Übungsblatt 12

Abgabe der schriftlichen Lösungen am 1. 2. 2018 bis 13.10 Uhr

Aufgabe 57 Sei p eine ungerade Primzahl und $\mathrm{ggT}(a,p)=1$. ***mündlich***

(a) Sei $i \geq 2$ und $b^2 \equiv_{p^{i-1}} a$. Zeigen Sie, dass es genau ein $x \in \mathbb{Z}_{p^i}$ gibt mit $x^2 \equiv_{p^i} a$ und $x \equiv_{p^{i-1}} b$. Wie kann x effizient berechnet werden?

(b) Berechnen Sie mit Ihrem Verfahren ausgehend von $6^2 \equiv_{19} 17$ die Wurzeln von 17 modulo 19^2 und modulo 19^3.

(c) Zeigen Sie für jedes $i \geq 1$, dass die Kongruenz $x^2 \equiv_{p^i} a$ entweder 0 oder 2 Lösungen hat.

Aufgabe 58 ***mündlich***

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

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.

(rechenintensiv)

Aufgabe 60 ***mündlich, rechenintensiv***

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 $a \in \mathcal{P}_n^{MRT}$ 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 ***10 Punkte***

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

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

(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 $w^{2^j u}$ hat.

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