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

SS 2004
18. Juni 2004

Einführung in die Zahlentheorie, Übungsblatt 9

Aufgabe 33

a) Für $k = 2, 3, 5$ gebe man explizit die Untergruppe $G(k) \subset \mathbb{F}_{31}^*$ mit k Elementen an.

b) Man zeige, dass sich jedes $x \in \mathbb{F}_{31}^*$ eindeutig als Produkt

$$x = x_1 x_2 x_3 \qquad \text{mit } x_1 \in G(2), x_2 \in G(3), x_3 \in G(5)$$

schreiben lässt.

c) Man gebe diese Zerlegung für $x = 3$ und $x = 10$ explizit an.

Aufgabe 34

Für eine ganze Zahl $N \geqslant 2$ sei $\lambda(N)$ die kleinste positive ganze Zahl λ, so dass

$$x^\lambda = \overline{1} \qquad \text{für alle } x \in (\mathbb{Z}/N)^*.$$

a) Man beweise: Es gibt stets ein Element $x_0 \in (\mathbb{Z}/N)^*$ mit der Ordnung $\lambda(N)$.

b) Sei $N = pq$ mit ungeraden Primzahlen $p \neq q$. Man zeige

$$\lambda(N) = \frac{\varphi(N)}{\gcd(p-1, q-1)}.$$

Aufgabe 35

Sei $N = pq$ mit ungeraden Primzahlen $p \neq q$ und sei $e \geqslant 3$ eine ganze Zahl mit $\gcd(e, \varphi(N)) = 1$. Man zeige: Die RSA-Verschlüsselung

$$E : \mathbb{Z}/N \longrightarrow \mathbb{Z}/N, \qquad E(x) := x^e,$$

hat mindestens 9 Fixpunkte, d.h. Elemente $\xi \in \mathbb{Z}/N$ mit $E(\xi) = \xi$.

Aufgabe 36

Für die Primzahl $p := 101$ ist $g := 2$ eine Primitivwurzel. Seien $\alpha, \beta \in \mathbb{Z}/(p-1)$ und

$$g^\alpha \equiv 44 \bmod p, \quad g^\beta \equiv 72 \bmod p.$$

Man berechne $K := g^{\alpha\beta} \bmod p$.

Dieses Übungsblatt wird nicht korrigiert.
Es wird in der Übungsstunde am Mittwoch, den 30. Juni 2004, besprochen.