DHBW
Duale Hochschule
Baden-Württemberg
CAS
Center for Advanced Studies

IT-Security Cryptography and Secure Communications

Exercise: **Introduction to Number Theory**
Lecturer: *Prof. Dr. Michael Eichberg*
Version: 2023-10-12

1. Compute the result of $5^9 \; mod \; 7$ by hand. Don't use a calculator!

2. Which numbers are relative prime to 21?

3. Compute the $gcd(1037, 768)$ using the Euclidean algorithm.

4. Determine the result of Euler's Totient function ϕ for the value 37. Don't look it up; just think about it.

5. Convince yourself that Fermat's (little) theorem holds. E.g., for the numbers: $a = 9, p = 7$.

6. Convince yourself that Euler's theorem holds. E.g., for the following values: a=7 and n=9.

7. Execute the Miller-Rabin Algorithm for n = 37.