ELEMENTARE ZAHLENTHEORIE

SS 2017

CAROLINE LASSUEUR

TU KAISERSLAUTERN

ELEMENTARE ZAHLENTHEORIE SS 2017

A. ORGANISATION

- **VORLESUNG:** → Mo. 13:45 - 15:15 (24-102)

  ⚠ 17. April: Ostermontag ⇝ keine Vorlesung
  1. Mai: Maifeiertag ⇝ keine Vorlesung
  5. Juni: Pfingstmontag ⇝ keine Vorlesung

  } Nur 11 Wochen !

  ⚠ ⇝ Grosser Einfluss auf die Übungsblätter !

- **ÜBUNGEN:** → Hauptassistentin: Dr. Inga Schwabrow (48-406)

  → 2. Übungsleiter: Tobias Ruhwedel

  → Termine: Mo. 08:15 - 09:45
  Di. 15:30 - 17:00
  Mi. 11:45 - 13:15
  Anfang: 3. Vorlesungswoche

ELEMENTARE ZAHLENTHEORIE SS 2017

A. ORGANISATION

- ÜBUNGEN: → Übungsblätter:

  ⚠ Blatt 1 : Nur 3 Aufgaben (wegen Ostermontag)
  Abgabe: es reicht, nur 2 Aufgaben abzugeben
  3. zählt als Bonus

  ⚠ Blatt 2 : Nur 3 Aufgaben (wegen Maifeiertag)
  Abgabe: es reicht, nur 2 Aufgaben abzugeben
  3. zählt als Bonus

  Blatt 3 → Blatt 7 : 4 Aufgaben

ELEMENTARE ZAHLENTHEORIE SS 2017

A. ORGANISATION

1. Woche : X
2. Woche : V — Mo.: Blatt 1 online ⇝ Fr.: Abgabe
3. Woche : X Ü
4. Woche : V E — Mo.: Blatt 2 online ⇝ Fr.: Abgabe
5. Woche : V Ü — Mo.: Blatt 3 online
6. Woche : V — ↘ Fr.: Abgabe
7. Woche : V Ü — Mo.: Blatt 4 online
8. Woche : X — ↘ Fr.: Abgabe
9. Woche : V Ü — Mo.: Blatt 5 online
10. Woche : V — ↘ Fr.: Abgabe
11. Woche : V Ü — Mo.: Blatt 6 online
12. Woche : V — ↘ Fr.: Abgabe
13. Woche : V Ü — Mo.: Blatt 7 online (Ohne Abgabe)
14. Woche : V

ELEMENTARE ZAHLENTHEORIE SS 2017

A. ORGANISATION

- ÜBUNGEN:

→ Leistungsnachweis: Um einen Übungsschein zu erhalten, brauchen Sie:

1. 50% der Punkte auf die Übungsaufgaben insgesamt.
2. Aktive Teilnahme an den Übungen. (Insbesondere Anwesenheit!)
3. Sinnvolle Bearbeitung der Aufgaben: 1 Punkt in 2 Aufgaben pro Blatt

Abgabe: in Gruppen bis zu 2 Personen.

→ Anmeldung: im URM bis Fr. 28.10, 12:00 Uhr

→ Weitere Fragen: Inga Schwabrow ist alle 2 Wochen im Lernzentrum.

ELEMENTARE ZAHLENTHEORIE SS 2017

A. ORGANISATION

- PRÜFUNG: → die Prüfung über die Vorlesung ist eine mündliche Prüfung

- SKRIPT: → Die Vorlesung basiert auf dem Skript von T. Mankvig, das sehr detailliert ist.

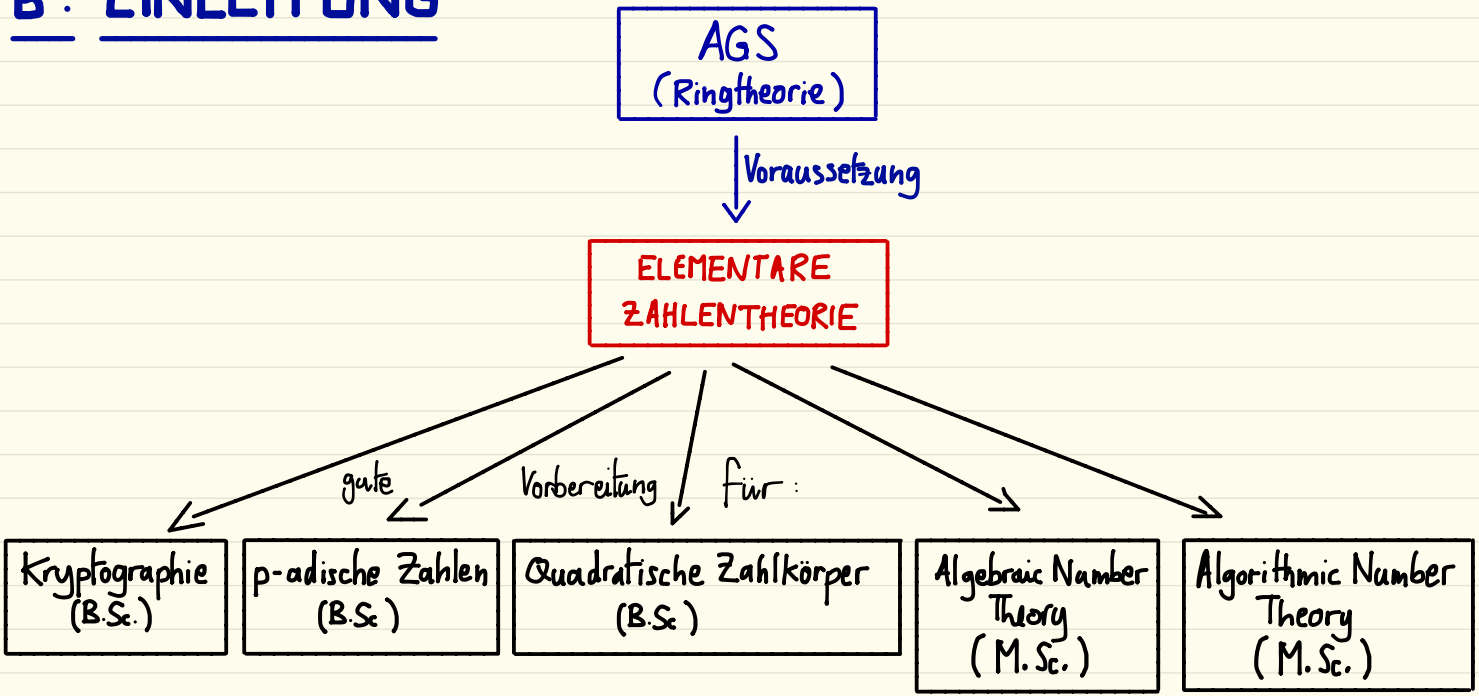
  → Deswegen schreibe ich nur ein Kurzskript, dessen Schreibstil bewusst knapp gehalten ist.

  → Online: jeweils Montags (nach der Vorlesung)

- LITERATUR: → Auf der Webseite.

ELEMENTARE ZAHLENTHEORIE SS 2017

B. EINLEITUNG



ELEMENTARE ZAHLENTHEORIE SS 2017

B. EINLEITUNG

(1) Bedeutung von "elementar" in ELEMENTARE ZAHLENTHEORIE:

- ⚠ "elementar" bedeutet weder "einfach" noch "einfache Methoden" ! (leider!)
- "elementar" bedeutet, dass die Theorie sich mit dem Ring $\mathbb{Z}$ der ganzen Zahlen beschäftigt. (Und nicht mit komplizierteren Ringen wie z.B. $\mathbb{Z}[i]$ oder $\mathbb{Z}[\sqrt{2}]$.)

(2) Probleme, die untersucht werden, sind z.B.:

- ∃? ganzzahlige Lösung für die Gleichung $a_1X_1 + \cdots + a_nX_n = c$ mit $a_1, \ldots, a_n, c \in \mathbb{Z}$?
- Wie viele pe$\mathbb{P}$ gibt es mit $p \equiv a \pmod 4$, wobei $a = 0,1,2,3$?
- Gibt es unendlich viele Primzahlzwillinge ?
- Ist jede gerade Zahl ≥ 4 Summe zweier Primzahlen?

ELEMENTARE ZAHLENTHEORIE SS 2017

B. EINLEITUNG

(2) Probleme, die untersucht werden, sind z.B.:

- Welche Zahlen $n \in \mathbb{N}$ lassen sich als Summe zweier Quadratzahlen darstellen, d.h.

$$n = x^2 + y^2 \text{ mit } (x,y) \in \mathbb{Z}^2 \quad ?$$

- Wie kann man feststellen, ob eine Zahl eine Primzahl ist?
  z.B.: Ist $2^q - 1 \in \mathbb{P}$ $\forall q \in \mathbb{P}$?
  Ist $2^{(2^n)} + 1 \in \mathbb{P}$ $\forall n \in \mathbb{N}$?

⚠ Viele dieser Fragen sind: einfach zu stellen, aber sehr schwer zu beantworten!

ELEMENTARE ZAHLENTHEORIE SS 2017

C. PROGRAMM

I. lineare diophantische Gleichungen
II. multiplikative Funktionen
III. Sätze von Euler, Fermat and Wilson
IV. das RSA-Verfahren
V. Primitivwurzeln modulo n
VI. das quadratische Reziprozitätsgesetz