Imperial College
London

BSc and MSci EXAMINATIONS (MATHEMATICS)

May-June 2008

This paper is also taken for the relevant examination for the Associateship of the Royal College of Science.

M3P14/M4P14

Elementary Number Theory

Date: Thursday, 15th May 2008 Time: 14.00 pm – 16.00 pm

This paper has FIVE questions.
Candidates should write their solutions in a single answer book.
Supplementary answer books should be used as necessary.

Affix one of the labels provided to each answer book that you use.
DO NOT use the label with your name on it.

Answer all the questions. Each question carries equal weight.

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.

1. In this question, $\mathrm{hcf}(a,b)$ denotes, as usual, the highest common factor of two positive integers a, b.

   (a) Prove, without assuming that every integer is uniquely the product of primes, that, if $c|ab$ and $\mathrm{hcf}(c,a) = 1$, then $c|b$.

   (b) For a, b positive integers, and $d = \mathrm{hcf}(a,b)$, write

   $$g = ab/d.$$

   Prove, without assuming that every integer is uniquely the product of primes, that g is an integer; that a, b both divide g; and that, if a, b both divide some integer t, then g also divides t.

2. In this question, we study the equation

   $$y^2 = x^3 + 7$$

   for x, y integers.

   (a) Suppose that (x,y) is a solution in integers. Show that x must be odd.

   (b) Show that $y^2 + 1 = (x+2)(x^2 - 2x + 4)$.

   (c) Show that $x^2 - 2x + 4$ must be congruent to 3 mod 4. Explain why $x^2 - 2x + 4$ must be divisible by some prime q satisfying $q \equiv 3 \pmod 4$.

   (d) Reduce the original equation $y^2 = x^3 + 7$ modulo q, and use the resulting congruence to show that -1 is a quadratic residue modulo q. Explain why this is impossible, thereby proving that $y^2 = x^3 + 7$ has no solutions in integers.

3. Recall that a positive integer n is said to be perfect if $\sigma(n) = \sum_{d|n} d = 2n$.

   (a) State, withouth proof, a result characterising all even perfect numbers.

   (b) Let p and q be distinct odd primes; show that a number n of the form $n = p^a q^b$ can never be a perfect number.

4. (a) State in how many ways can $n = 1,125$ be written as a sum of two integer squares. Briefly justify your answer quoting (without proof) any general results that you need.

   (b) Recall that a Gaussian prime is a prime in the ring $\mathbb{Z}[i]$ of Gaussian integers. Find the decomposition of $n = 1,125$ in Gaussian primes. Hence find all integer solutions of the equation:

$$x^2 + y^2 = 1,125.$$

5. (a) Calculate $\mathrm{hcf}(3 + 9i, 4 - 2i)$ in $\mathbb{Z}[i]$.

   (b) Find all solution $x, y \in \mathbb{Z}[i]$ of the equation

$$(3 + 9i)x + (4 - 2i)y = 1 + i.$$

   Justify your answer.