W.Knapp Tübingen, den 1. Februar 2007

46. Sei n eine ungerade natürliche Zahl > 1 mit der Primfaktorzerlegung $n = \prod_{k=1}^{r} p_k^{e_k}$ und x sei eine zu n teilerfremde natürliche Zahl. Beweisen Sie:
   (a) x ist eine quadratischer Rest modulo n, d.h. es gilt $x \equiv y^2 \pmod n$ für ein $y \in \mathbb{Z}$, genau dann, wenn x ein quadratischer Rest modulo $p_k^{e_k}$ für alle k ist.
   (b) x ist eine quadratischer Rest modulo $p_k^{e_k}$ für ein k genau dann, wenn x ein quadratischer Rest modulo p_k ist.
   (c) Welche Konsequenzen ergeben sich daraus für das Jacobi-Symbol? Wie müsste demnach ein quadratisches Rest-Symbol modulo n definiert werden? (4 Punkte)

47. Sei p eine ungerade Primzahl und weiter $a, b, c \in \mathbb{Z}$ mit $a \not\equiv 0 \pmod p$.
   Beweisen Sie: Die quadratische Gleichung modulo p
   $$ax^2 + bx + c \equiv 0 \pmod p$$
   hat modulo p genau $1 + \left(\frac{b^2-4ac}{p}\right)$ Lösungen. (4 Punkte)
   Hinweis: Betrachten Sie den Körper $\mathbb{F}_p = \mathbb{Z}/p$.

48. Beweisen Sie: Eine ungerade Primzahl p ist Summe von zwei Quadraten natürlicher Zahlen x und y (also $p = x^2 + y^2$) höchstens dann, wenn $p \equiv 1 \pmod 4$ gilt. (4 Punkte)
   Hinweis: Verwenden Sie die Übungsaufgabe 47.

49. Sei $R = \mathbb{Z}[i] = \{z = x + iy \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{C}$ der Ring der ganzen Gaußschen Zahlen. Für $z = x + iy$ setze $\mathrm{N}(z) := z\overline{z} = x^2 + y^2$. $\mathrm{N}(z)$ heiße die *Norm* von z.
   Beweisen Sie:
   (a) $R = \mathbb{Z}[i]$ ist ein euklidischer Ring mit euklidischer Norm $z \mapsto \mathrm{N}(z)$, d.h. R ist ein Integritätsbereich und für alle $z_1, z_2 \in R$ mit $z_2 \neq 0$ existieren $q, r \in R$ mit $z_1 = qz_2 + r$ und $\mathrm{N}(r) < \mathrm{N}(z_2)$ oder $r = 0$.
   (R ist deshalb ein Hauptidealring und die Begriffe „Primelement“ und „irreduzibles Element“ fallen in R zusammen.)
   (b) Für $a = u + iv \in R$ gilt $\mathrm{N}(a) = 1$ genau dann, wenn a eine Einheit in R ist, d. h. $a \in \{1, -1, i, -i\}$.
   (c) Wenn $\pi = x + iy$ ein Primelement in R ist, so ist auch $\overline{\pi} = x - iy$ ein Primelement in R. $\pi = x + iy$ mit $x > 0$ ist genau dann ein Primelement in R, wenn $\pi = p \equiv 3 \pmod 4$ mit einer ungeraden Primzahl p ist oder $\mathrm{N}(\pi) = x^2 + y^2$ eine Primzahl $p = 2$ oder $p \equiv 1 \pmod 4$ ist. (Hieraus folgt der Kehrsatz zum Resultat von Übungsaufgabe 48.) (12 Punkte)

Die Übungsaufgaben sind schriftlich zu bearbeiten und vor der Vorlesung am Dienstag, dem 6. Februar 2007, abzugeben.