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

24.05.2006

Übungen zur Vorlesung

Elementare Zahlentheorie

SoSe 2006

Blatt 4

Abgabe: Donnerstag, den 01.06.2006, zu Beginn der Vorlesung

Aufgabe 1.

(a) Bestimme die letzten drei Ziffern in der Dezimaldarstellung von 11^{1003}.
(b) 4147 teilt $12^{512} - 1$.
(c) $1835^{1910} + 1986^{2061} \equiv 0 \ (7)$.
(d) Zeige, daß $a^{13} \equiv a \ (273)$ für alle $a \in \mathbb{Z}$ gilt.

Aufgabe 2.
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) Zeige, daß $\varphi(2^n - 1)$ ein Vielfaches von n ist.

Aufgabe 3.

(a) Zeige: 2 ist Primitivwurzel von 19, aber nicht von 17.
(b) Bestimme die 8 Primitivwurzeln mod 17.
(c) Zeige, daß 15 keine Primitivwurzel besitzt, durch Berechnung der Ordnungen der Zahlen $2, 4, 7, 8, 11, 13$ und 14 modulo 15.

Aufgabe 4.
Sei r eine Primitivwurzel der ungeraden Primzahl p. Beweise:
(a) $r^{\frac{p-1}{2}} \equiv -1 \ (p)$.
(b) Gilt $p \equiv 1 \ (4)$, so ist $-r$ ebenfalls Primitivwurzel von p.
(c) Gilt $p \equiv 3 \ (4)$, so hat $-r$ die Ordnung $\frac{p-1}{2}$ mod p.