Übungen zur **Blatt 8**
Elementaren Zahlentheorie 03.05.2013

Falko Lorenz, Karin Halupczok SoSe 2013

Abgabetermin: Mittwoch, 12. Juni 2013, bis 16:10 Uhr in die Briefkästen

Aufgabe 29:

Für die Eulersche φ-Funktion zeige man:

(a) Aus $(m,n)=d$ folgt $\varphi(mn)\varphi(d)=d\varphi(m)\varphi(n)$.

(b) Aus $a \mid b$ folgt $\varphi(a) \mid \varphi(b)$.

(c) $\lim_{n\to\infty} \varphi(n)=\infty$, d. h. für jedes $C>0$ ist $\varphi(n)\le C$ nur für endlich viele n.

(d) Mit Ausnahme von $n=2$ und $n=6$ gilt $\varphi(n)\ge\sqrt{n}$. (4P extra)

Aufgabe 30:

Für $m,n\in\mathbb{N}$ mit $m \mid n$ zeige man, daß der natürliche Homomorphismus

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$$

surjektiv ist. (Hinweis: Betrachte den Fall $n=mp$, p prim.)

Aufgabe 31:

Sei n eine natürliche Zahl >2. Genau dann gilt

(H) $$x^{n-1}\equiv 1 \bmod n \qquad \text{für alle zu } n \text{ primen } x \text{ aus } \mathbb{Z},$$

wenn folgende Bedingungen erfüllt sind:
n ist ungerade, n ist quadratfrei, und wenn $n=p_1p_2\cdots p_r$ die Primfaktorzerlegung von n ist, so gilt

(*) $$p_i-1 \;\Big|\; \prod_{j\neq i} p_j - 1 \text{ für jedes } 1\le i\le r.$$

Man beweise dies und gebe (für 2P extra) ein $n\notin\mathbb{P}$ an, für welches (H) gilt.
(Hinweis: (*) ist gleichwertig mit $p_i-1 \mid p_1\cdots p_r-1$ für jedes $1\le i\le r$.)

Aufgabe 32:

Sei p eine *Sophie-Germain-Primzahl*, d. h. mit p sei auch $q:=2p+1$ eine Primzahl.
Wieviel Erzeuger hat $(\mathbb{Z}/q\mathbb{Z})^\times$?
Man zeige: Für jedes $g\in\mathbb{N}$ mit $2\le g\le p$ ist g oder $-g$ eine Primitivwurzel mod q.
(Hinweis: Jedenfalls ist es ratsam, den Fall $p=2$ vorab zu erledigen.)