MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
PROF. DR. O. FORSTER

SS 2009
6. Mai 2009

Algorithmische Zahlentheorie

Übungsblatt 3

Aufgabe 9

Seien m_1, m_2 natürliche Zahlen und $d := \gcd(m_1, m_2)$.

a) Man zeige: Das System von Kongruenzen

$$x \equiv a \bmod m_1,$$
$$x \equiv b \bmod m_2$$

ist genau dann simultan lösbar, wenn $a \equiv b \bmod d$. In diesem Fall ist die Lösung modulo $\mathrm{lcm}(m_1, m_2)$ eindeutig bestimmt.

b) Man löse das System

$$x \equiv 23 \bmod 1001,$$
$$x \equiv 9 \bmod 10003.$$

Aufgabe 10

Sei R ein kommutativer Ring mit Einselement. Ein Element $x \in R$ heißt *idempotent*, wenn $x^2 = x$. Die Elemente 0 und 1 heißen triviale Idempotente.

a) Man zeige: Der Restklassenring $\mathbb{Z}/N$ ($N \geqslant 2$ ganz) besitzt genau dann nicht-triviale Idempotente, wenn N keine Primzahlpotenz (p^k, p prim, $k \geqslant 1$) ist.

b) Genauer gilt: Die Anzahl der Idempotente in $\mathbb{Z}/N$ ist 2^r, wobei r die Anzahl der verschiedenen Primteiler von N ist.

c) Man gebe alle Idempotente von $\mathbb{Z}/360$ an.

Aufgabe 11

Sei $N \geqslant 2$ und $\varphi(N)$ die Eulersche Phi-Funktion. Man zeige: Das Bild der Abbildung

$$\gamma : \mathbb{Z}/N \longrightarrow \mathbb{Z}/N, \quad x \mapsto \gamma(x) := x^{\varphi(N)} \bmod N$$

ist genau die Menge der Idempotente von $\mathbb{Z}/N$.

---

b.w.

Aufgabe 12

Sei R ein kommutativer Ring mit Einselement, $I_R \subset R$ die Menge seiner idempotenten Elemente und

$$W_R := \{x \in R : x^2 = 1\}$$

die Menge der Quadratwurzeln von 1 in R.

a) Man zeige: Ist $2 := 1 + 1$ invertierbar in R, so ist die Abbildung

$$\alpha : R \longrightarrow R, \quad x \mapsto \alpha(x) := 2x - 1$$

bijektiv und es gilt $\alpha(I_R) = W_R$.

b) Sei $R := \mathbb{Z}/2^n$. Man zeige: Für die Anzahl der Quadratwurzeln von 1 gilt:

$$\#W_{\mathbb{Z}/2^n} = \begin{cases} 1 & \text{für } n = 1, \\ 2 & \text{für } n = 2, \\ 4 & \text{für } n \geqslant 3. \end{cases}$$

c) Man gebe im Fall $R := \mathbb{Z}/360$ alle Elemente von W_R an.

d) Der Restklassenring $\mathbb{Z}/N$ enthalte eine Quadratwurzel $x \neq \pm 1$ von 1. Man gebe ein Verfahren an, wie man aus x einen nicht-trivialen Teiler von N konstruieren kann.

Abgabetermin: Freitag, 15. Mai 2009, 14 Uhr, Übungskasten im 1. Stock