Queen Mary University of London

MTH4104 **Introduction to Algebra**

Extra questions for chapter 2 **Spring 2021**

These questions are for you to practice with on your own schedule. You may e.g. want to try some each week as their topics come up in lectures, or use them in exam revision.

2 Modular arithmetic

2.1 Integer division

Question 2.1.1 A relation R on a set X is said to be *antisymmetric* if, for any elements $a, b \in X$, if aRb and bRa both hold then $a = b$.

(a) Prove that the divisibility relation $|$ on the set of positive integers is antisymmetric.

(b) Prove that $|$ is not antisymmetric on the set of all integers.

2.2 Congruence mod m

Question 2.2.1 Let a be an integer. Suppose you don't know what a is; you only know what the congruence classes $[a]_4$ and $[a]_5$ are. From this information, is it possible to deduce the following congruence classes? Justify your answers.

(a) $[a]_2$

(b) $[a]_3$

(c) $[a]_{20}$

Question 2.2.2 Let m and n be positive integers and a any integer.

(a) Prove that, as sets,
$$[a]_m \cap [a]_n = [a]_{\mathrm{lcm}(m,n)}.$$

(b) I have a secret integer a in mind. I don't tell you what a is, but I do tell you the remainders when a is divided by m and when a is divided by n. Explain why the equation in part (a) implies that you can work out what the remainder is[1] when a is divided by $\mathrm{lcm}(m,n)$.

[1] This principle, the *Chinese Remainder Theorem*, is used by several old riddles: see for example `https://www.cut-the-knot.org/blue/chinese.shtml`.

2.3 Arithmetic with congruence classes

Question 2.3.1 Explain how you could work out the remainder of 2^{80} modulo 19 *without* using a calculator or a computer.

2.4 gcd and Euclid's algorithm

Question 2.4.1

(a) Explain how to find the lcm of two positive integers using prime factorisations, similarly to how the gcd is found in the extra set of notes on QMplus "Greatest common divisors by prime factorisation".

(b) Prove that

$$\gcd(a,b)\cdot \mathrm{lcm}(a,b) = a\cdot b$$

for any two positive integers a and b.

(c) Describe an algorithm [i.e. a method] to compute the least common multiple of two positive integers which is efficient even when the integers are large.

You can use Euclid's algorithm, but not prime factorisations, as we have no efficient way to find the prime factorisation of a large number.

Question 2.4.2 Prove that

$$a\gcd(b,c) = \gcd(ab,ac)$$

for all positive integers a,b,c.

Question 2.4.3 This question explores how quickly the remainders in Euclid's algorithm decrease in size.

(a) Let $b_0, b_1, b_2, \ldots$ be the successive remainders computed in the course of Euclid's algorithm. Prove that $b_{i+2} < b_i/2$ for any $i \geq 1$.

[Hint: consider two cases, $b_{i+1} \leq b_i/2$ and $b_{i+1} > b_i/2$.]

(b) Let N be a natural number. Use part (a) to fill in the blank to make the following assertion true (your answer should have an N in it somewhere). Explain why your answer is correct.

> Let a and b be two natural numbers, both less than 2^N. If the Euclidean algorithm is used to compute $\gcd(a,b)$, it will take at most _____ steps to finish.

2.5 Euclid's algorithm extended

Question 2.5.1 Using the extended Euclidean algorithm[2], find $\gcd(186,132)$, and find a pair of integers (x,y) such that

$$186x + 132y = \gcd(186,132).$$

[2] If you want more questions to practice the extended Euclidean algorithm, see `http://www.maths.qmul.ac.uk/~fink/ExtendedEuclid.html`.

Question 2.5.2

(a) Use the extended Euclidean algorithm to compute the greatest common divisor d of 206 and 64, and to find integers x and y such that $206x + 64y = d$.

(b) Write down another pair of integers (x', y') such that $206x' + 64y' = d$, different from the pair (x, y) you found in part (b).

Question 2.5.3 Let a and b be positive integers, and $d = \gcd(a, b)$.

(a) Prove that all solutions to the equation

$$ax + by = 0$$

with x and y integers are given by $x = kb/d$ and $y = -ka/d$, where k is an arbitrary integer.

(b) Suppose that x_0 and y_0 are the integers output by the extended Euclidean algorithm such that

$$ax_0 + by_0 = d.$$

Prove that all solutions to the equation

$$ax + by = d$$

are given by $x = x_0 + kb/d$ and $y = y_0 - ka/d$, where k is an arbitrary integer.

Question 2.5.4 Let a, b, and c be fixed integers. Prove that there is an integer solution to $ax + by = c$ if and only if $\gcd(a, b)$ divides c.

Question 2.5.5 Let a and b be nonnegative integers.

(a) If a and b are not both zero, prove that the greatest common divisor of a and b is the unique nonnegative integer $d \geq 0$ with the properties

(i) $d \mid a$ and $d \mid b$;

(ii) if e is a nonnegative integer satisfying $e \mid a$ and $e \mid b$, then $e \mid d$.

(b) If $a = b = 0$, prove that $d = 0$ is the unique non-negative integer that satisfies conditions (i) and (ii).

The reason the statement in (a) is interesting is that, if we had used it as the *definition* of "greatest common divisor", then $\gcd(0, 0) = 0$ would be true by definition (this is what you showed in part (b)) and we would not have had to tack this on as a special case.

2.6 Modular inverses

Question 2.6.1

(a) Explain why $[59]_{84}$ has a multiplicative inverse in $\mathbb{Z}_{84}$.

(b) Find a non-negative integer $b < 84$ such that $[59]_{84}^{-1} = [b]_{84}$.

Question 2.6.2 Find all solutions $x \in \mathbb{Z}_{31}$ to the equation

$$[16]_{31}\, x + [26]_{31} = [2]_{31}\, x + [3]_{31}.$$

Show your working. You are given that $[14]_{31}^{-1} = [20]_{31}$.

Question 2.6.3 Find all $X, Y \in \mathbb{Z}_{11}$ that satisfy the simultaneous system of linear equations

$$\begin{aligned} [5]_{11}\, X + [2]_{11}\, Y &= [6]_{11} \\ [4]_{11}\, X + \qquad Y &= [2]_{11}. \end{aligned}$$