Fachbereich Mathematik
Thomas Markwig

Sommersemester 2014, Blatt 5

Elementare Zahlentheorie

Abgabetermin: Mittwoch, 11/06/2014, 10:00
Aufgabe 18 ist eine Präsenzaufgabe und braucht nur von den Fernstudenten zur Lösung eingereicht zu werden. Zur Bearbeitung von Aufgabe 18 benötigt man Satz 7.5 der Vorlesung.

Aufgabe 17:

a. Bestimme Primitivwurzeln modulo n für $n = 242$ und $n = 343$.

b. Zeige, dass 2 eine Primitivwurzel modulo 3^k für alle $k \in \mathbb{Z}_{>0}$ ist.

Aufgabe 18:

a. Es sei $p \in \mathbb{P}$ eine Primzahl mit $p \equiv 3 \pmod 4$ und a ein Quadrat modulo p. Zeige, dass $x = a^{(p+1)/4}$ eine Lösung von $x^2 \equiv a \pmod p$ ist.

b. Zeige mit Hilfe des Primitivwurzelkriteriums, dass $a = 83$ ein quadratischer Rest modulo $n = 361$ ist und finde eine Lösung von $x^2 \equiv a \pmod{361}$.

c. Es sei jetzt $p \in \mathbb{P}$ eine Primzahl mit $p \equiv 5 \pmod 8$ und a ein Quadrat modulo p. Finde einen expliziten Ausdruck für eine Lösung der Gleichung $x^2 \equiv a \pmod p$.

Aufgabe 19: Es sei $p \in \mathbb{P}$ eine Primzahl, $k \in \mathbb{Z}_{>0}$ und $a = p^m \cdot b \in \mathbb{Z}$ mit $\operatorname{ggt}(b, p) = 1$.

a. Ist $m \geq k$, so hat die Gleichung $x^2 \equiv a \pmod{p^k}$ eine Lösung in $\mathbb{Z}$.

b. Ist $0 \leq m < k$, so sind die folgenden Aussagen gleichwertig:

   (a) $x^2 \equiv a \pmod{p^k}$ hat eine Lösung in $\mathbb{Z}$.

   (b) m ist gerade und die Gleichung $y^2 \equiv b \pmod{p^{k-m}}$ ist in $\mathbb{Z}$ lösbar.

Aufgabe 20: *(Quadratische Reste modulo 2)*

a. a ist genau dann quadratischer Rest modulo 2, wenn a ungerade ist.

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

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