UNIVERSITY OF LONDON

IMPERIAL COLLEGE LONDON

Course:	M 3/4 P 14
Setter:	Skorobogatov
Checker:	Keating
Editor:	Keating
External:	Cremona
Date:	March 3, 2006

BSc and MSci EXAMINATIONS (MATHEMATICS)
MAY–JUNE 2005

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

M 3/4 P 14 Elementary Number Theory

DATE: examdate TIME: examtime

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.

Setter's signature ....

Checker's signature ....

1. *i)* Let $a \geq 2$, $n \geq 2$ be integers such that $a^n - 1$ is prime. Prove that $a = 2$ and n is prime.

ii) Determine all integers a, $2 \leq a \leq 9$, for which there exists an integer n such that $an \equiv 63 \bmod 105$. Justify your answer.

iii) Prove that for any integer n we have $n^{97} \equiv n \bmod 105$.

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

2. *i)* Define the Möbius function and state the Möbius inversion theorem (no proof is required).

ii) Prove that every even perfect number can be written as $2^{p-1}(2^p - 1)$, where where p and $2^p - 1$ are primes.

iii) Find the number of elements in $(\mathbf{Z}/496)^*$.

iv) Find the number of elements of order 15 modulo 496. Justify your answer.

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

3. *i)* Sketch the proof of the existence of primitive roots modulo p^e, where $p > 2$ is prime (no detailed proof is required – four or five sentences will suffice).

ii) Using the ideas from part (i) find a primitive root modulo 3^{2005}. Justify your answer.

iii) p is an odd prime such that for any integer n, $0 < n < p$, we have that n is a quadratic non-residue modulo p if and only if n is a primitive root modulo p. What can you deduce about p? Justify your answer.

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

4. *i)* Let p and q be two odd primes. State the quadratic reciprocity law relating $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ (no proof is required).

ii) Calculate the Legendre symbol $\left(\frac{30}{67}\right)$, showing your working.

iii) Decide whether or not there exists an integer m such that $3 \equiv m^2 \bmod n$, where $n = 23, 24, 25, 26, 27$. Justify your answer.

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

5. *i)* Which of the numbers $101, 102, 103, 104, 105$ are the sums of two squares? Justify your answer.

ii) Find a positive integer $n \equiv 1 \bmod 8$, $n > 1000$, which is not the sum of two squares. Justify your answer.

iii) A real number α is such that there exist infinitely many rational numbers $\frac{p}{q}$ (in lowest terms) such that

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2}.$$

What can you say about α? Justify your answer.

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