Einführung in die Computeralgebra
Letztes Übungsblatt
SOMMERSEMESTER 2018

MICHAEL STOLL

6. Juli 2018

Abgabe:

Donnerstag, 12. Juli, bis 11:00 Uhr im Briefkasten (NW II, 2. Stockwerk rechts).

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

Schnellhefter und **Deckblatt** nicht vergessen!

Die Punkte aus diesem „halben“ Übungsblatt zählen als Extra-Punkte.

(1) **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)