TECHNISCHE UNIVERSITÄT
KAISERSLAUTERN

Fachbereich Mathematik
SS 2013

Prof. Dr. Wolfram Decker
Übungsblatt 06

Elementare Zahlentheorie

Abgabetermin: Mittwoch, 03.07.2013, 10 Uhr

Aufgabe 21: Zeigen Sie:

(i) (Eisenstein'sches Irreduzibilitäts–Kriterium) Sei

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Z}[x].$$

Wenn es ein $p \in \mathbb{P}$ gibt mit $p|a_i$ für $1 \leq i \leq n$ sowie $p^2 \nmid a_n$, so ist f irreduzibel in $\mathbb{Q}[x]$.

(ii) Für $p \in \mathbb{P}$ ist das Polynom

$$\Phi_p(x) := x^{p-1} + x^{p-2} + \cdots + x + 1$$

irreduzibel in $\mathbb{Q}[x]$.

Aufgabe 22:

(i) Seien R ein kommutativer Ring mit Eins, $a \in R$ und $n \in \mathbb{N}$. Formulieren Sie einen Algorithmus zur schnellen Berechnung von a^n.
Hinweis: Stellen Sie n im Dualsystem dar.

(ii) Zeigen Sie mit Hilfe des Satzes von Fermat, dass 1903 keine Primzahl ist.

Aufgabe 23: Zeigen Sie:

(i) Eine Carmichael–Zahl hat mindestens 3 verschiedene Primfaktoren.

(ii) Ist $p > 3$ eine Primzahl, so dass auch $2p - 1$ und $3p - 2$ Primzahlen sind, so ist

$$m := p(2p - 1)(3p - 2)$$

eine Carmichael–Zahl.

(iii) Benutzen Sie (ii), um zwei von 561 verschiedene Carmichael–Zahlen zu finden.

Aufgabe 24:

(i) Sei $p \in \mathbb{P}, p > 3$. Zeigen Sie:

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & \text{falls} \quad p \equiv \pm 1 \mod 12\,, \\ -1 & \text{falls} \quad p \equiv \pm 5 \mod 12\,. \end{cases}$$

(ii) Lösen Sie die Kongruenzen $x^2 \equiv 3 \mod p = 11$ und $p = 13$.

(iii) Finden Sie ähnlich wie in (i) Formeln für $\left(\frac{5}{p}\right), p \neq 2, 5$ und $\left(\frac{7}{p}\right), p \neq 2, 7$.