Mathematisches Institut
Abt. für Reine Mathematik
Dr. K. Halupczok

08.05.2007

Übungen zur Vorlesung

Elementare Zahlentheorie

SoSe 2007

Blatt 4

Abgabe: Dienstag, den 15.05.2007, zu Beginn der Vorlesung

Aufgabe 1.

(a) Bestimme $\mathrm{ord}_{17}(2)$, $\mathrm{ord}_{19}(3)$ und $\mathrm{ord}_{23}(5)$.

(b) Bestimme alle Primitivwurzeln mod 19.

Aufgabe 2.

(a) Seien $(a, n) = 1$ und $\mathrm{ord}_n(a) = n - 1$. Dann ist n eine Primzahl.

(b) Seien $(a, p) = 1$ und $\mathrm{ord}_p(a) = 2k$, wobei p prim und ungerade.
Dann ist $a^k \equiv -1(p)$.

Aufgabe 3.
Sei $F_n := 2^{2^n} + 1$ die n-te Fermatzahl.

(a) $2^{F_n - 1} \equiv 1(F_n)$

(b) Bestimme $\mathrm{ord}_{F_n}(2)$.

(c) Bestimme $\mathrm{ord}_{2^n - 1}(2)$.

(d) $\varphi(2^n - 1)$ ist ein Vielfaches von n.

Aufgabe 4.

(a) Sei r Primitivwurzel mod n. Zeige, dass r^k genau dann Primitivwurzel mod n ist, wenn $(k, \varphi(n)) = 1$.

(b) Sei $p > 2$ prim und $(a, p) = 1$. Zeige, dass a genau dann Primitivwurzel mod p ist, wenn $a^{\frac{p-1}{q}} \not\equiv 1(p)$ für alle Primteiler q von $p - 1$.