Queen Mary University of London

MTH4104 Introduction to Algebra

Week 3 coursework **due 14 February 2022**

You are to write up a careful and professionally presented solution to the question below. This is to be submitted on QMPlus as a single PDF file by 12:00 noon, Monday 14 February 2022.

Question to submit

(a) We have defined the relations $\equiv_6$ and $\equiv_{10}$ to be certain subsets of $\mathbb{Z}^2$. Their intersection

$$R = (\equiv_6) \cap (\equiv_{10})$$

is another subset of $\mathbb{Z}^2$, so it is also a relation on $\mathbb{Z}$. Complete the sentence: if $a, b \in \mathbb{Z}$, then aRb is true if and only if _____. [2 marks]

[You do not have to "simplify" your answer. This part of the question is only about relations as sets vs. true-or-false statements.]

(b) The relation R from part (a) is equal to $\equiv_m$ for some natural number m. What is m? [1 mark]

(c) Based on your answer to part (b), complete the following statement with a formula for p in terms of m and n, **and** write down a proof of your statement. [7 marks]

> Let m and n be positive integers. Then $(\equiv_m) \cap (\equiv_n) = (\equiv_p)$, where $p =$ _____.

Solution (a) If $a, b \in \mathbb{Z}$, then aRb is true if and only if $\boxed{a \equiv_6 b \text{ and } a \equiv_{10} b}$. This is because, by the definition of intersection, the pair (a, b) is in the set R if and only if it is in the set $\equiv_6$ and the set $\equiv_{10}$

(b) The answer is $m = \text{lcm}(6, 10) = 30$.

(c) The missing formula is $\boxed{p = \text{lcm}(m, n)}$.

Short model proof Proof of $(\equiv_m) \cap (\equiv_n) \subseteq (\equiv_p)$: Assume $(a, b) \in (\equiv_m) \cap (\equiv_n)$ for integers a and b. Then $a \equiv_m b$ and $a \equiv_n b$. So $b - a$ is a multiple of m and of n. Because the primes that divide p are the primes that divide m or n (counting repetitions), $b - a$ is a multiple of p. So $(a, b) \in \equiv_p$.

Proof of $(\equiv_p) \subseteq (\equiv_m) \cap (\equiv_n)$: Assume $(a, b) \in \equiv_p$, so $b - a$ is a multiple of p. Since p is a multiple of m and of n, $b - a$ is a multiple of m and of n. Therefore $b - a \in (\equiv_m) \cap (\equiv_n)$.

Proof with discussion The statement asserts equality of two sets, because relations are sets. So, to prove it, we show that any element of one set is also an element of the other.

I'll start by assuming a and b are integers such that $(a,b) \in \equiv_p$, since this is the easier direction. The assumption implies $a \equiv_p b$, that is, $\text{lcm}(m,n) = p \mid b-a$. By definition of lcm, m is a divisor of $\text{lcm}(m,n)$, and the divisor relation is transitive, so $m \mid b-a$. For the same reason $n \mid b-a$ also. These facts imply $a \equiv_m b$ and $a \equiv_n b$, and, just like in part (a), we can conclude $(a,b) \in (\equiv_m) \cap (\equiv_n)$.

Now assume a and b are integers such that $(a,b) \in (\equiv_m) \cap (\equiv_n)$. This implies $a \equiv_m b$ and $a \equiv_n b$, that is, $m \mid b-a$ and $n \mid b-a$. So $b-a$ is a common multiple of m and n. Every common multiple of m and n is in fact a multiple of their least common multiple: this assertion calls for proof itself, and I'll come back to it in a minute. But using this fact for the moment, we conclude $p = \text{lcm}(m,n) \mid b-a$, implying $(a,b) \in (\equiv_p)$.

What's left is to prove my claim about common multiples. I will give one full proof of this and an outline of a second. Here's the full proof. Suppose s is a common multiple of m and n but not a multiple of $p = \text{lcm}(m,n)$. Then the remainder r when s is divided by p, which we can write $r = p - ks$ for some $k \in \mathbb{Z}$, is a positive integer less than p. But m and n both divide p and s, so they both divide the right hand side, and therefore they both divide r. This means r is a positive common multiple of m and n less than $\text{lcm}(m,n)$, a contradiction.

A second way to do this is to argue by prime factorisations. The exponents in the prime factorisation of s must be greater than or equal to than the exponents for both m and n. The exponents for p are equal to the maximum of those for m and n, so the exponents for s are greater than or equal to these as well.