RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Präsenzübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 10 / 17.–19. Juni 2013

AUFGABE 1:
Sei $d \in \mathbb{Z}$ kein Quadrat. Wir betrachten die Pellsche Gleichung $p^2 - dq^2 = 1$.
Zeigen Sie: Ist $(p, q) \in \mathbb{Z}^2$ eine Lösung der Pellschen Gleichung, so ist auch $(p_n, q_n) \in \mathbb{Z}^2$ eine Lösung, wobei $p_n + q_n\sqrt{d} = (p + q\sqrt{d})^n$.

AUFGABE 2:
Geben Sie 8 verschiedene nicht-triviale (d.h. $(p, q) \neq (\pm 1, 0)$) Lösungen (der Pellschen Gleichung $p^2 - 5q^2 = 1$ mit $(p, q) \in \mathbb{Z}^2$ an.

AUFGABE 3:
Geben Sie einen (möglichst effizienten) Algorithmus an, der testet, ob eine natürliche Zahl $n \in \mathbb{N}, n > 1$ von der Gestalt $n = x^k$ mit $k > 1, x \in \mathbb{N}$ ist. Geben Sie eine obere Schranke für dessen Laufzeit an.

AUFGABE 4:
Sei $k \in \mathbb{N}$, so dass die 3 Zahlen $6k + 1, 12k + 1, 18k + 1$ allesamt prim sind.
Zeigen Sie, dass dann $(6k + 1)(12k + 1)(18k + 1)$ eine Carmichael-Zahl ist.

AUFGABE 5:
Sei $n = 561$ (die kleinste Carmichael-Zahl).
Wir faktorisieren $n - 1 = 56 \cdot 10$ partiell.
Zeigen Sie mit Hilfe des Pocklington-Tests, dass 561 nicht prim ist. Wählen Sie dazu $a = 2$ und $a = 5$.

Bemerkung: Benutzen Sie einen Taschenrechner. Überlegen Sie sich, warum man nicht alle $1 \leq a < n$ (in der Notation im Skript) durchprobieren muss.

AUFGABE 6:
Sei n ungerade. Zeigen Sie, dass die Menge $A = \{x \in U_n \mid x^{\frac{n-1}{2}} \equiv (\frac{x}{n}) \mod n\}$ eine Untergruppe von U_n ist.