Fachbereich Mathematik
Thomas Markwig

Sommersemester 2008, Blatt 5

Elementare Zahlentheorie

Abgabetermin: Donnerstag, 19/06/2008, 12:00
Fernstudenten reichen alle Aufgaben ein und ersetzen den hier angegebenen Abgabetermin durch den ihnen mitgeteilten. Für alle anderen Studenten sind die Aufgaben 19 und 20 eine Präsenzaufgabe, deren Lösung nicht eingereicht werden muß. Für die Lösung der Aufgaben 18, 19 und 20 b./c. wird die Vorlesung vom 16.6. benötigt.

Aufgabe 17:

a. a ist genau dann quadratischer Rest modulo 4, wenn $a \equiv 1 \pmod 4$.

b. Für $a \in \mathbb{Z}$ sind die folgenden Aussagen gleichwertig:

(a) a ist ein quadratischer Rest modulo 2^k für alle $k \geq 3$.

(b) a ist ein quadratischer Rest modulo 8.

(c) $a \equiv 1 \pmod 8$.

Hinweis, den Schritt b. $\Longrightarrow$ a. kann man mit Induktion nach k zeigen. Dabei sollte man sich für $x^2 = a + c \cdot 2^{k-1}$ die Zahl $y = x + c \cdot 2^{k-2}$ anschauen.

Aufgabe 18: Ist die Fermatsche Zahl $F_n = 2^{(2^n)} + 1$ eine Primzahl, so gilt

$$3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}.$$

Aufgabe 19: Es sei $p \in \mathbb{P}$ eine ungerade Primzahl.

a. Zeige,

$$\nu_{2,p} = \left| \left\{ n \;\middle|\; \frac{p-1}{4} < n \leq \frac{p-1}{2} \right\} \right|.$$

b. Zeige,

$$\left(\frac{2}{p}\right) \equiv \begin{cases} 1, & \text{falls } p \equiv \pm 1 \pmod 8, \\ -1, & \text{falls } p \equiv \pm 3 \pmod 8. \end{cases}$$

Aufgabe 20:

a. Zeige mit Hilfe des Primitivwurzelkriteriums, daß $a = 77$ ein quadratischer Rest modulo $n = 2197$ ist und finde eine Lösung von $x^2 \equiv a \pmod{2197}$.

b. Zeige mit Hilfe des Quadratischen Reziprozitätsgesetzes, daß $a = 77$ ein quadratischer Rest modulo $n = 2197$ ist.

c. Ist 195 ein quadratischer Rest modulo 1901?