Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Übungen zur Grundlagen der Mathematik im Wintersemester 2019/2020, Blatt 12
Fachbereich Mathematik, Stefan Geschke

A: Präsenzaufgaben am 13. Januar 2020

Eine natürliche Zahl $n \geq 2$ heißt *Primzahl*, falls n nur die *trivialen* Teiler 1, -1, n und $-n$ besitzt.

1. Für $u, v, n \in \mathbb{N}$ gelte $u \cdot v = n$. Zeigen Sie, dass $u \leq \sqrt{n}$ oder $v \leq \sqrt{n}$ gilt. Folgern Sie, dass jede natürliche Zahl $n \geq 2$, die keine Primzahl ist, einen Teiler t besitzt, so dass $2 \leq t \leq \sqrt{n}$ gibt.

   Lösung. Wäre $u > \sqrt{n}$ und $v > \sqrt{n}$, so würde aus den Monotonieeigenschaften der Multiplikation

   $$uv > u\sqrt{n} > \sqrt{n} \cdot \sqrt{n} = n$$

   folgen, was der Annahme $uv = n$ widerspricht.

2. Notieren Sie die kleinsten zehn Primzahlen. Welche der folgenden Zahlen sind Primzahlen?

   $$1, \quad \pi, \quad 101, \quad 2^7 - 1, \quad 2^8 + 1, \quad 10^{20} - 1$$

   Lösung. Die kleinsten zehn Primzahlen lautet $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$. 1 und π sind offensichtlich keine Primzahlen. Ausprobieren der Primzahlen bis 11 als Teiler zeigt, dass 101 eine Primzahl ist. $10^20 - 1$ ist keine Primzahl, denn die Zahl ist durch drei teilbar. Es gilt $2^7 - 1 - 127$. Wieder probieren wir die kleinen Primzahlen als Kandidaten für Teiler, wieder bis 11. Es zeigt sich, dass 127 eine Primzahl ist. Schließlich ist $2^8 + 1 = 257$. Wir probieren mögliche Primteiler bis 13 und stellen fest, dass auch 257 eine Primzahl ist.

3. Es sei $a \in \mathbb{Z} \setminus \{-1, 01\}$ und t die kleinste natürliche Zahl ≥ 2, die a teilt. Beweisen Sie, dass t existiert und eine Primzahl ist.

   Lösung.. Für die Existenz stellen wir fest, dass $|a|$ eine natürliche Zahl ist, die a teilt. Damit existiert eine natürliche Zahl > 1, die a teilt. Sei t die kleinste solche Zahl. Angenommen, t ist keine Primzahl. Dann hat t einen nichttrivialen Teiler s. Wir können > 0 annehmen. Sei $k \in \mathbb{N}$ mit $sk = t$. Dann ist $s < t$. Das widerspricht aber der Minimalität von t. Also ist t eine Primzahl.

B: Hausaufgaben zum 20. Januar 2020

1. Es sei $(G, *)$ eine Gruppe mit einem neutralen Element e. Zeigen Sie, dass für alle $g \in G$ gilt:

   (a) g hat höchstens ein inverses Element. (2 Punkte)

   (b) Für alle $k \in \mathbb{Z}$ gilt $(g^k)^{-1} = g^{-k}$. (Hier dürfen Sie 6.14 (1) benutzen.) (2 Punkte)

   (c) Für alle $k, \ell \in \mathbb{Z}$ gilt $(g^\ell)^k = g^{\ell \cdot k}$. (Für $k, \ell \in \mathbb{N}_0$ wurde das schon gezeigt.) (2 Punkte)

   (d) Die Menge $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ bildet eine Untergruppe von G. (2 Punkte)

Lösung. (a) Seien $a, b \in G$ beide invers zu g. Dann gilt $g * a = e = g * b$. Multiplikation mit a von links liefert oder Anwenden der Kürzregel liefert $a = b$.

(b) Wir müssen zeigen, dass g^{-k} zu g^k invers ist. Nach 6.14 (1) gilt $g^k * g^{-k} = g^{k-k} = g^0 = e$. Umgekehrt ist $g^{-k} * g^k = g^{-k+k} = g^0 = e$.

(c) Wir benutzen die Aussage für $k, \ell \in \mathbb{N}_0$ mehrmals, ohne dass extra aufzuführen. Wir betrachten zunächst den Fall, dass $k < 0$ ist und $\ell \geq 0$. Es gilt dann

$$(g^\ell)^k = ((g^\ell)^{-k})^{-1} = (g^{\ell \cdot (-k)})^{-1} = g^{\ell \cdot k}.$$

Für $\ell < 0$ und $k \geq 0$ erhalten wir

$$(g^\ell)^k = ((g^{-\ell})^{-1})^k = (g^{-\ell})^{-k} = g^{(-\ell)\cdot(-k)} = g^{\ell \cdot kl},$$

wobei wir den ersten Fall und (b) benutzt haben.

Für $\ell < 0$ und $k < 0$ erhalten wir schließlich

$$(g^\ell)^k = ((g^\ell)^{-1})^{-k} = ((g^{-1})^\ell)^{-k} = (g^{-1})^{-\ell \cdot k} = g^{\ell \cdot k},$$

wobei wir den zweiten Fall und (b) benutzen.

(d) Offenbar ist $\langle g \rangle$ eine nichtleere Teilmenge von G. Für $k, \ell \in \mathbb{Z}$ ist

$$g^k * (g^\ell)^{-1} = g^k * g^{-\ell} = g^{k-\ell} \in \langle g \rangle.$$

Das zeigt bereits, dass $\langle g \rangle$ eine Untergruppe von G ist.

2. Sei $m \in \mathbb{N}$ mit $m \geq 2$. Auf Blatt 4 hatten wir eine Multiplikation $\cdot$ auf der Menge $\mathbb{Z}_m$ definiert. Zeigen Sie, dass die bezüglich $\cdot$ invertierbaren Elemente von $\mathbb{Z}_m$ mit der Verknüpfung $\cdot$ eine Gruppe bilden. (Es ist leicht zu sehen, dass $(Z_m, +)$ eine Gruppe ist. Interessanterweise gibt aber offenbar auch die Multiplikation auf $\mathbb{Z}_m$ Anlass zu einer Gruppenstruktur, wenn man sich auf die bezüglich $\cdot$ invertierbaren Elemente beschränkt.) (4 Punkte)

Lösung. Sei $\mathbb{Z}_m^*$ die Menge der bezüglich $\cdot$ invertierbaren Elemente von $\mathbb{Z}_m$. Wir wissen, dass $\cdot$ eine zweistellige Versknüpfung auf $\mathbb{Z}_m$ ist. Sind $a, b \in \mathbb{Z}_m$ invertierbar mit Inversen a^{-1} und b^{-1}, so ist $a \cdot b$ ebenfalls invertierbar und das Inverse lautet $b^{-1} \cdot a^{-1}$, wie man leicht nachrechnet. Damit ist $\cdot$ eine zweistellige Verknüpfung auf $\mathbb{Z}_m^*$. Da $[1]_m$, dass neutrale Element bezüglich $\cdot$ in $\mathbb{Z}_m$, invertierbar ist, ist $[1]_m \in \mathbb{Z}_m^*$. Für jedes $a \in \mathbb{Z}_m^*$ ist das Inverse zu a ebenfalls invertierbar und daher in $\mathbb{Z}_m^*$ enthalten. Es folgt, dass $(\mathbb{Z}_m^*, \cdot)$ eine Gruppe ist.

3. Gegeben seien $a, b \in \mathbb{Z}$ mit $a \neq 0$. Weiter sei $L = \{ax + by : x, y \in \mathbb{Z}\}$. Zeigen Sie:

   (a) $a \in L$. (2 Punkte)

   (b) L ist eine Untergruppe von $\mathbb{Z}$. (2 Punkte)

   (c) Mit $a \in L$ ist wegen (b) auch $|a| \in L$. Also ist $L \cap \mathbb{N} \neq \emptyset$. Sei d das kleinste Element von $L \cap \mathbb{N}$. Dann ist d ein Teiler von a und b. (2 Punkte) (Hinweis: Man führe Divisionen mit Rest von a und b durch d durch und stelle fest, dass die Reste jeweils in L liegen.)

   (d) Alle gemeinsamen Teiler von a und b sind auch Teiler von d. (2 Punkte)

   Die Zahl d ist der größte gemeinsame Teiler von a und b. Aus der Aufgabe geht hervor, dass sich der größte gemeinsame Teiler von a und b in der Form $ax + by$ schreiben lässt, wobei die *Bézout-Koeffizienten* x und y ganze Zahlen sind.

   Lösung. (a) $a = a \cdot 1 + b \cdot 0 \in L$

   (b) Seien $x, x', y, y' \in \mathbb{Z}$. Dann gilt $ax + by - (ax' + by') = a(x - x') + b(y - y') \in L$. Damit ist L eine Untergruppe von $\mathbb{Z}$.

   (c) Wir führen nun eine Division mit Rest von a durch d durch. Seien also $q, r \in \mathbb{Z}$ mit $a = qd + r$ und $0 \leq r < d$. Dann ist $r = a - qd \in L$, da L eine Gruppe ist. Wegen der Minimalität von d muss aber $r = 0$ gelten. Sonst wäre r ein Element von $L \cap \mathbb{N}$, das kleiner als d ist.

Damit ist aber $a = qd$. Dasselbe Argument zeigt, dass d ein Teiler von b ist.

(d) Sei t ein Teiler sowohl von a als auch von b. Seien $x, y \in \mathbb{Z}$, so dass $d = ax + by$ gilt. Die Koeffizienten x und y existieren, weil $d \in L$ gilt. Nun teilt t mit a und b aber auch $d = ax + by$.