

TD: “Images et géométrie discrète”

Extended Euclid’s Algorithm

Let us consider the following Euclidean division algorithm.

Procedure *Convergents*((a,b), (p,q), (p',q'), i)

Input: (a,b), (p,q), (p',q'), i

Output: (p',q')

```

1 Let r be the remainder of the Euclidean division b/a;
2 Let u be the quotient of the Euclidean division b/a;
3 p'' ← up' + p;
4 q'' ← uq' + q;
5 if r > 0 then
6   | return Convergents((r,a), (p',q'), (p'',q''), i + 1);
7 else
8   | return (p',q')
```

Question 1 Let $(p_{-1}, q_{-1}) = (1, 0)$ and $(p_0, q_0) = (0, 1)$, what is the output of *Convergents*((5, 8), (p_{-1}, q_{-1}) , (p_0, q_0) , 0) ?

Question 2 Let us consider *Convergents*((a,b), (p_{-1}, q_{-1}) , (p_0, q_0) , 0) (with $0 \leq a < b$ and $\gcd(a, b) = 1$). We index the recursive calls by $i = 1 \dots n$. Show that

$$\forall i = 1 \dots n, p_i = u_i p_{i-1} + p_{i-2} \text{ and } q_i = u_i q_{i-1} + q_{i-2}.$$

Question 3 Similarly, with $r_{-1} = b$ and $r_0 = a$, show that

$$\forall i = 1 \dots n, r_i = r_{i-2} - u_i r_{i-1}$$

Question 4 Following previous results, prove the following statements:

1. $\forall i = 1 \dots n, p_{i-1} q_i - q_{i-1} p_i = \pm 1$
2. $\forall i = -1 \dots n, p_i b - q_i a = \pm r_i$

Since $r_n = \gcd(a, b) = 1$, what is $p_n b - q_n a$?

Question 5 Give the definition of uni-modularity. What is the geometrical interpretation of this definition ?

Question 6 In the domain in appendix, draw the Euclidean segment $[(0, 0) - (b, a)]$ and all convergents (q_i, p_i) for the input given in Question 1. With respect to the parity of i , can you say something on the position of convergents with respect to the segment ? If we construct a polygonal curve with only convergents (q_i, p_i) with even index i (plus a last point (b, a)). What kind of geometrical object I have constructed ?

Question 7 Let L_{odd} (resp. L_{even}) be the polygonal curve of convergents with odd index (resp. even index). Furthermore, we add the point (b, a) to the end of each list. For the input given in Question 1, are there integer points between L_{odd} and L_{even} ? Why ?

Question 8 For a general setting *Convergents*((a,b), (p_{-1}, q_{-1}) , (p_0, q_0) , 0), can you prove the statement of the previous question ?

Question 9 What is the complexity of *Convergents* with respect to a and b ?

