Diskmath Week 9

Emil Straschil

Hello

I am Emil.

I have a **website**:

emils.site (yes thats the URL)

repo: https://github.com/emil3tr/emil3tr.github.io

All materials will be uploaded there.

Any Feedback / Questions / Wishes / … ?

→ estraschil@student.ethz.ch

→ “Emil” (floxi4) on dinfk-discord

→ Diskmath-questions: ask here so others can benefit (:

Where are we right now?

Basics	Sets and Relations	Number Theory	Algebra	Logic
Abstraction	Sets	Division	Monoids	Proof Systems
Formulas	Set Operations	Primes	Groups	Logic
Statements	Relations	Modular Arith.	Euler Totient	Calculi
Prop. Logic	Equivalence	Diffie-Hellman	RSA	Res. Calculus
Pred. Logic	Partial Order		Rings	Prop. Logic
Proof Patterns	Functions		Polynomials	Pred. Logic
	Countability		Finite Fields	
			Err. Corr. Codes	



Questions?

Plan for Today

1. Organization
2. Follow Up last week
3. Rings
4. Kahoot
5. RSA + Diffie-Hellman
6. Exercises

Exam Prep. Session?

- Study / Exam tips
- Kahoot?
- Time to ask questions / discuss afterwards

Date / Time?

- Do. 17.12 15:00 (after AuD)
- Di. 15.12 16:00 (after here)
- Mi. 16.12 8:00 ?
- Any day 18:00 - 20:00 ?

Hand-in Exercises

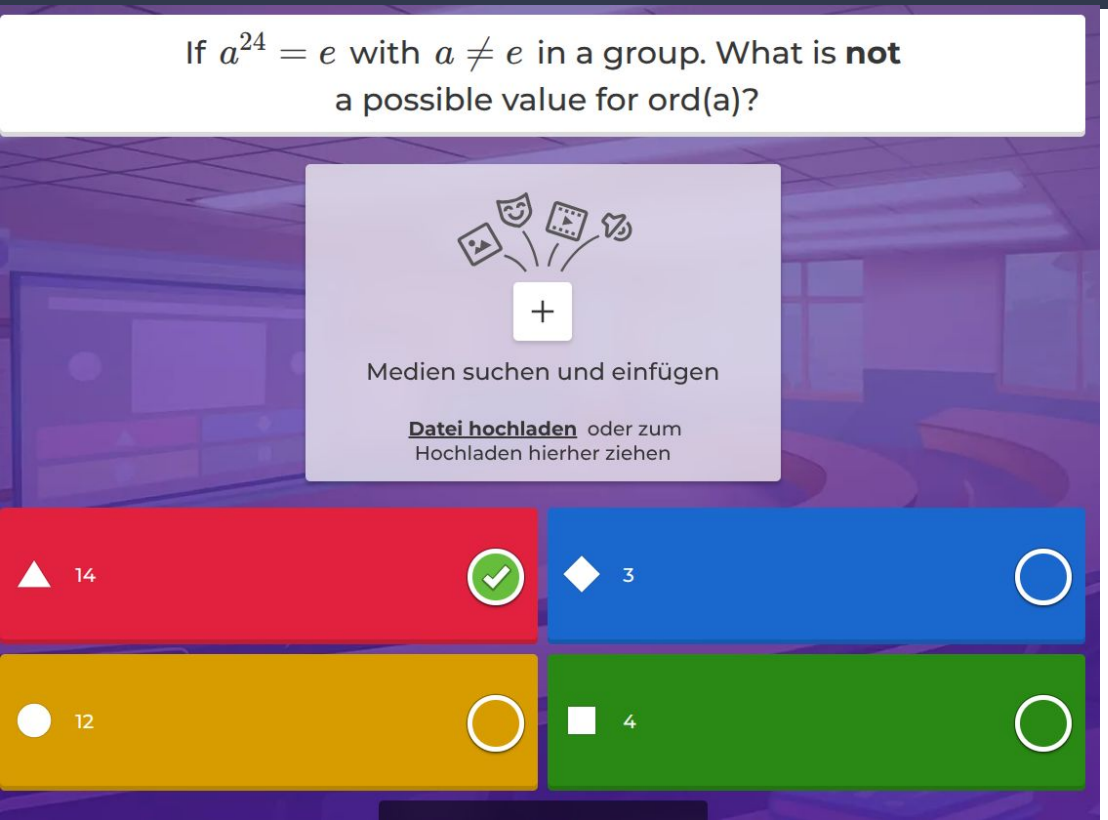
- **Optional** hand-in each week
- **No** bonus points

Should we discuss these exercises in class?

Last Week

- Carrier set can be empty

Kahoot



If ord(a) = 14 then

e

$= a^{24}$

$= a^{14} * a^{10}$

$= e * a^{10}$

$= a^{10}$

so ord(a) <= 10

Exercise 8.3.3

Abstract Algebra Book: Chapter 6.1 “Cosets”

Amazing Exercises, very relevant

Rings

Kahoot

RSA

Exercises