Activities Lesson Review: Euclid's algorithm

Please answer the question below. They ask you to summarise the class activities, referring to any learning evidence that you may provide, if necessary. The learning evidence can consist of your work on activities, (as well as notes taken during classes). As a rule of thumb, your summary should be half a page to one page long each (not including evidence). Your answers should be similar to your answers to the final section (*Putting it all together*) of each activity.

The task is worth up to 3 marks. Your answer should relate to the questions in the activities, and the discussions that happened in class. Note that these questions do not refer to the content of the modules - just explaining how to apply the Euclidean algorithm, for example, is off-topic in this task (and has already been assessed in the Number Theory Lesson Review).

Question 1.

Explain the proof of convergence of the Eulidean algorithm, using your answers to the last two tasks of the activity.

Task 43 (a): Proving r_n is a factor of a and b

To prove that r_n is a factor of a and b after n steps of the Euclidean algorithm, we use a loop-like structure similar to the algorithm itself:

Initialization: I would like to Start with

$k=n$.

Loop: Decrease k from n to 0 (inclusive).

Step k: At each step k, we prove that r_n is a factor of r_k.

The proof hinges on the observation that if $r_k+1 = r_k \mid r_k-1|$ (as shown in the Euclidean algorithm), then r_k is indeed a factor of r_k-1. By this logic, r_n is a factor of r_n-1, and we can iteratively deduce that r_n is a common factor of all previous remainders, hence a factor of a and b.

Task 43 (b): Proving r_n is the gcd of a and b

To prove that r_n is the greatest common divisor (gcd) of a and b, we follow a similar loop-like structure:

Initialization: Start with $k=1$.

Loop: Increase k from 1 to n.

Step k: At each step kk, we prove that any common factor f of r_0 and r_1 must also be a factor of r_k.

The key insight is that if f is a common factor of $r0$ and $r1$, then it must be a factor of each subsequent remainder rk. Therefore, rn is the gcd of a and b because it's the largest number that divides all of the remainders produced by the Euclidean algorithm.

Task 44: Possibility of Infinite Loop

The method used by the Euclidean algorithm cannot result in an infinite loop. This is because with each iteration, the remainders rk decrease until they eventually reach zero (leading to the termination of the algorithm). The key step in the Euclidean algorithm is $rk+1=rk \ |rk-1|$, ensuring that the sequence of remainders decreases with each step, ultimately leading to the termination of the algorithm.

Question 2.

Please reflect on your experience completing this activity:

- What was the main learning outcome that you took out from the activity?

  The main learning outcome of this task is the better understanding of the Euclidean's algorithm and its proof by using simple step by step procedure which had nothing but basic logic.

- how did you approach the tasks?

I approached the task by using the hints given and provided outline to demonstrate that rn is a factor of a and b, leveraging previous knowledge to justify each step. In Task 44, I considered the potential for an infinite loop by comparing rk with $rk-1$ and discussed the implications within the context of the algorithm.

- Did you work on it in a group (for example in the seminar classes) as intended?

  No I worked alone.