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

Solution: The definitions of all these terms may be found in the lecture slides.

2. Determine the following using Euclid's algorithm:
   (a) $\gcd(23, 29)$
   (b) $\gcd(893, 703)$
   (c) $\gcd(1045, 77)$

Solution:

(a)

$$\begin{aligned} 29 &= 1 \times 23 + 6 \\ 23 &= 3 \times 6 + 5 \\ 6 &= 1 \times 5 + 1 \\ 5 &= 5 \times 1 \end{aligned}$$

$\rightarrow \gcd(23, 29) = 1$

(b)

$$\begin{aligned} 893 &= 1 \times 703 + 190 \\ 703 &= 3 \times 190 + 133 \\ 190 &= 1 \times 133 + 57 \\ 133 &= 2 \times 57 + 19 \\ 57 &= 3 \times 19 \end{aligned}$$

$\rightarrow \gcd(893, 703) = 19$

(c)

$$\begin{aligned} 1045 &= 13 \times 77 + 44 \\ 77 &= 1 \times 44 + 33 \\ 44 &= 1 \times 33 + 11 \\ 33 &= 3 \times 11 \end{aligned}$$

$\rightarrow \gcd(1045, 77) = 11$

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) $123 \bmod 3$

Solution:

(a) $4; 35 = 31 \times 1 + 4$

(b) $3; 3 = 1000 \times 0 + 3$

(c) $2; 65 = 3 \times 21 + 2$

(d) $1; 236 = 5 \times 47 + 1$

(e) $0; 123 = 41 \times 3 + 0$

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) $41^{-1} \bmod 195$

Solution:

(a)

$$\begin{aligned} 31 &= 10 \times 3 + 1 \\ 3 &= 3 \times 1 \end{aligned}$$

Therefore $\gcd(31, 3) = 1$ so $3^{-1} \bmod 31$ exists. Now use back substitution.

$$1 = 31 - 10 \times 3$$

Therefore $1 \equiv -10 \times 3 \pmod{31}$ so $3^{-1} \bmod 31 = -10 \bmod 31 = 21$.

(b)

$$\begin{aligned} 91 &= 4 \times 21 + 7 \\ 21 &= 3 \times 7 \end{aligned}$$

Therefore $\gcd(91, 21) = 7$ so $21^{-1} \bmod 91$ does not exist.

(c)

$$195 = 5 \times 39$$

Therefore $\gcd(195, 39) = 39$ so $39^{-1} \bmod 195$ does not exist.

(d)

$$\begin{aligned} 195 &= 4 \times 41 + 31 \\ 41 &= 1 \times 31 + 10 \\ 31 &= 3 \times 10 + 1 \\ 10 &= 10 \times 1 \end{aligned}$$

Therefore $\gcd(195, 41) = 1$ so $41^{-1} \bmod 195$ exists. Now use back substitution.

$$\begin{aligned} 1 &= 31 - 3 \times 10 \\ &= 31 - 3 \times (41 - 1 \times 31) \\ &= 4 \times 31 - 3 \times 41 \\ &= 4 \times (195 - 4 \times 41) - 3 \times 41 \\ &= 4 \times 195 - 19 \times 41 \end{aligned}$$

Therefore $1 \equiv -19 \times 41 \pmod{195}$ so $41^{-1} \bmod 195 = -19 \bmod 195 = 176$.

5. Demonstrate that $\mathbb{Z}_5$ is a field by writing out the addition and multiplication tables. (What do you need to check?)

Solution: Note that the multiplication table only applies to $\mathbb{Z}_5 \setminus \{0\}$.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

We need to check that the tables are groups in both cases. Particularly we can check the closure property

(only the group elements appear in the table) and the inverse property (each row has the identity element). We should also show the distributive law holds: $a(b+c) = ab+ac$. This always holds for modular arithmetic.

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?

Solution:

(a) Since 11 is prime, $\mathbb{Z}_{11}^*$ is a group and all numbers less than 11 are in the group. There are therefore 10 elements.

We can find a generator by trial and error. We only need to check that $g^2 \bmod 11 \neq 1$ and $g^5 \bmod 11 \neq 1$ to check that g is a generator.

Let us try $g = 2$. Then $g^2 \bmod 11 = 4$ and $g^5 \bmod 11 = 32 \bmod 11 \neq 1$ so $g = 2$ is indeed a generator. Its powers are: $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$.

(b) If we write out the numbers less than 12 and remove all of those which are not coprime to 12 we are left with $\{1, 5, 7, 11\}$. Thus $\mathbb{Z}_{12}^*$ has 4 elements. (Later we have seen that the order of $\mathbb{Z}_{12}^*$ is $\phi(12) = 4$.) We can check that for each of these 4 elements its square is 1. Therefore there is no generator for this group.

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.

Solution: Using multiplication modulo n will never make a multiplicative group when n is an even number greater than 2. This is because the even values in the group (excluding 0) will not be prime to n and therefore will not have inverses.

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 $z = x_1 \oplus x_2 \oplus (x_1 \wedge x_2)$.

Solution:

x_1	x_2	$z = x_1 \vee x_2$	$a = x_1 \oplus x_2$	$b = x_1 \wedge x_2$	$z = a \oplus b$
1	1	1	0	1	1
1	0	1	1	0	1
0	1	1	1	0	1
0	0	0	0	0	0

The column with a shows the XOR truth table. The third column shows the truth table for $\vee$. The final column shows the second derivation for z.