Übungszettel 6

Pseudoprim Zahlen. Carmichael-Zahlen.

Miller-Rabin-Primzahlentest

Definition. Seien n und a natürliche Zahlen. Die Zahl n heißt *pseudoprim zur Basis* a, wenn n zusammengesetzt ist und die Kongruenz

$$a^{n-1} \equiv 1 \,(\mathrm{mod}\ n)$$

gilt.

Aufgabe 1. Für $n = 15$ finden Sie alle Zahlen $a \in \mathbb{Z}_{15}^*$, so daß n pseudoprim zur Basis a ist.

Aufgabe 2. Prüfen Sie nach, daß 101101 eine Carmichael-Zahl ist.

Aufgabe 3. Beweisen Sie: Wenn $6k+1, 12k+1$ und $18k+1$ Primzahlen sind, dann ist ihr Produkt eine Carmichael-Zahl.

Aufgabe 4. Finden Sie eine Carmichael-Zahl, die größer als 101101 ist.

Definition. Sei n eine ungerade Zahl und sei $n-1 = m2^h$, wobei m eine ungerade Zahl ist und $h \geqslant 1$ ist. Setzen wir

$$L_n = \{a \in \mathbb{Z}_n^* \,|\, a^m \equiv 1 \,(\mathrm{mod}\ n) \ \text{ oder } \ \exists\, i,\, 0 \leqslant i < h : \ a^{m2^i} \equiv -1 \,(\mathrm{mod}\ n)\}.$$

Nach Monier-Rabin Satz gilt:
- $|L_n| = n-1$, wenn n eine Primzahl ist;
- $|L_n| \leqslant \varphi(n)/4$, wenn n eine zusammengesetze Zahl ist, $n \neq 9$.

Aufgabe 5. Finden Sie alle Elemente der Menge L_n für $n = 91$.

Aufgabe 6. Mit welcher Wahrscheinlichkeit erhalten wir die Antwort "n ist eine Primzahl..." im Miller-Rabin-Test für die Zahl $n = 91$ und den Parameter $s = 2$?