

Elementare Zahlentheorie

Abgabetermin: Donnerstag, 10/06/2010, 12:00

Aufgabe 17:

- Bestimme Primitivwurzeln modulo n für $n = 242$ und $n = 343$.
- Zeige, dass 2 eine Primitivwurzel modulo 3^k für alle $k \in \mathbb{Z}_{>0}$ ist.

Aufgabe 18:

- 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.
- Zeige mit Hilfe des Primitivwurzelkriteriums, dass $a = 83$ ein quadratischer Rest modulo $n = 361$ ist und finde eine Lösung von $x^2 \equiv a \pmod{361}$.
- Freiwillige Zusatzaufgabe*
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 $\text{ggT}(b, p) = 1$.

- Ist $m \geq k$, so hat die Gleichung $x^2 \equiv a \pmod{p^k}$ eine Lösung in \mathbb{Z} .
- Ist $0 \leq m < k$, so sind die folgenden Aussagen gleichwertig:
 - $x^2 \equiv a \pmod{p^k}$ hat eine Lösung in \mathbb{Z} .
 - 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 ist genau dann quadratischer Rest modulo 2, wenn a ungerade ist.
- a ist genau dann quadratischer Rest modulo 4, wenn $a \equiv 1 \pmod{4}$.
- Für $a \in \mathbb{Z}$ sind die folgenden Aussagen gleichwertig:
 - a ist ein quadratischer Rest modulo 2^k für alle $k \geq 3$.
 - a ist ein quadratischer Rest modulo 8.
 - $a \equiv 1 \pmod{8}$.