Introduction to Cryptography: Homework 7

November 10, 2021

Requirements about the delivery of this assignment:

- Submit a pdf-document via Brightspace;
- Make sure that you write both name and student number on all documents (not only in the file name).

Deadline: Monday, November 22, 17:00 sharp!

Grading: You can score a total of 100 points for the hand-in assignments. To get full points, please **explain all answers clearly and do everything without a calculator!**

Exercises:

1. **Brightspace quiz.** Make the Brightspace quiz on groups, "Practicing with groups". Go to Activities -> Quizzes. [You can attempt the quiz as often as you would like/need. Some of the questions will be easier after the next lecture, but just see how far you can get on your own. It will be an assignment for next week again.]

2. **Long division.**

   (a) Use long division to compute the quotient and remainder when dividing 223092870 by 31.

   (b) What are the quotient q and remainder r? [Hint: $223092870 = q \cdot 31 + r$.]

   (c) What is 223092870 modulo 31?

3. **Factorisation.** Factor $n = 4592700$ without using a computer. [Hint: Use the tests described in Subsection 17.2.3 of the lecture notes.]

4. **Modular groups introduction.**

   (a) Copy and fill Table 1 for addition modulo 9. [You do not have to add an explanation, there is only one correct way.]

   (b) Draw and fill a similar table, for multiplication modulo 9. [You do not have to add an explanation, there is only one correct way.]

   (c) Is $((\mathbb{Z}/9\mathbb{Z}) \setminus \{0\}, \times)$ a group?

   (d) What elements do you have to remove to obtain a group? I.e., for what set $A = \{a_0, a_1, \ldots, a_{n-1}\} \subset \mathbb{Z}/9\mathbb{Z}$ is $((\mathbb{Z}/9\mathbb{Z}) \setminus A, \times)$ a group?

   (e) Give a similar table that shows the multiplication in the group you found in (d).

+	0	1	2	3	4	5	6	7	8
0									
1									
2									
3									
4									
5									
6									
7									
8									

Table 1: Addition table modulo 9.

Hand in assignment:

1. **(30 points) Long division.**
   - (a) Use long division to compute the quotient and remainder when dividing 6758371 by 17. 20 pt
   - (b) What are the quotient q and remainder r? [Hint: $6758371 = q \cdot 17 + r$.] 5 pt
   - (c) What is 6758371 modulo 17? 5 pt

2. **(30 points) Groups.** Consider *the set* $\mathbb{Z}/12\mathbb{Z}$.
   - (a) We have seen in the lecture that $(\mathbb{Z}/12\mathbb{Z}, +)$ is a group. Is $\mathbb{Z}/12\mathbb{Z}$ a group when you consider modular multiplication as operation instead of modular addition? I.e., is $(\mathbb{Z}/12\mathbb{Z}, \times)$ a group? 5 pt
   - (b) Is $((\mathbb{Z}/12\mathbb{Z}) \setminus \{0\}, \times)$ a group? 5 pt
   - (c) For what $\{0\} \subseteq A \subseteq \mathbb{Z}/12\mathbb{Z}$ is $((\mathbb{Z}/12\mathbb{Z}) \setminus A, \times)$ a group? [Find an A of minimal size that suffices.] 15 pt
   - (d) What is the order of this group $((\mathbb{Z}/12\mathbb{Z}) \setminus A, \times)$? 5 pt

3. **(40 points) Subgroups.** Consider the group $\mathcal{G} = (\mathbb{Z}/12\mathbb{Z}, +)$.
   - (a) What is the order of 4? 2 pt
   - (b) What is the order of 5? 3 pt
   - (c) Is $A = \{4, 8\}$ a subgroup of $\mathcal{G}$? 5 pt
   - (d) Is $B = \{0, 2, 4, 8, 10\}$ a subgroup of $\mathcal{G}$? 5 pt
   - (e) Is $C = \{0, 1, 2, 4, 8, 10\}$ a subgroup of $\mathcal{G}$? 5 pt
   - (f) What is the smallest subgroup of $\mathcal{G}$ containing A? 5 pt
   - (g) What is the smallest subgroup of $\mathcal{G}$ containing C? 5 pt
   - (h) Show that the smallest subgroup of $\mathcal{G}$ containing B is a cyclic group. 10 pt