Magma Assignment 01

Combinatorics and Cryptography

Fact 1. *Let $a, b \in \mathbb{Z}$, not both even. The following transformation is* gcd-preserving*:*

$$(a,b) \mapsto \begin{cases} \left(\frac{a-b}{2}, b\right) & a \text{ and } b \text{ are odd,} \\ \left(\frac{a}{2}, b\right) & a \text{ is even and } b \text{ is odd,} \\ \left(a, \frac{b}{2}\right) & a \text{ is odd and } b \text{ is even.} \end{cases}$$

Fact 2. *The proof of the Euclidean algorithm for computing the greatest common divisor relies on the iteration of a(nother) gcd-preserving transformation.*

Task

Implement an algorithm which computes $\gcd(a,b)$ for each $a, b \in \mathbb{Z}$ using the gcd-preserving transformation of Fact 1. Submit the magma code in a .txt file in such a way it can be copied and pasted in the terminal (or loaded from). Comments are appreciated but not mandatory. If you want to provide additional documents to explain your solution, attach it in a different file.

Important: call the required 2-input function `binaryGCD`.

Points

Submitting a working solution will give you up to two points.

Hints

- implement an auxiliary function which applies the reduction of Fact 1 and repeatedly call it in `binaryGCD`;
- figure out what the final iteration looks like,
- the exercise can be possibly solved by *only* using divisions by 2.