LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley
Martin Hofer

Wintersemester 2015/16
8. April 2016

Zahlentheorie (Lehramt Gymnasium)

Nachholklausur

Nachname:	Vorname:	Matrikelnummer:

Abschluss: ❍ Lehramt Gymn. (modularisiert) ❍ Lehramt Gymn. (nicht modul.)

❍ Anderes: _____

❑ Ich stimme zu, dass mein Klausurergebnis im Internet nach Angabe meiner Matrikelnummer und meines bei Klausuranmeldung angegebenen Passworts abrufbar sein wird.

Bitte beachten Sie:

- Schalten Sie Ihr Mobiltelefon aus und verstauen Sie es zusammen mit allen weiteren nicht zugelassenen Hilfsmitteln in Ihrer Tasche.
- Legen Sie Ihren Lichtbild- und Studienausweis sichtbar auf den Tisch.
- Überprüfen Sie, ob Sie **fünf Aufgaben** erhalten haben.
- Schreiben Sie mit einem **dokumentenechten** Stift, jedoch nicht in den Farben rot und grün.
- Schreiben Sie auf **jedes Blatt** Ihren **Nach- und Vornamen**. Lösen Sie bitte jede Aufgabe auf den dafür vorgesehenen Blättern. Versehen Sie auch zusätzliche Blätter mit Nach- und Vornamen sowie der Aufgabennummer. Vermerken Sie deutlich, wenn Ihre Lösung auf weiteren Blättern fortgesetzt wird.
- Geben Sie zu jeder Aufgabe nur eine Lösung ab; streichen Sie deutlich durch, was nicht gewertet werden soll.
- Sie haben **120 Minuten** Zeit, die Klausur zu bearbeiten.

Viel Erfolg!

1	2	3	4	5	Summe
/8	/6	/11	/8	/10	/43

Name: _____

Aufgabe 1. (8 Punkte)

a) Bestimmen Sie das Inverse von $\overline{50}$ in $\mathbb{Z}/123457\mathbb{Z}$. (4 Punkte)

b) Bestimmen Sie eine Lösung von $z^5 \equiv 7 \pmod{27}$. (4 Punkte)

Natürlich müssen auch hier die Antworten vollständig begründet und die aufgestellten Behauptungen bewiesen werden.

Name: _____ Fortsetzung zu **Aufgabe 1**.

Name: _____

Aufgabe 2. (6 Punkte)

a) Entscheiden Sie, ob $x^2 \equiv 425 \pmod{929}$ eine Lösung hat. (4 Punkte)
Hinweis: 929 *ist eine Primzahl.*

b) Seien $m, n \geq 2$ zwei ungerade zueinander teilerfremde natürliche Zahlen und $\left(\frac{n}{m}\right)$ das Jacobi-Symbol. Zeigen Sie durch die Angabe eines expliziten Gegenbeispiels, dass $\left(\frac{n}{m}\right) = 1$ nicht impliziert, dass n ein Quadrat modulo m ist. (2 Punkte)

Natürlich müssen auch hier die Antworten vollständig begründet und die aufgestellten Behauptungen bewiesen werden.

Name: _____ Fortsetzung zu **Aufgabe 2**.

Name: _____

Aufgabe 3. (11 Punkte) Sei p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Körper mit p Elementen. Für $a \in \mathbb{Z}$ bezeichne $\bar{a}$ die Restklasse in $\mathbb{F}_p$. Sei $\mathbb{Z}[X]$ der Polynomring in X über $\mathbb{Z}$.

a) Zeigen Sie, dass

$$\begin{aligned} \varphi\colon \mathbb{Z}[X] &\to \mathbb{F}_p, \\ h(X) &\mapsto \overline{h(0)} \end{aligned}$$

ein Homomorphismus von Ringen ist. Zeigen Sie ferner, dass φ surjektiv ist.(3 Punkte)

b) Zeigen Sie $\ker(\varphi) = (p, X)$. (4 Punkte)

c) Zeigen Sie, dass (p, X) ein maximales Ideal ist. (2 Punkte)

d) Ist $(X) \subseteq \mathbb{Z}[X]$ ein Primideal? (2 Punkte)

Natürlich müssen auch hier die Antworten vollständig begründet und die aufgestellten Behauptungen bewiesen werden.

Name: _____ Fortsetzung zu **Aufgabe 3**.

Name: _____

Aufgabe 4. (8 Punkte) Sei $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$, wobei $i^2 = -1$, der Ring der ganzen Gaußschen Zahlen.

a) Beweisen Sie, dass 13 reduzibel in $\mathbb{Z}[i]$ ist. (3 Punkte)

b) Beweisen Sie, dass 3 irreduzibel in $\mathbb{Z}[i]$ ist. (5 Punkte)

Natürlich müssen auch hier die Antworten vollständig begründet und die aufgestellten Behauptungen bewiesen werden.

Name: _____ Fortsetzung zu **Aufgabe 4**.

Name: _____

Aufgabe 5. (10 Punkte)
Beweisen oder widerlegen Sie folgende Aussagen (jeweils 2 Punkte):

a) $\sqrt{-7}$ ist in $\mathbb{Q}(\zeta_7)$ enthalten, wobei $\zeta_7 = \exp(2\pi i/7)$.

b) Zu jedem Nullteiler $\bar{x} \in \mathbb{Z}/125\mathbb{Z}$ gibt es eine natürliche Zahl k mit $\bar{x}^k = \bar{0}$.

c) Sei $R = \mathbb{Z}[\sqrt{-5}]$. Dann ist $R[X]$ faktoriell.

d) Das System von simultanen Kongruenzen

$$\begin{aligned} y &\equiv 50 \pmod{100}, \\ y &\equiv 51 \pmod{105}, \end{aligned}$$

hat mindestens eine Lösung $y \in \mathbb{Z}$.

e) Es gibt ein Polynom $f \in \mathbb{Z}[X]$ mit

$$\begin{aligned} f &\equiv X \pmod{X^2+1}, \\ f &\equiv X^7 \pmod{X^7+5X+5}. \end{aligned}$$

Name: _____ Fortsetzung zu **Aufgabe 5**.