

## Übungsblatt 11

### Aufgabe 58

*mündlich*

Berechnen Sie  $\varphi(75\,600)$ ,  $\varphi(14\,948)$ ,  $\log_{7,3} 4$ ,  $\log_{37,2} 3$ ,  $\text{ord}_7(2)$  und  $\text{ord}_{31}(2)$ .

### Aufgabe 59 Zeigen Sie:

*mündlich*

(a) Primzahlpotenzen  $p^k$  sind keine Carmichaelzahlen.

*Hinweis:* Berechnen Sie  $(p^{k-1} + 1)^{p^k - 1} \bmod p^k$ .

(b) Jede Carmichaelzahl  $n$  ist quadratfrei.

(c) Eine ungerade, zusammengesetzte und quadratfreie Zahl  $n$  ist genau dann eine Carmichaelzahl, wenn  $p - 1$  für jeden Primteiler  $p$  von  $n$  die Zahl  $n - 1$  teilt.

(d) Jede Carmichaelzahl  $n$  lässt sich in drei teilerfremde Faktoren  $n_1, n_2, n_3 > 1$  zerlegen.

(e) 561, 2465, 1729, 172081, 294409 und 56052361 sind Carmichaelzahlen.

### Aufgabe 60

*mündlich*

Eine ungerade zusammengesetzte Zahl  $n$  heißt stark pseudoprim zu einer Basis  $a \in \mathbb{Z}_n^*$ , falls der Miller-Rabin-Test diese Zahl bei Wahl der Basis  $a$  als prim klassifiziert ( $n$  ist also genau dann stark pseudoprim zur Basis  $a$ , wenn  $a \in \mathcal{P}_n^{\text{MRT}}$  ist).

Zeigen Sie, dass die Zahl  $n_1 = 3215031751$  stark pseudoprim zu jeder der Basen 2, 3, 5, 7 ist. (Tatsächlich ist dies die einzige Zahl  $n < 2,5 \cdot 10^{10}$  mit dieser Eigenschaft.)

### Aufgabe 61 Betrachten Sie folgendes Zufallsexperiment:

*mündlich*

Ein probabilistischer Primzahltest  $T$  (mit einseitiger Fehlerwahrscheinlichkeit  $\varepsilon$  im Fall einer zusammengesetzten Eingabe) wird auf eine zufällig gewählte ungerade Binärzahl  $n \in [2^l, 2^{l+1} - 1]$  angewandt.

Bestimmen Sie näherungsweise die Wahrscheinlichkeiten der beiden Ereignisse » $n$  ist prim« (Ereignis  $A$ ) und » $T(n)$  gibt prim aus« (Ereignis  $B$ ). Wie groß sind die bedingten Wahrscheinlichkeiten  $\Pr[A|B]$ ,  $\Pr[B|\bar{A}]$  und  $\Pr[B|A]$  im Fall  $\varepsilon = 2^{-m}$ ,  $m = 1, 2, 5, 10, 20, 30, 50, 100$ ? Interpretieren Sie diese Zahlen.

### Aufgabe 62

**10 Punkte**

Für eine ungerade Zahl  $n$  sei  $j = \max\{0 \leq i \leq m \mid \exists a \in \mathbb{Z}_n^* : a^{2^i} \equiv_n -1\}$ , wobei  $n - 1 = 2^m u$  und  $u$  ungerade ist. Zudem sei  $J_n = \{a \in \mathbb{Z}_n^* \mid a^{2^j} \equiv_n \pm 1\}$ .

(a) Berechnen Sie für  $n = 221$  die Mengen  $\mathcal{P}_n^{\text{FT}}$ ,  $\mathcal{P}_n^{\text{MRT}}$  und  $J_n$ .

(b) Zeigen Sie, dass  $n$  genau dann zusammengesetzt ist, wenn die Kongruenz  $x^2 \equiv_n 1$  eine nichttriviale Lösung  $z$  (d.h.  $z \not\equiv_n \pm 1$ ) der Form  $w^{2^j}$  hat.

(c) Folgern Sie, dass  $x \mapsto wx$  eine Injektion von  $\mathcal{P}_n^{\text{MRT}}$  in die Menge  $\mathbb{Z}_n^* - \mathcal{P}_n^{\text{MRT}}$  (und daher  $\|\mathcal{P}_n^{\text{MRT}}\| \leq \varphi(n)/2$ ) ist.