Mathematisches Institut der Universität München
Sommersemester 2014

Daniel Rost
Lukas-Fabian Moser

Grundlagen der Mathematik II
Lösungsvorschlag zum 3. Tutoriumsblatt

Aufgabe 1.

a) In Hinblick auf Teilaufgabe b) lohnt es sich, den ggT nicht mittels Primfaktorzerlegung, sondern mit dem Euklidischen Algorithmus zu bestimmen:

$$\begin{aligned} 180 &= 2 \cdot 76 + 28 \\ 76 &= 2 \cdot 28 + 20 \\ 28 &= 1 \cdot 20 + 8 \\ 20 &= 2 \cdot 8 + \boxed{4} \\ 8 &= 2 \cdot 4 + 0. \end{aligned}$$

Der letzte Rest > 0, der sich im Euklidischen Algorithmus ergibt, ist ein größter gemeinsamer Teiler von 76 und 180, in diesem Fall also $d = 4$.

b) Zur Bestimmung von m_1 und m_2 mit $4 = 76m_1 + 180m_2$ liest man die Rechnung aus dem Algorithmus rückwärts:

$$\begin{aligned} 4 &= 20 - 2 \cdot 8 = 20 - 2 \cdot (28 - 1 \cdot 20) \\ &= 3 \cdot 20 - 2 \cdot 28 = 3 \cdot (76 - 2 \cdot 28) - 2 \cdot 28 \\ &= 3 \cdot 76 - 8 \cdot 28 = 3 \cdot 76 - 8 \cdot (180 - 2 \cdot 76) \\ &= 19 \cdot 76 - 8 \cdot 180, \end{aligned}$$

also können wir $m_1 := 19$ und $m_2 := -8$ nehmen.

c) Laut Vorlesung ist die Gleichung genau dann lösbar, wenn $d = 4$ ein Teiler von 32 ist – dies trifft zu, und zwar ist $32 = d \cdot m_3$ mit $m_3 = 8$. Eine Lösung ist dann gegeben durch die Klasse $\overline{x} = \overline{m_1} \cdot \overline{m_3} = \overline{19 \cdot 8} = \overline{152}$.

d) Wieder laut Vorlesung besitzt die Gleichung genau d verschiedene Lösungen, nämlich (mit $q := \frac{180}{d} = 45$)

$$\overline{152}, \quad \overline{152} + \overline{q} = \overline{197}, \quad \overline{152} + 2\overline{q} = \overline{62}, \quad \overline{152} + 3\overline{q} = \overline{107}.$$

Aufgabe 2.

a) Für $a = 0$ (Induktionsanfang) ist $\overline{0}^p = \overline{0}$ zweifellos in $\mathbb{Z}_p$ korrekt. Für den Induktionsschritt $a \to a + 1$ sei schon bewiesen, daß $\overline{a}^p = \overline{a}$ gilt. Dann ist

$$\begin{aligned} \overline{a+1}^p &= (\overline{a} + \overline{1})^p && (\text{„Freshman's Dream“ } \dots) \\ &= \overline{a}^p + \overline{1}^p && (\text{Induktionsvoraussetzung } \dots) \\ &= \overline{a} + \overline{1} \\ &= \overline{a+1}, \end{aligned}$$

was zu beweisen war.

b) Da $\mathbb{Z}_p$ ein Körper ist, ist jedes $\overline{a} \in \mathbb{Z}_p$ mit $\overline{a} \neq \overline{0}$ invertierbar. Damit folgt aber aus der in a) bewiesenen Beziehung $\overline{a}^p = \overline{a}$ durch Multiplikation mit $\overline{a}^{-1}$ auf beiden Seiten unmittelbar $\overline{a}^{p-1} = \overline{1}$.

c) Für eine multiplikativ geschriebene abelsche Gruppe $(G, \cdot)$ mit $|G| = n$, deren neutrales Element (wie in diesem Fall üblich) als 1 bezeichnet wird, besagt der Satz von Euler-Fermat: Für jedes $g \in G$ gilt

$$\underbrace{g \cdot g \cdot \ldots \cdot g}_{n \text{ Faktoren}} = 1,$$

also $g^n = 1$. Für den Körper $\mathbb{Z}_p$ ist nun, wie für jeden Körper, $(\mathbb{Z}_p)^* = \mathbb{Z}_p \setminus \{\overline{0}\}$ eine Gruppe mit der Multiplikation des Körpers als Verknüpfung. Sie besitzt $p-1$ Elemente, und der Satz von Euler-Fermat besagt dann: Für alle $\overline{a} \in (\mathbb{Z}_p)^*$ gilt $\overline{a}^{p-1} = \overline{1}$.

Die Gleichung $x^{p-1} = \overline{1}$ hat in $\mathbb{Z}_p$ also die Lösungen $\overline{1}, \overline{2}, \ldots, \overline{p-1}$, also insgesamt $p-1$ verschiedene Lösungen.

Aufgabe 3.

a) Es ergibt sich mit etwas Probieren etwa die folgende Tabelle:

n	Typ von n
2	Primzahl
3	Primzahl
4	nicht gemischt-zusammengesetzt (nur $4 = 2 \cdot 2$ ist möglich)
5	Primzahl
6	gemischt-zusammengesetzt (z.B. $6 = 2 \cdot 3$)
7	Primzahl
8	gemischt-zusammengesetzt (z.B. $8 = 2 \cdot 4$)
9	nicht gemischt-zusammengesetzt (nur $9 = 3 \cdot 3$ ist möglich)
10	gemischt-zusammengesetzt (z.B. $10 = 2 \cdot 5$)
11	Primzahl
12	gemischt-zusammengesetzt (z.B. $12 = 3 \cdot 4$)
13	Primzahl
14	gemischt-zusammengesetzt (z.B. $14 = 2 \cdot 7$)
15	gemischt-zusammengesetzt (z.B. $15 = 3 \cdot 5$)
16	gemischt-zusammengesetzt (z.B. $16 = 2 \cdot 8$)
17	Primzahl
18	gemischt-zusammengesetzt (z.B. $18 = 2 \cdot 9$)
19	Primzahl
20	gemischt-zusammengesetzt (z.B. $20 = 4 \cdot 5$)

b) In a) hat sich bei den Versuchen gezeigt, daß die einzigen Zahlen, die keine Primzahlen sind und sich nicht ohne weiteres als Produkt zweier *verschieder* Zahlen > 1 schreiben lassen, die Quadrate von Primzahlen zu sein scheinen, so daß man vermuten kann: Eine Zahl $n \geq 2$ ist genau dann gemischt-zusammengesetzt, wenn sie weder eine Primzahl noch das Quadrat einer Primzahl ist.

c) Angenommen, $n \geq 2$ ist weder Primzahl noch das Quadrat einer Primzahl. Wähle einen beliebigen Primfaktor p von n und schreibe $n = p \cdot q$ mit $q = \frac{n}{p}$. Hier gilt $p > 1$ (weil p eine Primzahl ist) und $q > 1$ (weil sonst $n = p$ eine Primzahl wäre). Wenn wir nun $p \neq q$ zeigen können, so haben wir bewiesen, daß n gemischt-zusammengesetzt ist. Aber es gilt $p \neq q \iff p \neq \frac{n}{p} \iff p^2 \neq n$, und dies ist wahr, da n ja nicht das Quadrat irgendeiner Primzahl, also insbesondere nicht das Quadrat von p ist.

Nehmen wir nun umgekehrt an, $n \geq 2$ sei gemischt-zusammengesetzt. Dann ist n insbesondere zusammengesetzt, also keine Primzahl. Wir beweisen nun, daß n auch nicht das Quadrat einer Primzahl ist: Nach Voraussetzung ist $n = a \cdot b$ mit $a, b > 1$ und $a \neq b$. Angenommen, $n = p^2$ wäre das Quadrat einer Primzahl. Dann gäbe es für die Zerlegung $p^2 = ab$ (wie man mittels Primfaktorzerlegung sieht) nur die folgenden drei Möglichkeiten:

- $a = 1$ und $b = p^2$; dies kann aber nicht sein wegen $a, b > 1$,
- $a = p^2$ und $b = 1$; dies kann aus dem gleichen Grund nicht sein,
- $a = b = p$; dies kann nicht sein wegen $a \neq b$.

Also haben wir in jedem Fall einen Widerspruch erhalten, und damit kann n nicht das Quadrat einer Primzahl sein.

Aufgabe 4.

a) Ist n gemischt-zusammengesetzt, also $n = a \cdot b$ mit $a, b > 1$ und $a \neq b$, so gilt insbesondere $a, b < n$. Also tauchen die beiden (verschiedenen!) Zahlen a, b im Produkt $(n-1)! = 1 \cdot 2 \cdot \ldots \cdot (n-1)$ auf, d.h. es gilt $n = ab \mid (n-1)!$, und das bedeutet $\overline{(n-1)!} = \overline{0}$ in $\mathbb{Z}_n$.

b) Es sei n zusammengesetzt und $n \neq 4$. Wir dürfen nach a) annehmen, daß n *nicht* gemischt-zusammengesetzt ist, was nach Aufgabe 3 bedeutet: Wir dürfen annehmen, daß $n = p^2$ das Quadrat einer Primzahl ist, und wegen $n \neq 4$ gilt dabei $p \neq 2$.

Wir müssen zeigen, daß $\overline{(n-1)!} = \overline{0}$ in $\mathbb{Z}_n$ ist, daß also $(n-1)!$ durch $n = p^2$ teilbar ist. Dies folgt beispielsweise daraus, daß das Produkt $(n-1)!$ sowohl den Faktor p als auch den Faktor $2p$ enthält (denn es ist $p < 2p < p^2 = n$ wegen $p > 2$), also durch $2p^2$ und damit insbesondere durch p^2 teilbar ist.

c) Für $n = 4$ gilt $(n-1)! = 3! = 6$, und $\overline{6} = \overline{2} \neq \overline{0}$ in $\mathbb{Z}_4$.

Damit haben wir die allgemeinste Form des Satzes von Wilson bewiesen, die da lautet: Für eine natürliche Zahl $n \geq 2$ gilt in $\mathbb{Z}_n$:

$$\overline{(n-1)!} = \begin{cases} \overline{-1} & \text{falls } n \text{ eine Primzahl ist,} \\ \overline{0} & \text{falls } n \text{ zusammengesetzt und } n \neq 4 \text{ ist,} \\ \overline{2} & \text{falls } n = 4 \text{ ist.} \end{cases}$$

Strenggenommen haben wir in unseren Beweisen immer $n \geq 3$ vorausgesetzt, aber man kann überprüfen, daß die Aussage auch für $n = 2$ korrekt ist – man beachte dabei, daß $\overline{-1} = \overline{1}$ in $\mathbb{Z}_2$ gilt.