Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

SS 2008
2. Juli 2008

Primzahlen. Eine Einführung in die Zahlentheorie

Übungsblatt 6

Aufgabe 21

Seien g und g' zwei Primitivwurzeln modulo einer Primzahl p Man zeige:

$$\log_{g'}(g) \cdot \log_g(g') \equiv 1 \bmod (p-1).$$

Aufgabe 22

Sei g Primitivwurzel modulo einer ungeraden Primzahl p. Man beweise:
Genau dann ist $-g$ ebenfalls Primitivwurzel modulo p, falls $p \equiv 1 \bmod 4$.

Aufgabe 23

Sei p eine Primzahl der Gestalt $p = 2q + 1$, wobei q ebenfalls prim sei. Man zeige: Ein Element $g \not\equiv \pm 1 \bmod p$ ist genau dann Primitivwurzel modulo p, falls g quadratischer Nichtrest modulo p ist.

Aufgabe 24

Sei p eine Primzahl mit $p \equiv 3 \bmod 4$ und a quadratischer Rest modulo p. Man zeige:
i) Das Element $x := a^{(p+1)/4}$ ist Lösung der Kongruenz $x^2 \equiv a \bmod p$.
ii) Das Element x ist ebenfalls quadratischer Rest modulo p.

Abgabetermin: Mittwoch, 9. Juli 2008, 14 Uhr, Übungskasten im 1. Stock

Klausurtermin: Freitag, 11. Juli 2008, 14 hct.