Übungen zur Algebraischen Zahlentheorie I

Wintersemester 2010/11

Universität Heidelberg
Mathematisches Institut
Prof. A. Schmidt
Dr. A. Holschbach

Blatt 1
Abgabetermin: Mittwoch, 20.10.2010, 16.15 Uhr

Aufgabe 1. Man zeige, dass es unendlich viele Primzahlen $p \equiv -1 \bmod 3$ gibt.

Aufgabe 2. Seien p, q zwei verschiedene Primzahlen und $N = pq$. Weiterhin sei $m \in \mathbb{N}$ mit $m \equiv 1 \bmod \varphi(N)$. Man zeige: Für *jede* ganze Zahl h gilt $h^m \equiv h \bmod N$.[†]

Aufgabe 3. Seien a, n natürliche Zahlen und $n \geq 2$, so dass $a^n - 1$ eine Primzahl ist. Man beweise, dass $a = 2$ und n eine Primzahl ist.

Eine Funktion $f\colon \mathbb{N} \to \mathbb{C}$ heißt *zahlentheoretische* Funktion. f heißt *multiplikativ*, wenn für teilerfremde $m, n \in \mathbb{N}$ stets $f(mn) = f(m)f(n)$ gilt.

Aufgabe 4. Die *Möbius-Funktion* $\mu\colon \mathbb{N} \to \mathbb{C}$ ist definiert durch:

$$\mu(n) = \begin{cases} 1, & \text{wenn } n = 1, \\ (-1)^k, & \text{wenn } n \text{ ein Produkt von } k \text{ paarweise verschiedenen Primzahlen ist,} \\ 0, & \text{wenn } n \text{ durch eine Quadratzahl } > 1 \text{ teilbar ist.} \end{cases}$$

Man zeige:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{für } n > 1, \end{cases}$$

wobei die Summation über alle natürlichen Teiler von n durchgeführt wird. Man folgere: Sind f, F zahlentheoretische Funktionen mit $F(n) = \sum_{d|n} f(d)\ \forall\, n \in \mathbb{N}$, so gilt

$$f(n) = \sum_{d|n} F(d)\mu\left(\frac{n}{d}\right) \quad \forall\, n \in \mathbb{N} \qquad \textit{(Möbius'sche Umkehrformel).}$$

Zusatzaufgabe: Seien f und g multiplikative zahlentheoretische Funktionen. Man zeige, dass die Funktion

$$(f \star g)(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

wieder multiplikativ ist.

[†] Auf dieser einfachen Tatsache basiert der sogenannte *RSA-Verschlüsselungsalgorithmus*. Bei diesem hat jeder Teilnehmer einen öffentlichen Schlüssel (e, N), bei dem N das Produkt zweier verschiedener Primzahlen und $e \in \mathbb{N}$ teilerfremd zu $\varphi(N)$ ist, und einen privaten Schlüssel (d, N), wobei $d \in \mathbb{N}$, $de \equiv 1 \bmod \varphi(N)$ gilt. Hat man eine Nachricht in Form einer natürlichen Zahl $a < N$, die man diesem Teilnehmer verschlüsselt zukommen lassen will, so berechnet man $b = a^e \bmod N$ und sendet dies an den Teilnehmer. Dieser kann es dann mit seinem privaten Schlüssel dechiffrieren, indem er $b^d \equiv a \bmod N$ berechnet. (Größere Nachrichten werden in kleine Pakete zerteilt und verschlüsselt).
Die Sicherheit des Verfahrens beruht auf der Tatsache, dass die Bestimmung von d als Inversem von e in $(\mathbb{Z}/N\mathbb{Z})^\times$ die Kenntnis von $\varphi(N)$ und damit der Primfaktorzerlegung von N erfordert. Für genügend große N ist die Faktorisierung mit den heute bekannten Methoden aber praktisch unmöglich.