Mathematisches Institut
Prof. Dr. R. Wallisser

09.07.2002

Übungen zur Vorlesung

Elementare Zahlentheorie — SS 2002

Blatt 12

Abgabe: Dienstag, 16.07.02, 9.00 Uhr, vor der Vorlesung

Aufgabe 1.
Es sei g eine Primitivwurzel mod p^s, $s \in \mathbb{N}$, $p \in \mathbb{P}$, $p > 2$. Man zeige: Wird $c \in \{0, 1\}$ so gewählt, daß $g_1 = g + cp^s$ ungerade ist, so ist g_1 eine Primitivwurzel mod $2 \cdot p^s$.

Aufgabe 2.
Sei $p \in \mathbb{P}$, $p > 2$. Man zeige, daß für das Produkt P aller quadratischen Reste modulo p gilt: $P \equiv (-1)^{(p+1)/2} (\operatorname{mod} p)$.

Aufgabe 3.

a) Sei $p \in \mathbb{P}$ und $p \equiv 3 (\operatorname{mod} 4)$. Man zeige: Ist $p' = 2p + 1$ ebenfalls prim, so ist $2^p \equiv 1 (\operatorname{mod} p')$.

b) Zeigen Sie: Die Mersenneschen Zahlen $2^{11} - 1$ und $2^{83} - 1$ sind keine Primzahlen.

Aufgabe 4.
Man bestimme diejenigen ungeraden Primzahlen p, $p \neq 5$, für welche 5 quadratischer Rest modulo p ist.

Ergänzungsaufgabe.
Man zeige:

a) Der periodische Dezimalbruch

$$\alpha := 0.c_1 c_2 \dots c_k \, \overline{a_1 a_2 \dots a_n}$$

stellt die rationale Zahl

$$\alpha = \frac{c_1 c_2 \dots c_k}{10^k} + \frac{a_1 a_2 \dots a_n}{10^k (10^n - 1)}.$$

dar.

b) Für $\alpha = \frac{s}{t}$, $s \in \mathbb{N}$, $t \in \mathbb{N}$, $s < t$, $\operatorname{ggT}(s,t) = 1$ läßt sich mit $t = 2^{k_1} \cdot 5^{k_2} \cdot m, \operatorname{ggT}(m, 10) = 1,\ k = \max(k_1, k_2)$ α in der Form $\alpha = \frac{\ell}{10^k m}, \operatorname{ggT}(m, \ell) = 1, \ell \not\equiv 0 (\operatorname{mod} m),\ 1 \leq \ell < 10^k m$ schreiben. Dabei sind k, ℓ und m durch α eindeutig bestimmt.

c) Ist $n = \operatorname{ord}_m 10$, so gilt

$$10^k \alpha = \frac{\ell}{m} = c_1 c_2 \dots c_k + \frac{a_1 \cdot a_2 \dots a_n}{10^n - 1}.$$

d.h. $\alpha = 0.c_1 c_2 \dots c_k \overline{a_1 a_2 \dots a_n}$. Man überlege sich, daß n die kürzeste Periode ist.

d) Für $m = 3$ ist $n = 1$; für $m = 7$ ist $n = 6$.