Imperial College
London

UNIVERSITY OF LONDON

Course: M3/4P14
Setter: Skorobogatov
Checker: Buzzard
Editor: James
External: Rippon
Date: March 4, 2005

BSc and MSci EXAMINATIONS (MATHEMATICS)
MAY–JUNE 2004

This paper is also taken for the relevant examination for the Associateship.

M3/4P14 Elementary Number Theory

Date: Monday, 24th May 2004 Time: 10 am –12 noon

Credit will be given for all questions attempted but extra credit will be given for complete or nearly complete answers.

Calculators may not be used.

Statistical tables will not be available.

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

1. (i) State the Chinese Remainder Theorem.

   (ii) Prove that for any integer n we have $n^7 \equiv n \bmod 42$.

   (iii) Prove that there is an integer n such that the congruences

   $$3n \equiv 68 \bmod 101, \quad 3n \equiv 90 \bmod 102, \quad 3n \equiv 14 \bmod 103$$

   simultaneously hold. (You are not required to explicitly find such an integer.)

   (In (ii) and (iii) you may use any results from the course as long as you clearly state them.)

2. (i) Define Euler's ϕ-function.

   (ii) State the Fermat-Euler theorem.

   (iii) How many elements are there in $(\mathbf{Z}\,/\,48)^*$?

   (iv) For each value of $a = 1, 2, 3, \ldots$ find an element of order a in $(\mathbf{Z}\,/\,48)^*$, or prove that none exists.

   (In (iii) and (iv) you may use any results from the course as long as you can clearly state them.)

3. (i) Prove Wilson's theorem that if p is a prime, then $(p-1)! \equiv -1 \bmod p$.

   (ii) Let p be a prime. Prove that the product of all integers from 1 to $p^2 - 1$ which are not divisible by p is congruent to -1 modulo p.

   (You may use any results from the course as long as you clearly state them.)

4. (i) State the theorem from the course that describes the positive integers that can be written as a sum of two squares.

   (ii) Which of the following integers are sums of two squares: $2^8 - 2$, $2^8 - 1$, 2^8, $2^8 + 1$, $2^8 + 2$?. (Note that $2^7 - 1 = 127$ and $2^8 + 1 = 257$ are primes.)

   (iii) Decide whether or not there exists an integer m such that $2 \equiv m^2 \bmod n$, where $n = 2^8 - 2$, $2^8 - 1$, $2^8 + 1$, $2^8 + 2$. (You may use any results from the course as long as you clearly state them.)

5. (i) State Liouville's theorem.

   (ii) Are the following numbers algebraic or transcendental? Justify your answers.

$$\alpha = \sum_{n=1}^{\infty} 2^{-n!}, \ \beta = \sum_{n=1}^{\infty} 2^{-(n^n)}, \ \gamma = \sum_{n=1}^{\infty} 2^{-n/3}.$$