**Zahlentheorie und Kryptologie, SS2014**
**M. Hortmann**

# Blatt 8

## Aufgabe 1

Eine Zahl $n \in \mathbb{N}, n \geq 3$ , heißt Carmichael-Zahl, wenn *n* nicht prim ist und wenn trotzdem gilt: $\forall a \in \mathbb{Z}_n:\ a^{n-1} = 1$.

a) Sei $k \in \mathbb{N}$ und $6k+1$ , $12k+1$ und $18k+1$ seien Primzahlen. Zeigen Sie, daß dann das Produkt $(6k+1)(12k+1)(18k+1)$ eine Carmichael Zahl ist. Berechnen Sie 10 solche Carmichael-Zahlen. Suchen Sie im Internet eine möglichst große Liste von Carmichael-Zahlen.

b) Man zeige: Ist *n* eine Carmichael-Zahl, so kommt kein Primfaktor von *n* mehrfach vor.

c) Man zeige: Eine Carmichael-Zahl besitzt mehr als 2 Primfaktoren.

d) Man berechne für möglichst viele ungeraden Zahlen größer als 10.000 und 20.000 den Bruch $\frac{|U_n|}{|\mathbb{Z}_n^*|}$ und ordne die Werte in eine Statistik ein. Dabei bitte die Anzahl der Carmichael-Zahlen mitzählen: bei denen ist der Bruch gleich 1.[1]

e) Man zeige: Ist $n > 1$ keine Primzahl, so ist die Untergruppe $U_n := \left\{ a \in \mathbb{Z}_n^* \,\middle|\, a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \right\} \subset \mathbb{Z}_n^*$ echt. [2]

f) Wer Lust hat, programmiere den Miller-Rabin-Test.

1 size 10 {lline setZ_n^"*"rline =%varphi(n)}= die Eulersche Phi-Funktion, in Pari eulerphi(n). Es gibt eine einfache Formel dafür, welche aber die Primfaktorzerlegung von n benutzt: in der gegebenen Größenordnung kein Problem.

2 Könnte schwer sein. Recherchieren Sie ggf. in der Literatur bzw. im Netz.