Course 2316 — Sample Paper 1

Timothy Murphy

April 20, 2015

Attempt 5 questions. All carry the same mark.

1. State and prove the Fundamental Theorem of Arithmetic (for $\mathbb{N}$).

   Prove that there are an infinity of primes $\equiv 3 \bmod 4$.

   What can you say about primes $\equiv 1 \bmod 4$?

2. Given $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$ and $r, s \in \mathbb{Z}$, prove that there exists $x \in \mathbb{Z}$ such that

   $$x \equiv r \bmod m, \quad x \equiv s \bmod n.$$

   Find the smallest positive integer x such that

   $$x \equiv 3 \bmod 5,\ x \equiv 7 \bmod 11,\ x \equiv 12 \bmod 13.$$

   Find the largest integer x *not* expressible in the form

   $$x = 7a + 11b$$

   with $a, b \geq 0$.

3. Show that if

   $$M = a^e - 1 \quad (a, e > 1)$$

   is prime then $a = 2$ and e is prime.

   Find the smallest number

   $$M = 2^p - 1$$

   (with p prime) that is *not* prime.

4. Prove that if p is an odd prime, then the multiplicative group $(\mathbb{Z}/p)^\times$ is cyclic.

   Find the orders of all the elements of $(\mathbb{Z}/17)^\times$.

5. State and prove Gauss' Law of Quadratic Reciprocity.

   Does there exist an integer x such that

$$x^2 \equiv 17 \bmod 30?$$

   If there is, find the least such integer ≥ 0.

6. Prove that the ring Γ of gaussian integers $m + ni$ is a Unique Factorisation Domain, and determine the units and primes in this domain.

   Show that an integer $n > 0$ can be expressed in the form

$$n = a^2 + b^2 \quad (a, b \in \mathbb{N})$$

   if and only if each prime $p \equiv 3 \bmod 4$ divides n to an even power.

   In how many ways can 1 million be expressed as a sum of two squares?

7. Define an *algebraic number* and an *algebraic integer*.

   Show that the algebraic numbers form a field, and the algebraic integers form a commutative ring.

   Prove that $(\sqrt{2} + \sqrt{3})/2$ is not an algebraic integer.

8. Show that the ring $\mathbb{Z}[\sqrt{3}]$ formed by the numbers $m + n\sqrt{3}$ $(m, n \in \mathbb{Z})$ is a Unique Factorisation Domain.

   Determine the units and primes in this domain.

   Is $\mathbb{Z}[\sqrt{6}]$ a Unique Factorisation Domain?