Elementary Number Theory:
9 Creditpunkte Nachklausur

Sommer 2016

11 Oktober 2016

Name: _____ Matrikelnummer: _____

Anleitungen

- Diese Klausur besteht aus 6 Aufgaben auf 9 Blätter. Die letzten zwei Blätter können als Notizpapier benutzt werden. Zusätzliche Blätter werden bei Bedarf zur Verfügung gestellt.
- Man muss alle entsprechende Schritte zeigen. Eine Lösung ohne ausreichende Eklärung kann die vollständige Punktzahl nicht erreichen.
- Man darf Sätze aus der Vorlesung benutzen außer wenn es explizit festgelegt wird. Wenn man solches Ergebnis benutzt, muss man es deutlich aufschreiben.
- Schreiben Sie die Lösung auf das entsprechende Blatt ggf. die Rückseite davon.
- Schreiben Sie **deutlich und leserlich**. Punkte werden abgezogen, falls entweder die Lösung oder die logische Reihenfolge nicht verstanden werden können.
- Nicht-programmierbare Taschenrechner sind erlaubt.

Aufgabe:	1	2	3	4	5	6	Gesamtsumme
Punkte:							

1. Es seien $p, a_1, \ldots, a_n \in \mathbb{N}$ mit p prim.
   (a) Falls $p \mid a_1 a_2 \cdots a_n$ gilt, beweisen Sie, dass es ein j gibt mit $p \mid a_j$ für $1 \leq j \leq n$.
   (b) Es seien $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s \in \mathbb{N}$ Primzahlen mit

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

   Beweisen Sie ohne Gebrauch des Fundamentalsatzes der Arithmetik, dass $r = s$ und, nach Vertauschen der Ordnung, $p_j = q_j$ für jedes $1 \leq j \leq r$ gilt.

2. In dieser Aufgabe betrachten Sie den Ring $\mathbb{Z}[i]$. Es sei $\beta = a + bi$ mit $a, b \in \mathbb{Z}$. Beweisen Sie folgendes.
   (a) Falls eines von a, b gerade ist und eines ungerade ist, gilt $1 + i \nmid \beta$.
   (b) Falls a, b beide ungerade sind, gilt $1 + i \mid \beta$
   (c) Es gilt $2 \mid \beta$ genau dann wenn a, b beide gerade sind.

3. Verwenden Sie das Verfahren von sukzessiven Quadraten um $7^{852} \pmod{853}$ auszurechnen. Kann man damit bestimmen, ob 853 prim ist oder nicht?

4. Es sei $n \in \mathbb{N}$ eine Carmichael-Zahl.
   (a) Zeigen Sie, dass n ungerade ist. (Hinweis: Betrachten Sie $(n-1)^n$.)
   (b) Es sei $e \in \mathbb{Z}$ die größte Zahl mit $p^{e+1} \mid n$. Beweisen Sie, dass $p^{e+1} \mid p^{en} - p^e$
   (c) Benutzen Sie Teil (b), um zu beweisen, dass jede Carmichael-Zahl quadratfrei ist. Das heißt, falls p prim und $p \mid n$ gelten, dann gilt $p^2 \nmid n$.

5. Für folgende d, finden Sie mit dem Kettenbruchalgorithmus die Kettenbruchdarstellung von $\sqrt{d}$ und die kleinste Lösung $(x, y) \in \mathbb{N}^2$ zur Gleichung $x^2 - dy^2 = 1$.
   (a) $d = 10$
   (b) $d = 14$

6. Es sei E die elliptische Kurve von $y^2 = x^3 - x$ und $T = \{\mathcal{O}, (0,0), (1,0), (-1,0)\} \subseteq E(\mathbb{Q})$. (Hinweis: $\Delta(E) = 4$.)
   (a) Zeigen Sie, dass $T \subseteq E(\mathbb{Q})_{\text{tor}}$ gilt.
   (b) Finden Sie die Menge $E(\mathbb{F}_p)$ für $p = 3, 5$.
   (c) Beweisen Sie, dass $T = E(\mathbb{Q})_{\text{tor}}$.
   (d) Beweisen Sie, dass $4 \mid \#E(\mathbb{F}_p)$ für jede ungerade Primzahl p.