Übungen zur Kursvorlesung Elementare Zahlentheorie

Sommersemester 2010 Blatt 6

W.Knapp Tübingen, den 12. Mai 2010

23. Es sei G eine multiplikativ geschriebene endliche abelsche Gruppe. Dann heiße $w_G := \prod_{x\in G} x$ das *Wilson-Element* von G.
Warum muss hierzu G kommutativ und endlich sein?
   (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. (Dieser Sachverhalt wurde in der Vorlesung mittels des Satzes von Lagrange bewiesen.) (3 Punkte)

24. Beweisen Sie: Ist $m > 4$ keine Primzahl, so gilt $(m-1)! \equiv 0 \pmod{m}$.

25. Sei p eine ungerade Zahl mit $p \geq 3$. Beweisen Sie:
   p ist genau dann eine Primzahl, wenn die Kongruenz
   $$((\frac{p-1}{2})!)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$
   gilt. (3 Punkte)

26. Sei eine Primzahl p gegeben. Beweisen Sie:
   Dann gilt für alle $n \in \mathbb{Z}$ und alle $(a_k)_{0\leq k\leq m} \in \mathbb{N}^{m+1}$ mit $m \in \mathbb{N}$ die Kongruenz
   $$n^{\sum_{k=0}^{m} a_k p^k} \equiv n^{\sum_{k=0}^{m} a_k} \pmod{p}.$$
   (3 Punkte)

27. Zeigen Sie: Für alle $n \in \mathbb{Z}$ gilt
   $$4501770 \mid n^{97} - n.$$
   (3 Punkte)

28. Bestimmen Sie alle Primitivwurzeln modulo p in der Menge der Reste $\{1, \ldots, p-1\}$ für alle Primzahlen $p < 20$.
Lässt sich vielleicht eine Regel zur Anzahl dieser Primitivwurzeln modulo p beobachten?

Die Übungsaufgaben 23, 25, 26 und 27 sind schriftlich zu bearbeiten und in der Vorlesungspause am Dienstag, dem 1. Juni 2010, abzugeben.