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)

Solution:

(a) Assume z is an integer and that z^2 is divisible by 17. By the division algorithm we know that $z = 17q + r$ for some integers q and r where q is the quotient and r is the remainder with $0 \leq r < 17$. We need to show that $r = 0$. Consider $z^2 = (17q+r)^2 = (17^2q^2+34qr+r^2)$; now z^2 is divisible by 17. Therefore, r^2 is divisible by 17; however this can only be true in the case that $r = 0$ as 17 does not divide i^2 for any $i : 1 \leq i \leq 16$ as it is prime.

(b) We use a similar proof method that showed $\sqrt{2}$ is irrational in lectures. We do this using proof by contradiction. Assume $\sqrt{17}$ is rational, so $\sqrt{17} = \frac{a}{b}$ where a, b are integers in lowest terms with no common factors. So we now square both sides $17 = \frac{a^2}{b^2}$. So $a^2 = 17b^2$; so a^2 is divisible by 17; therefore, by the first part of the question a is divisible by 17. So $a = 17a'$ for some integer a'; so $b^2 = \frac{a^2}{17} = \frac{17^2a'}{17} = 17a'$; so, in turn, b^2 is divisible by 17 and therefore so is b again by the first part. However this contradicts that a and b have no common factors as 17 is a common factor.

□

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)

Solution:

(a) Any plausible g here such as $g(x) = 2x$, so $g(2) = 4$ and so on. This is clearly injective as $g(x) = g(y)$ implies $x = y$. However, it is not surjective as elements that are not divisible by 4, such as 2 and 6, are not mapped to. No marks if g is not a function from E to E.

(b) They need to produce a bijection from $g : \mathbb{Z} \to E$ such as $g(n) = 4n$ for $n \geq 0$ and $g(n) = -4n - 2$ for $n < 0$ and explain why it is a bijection. No marks if the function is not from $\mathbb{Z}$ to E. Reduce marks if the function is not given explicitly (such as, as an enumeration).

□

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)

   Solution:

   (a) For reflexivity they need to show $(a, b)R(a, b)$ (and not $(a, a)R(a, a)$ which although true isn't what is required); this is clear as $ab = ba$.

   (b) For symmetry they need to show that if $(a, b)R(c, d)$ then $(c, d)R(a, b)$; this is clear as $ad = bc$ iff $cb = da$.

   (c) For transitivity they need to show that if $(a, b)R(c, d)$ and $(c, d)R(e, f)$ then $(a, b)R(e, f)$; as $ad = bc$ and $cf = de$ therefore $adcf = bcde$, and so as all the integers are positive $af = be$.

   □

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)

   Solution:

   (a) For the base case $n = 1$. LHS is 2 as is RHS. 1 mark for this. For the inductive step assume it holds for $n = k$. Show it for $n = k + 1$.

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

   Using the IH, LHS is

$$(k-1)2^{k+1} + 2 + (k+1)2^{k+1} = 2k2^{k+1} + 2 = k2^{k+2} + 2$$

   as required. 6 marks here; 3 for using induction hypothesis and 3 for getting it all correct.

   (b) If p is prime and $p \not| a$ then $a^{p-1} \equiv 1 \pmod{p}$. So, $11^{14} = 11^{12}11^2$. Therefore, $11^{14} \equiv 11^2 \pmod{7} \equiv 2 \pmod{7}$ because $11^6 \equiv 1 \pmod{7}$.

   □

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)

   Solution:
   Assume a, b, m are positive integers and $d = \gcd(a, m)$. First we show that if the congruence

$ax \equiv b \pmod{m}$ has an integer solution z then $d|b$. Assume $ax \equiv b \pmod{m}$ has the integer solution z. So $az \equiv b \pmod{m}$ which by definition of $\equiv \pmod{m}$, means $m|(az - b)$. So $az - b = cm$ for some integer c and so $az - cm = b$. Since $d = \gcd(a, m)$, $d|az$ and $d|cm$, and therefore $d|b$ as required. 5 marks for this half of the proof.

Now for the other implication: if $d|b$ then the congruence $ax \equiv b \pmod{m}$ has an integer solution z. Assume $d|b$, so $b = cd$ for some integer c. We now use Bézout's theorem, that $d = as + tm$ for some integers s, t. So, $b = csa + ctm$. Consequently $ctm = b - csa$ and so $m|(acs - b)$ and therefore by definition $acs \equiv b \pmod{m}$. However cs is an integer and therefore is a solution z to $ax \equiv b \pmod{m}$. 5 marks for this half. □

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