# PRO-/SEMINAR ÜBER ELEMENTARE ZAHLENTHEORIE

PROF. DR. U. GÖRTZ, P. HARTWIG, SS 2012

In diesem Seminar wollen wir einige Ergebnisse der Zahlentheorie erarbeiten, deren Beweise (im wesentlichen) ohne die Verwendung analytischer oder fortgeschrittener algebraischer Methoden auskommen, zum Beispiel den Satz von Lagrange, dass sich jede natürliche Zahl als Summe von vier Quadratzahlen schreiben lässt und Spezialfälle des Satzes von Dirichlet, dass für teilerfremde Zahlen $m$, $n$ unendlich viele Primzahlen $p$ existieren, derart dass $p - m$ durch $n$ teilbar ist.

**Literatur:** Wir richten uns nach dem Buch [S] von A. Schmidt. Aus dem Uni-Netz ist das Buch elektronisch verfügbar, siehe den Link auf
`http://www.esaga.uni-due.de/buecher/`. Es gibt viele weitere Bücher zur Zahlentheorie, die zusätzlich nützlich sein können. Einige sind unten im Literaturverzeichnis angegeben; schauen Sie in der Bibliothek mal in das eine oder andere hinein!

**Anforderungen/Vorkenntnisse:** Gute Kenntnisse in Linearer Algebra. Die Motivation, sich ein mathematisches Thema anzueignen.

**Organisatorisches:** Der Vortrag soll an der Tafel gehalten werden und nicht länger als 80 Minuten dauern. Danach soll sich in einer kurzen Feedback-Runde jeder der Zuhörer kurz zu Stärken und Schwächen des Vortrags äußern.

Für das Pro-/Seminar gilt Anwesenheitspflicht; es wird eine aktive Teilnahme erwartet. Für den Fall, dass Sie an einem Termin aus wichtigen Gründen verhindert sind, entschuldigen Sie sich bitte vorher bei einem der Veranstalter und bei der/dem Vortragenden. An Teilnehmer, die Termine unentschuldigt versäumen oder insgesamt mehr als zwei Termine versäumen, kann kein Pro-/Seminarschein ausgegeben werden.

Für die mit $*$ gekennzeichneten Vorträge kann wahlweise ein Proseminarschein oder ein Seminarschein vergeben werden. Je nachdem, ob mehr Interesse an Proseminar- oder Seminarvorträgen besteht, werden wir einige der Vorträge auslassen.

**Termin:** Do, 8-10, T03 R04 D10, Beginn: 12.4.2012

## Programm

1. **Primzahlen.** Wir beginnen mit der Definition der Teilbarkeit und von Primzahlen und beweisen den Satz über die eindeutige Primfaktorzerlegung von ganzen Zahlen.

*Inhalt des Vortrags:* [S] 1.1, 1.2. Satz 1.2.6 und die Bemerkung können gegebenenfalls weggelassen werden.

2. **Kongruenzen.** Wir führen die Sprechweise der Kongruenzen ein. Den Begriff des *Rings* setzen wir aus der Linearen Algebra als bekannt voraus (allerdings nicht den Begriff des *Quotienten nach einem Ideal*).

*Inhalt des Vortrags:* [S] 1.3 bis einschließlich Korollar 1.3.12.

3. **Die Eulersche $\varphi$-Funktion, der kleine Satz von Fermat.** In diesem Vortrag wird die Eulersche $\varphi$-Funktion eingeführt, die angibt, wie viele Zahlen zwischen 1 und $n$ teilerfremd zu $n$ sind. Wir beweisen den Satz von Wilson und den kleinen Satz von Fermat.

*Inhalt des Vortrags:* [S] 1.3 ab Definition 1.3.13; 1.4, 1.5.

4. **Polynomkongruenzen und Primitivwurzeln.** Erinnern Sie kurz an den Begriff des Polynoms und erklären Sie, wann Polynome $\in \mathbb{Z}[X]$ kongruent modulo $n$ heißen. Im zweiten Teil des Vortrags wird der Begriff der Primitivwurzel eingeführt.

*Inhalt des Vortrags:* [S] 1.6, 1.7

5. **Das quadratische Reziprozitätsgesetz I.** Das quadratische Reziprozitätsgesetz ist einer der berühmtesten Sätze der Zahlentheorie. Es wurde zuerst um 1800 von C. F. Gauß bewiesen. Verallgemeinerungen dieses Satzes sind auch heute noch Gegenstand der Forschung.

*Inhalt des Vortrags:* [S] 2.1 und Erläuterung der Aussage des quadratischen Reziprozitätsgesetzes; Beispiele dazu.

6. **Das quadratische Reziprozitätsgesetz II.** In diesem Vortrag behandeln wir einen Beweis des quadratischen Reziprozitätsgesetzes.

*Inhalt des Vortrags:* [S] 2.2, und eine Auswahl aus 2.3, so wie es die Zeit zulässt.

7. **Quadratsummen.** Die Frage, ob eine Zahl als Summe von Quadratzahlen darstellbar ist, ist eine klassische Frage der Zahlentheorie. Wir beweisen ein Kriterium dafür, dass eine Primzahl Summe von zwei Quadratzahlen ist, und beweisen, dass jede natürliche Zahl Summe von vier Quadratzahlen ist.

*Inhalt des Vortrags:* [S] 2.4. Gegebenenfalls kann 2.4.4 gekürzt oder ausgelassen werden; 2.4.5 soll auf jeden Fall behandelt werden.

8. **Hindernisse.** In diesem und den folgenden beiden Vorträgen betrachten wir Kriterien für die Lösbarkeit von Polynomgleichungen in den ganzen Zahlen - sogenannter diophantischer Gleichungen. Zunächst geht es um "triviale" Eigenschaften, die eine Lösbarkeit durch ganze Zahlen verhindern. Wenden Sie Ihre Kenntnisse über Lineare Gleichungssysteme aus der Vorlesung *Lineare Algebra 1* an.

*Inhalt des Vortrags:* [S] 3.1, 3.2.

9. **Der Satz von Chevalley-Warning.** Der Satz von Chevalley-Warning ist ein Ergebnis über die Lösungsmengen gewisser Systeme von Polynomgleichungen über $\mathbb{Z}/p\mathbb{Z}$, wobei $p$ eine Primzahl ist. Im zweiten Teil des Vortrags studieren wir dann Lösungen in $\mathbb{Z}/p^r\mathbb{Z}$.

*Inhalt des Vortrags:* [S] 3.3, 3.4

10. **Die Gleichung von Lind und Reichardt.** Die Gleichung von Lind und Reichardt ist ein Beispiel für eine Gleichung, bei der es keine Hindernisse für die Lösbarkeit im Sinne des 8. Vortrags gibt, die aber dennoch nicht lösbar ist.

*Inhalt des Vortrags:* [S] 3.5

11. *** Primzerlegung in $\mathbb{Z}[i]$.** Wir verallgemeinern nun den Satz über die eindeutige Primfaktorzerlegung in $\mathbb{Z}$ auf den Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen und kommen noch einmal auf die Frage der Darstellbarkeit einer Zahl als Summe von zwei Quadratzahlen zurück.

*Inhalt des Vortrags:* [S] 4.3, 4.4

12. *** Pythagoräische Zahlentripel, erweiterte Zahlringe.** In diesem Vortrag wird der Ring $\mathbb{Z}[i]$ benutzt, um Pythagoräische Zahlentripel zu studieren. Außerdem betrachten wir allgemeinere Erweiterungsringe von $\mathbb{Z}$, die zu $\mathbb{Z}[i]$ analog sind.

*Inhalt des Vortrags:* [S] 4.5, 4.6

13. *** Hauptsatz über endlich erzeugte abelsche Gruppen.** Der Hauptsatz über endlich erzeugte abelsche Gruppen besagt, dass jede solche Gruppe isomorph ist zu

$$\mathbb{Z}^r \times \prod_{i=1}^{n} \mathbb{Z}/p_i^{r_i}\mathbb{Z}$$

für geeignete $r, n \geq 0$, $r_i > 0$ und Primzahlen $p_i$. Dieser Satz ist nicht nur in der Zahlentheorie von Bedeutung, sondern überall, wo abelsche Gruppen eine Rolle spielen.

*Inhalt des Vortrags:* [S] 5.2

14. *** Ganze algebraische Zahlen.** Wir führen den Begriff einer ganzen algebraischen Zahl und ihres Minimalpolynoms ein. Geben Sie Beispiele!

*Inhalt des Vortrags:* [S] 5.3; Lemma 5.3.2 und Korollar 5.3.3 können ausgelassen werden.

15. *** Kreisteilungspolynome.** Die Kreisteilungspolynome sind die Minimalpolynome von *primitiven Einheitswurzeln.*

*Inhalt des Vortrags:* [S] 5.4

16. *** Primzahlen mit vorgegebener Restklasse.** Wir wenden die Ergebnisse aus den vorhergehenden Vorträgen an und zeigen, dass es zu jeder natürlichen Zahl $n$ unendlich viele Primzahlen $p$ mit $p \equiv 1 \mod n$ gibt. Dies ist ein Spezialfall des berühmten Satzes von Dirichlet über Primzahlen in arithmetischen Progressionen.

*Inhalt des Vortrags:* [S] 5.5; Geben Sie den Satz von Dirichlet an und sagen Sie etwas zum Beweisprinzip: [S] 8.6

## Literatur


[BS] Z. Borevich, I. Shafarevich, *Number theory*, Academic Press.
[Bu] P. Bundschuh, *Einführung in die Zahlentheorie*, Springer.
[F] G. Frey, *Elementare Zahlentheorie*, Vieweg.
[HW] G. Hardy, E. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press.
[MSP] S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie*, Vieweg.
[RU] R. Remmert, P. Ullrich, *Elementare Zahlentheorie*, Birkhäuser.
[SF] H. Scheid, A. Frommer, *Zahlentheorie*, Spektrum Akad. Verlag.
[S] A. Schmidt, *Einführung in die algebraische Zahlentheorie*, Springer.