I. Bouw
F. Kiraly

20.05.2008
SS 2008

Übungen zur elementaren Zahlentheorie - Blatt 6

Abgabe bis 05.06.2008 um 10:00

Aufgabe 21: Pseudoprimzahlen Teil I (1+1 = 2 P)
Zeigen Sie:

(a) 205 ist eine Pseudoprimzahl zur Basis 42.

(b) Es existiert eine Basis, sodass 42 Pseudoprimzahl zu dieser Basis ist. 42 ist jedoch keine Carmichael-Zahl.

Aufgabe 22: Pseudoprimzahlen Teil II ($\frac{3}{2} + \frac{3}{2} + 2 = 5$ P)
Seien a und b ganz und n ganz und positiv. Zeigen Sie:

(a) Ist n ungerade und pseudoprim zur Basis a , so auch zur Basis $n - a$.

(b) Ist n pseudoprim zu den Basen a und b , so auch zur Basis ab .

(c) Ist n pseudoprim zur Basis a und existiert das Inverse a^{-1} von a modulo n (d.h. $a^{-1} \cdot a \equiv 1 \bmod n$ und $0 \leq a^{-1} < n$), so ist n auch pseudoprim zur Basis a^{-1} .

Aufgabe 23: Starke Pseudoprimzahlen (1+1+2+1 = 5 P)
Eine Poulet-Zahl ist eine Pseudoprimzahl zur Basis 2. Zeigen Sie:

(a) n=1387 ist eine Poulet-Zahl.

(b) n ist keine starke Poulet-Zahl.

(c) $\mathrm{ord}_n\, 2 | 1386$

(d) Berechnen Sie $\mathrm{ord}_n\, 2$.

Aufgabe 24: Carmichael-Zahlen (1+1+1+2 = 5 P)
Zeigen Sie oder widerlegen Sie:

(a) 41041 ist eine Primzahl.

(b) 41041 ist eine Carmichael-Zahl. Benutzen Sie hierfür das Kriterium von Korselt (Satz 4.3.7) und nicht den Chinesischen Restsatz.

(c) 41041 ist eine Carmichael-Zahl. Benutzen Sie hierfür den Chinesischen Restsatz (Lemma 4.3.6) und nicht das Kriterium von Korselt.

(d) Es existiert eine Carmichael-Zahl mit Primfaktorzerlegung $7 \cdot 23 \cdot p$, wobei $p \geq 42$ prim ist.

Aufgabe 25: Der Miller-Rabin-Test (1+1+1 = 3 P)
Sei $n = 1373653$.

(a) Führen Sie den Miller-Rabin-Test für n mit den Basen 2 und 3 durch.

(b) Wie hoch ist die durch den Miller-Rabin-Test erhaltene Wahrscheinlichkeit, dass n prim ist, wenn 2 und 3 zufällig gewählt wären?

(c) Reicht die Antwort von (b), um zu schließen, dass n eine Primzahl ist? Wie ist das im Allgemeinen?