The GCD–Formula vs. the Euclidean Algorithm

Drawbacks: 1) The formula doesn’t enable us to find solutions to linear Diophantine equations.

2) For larger integers, it is extremely difficult (and time consuming) to find their prime decompositions.

Example: Consider

\[ m = 4153748649902217077, \ n = 4153748674359113993 \]

To compute

\[ g := \gcd(m, n) = 2038074743, \]

using the program package MATHEMATICA, my (old) computer required the following times:

- to compute \( \gcd(m, n) \), using the Euclidean algorithm: 0.05 seconds
- to compute the prime decomposition of \( m \): 14.45 seconds \( (m = 2038074739 \cdot g) \)
- to compute the prime decomposition of \( n \): 58.44 seconds \( (n = g \cdot 2038074751) \)