Mathematisches Institut
Abt. für Reine Mathematik
Dr. K. Halupczok

05.06.2007

Übungen zur Vorlesung
Elementare Zahlentheorie
SoSe 2007

Blatt 7

Abgabe: Dienstag, den 12.06.2007, zu Beginn der Vorlesung

Aufgabe 1.

(a) Sei $\alpha \in \mathbb{R}$ Nullstelle des Polynoms

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \quad (n \in \mathbb{N},\ a_0, \ldots a_{n-1} \in \mathbb{Z}).$$

Dann ist α ganzzahlig oder irrational.

(b) Die Zahl $\sqrt{2} + \sqrt{3}$ ist irrational.

Aufgabe 2.

Ein Problem aus dem alten China:

Eine Bande von 17 Piraten hat einen Sack mit Münzen erbeutet. Bei dem Versuch das Beuteglück gleichmäßig aufzuteilen, bleiben drei Münzen übrig. Bei dem Streit darüber, wer diese drei Münzen erhalten soll, wird ein Pirat getötet. Der Reichtum wird neu verteilt, doch dieses Mal bleiben zehn Münzen zurück. Es entbrennt abermals ein Streit, und wieder bleibt ein Pirat auf der Strecke. Nun aber kann das Beutegut endlich gerecht verteilt werden. Wie groß war die kleinstmögliche Anzahl von Münzen, die erbeutet wurde?

Aufgabe 3.

Sei p prim und $a \in \mathbb{Z}$. Zeige mit Hilfe des Satzes von Wilson:

(a) $(p-1)! \equiv p-1 \mod 1 + 2 + \cdots + (p-1)$
(b) $p|(a^p + (p-1)!\, a)$ und $p|(a + (p-1)!\, a^p)$
(c) Sei $p \geq 3$. Dann gilt: $1^2 \cdot 3^2 \cdot 5^2 \cdot \cdots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p$.

Aufgabe 4.

Das Kongruenzensystem

$$x \equiv a \bmod n,\ x \equiv b \bmod m$$

besitzt genau dann eine Lösung, wenn $(n, m)|(a-b)$. Falls eine Lösung existiert, ist sie eindeutig modulo $[n, m]$.