DMMR Coursework 1

October 3rd, 2019

1. (a) Prove that if the square of integer z is divisible by 17 then z is divisible by 17. (6 marks)

   (b) Prove that $\sqrt{17}$ is irrational. (6 marks)

2. Recall that for sets A and B, $|A| = |B|$ if there is a bijection $f : A \to B$, a function f that is both injective (one-to-one) and surjective (onto). Let $E = \{0, 2, 4, \ldots\}$ be the set of non-negative even integers.

   (a) Give an example of a function $g : E \to E$ that is injective but not surjective. (3 marks)

   (b) Prove that $|\mathbb{Z}| = |E|$ by defining an explicit bijection. (5 marks)

3. $A = \mathbb{Z}^+ \times \mathbb{Z}^+$ is the set of pairs (a, b) of positive integers a, b. Consider the following binary relation R on A: $(a, b)R(c, d)$ iff $ad = bc$. You are to show that R is an equivalence relation, as follows.

   (a) Prove that R is reflexive (3 marks)

   (b) Prove that R is symmetric (3 marks)

   (c) Prove that R is transitive (4 marks)

4. (a) Prove by induction that for every positive integer n (7 marks)

$$\sum_{j=1}^{n} j2^j = (n-1)2^{n+1} + 2$$

   (b) Using Fermat's little theorem compute 11^{14} mod 7. (3 marks)

5. Assume a, b, m are positive integers and $d = \gcd(a, m)$. Prove the following equivalence: the congruence $ax \equiv b \pmod{m}$ has an integer solution z iff $d|b$. (You can use Bézout's theorem in the proof.) (10 marks)

Solutions to questions to be handed in to the ITO before 10.00am on Monday 21st October. Don't forget to write your student number clearly on your solution sheet. No other method of submission (such as by email) will be accepted.

Good Scholarly Practice: Please remember the University requirement as regards all assessed work for credit. Details about this can be found at:

http://web.inf.ed.ac.uk/infweb/admin/policies/academic-misconduct