Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Information Technology
FH Zentralschweiz

Mathematical Basis II - Exercise

Prof. Dr. Josef F. Bürgler

I.BA_MOVK_MM, Semesterweek 02

Please write down to solution of the exercises in a consise but comprehensible way. Numerical results should be accurate to 4 digits. Sketches should be correct qualitatively. At least 75% of the exercises have to be solve satisfactorily. Due time is one week after we have discussed the corresponding topic in class.

1 Generator or primitive element of a group

Is 3 a generator of $(\mathbb{Z}_{11}^{\star}, \cdot)$. Find a generator of $(\mathbb{Z}_{11}^{\star}, \cdot)$.

2 Field

Show that if p is prime, then $\mathbb{Z}_p$ together with addition and multiplication modulo p constitues a field. Check whether the rules (i)-(ix) hold?

3 The Galois Field $GF(2^2)$

A theorem says that there is a finite filed with $2^2 = 4$ elements, because 4 is the 2nd power of the prime number 2. Let's call this field $GF(2^2)$. Let's represent the elements by bitstrings of length two: 00, 01, 10, and 11. Assume 00 is the neutral element with respect to addition and 01 the neutral element with respect to multiplication.
Complete the following tables for addition (left) and multiplication (right):

$+$	00	01	10	11
00	00	01	10	11
01	01			
10	10			
11	11			

$\cdot$	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10		
11	00	11		

Note: in order to have inverse elements, the tables must be latin squares, i.e. each element occurs exactly once in each row and exactly once in each column. It helps to watch the Youtube video Was sind Galoiskörper?

4 Legendre symbol

Compute $\left(\frac{713}{1009}\right)$ using the rules on slides of the presentation (Solution is -1).

5 Quadratic congruence

Does the linear congruence $x^2 \equiv 446 \pmod{1129}$ have a solution x? You need not compute x; just decide, if a solution exists. Use the Legendre symbol $\left(\frac{446}{1129}\right)$ to answer this question! (Solution is YES).

6 Quadratic congruence

Implement the square and multiply algorithm and check, if it works reasonable even the numbers have 100 or more digits. Compare Your results with the `pow` function in python.

7 Bases a to which 45 is a Fermat pseudoprimes (< 45)

Show, that the bases a to which 45 is a Fermat pseudoprime are 1, 8, 17, 19, 26, 28, 37, 44.

8 Fermat pseudoprimes to base $a = 2$

A Fermat pseudoprime to base a is a number p such that $a^{p-1} \equiv 1 \pmod{p}$. Compute, using appropriate python code, all Fermat pseudoprimes to base 2 for $2 < p \leq 2000$.

9 Prime number tests

Verify, that

$$\begin{aligned}
2^{561} &\equiv 2 \bmod 561\\
3^{561} &\equiv 3 \bmod 561\\
4^{561} &\equiv 4 \bmod 561\\
&\vdots\\
560^{561} &\equiv 560 \bmod 561
\end{aligned}$$

Have fun with crypto!