Wiederholungsklausur Modul Einführung in die Zahlentheorie

Prof. Dr. Andreas Stein

10:00 - 13:00 Uhr, **26.03.2010**, W03 1-161

Die erlaubte Bearbeitungszeit der Klausur beträgt **130 Minuten**. Zusätzlich erhalten Sie **20 Minuten** Zeit, um die Klausur zu lesen und das Deckblatt **leserlich und in Druckbuchstaben** auszufüllen und zu unterschreiben. Bitte schreiben Sie Ihren Namen auf jedes Blatt.

Hilfsmittel sind keine erlaubt. Insbesondere werden Taschenrechner nicht zugelassen. Jegliche Hilfe während der Klausur ist verboten. Da es Teilpunkte geben wird, ist es in Ihrem Interesse, **detaillierte Begründungen** anzugeben und **alle Beweisschritte** zu zeigen. Bei Rechenaufgaben müssen **alle Schritte** nachvollziehbar sein.
Bitte beantworten Sie alle Fragen in den zur Verfügung gestellten Freiräumen. Sollten Sie mehr Platz benötigen, können Sie auch die Rückseite verwenden.

Es müssen alle Aufgaben bearbeitet werden. Die Klausur geht zu **70 %** in die Modulnote ein. Um die Klausur zu bestehen, benötigen Sie **17,5 Punkte**.

Viel Erfolg!

Name, Vorname: ______________________ Matr.-Nr: ______________

Studiengang: ______________ Fach/Fächer: ______________________

Zur Kenntnis genommen: ______________

(Unterschrift)

1	
2	
3	
4	
5	
6*	
Summe	

1. (10 Punkte)

a. (2 Punkte) Geben Sie präzise Definitionen für die folgenden Begriffe an.

(i) Das Legendre Symbol $\left(\frac{a}{p}\right)$.

(ii) k ist der Index von a zur Basis g modulo m.

b. (2 Punkte) Formulieren Sie präzise den Satz über die quadratische Reziprozität von Gauß.

c. (6 Punkte) Bestimmen Sie mit Begründung, ob die folgenden Aussagen wahr oder falsch sind.

(i) Sind g, h Primitivwurzeln modulo einer ungeraden Primzahl p und ist a eine zu p teilerfremde ganze Zahl, so gilt:

$$\operatorname{ind}_h(a) \equiv \operatorname{ind}_g(a) \operatorname{ind}_h(g) \pmod{(p-1)} .$$

(ii) $2010^{2010} + 1$ ist durch 13 teilbar. [Hinweis: $2010 = 2 \cdot 3 \cdot 5 \cdot 67$.]

(iii) Sei l eine natürliche Zahl, so dass $p = 2^l + 1$ eine Primzahl ist. Dann ist jeder quadratische Nichtrest modulo p eine Primitivwurzel modulo p.

2. (15 Punkte)

a. (10 Punkte) Bestimmen Sie ganze Zahlen a, b, so dass

(i) $a^2 + b^2 = 2009$.

(ii) $a^2 + b^2 = 2010$.

b. (5 Punkte) Bestimmen Sie die Anzahl der Lösungen der folgenden linearen Kongruenz:

$$374x \equiv 102 \pmod{578} .$$

Name, Vorname:______________________

3. (15 Punkte)

a. (10 Punkte) Beweisen Sie: Für alle ganzen Zahlen a ist $\frac{4}{7}a^7 + \frac{2}{5}a^5 + \frac{1}{35}a$ eine ganze Zahl.

b. (5 Punkte) Beweisen Sie, dass es keine natürliche Zahl n mit $\phi(n) = 14$ gibt.

4. (15 Punkte) Bestimmen Sie alle inkongruenten Lösungen der folgenden Polynomkongruenz modulo $175 = 5^2 \cdot 7$.

$$x^4 + x \equiv 0 \pmod{175} .$$

5. (15 Punkte) Für die Primitivwurzel $g = 3$ modulo 17 ergeben sich folgende Indizes:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{ind}_3(a)$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

a. (10 Punkte) Finden Sie anhand dieser Information alle Werte c, $1 \leq c \leq 16$, so dass die Polynomkongruenz

$$cx^4 \equiv 2 \pmod{17}$$

lösbar ist. Geben Sie dann jeweils die Anzahl der inkongruenten Lösungen modulo 17 an.

b. (5 Punkte)
Bestimmen Sie mittels Indexarithmetik den Rest bei der Division von $3^{31}\,9^{45}\,10^{11}\,13^{57}$ durch 17.

6*. (6 Bonuspunkte) *Bonusaufgaben werden strikt bewertet.*

a. (3 Bonuspunkte) Sei p eine Primzahl mit $p \geq 5$ und a eine ganze Zahl mit $\mathrm{ggT}(a, p) = 1$. Beweisen Sie: Falls $p \equiv 1 \pmod{6}$, so hat die Kongruenz $x^3 \equiv a \pmod{p}$ entweder 0 oder 3 Lösungen modulo p, und falls $p \equiv 5 \pmod{6}$, so hat die Kongruenz $x^3 \equiv a \pmod{p}$ eine eindeutige Lösung modulo p.

b. (3 Bonuspunkte) Beweisen Sie, dass die Kongruenz

$$4x^2 + 3x + 21 \equiv 0 \pmod{47}$$

eine Lösung besitzt.