Einführung in die Computeralgebra

Letztes Übungsblatt

SOMMERSEMESTER 2016

MICHAEL STOLL

8. Juli 2016

Abgabe:

Donnerstag, 14. Juli, bis 10:00 Uhr im Briefkasten (NW II, 2. Stockwerk rechts).

Übungsaufgaben bitte **handschriftlich** bearbeiten (außer Programmieraufgaben);
nur ein Name pro Blatt! —

Schnellhefter und **Deckblatt** nicht vergessen!

(1) Sei $n \in \mathbb{Z}_{\geq 1}$.

(a) Zeigen Sie: Ist $2^n - 1$ prim, dann muss auch n prim sein.

(b) Zeigen Sie: Ist $2^n + 1$ prim, dann muss $n = 2^k$ sein für ein $k \geq 0$. (15+15)

(2) **Programmieraufgabe:**

Verwenden Sie den Pocklington-Lehmer-Test, um zu zeigen, dass $N = 77! + 1$ prim ist. (20)

(3) **Programmieraufgabe:**

(a) Implementieren Sie PollardRho in Magma.

(b) Verwenden Sie Ihre Implementation, um einen Primfaktor von F_8 zu finden.
HINWEIS: Verlieren Sie nicht die Geduld!

(c) Modifizieren Sie Ihre Implementation, sodass Sie den Startwert x_0 vorgeben können und zusätzlich die Anzahl der Iterationsschritte zurückgegeben wird.
Bestimmen Sie die Häufigkeitsverteilung der Anzahl der Iterationen und die Häufigkeitsverteilung der gefundenen Teiler für $N = 2047$ und alle Anfangswerte $x_0 = 0, 1, \dots, 2046$. (15+15+20)

(4) BONUS PROBLEM.

Find a natural number $n > 1000$ such that $n! + 1$ is prime and prove that it is prime. (30 extra points)