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

SS 2004
4. Juni 2004

Einführung in die Zahlentheorie, Übungsblatt 7

Aufgabe 25

Sei g ein Element der Ordnung $r < \infty$ einer Gruppe G und

$$a := g^k, \quad k \geqslant 2.$$

Man zeige: Das Element a hat die Ordnung

$$\operatorname{ord}(a) = \frac{r}{\gcd(k,r)}.$$

Aufgabe 26

Sei $p \geqslant 3$ eine Primzahl und q eine weitere Primzahl. Man beweise

(1) Falls $q \nmid p-1$, ist die Gleichung

$$x^q \equiv a \bmod p$$

für alle $a \in \mathbb{Z}$ lösbar. Die Lösung ist modulo p eindeutig bestimmt.

(2) Falls $q \mid p-1$, so ist die Gleichung

$$x^q \equiv a \bmod p$$

für $a \not\equiv 0 \bmod p$ genau dann lösbar, falls

$$a^{(p-1)/q} \equiv 1 \bmod p.$$

Es gibt dann q verschiedene Lösungen modulo p.

Aufgabe 27

Man bestimme die kleinste Primzahl p, so dass 10 Primitivwurzel modulo p, aber nicht Primitivwurzel modulo p^2 ist.

Aufgabe 28

Man zeige: Im 16-adischen System ist die Periodenlänge von $1/p$, ($p \geqslant 3$ prim), maximal $(p-1)/2$. Man gebe alle Primzahlen < 100 an, für die diese Schranke erreicht wird.

Bemerkung. Für die beiden letzten Aufgaben ist Computer-Unterstützung nützlich.

Dieses Übungsblatt wird nicht korrigiert.
Es wird in der Übungsstunde am Mittwoch, den 16. Juni 2004, besprochen.