primitive roots modulo n exist? (Provide as complete a list as you are able, without justifying your answer).

   (c) (4+4 marks) Let p and q be distinct odd prime numbers. Also, let g_1 be a primitive root modulo p, and g_2 a primitive root modulo q.

   (i) Suppose that $x \equiv g_1 \pmod{p}$ and $x \equiv g_2 \pmod{q}$. Show that whenever one has $x^n \equiv 1 \pmod{pq}$, then $(p-1)|n$ and $(q-1)|n$.

   (ii) Prove that there exists a residue $w \pmod{pq}$ having order equal to the least common multiple of $p-1$ and $q-1$.

   (d) (5+4 marks) Let p and q be distinct odd primes with $p < q$, and suppose that $a^{pq} \equiv a^{-1} \pmod{pq}$ for all integers a with $(a, pq) = 1$.

   (i) Prove that $(p-1)|(q+1)$ and $(q-1)|(p+1)$.

   (ii) Deduce that $|p-q| = 2$, and hence show that $p = 3$ or $p = 5$.

4. (a) (2+3 points) Let θ be an irrational number possessing continued fraction expansion $[a_0; a_1, a_2, \ldots]$. Define what is meant by the n^{th} convergent p_n/q_n to θ, and show that

$$p_0 = a_0, \quad q_0 = 1, \quad p_1 = a_0a_1 + 1, \quad q_1 = a_1.$$

   (b) (2+5 marks) State and prove Dirichlet's Theorem on Diophantine approximation.

   (c) (2+4 marks) (i) Explain what is meant by (a) an algebraic number, and (b) a transcendental number.

   (ii) Let θ be a real algebraic number of degree n. State Liouville's Theorem concerning Diophantine approximations to θ.

   (d) (7 marks) Let $3 \cdot b_1b_2\ldots$ be the decimal expansion of π, so that $b_1 = 1$, $b_2 = 4$, and b_n is the n^{th} decimal digit of π. Use Liouville's Theorem to prove the transcendence of

$$\sum_{n=1}^{\infty} 2015^{-(b_n+1)n!}.$$

5. (a) (2+2 marks) Define what is meant by a multiplicative function. Prove that when $f(n)$ is multiplicative, then so too is $g(n) = f(n^3)$.

   (b) (3+3 marks) Let $\tau(n)$ denote the number of positive divisors of n.

   (i) Show that for every prime p and every natural number h, one has $\tau(p^{3h}) \leq \tau(p^h)^2$.

   (ii) Apply multiplicativity to show that for each $n \in \mathbb{N}$, one has $\tau(n^3) \leq \tau(n)^2$.

   (c) (6 marks) Using your answer to (b)(ii), prove that for $x \geq 2$, one has

$$\sum_{1\leq n\leq x} \sqrt{\tau(n^3)} \leq x \log x + O(x).$$

   (d) (5+4 marks) (i) State and prove the Möbius inversion formula.

   (ii) Let $\omega(n)$ denote the number of distinct prime divisors of the integer n. Prove that

$$\sum_{d|n} \mu(n/d)\tau(d^3) = 3^{\omega(n)} \quad \text{and} \quad \tau(n^3) = \sum_{d|n} 3^{\omega(d)}.$$

End of examination.