Übungsblatt 11

Abgabe für die mündlichen Aufgaben bis 07. 07. 2020 und für die schriftliche Aufgabe bis 14. 07. 2020

Aufgabe 58 Sei $(G, \cdot, 1)$ eine endliche Gruppe der Ordnung m. ***mündlich***

(a) Zeigen Sie, dass für jedes $a \in G$ ein $k > 0$ existiert mit $a^k = 1$.

(b) Zeigen Sie, dass für jedes $a \in G$ die Menge $\langle a \rangle = \{a^i \mid i \geq 0\}$ eine Untergruppe von G mit genau $\operatorname{ord}(a)$ Elementen bildet. Folgern Sie $\operatorname{ord}(a)|m$ und $a^m = 1$.

(c) Zeigen Sie, dass für jedes $a \in G$ die Äquivalenz $a^i = a^j \Leftrightarrow i \equiv_{\operatorname{ord}(a)} j$ gilt.

(d) Zeigen Sie, dass $\operatorname{ord}(a^i) = \operatorname{ord}(a)/\operatorname{ggT}(\operatorname{ord}(a), i)$ für jedes $a \in G$ gilt.

(e) Geben Sie einen Isomorphismus zwischen den Gruppen $\langle a \rangle$ und $(\mathbb{Z}_{\operatorname{ord}(a)}, +)$ an.

(f) Bestimmen Sie für die Gleichung $a^x = b$ $(a, b \in G)$ alle Lösungen $x \in \mathbb{Z}_{\operatorname{ord}(a)}$.

Aufgabe 59 ***mündlich***

Seien a, b Elemente einer abelschen Gruppe G mit Ordnungen $\operatorname{ord}(a)$ und $\operatorname{ord}(b)$.

(a) Zeigen Sie, dass ab die Ordnung $\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b)$ hat, falls $\operatorname{ord}(a)$ und $\operatorname{ord}(b)$ teilerfremd sind. Gilt dies auch, wenn G nicht abelsch ist?

(b) Lässt sich die Aussage in Teilaufgabe (a) zu $\operatorname{ord}(ab) = \operatorname{kgV}(\operatorname{ord}(a), \operatorname{ord}(b))$ oder zu $\operatorname{ord}(ab) = \operatorname{kgV}(\operatorname{ord}(a), \operatorname{ord}(b))/\operatorname{ggT}(\operatorname{ord}(a), \operatorname{ord}(b))$ verallgemeinern?

Aufgabe 60 ***mündlich***

(a) Zeigen Sie, dass ein Polynom $p(x) \in \mathbb{F}[x]$ vom Grad $n \geq 1$ über einem Körper $\mathbb{F}$ höchstens n Nullstellen besitzt.

(b) Folgern Sie, dass die Einheitengruppe $\mathbb{F}_q^*$ eines endlichen Körpers $\mathbb{F}_q$ zyklisch ist.

(c) Finden Sie Polynome $q_d(x) \in \mathbb{Z}_6[x]$ vom Grad $d = 0, 1, 2$ mit möglichst vielen Nullstellen.

(d) Zeigen Sie, dass ein Polynom $q_d(x) \in \mathbb{Z}_m[x]$ vom Grad $d \geq 1$ für quadratfreies $m \geq 2$ höchstens dm/p Nullstellen hat, wobei p der kleinste Primteiler von m ist. In welchen Fällen ist diese Schranke scharf?

Aufgabe 61 ***mündlich***

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

Aufgabe 62 Zeigen Sie: ***mündlich***

(a) Keine gerade Zahl n ist eine Carmichaelzahl.

(b) Für kein $k \geq 2$ und keine Primzahl $p > 2$ ist $n = p^k$ eine Carmichaelzahl. (*Hinweis:* Zeigen Sie, dass $a = p^{k-1} + 1$ kein falscher Primzahlzeuge für n ist.)

(c) Jede Carmichaelzahl n ist quadratfrei. (*Hinweis:* Zeigen Sie, dass $\operatorname{ord}_{p^2}(p+1) = p$ ist, und benutzen Sie im Fall $p^2|n$ den chinesischen Restsatz zur Konstruktion einer Zahl $a \in \mathbb{Z}_n^*$ mit $a^{n-1} \not\equiv_n 1$.)

(d) 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.

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

Aufgabe 63 ***mündlich***

(a) Verifizieren Sie, dass 561, 1729, 2465, 172081, 294409 und 56052361 Carmichaelzahlen sind.

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

Aufgabe 64 ***mündlich***

Betrachten Sie folgendes Zufallsexperiment:

> Ein probabilistischer Primzahltest T (mit einseitiger Fehlerwahrscheinlichkeit ε 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 $\Pr[\overline{A}|B]$, $\Pr[B|\overline{A}]$ und $\Pr[B|A]$ im Fall $\varepsilon = 2^{-m}$, $m = 1, 2, 5, 10, 20, 30, 50, 100$ und $l = 1024$? Interpretieren Sie diese Zahlen.

Aufgabe 65 ***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 $U_n = \{a \in \mathbb{Z}_n^* \mid a^{2^j u} \equiv_n \pm 1\}$.

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

(b) Zeigen Sie, dass n genau dann zusammengesetzt ist, wenn n eine Primzahlpotenz $n = p^k$ mit $k \geq 2$ ist oder 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 es eine Zahl $w \in \mathbb{Z}_n^*$ gibt, so dass $x \mapsto wx$ eine Injektion von $\mathcal{A}_n^{\mathrm{MRT}}$ in die Menge $\mathbb{Z}_n^* - \mathcal{A}_n^{\mathrm{MRT}}$ (und daher $\|\mathcal{A}_n^{\mathrm{MRT}}\| \leq \varphi(n)/2$) ist.