Übungen zu Vertiefung Elementare Zahlentheorie

WS 2010/2011, Blatt 8

Aufgabe 29. Zeigen Sie für jede ungerade Zahl a und jedes $e \geq 3$:

$$a^{2^{e-2}} \equiv 1 \pmod{2^e}.$$

Vergleichen Sie dieses Resultat mit dem Satz von Euler.

Aufgabe 30. Seien p eine Primzahl und a eine zu p teilerfremde Zahl der Ordnung d modulo p. Zeigen Sie: Die Ordnung von a^k (k ganz) ist $d/\mathrm{ggT}(k, d)$.

Aufgabe 31. Seien p eine Primzahl und a eine zu p teilerfremde Zahl. Zeigen Sie: a ist genau dann eine Primitivwurzel modulo p, wenn

$$a^{(p-1)/q} \not\equiv 1 \pmod{p}$$

für jeden Primteiler q von $p - 1$.

Aufgabe 32. (a) Erstellen Sie eine Index-Tabelle für die Primzahl 17 und die Primitivwurzel 3.
(b) Verwenden Sie die Index-Tabelle, um die folgenden Gleichungen zu lösen:

$$x^{20} \equiv 13 \pmod{17}; \quad x^{12} \equiv 13 \pmod{17}; \quad x^{11} \equiv 9 \pmod{17}.$$

Abgabe bis Freitag, 10.12.2010, 12:00 Uhr