Übungen zu Vertiefung Elementare Zahlentheorie

WS 2010/2011, Blatt 8

Aufgabe 29. Show for any odd integer a and any $e \geq 3$:

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

Compare this result with Euler's theorem.

Aufgabe 30. Let p be a prime number and a an integer relatively prime to p of order d modulo p. Show: The order of a^k (k an integer) is $d/\gcd(k,d)$.

Aufgabe 31. Let p be a prime number and a an integer relatively prime to p. Show: a is a primitive root modulo p if and only if

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

for every prime divisor q of $p-1$.

Aufgabe 32. (a) Construct an index table for the prime number 17 and the primitive root 3.
(b) Use the index table to solve the following congruences:

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

Abgabe bis Freitag, 10.12.2010, 12:00 Uhr