

## Homework 9

*Lecturer: Daniel Slamanig, TA: Karen Klein**Due: 23.59 CET, Dec 12, 2018*

To get credit for this homework it must be submitted no later than Wednesday, December 12th via email to `michael.walter@ist.ac.at`, please use “MC18 Homework 9” as subject. Please put your solutions into a single pdf file<sup>1</sup> and name this file Yourlastname\_HW9.pdf.

## 1. Groups

- Let  $N \in \mathbb{Z}_{\geq 0}$  and let  $G = \mathbb{Z}_N$ . Prove that  $G$  is a group under the operation  $a \cdot b = (a + b) \bmod N$ .
- List the elements of  $\mathbb{Z}_{10}^*$ ; what is its order?; What are the orders of 3 and 9?; Is  $\mathbb{Z}_{10}^*$  cyclic?
- Does the set  $\mathbb{Z}_{15} \setminus \{0\}$  form a group under multiplication? If not, why?

## 2. Extended Euclidean Algorithm:

- **[B.1 in book, 2nd edition]** Prove correctness of the extended Euclidean algorithm (extGCD).
- Use the extGCD to compute  $X, Y$  for  $a = 2498$  and  $b = 8712$ . Illustrate all steps.
- Discuss how extGCD can be used to compute the multiplicative inverse.

## 3. Euler phi function

- Let  $p$  be prime and  $e \geq 1$  an integer. Show that  $\varphi(p^e) = p^{e-1}(p - 1)$ .
- Let  $p, q$  be relatively prime. Show that  $\varphi(pq) = \varphi(p) \cdot \varphi(q)$ .

---

<sup>1</sup>If you don't know how to do it, you can use e.g. <https://www.pdfmerge.com/>