Übungen zur Kursvorlesung Elementare Zahlentheorie

Wintersemester 2006/07 — Blatt 7

W.Knapp — Tübingen, den 25. November 2006

27. Es sei G eine multiplikativ geschriebene endliche abelsche Gruppe. Dann heiße $w_G := \prod_{x\in G} x$ das *Wilson-Element* von G.
    Warum ist die Voraussetzung der Kommutativität und der Endlichkeit von G hier unentbehrlich?
    (a) Beweisen Sie, dass
    $$w_G = \prod_{\substack{x\in G\\ \operatorname{ord}(x)=2}} x$$
    gilt. Warum ist dies eine Verallgemeinerung des Satzes von Wilson?
    (b) Beweisen Sie, dass für alle $x \in G$ die Beziehung $x^{|G|}w_G = w_G$ gilt und schließen Sie daraus, dass stets $x^{|G|} = 1$ gilt. (Dies ergibt einen weiteren Beweis für (2.20) der Vorlesung im Spezialfall einer abelschen Gruppe G.)

    (3 Punkte)

28. Sei $1 \le q \in \mathbb{N}$ und p sei eine Primzahl.
    Beweisen Sie, dass es genau ein $k \in \mathbb{N}$ mit $1 \le k \le p-1$ gibt derart, dass für alle $n \in \mathbb{Z}$ die Kongruenz $n^q \equiv n^k \pmod p$ gilt. (3 Punkte)
    Hinweis: Vergleichen Sie mit den Übungsaufgaben 23 und 24.

29. Beweisen Sie: Ist $1 < q \in \mathbb{N}$, so existiert eine größte natürliche Zahl m derart, dass für alle $n \in \mathbb{Z}$ die Kongruenz $n^q \equiv n \pmod m$ gilt.
    Und zwar ist m das Produkt aller verschiedenen Primzahlen p mit der Eigenschaft, dass $p-1$ ein Teiler von $q-1$ ist.
    Hinweis: Beachten Sie, dass für alle Primzahlen Primitivwurzeln modulo p existieren.

    (4 Punkte)

30. Bestimmen Sie die größte natürliche Zahl, welche alle Zahlen $n^q - n$ mit beliebigem $n \in \mathbb{Z}$ teilt, für $q = 97$ und $q = 211$.

    (2 Punkte)

Die Übungsaufgaben sind schriftlich zu bearbeiten und vor der Vorlesung am Dienstag, dem 5. Dezember 2006, abzugeben.