Imperial College
London

UNIVERSITY OF LONDON

BSc and MSci EXAMINATIONS (MATHEMATICS)

May-June 2006

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

M3P14/M4P14

Elementary Number Theory

Date: Friday, 26th May 2006 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.

1. (a) Show that the congruence $ax \equiv b$ mod m has hcf(a, m) solutions if hcf(a, m) divides b, and no solutions otherwise.

   (b) Find all solutions of the congruence: $52x \equiv 8$ mod 68.

2. (a) State and prove a condition on strictly positive integers b, k, m, implying that the congruence:
$$x^k \equiv b \quad \text{mod } m$$
has a unique integer solution x modulo m.

   (b) Create a table of indices modulo 13 using the primitive root 2.

   (c) Use your table to find all solutions of the congruence
$$3x^{10} \equiv 4 \quad \text{mod } 13.$$

3. (a) Assuming that $2^{128} \equiv 137$ mod 323, calculate 2^{161} mod 323.
What can you conclude about the possible primality of 323?

   (b) Define the Lagrange and Jabobi symbols.
Evaluate the Jacobi symbol $\left(\frac{26}{323}\right)$.

4. (a) Calculate hcf$(9 + 11i, 4 - 10i)$ in the ring $\mathbb{Z}[i]$ of Gaussian integers.

   (b) List all primes in the ring $\mathbb{Z}[i]$ of Gaussian integers (up to units).

   (c) Prove that, if $p \equiv 1$ mod 4 is an integer prime, then p is not a prime in $\mathbb{Z}[i]$. (You may use standard results in quadratic reciprocity without proof, provided that you state them correctly.)

5. (a) In how many ways can $n = 117$ be written as a sum of two squares?

   (b) Show that, if $n = 4^t(8m + 7)$ (where t, m are integers ≥ 0), then n is not the sum of three squares.
Exhibit a number larger than 10000 which is not the sum of three squares.