TTM4135 Worksheet 1: Intro and Basic Number Theory

Tjerand Silde and Emil August Hovd Olaisen
{tjerand.silde, emil.august.olaisen}@ntnu.no

Spring 2026

1. Review the definitions of the following terms:
   (a) confidentiality
   (b) integrity
   (c) availability
   (d) entity authentication
   (e) data origin authentication
   (f) non-repudiation
   (g) group generator
   (h) finite field
2. Determine the following using Euclid's algorithm:
   (a) $\gcd(23, 29)$
   (b) $\gcd(893, 703)$
   (c) $\gcd(1045, 77)$
3. Without using a calculator, compute the values of $a \bmod b$ and write each a value as $a = bq + r$ where $0 \leq r < b$:
   (a) $35 \bmod 31$
   (b) $3 \bmod 1000$
   (c) $65 \bmod 21$
   (d) $236 \bmod 5$
   (e) $123 \bmod 3$
4. Use the Euclidean algorithm to find which of the following inverses exist. For those that do exist use back substitution to find the inverse.
   (a) $3^{-1} \bmod 31$
   (b) $21^{-1} \bmod 91$
   (c) $39^{-1} \bmod 195$
   (d) $41^{-1} \bmod 195$
5. Demonstrate that $\mathbb{Z}_5$ is a field by writing out the addition and multiplication tables. (What do you need to check?)
6. (a) How many elements are there in $\mathbb{Z}_{11}^*$? Find a generator for this group.
   (b) How many elements are there in $\mathbb{Z}_{12}^*$? Does this group have a generator?
7. Suppose that we try to define $GF(2^8)$ in a different way by defining multiplication of two strings to be multiplication modulo 2^8. Show that this would *not* satisfy the requirements to be a field.
8. Write the XOR operation ($\oplus$) as a Boolean truth table. Then show, using their truth tables, that $z = x_1 \vee x_2$ defines the same Boolean function as $z = x_1 \oplus x_2 \oplus (x_1 \wedge x_2)$.