Universität Ulm
Gerhard Baur
Bianca Jaud

Übungen zum Seminar
Grundlagen der Mathematik
Blatt 10
Abgabe: Dienstag 12.01.2016

Aufgabe 1 (15 Punkte + 5 Bonuspunkte = 20 Punkte)

1) Lesen Sie sich die Texte zu den Themen Teilbarkeit und Primzahlen durch.

2) Machen Sie sich Gedanken darüber, wie Sie diese Inhalte in einer bzw. mehreren Schulstunden aufarbeiten würden.

3) Entwerfen Sie ein Arbeitsblatt für Schüler, die dieses Thema erarbeiten sollen*.

Hinweise:
Insgesamt gibt es für die Bearbeitung dieses Übungsblattes 15 Punkte. Das von Ihnen erstellte Arbeitsblatt geben Sie bitte am 12.01.2016 vor der Übung ab. Besonders gut gelungene Arbeitsblätter werden mit Bonuspunkten belohnt.
Es sollen einige Freiwillige ihre Entwürfe kurz in der Übung vorstellen, dass über die verschiedenen Möglichkeiten diskutiert werden kann.

Diese Aufgabe dient als Übung und Vorbereitung für Ihre künftige Laufbahn als Lehrer. Es soll die Verbindung zwischen dem Lernstoff, den Sie in der Universität gelehrt bekommen und dem Schulstoff aufzeigen.

Dieses Übungsblatt geben Sie bitte alleine ab und nicht wie üblich zu zweit!

*Schon in den Klassen 5/6 werden nach den Bildungsplänen 2016 Primzahlen und Teilbarkeitsregeln eingeführt. Dies ist in den Standards für inhaltsbezogene Kompetenzen unter der Leitidee Zahl-Variable-Operation eingebettet (siehe auch http://www.bildungsplaene-bw.de).

Cauchy ist närrisch und es gibt keinen Weg, mit ihm zurechtzukommen, obgleich er gegenwärtig der Mathematiker ist, der am besten weiß, wie Mathematik gemacht werden sollte.
Niels Abel (1802 - 1829)

§ 1 Teilbarkeit

Definition:

Eine ganze Zahl n heißt durch eine ganze Zahl $m \neq 0$ **teilbar,** wenn es eine ganze Zahl x gibt mit

$$n = xm.$$

Wir schreiben hierfür $m|n$. Gebräuchliche Sprechweisen sind auch:

"m teilt n","m ist ein **Teiler** von n" oder "n ist ein **Vielfaches** von m".

Ist n nicht durch m teilbar, so schreiben wir $m \not| n$.

Ist $0 < m < n$ und $m|n$, so nennen wir m einen **eigentlichen Teiler** von n.

Bemerkung:

In einer Beziehung $m|n$ lassen wir $m = 0$ niemals zu. Wenn wir $m|n$ schreiben, vereinbaren wir grundsätzlich, dass $m \neq 0$ ist. $n = 0$ kann man aber bedenkenlos zulassen. Dann gilt: $m|0 \ \forall\, m \neq 0$.

Satz 1: (Rechenregeln)

Es seien $m, n, q, x, y \in \mathbb{Z}$. Dann gilt:

(i) $m|n \Rightarrow m|nx$

(ii) $m|n$ und $n|q \Rightarrow m|q$

(iii) $m|n$ und $m|q \Rightarrow m|(nx + qy)$

$\Big($allgemeiner: $m|n_i,\ i = 1, \ldots, k \Rightarrow m \Big| \sum_{i=1}^{k} x_i n_i \ \ (n_i,\ x_i \in \mathbb{Z})$ $\Big)$

(iv) $m|n$ und $n|m \Rightarrow m = \pm n$

(v) $m, n \in \mathbb{N}$ und $m|n \Rightarrow m \leq n$

(vi) $m|n,\ q \neq 0 \Rightarrow qm|qn$

Bemerkung:

Aus (v) folgt: Jede von 0 verschiedene Zahl besitzt nur endlich viele Teiler.

Satz 2 (Division mit Rest):

Seien m, n gegebene ganze Zahlen mit $m > 0$. Dann gibt es ganze Zahlen q und r mit

$$n = qm + r \quad \text{und} \quad 0 \leq r < m.$$

Diese Zahlen q und m sind eindeutig bestimmt.

Zusatz: Genau dann gilt $m|n$, wenn $r = 0$ gilt.

Beweis:

- Existenz: Betrachte die Menge

  $$S = \{n - xm : \ x \in \mathbb{Z}\} \cap \mathbb{N}_0 \ \ (= n, \ n \pm m, n \pm 2m, \ldots, \} \cap \mathbb{N}_0).$$

  Diese Menge S ist sicherlich $\neq \emptyset$, und besitzt daher ein Minimum, etwa r. Dann erfüllt r die Ungleichung $0 \leq r < m$. Mit r ist aber auch q gefunden, denn r ist als Element von S von der Form $r = n - qm$.

- Eindeutigkeit: Sei q_1, r_1 ein weiteres Paar mit

  $$n = q_1 m + r_1, \quad \text{und} \quad 0 \leq r_1 < m$$

  Wir zeigen $r_1 = r$. Wäre nämlich $r_1 \neq r$, etwa $r < r_1$, so wäre $0 < r_1 - r < m$. Andererseits ist $r_1 - r = n - q_1 m - (n - qm) = m(q - q_1)$ also $m|(r_1 - r)$ im Widerspruch zu Satz 1 (v). Also ist doch $r = r_1$ und damit auch $q = q_1$.

- Der Zusatz ist offensichtlich.

Bemerkung:

In der Praxis bekommt man q und r , indem man die Division nach dem Grundschulalgorithmus durchführt, also $q = [\frac{n}{m}]$ setzt und r als $n - qm$ wählt.

Definition:

Eine ganze Zahl m heißt **gemeinsamer Teiler** zweier ganzer Zahlen n_1 und n_2, wenn gilt: $m|n_1$ und $m|n_2$. Sind n_1 und n_2 nicht beide $= 0$, so existiert das Maximum aller (endlich vielen) gemeinsamen Teiler von n_1 und n_2 ,und wie nennen dieses den **größte gemeinsame Teiler (ggT)** von n_1 und n_2 und bezeichnen es mit (n_1, n_2) .

Ist $(n_1, n_2) = 1$, so heißen n_1 und n_2 **teilerfremd** oder **relativ prim.**

In ähnlicher Weise definiert man gemeinsame Teiler und den größten gemeinsamen Teiler von endlich vielen Zahlen $n_1, \ldots, n_k$, (die nicht alle $= 0$ sind).

Beispiel:

$n_1 = 72$ und $n_2 = 42$ haben die gemeinsamen Teiler ± 1, ± 2, ± 3 und ± 6 , also ist $(72, 42) = 6$.

Satz 3 (Euklidscher Algorithmus):

Seien n und $m > 0$ zwei ganze Zahlen. Führt man dann den Divisionsalgorithmus aus Satz 2 wiederholt durch in folgender Form:

$$\begin{array}{rl} n = mq_1 + r_1, & 0 < r_1 < m, \\ m = r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 = r_2q_3 + r_3, & 0 < r_3 < r_2, \\ \vdots & \vdots \\ r_{j-3} = r_{j-2}q_{j-1} + r_{j-1}, & 0 < r_{j-1} < r_{j-2} \\ r_{j-2} = r_{j-1}q_j + r_j, & 0 < r_j < r_{j-1}, \\ r_{j-1} = r_jq_{j+1} & \end{array} ,$$

so gilt:

(i) Der Algorithmus bricht nach endlich vielen Schritten ab.

(ii) Der größte gemeinsame Teiler von n und m ist r_j, also der letzte von Null verschiedene Rest.

(iii) Es gibt ganze Zahlen x und y mit

$$(n, m) = xm + yn.$$

Beweis:

(i) Dies ist klar. Die Folge der Zahlen r_i sind > 0, ganzzahlig und streng monoton fallend

(ii) Jeder gemeinsame Teiler d von n und m ist auch Teiler von r_1, wie man aus der 1. Zeile sieht. Damit ist aber auch $d|r_2$ (wegen der zweiten Zeile) und damit (induktiv) auch von r_j.

Ist umgekehrt d ein Teiler von r_j, so gilt auch $d|r_{j-1}$ (letzte Zeile), also auch $d|r_{j-2}$ (vorletzte Zeile) usw., also auch $d|m$ und $d|n$.

Insgesamt folgt: $r_j = (n, m)$.

(iii) Dies sieht man, indem man die vorletzte Zeile nach r_j auflöst und sukzessive von unten nach oben die r_{j-1}, r_{j-2} usw. eliminiert:

$$r_j = r_{j-2} - r_{j-1}q_j = r_{j-2} - (r_{j-3} - r_{j-2}q_{j-1})q_j = (1 + q_{j-1}q_j)r_{j-2} - q_jr_{j-3} = \ldots$$

Beispiel:
Gesucht ist $(963, 657)$:

$$\begin{aligned} 963 &= 1 \cdot 657 + 306 \\ 657 &= 2 \cdot 306 + 45 \\ 306 &= 6 \cdot 45 + 36 \\ 45 &= 1 \cdot 36 + 9 \\ 36 &= 4 \cdot 9 \end{aligned}$$

Also ist $(963, 657) = 9$. Schließlich stellen wir 9 als ganzzahlige Linearkombination von 963 und 657 dar:

$$\begin{aligned} 9 &= 45 - 1 \cdot 36 \\ &= 45 - (306 - 6 \cdot 45) \\ &= 7 \cdot 45 - 306 \\ &= 7 \cdot (657 - 2 \cdot 306) - 306 \\ &= 7 \cdot 657 - 15 \cdot 306 \\ &= 7 \cdot 657 - 15 \cdot (963 - 657) \\ &= 22 \cdot 657 - 15 \cdot 963 \end{aligned}$$

Als Anwendung betrachten wir die Diophantische Gleichung

$$(*) \quad ax + by = n$$

mit gegebenen $a, b, n \in \mathbb{Z}$ (a, b nicht beide $= 0$) und fragen nach ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$.

Satz 4:

Die Diophantische Gleichung $(*)$ ist lösbar $\iff (a, b) | n$. Im Falle der Lösbarkeit kann eine Lösung mit dem Euklidischen Algorithmus berechnet werden.

Beweis:

- Sei $(*)$ lösbar $\Rightarrow d := (a, b)$ erfüllt $d|a$ und $d|b \Rightarrow d|ax + by = n$.
- Sei $d := (a, b) \underbrace{\Rightarrow}_{\text{Euklid}} \exists\, c_1, c_2 \in \mathbb{Z}$ mit $ac_1 + bc_2 = d$.

  Wegen $d|n$ ist $g := \dfrac{n}{d} \in \mathbb{Z}$. Setze nun $x := c_1 \cdot g,\ y := c_2 \cdot g$
  $\Rightarrow ax + by = ac_1 g + ac_2 g = g \cdot d = n$.

Bemerkungen:

(i) Ist $(a,b)=1$, so ist $(*)$ immer lösbar. Ein Zahlenbeispiel:
$3x+4y=11:\ \ (3,4)=1$ und $1=\underbrace{-1}_{=c_1}\cdot 3+\underbrace{+1}_{=c_2}\cdot 4;$
$g=11,\ x=-11,\ y=+11$ tut's.

(ii) Beispiel: $2x+4y=3$ ist unlösbar (in ganzen Zahlen)

(iii) Beispiel: $(657,963)=9\ \Rightarrow 657x+963y=36$ ist lösbar, denn $9|36$.
Nun ist (s.o.) $9=\underbrace{22}_{=c_1}\cdot 657+\underbrace{-15}_{=c_2}\cdot 963;$
$g=\dfrac{36}{9}=4\Rightarrow\ x=22\cdot 4=88,\ y=-15\cdot 4=-60$ ist eine Lösung.

(iv) Eindeutig brauchen Lösungen von (*) nicht zu sein. Ist nämlich $ax+by=n,$ so ist auch $a(x+x')+b(y+y')=n,$ falls nur $ax'=-by'$ gilt.

Definition:

Es seien $m_1,m_2\in\mathbb{Z}\backslash\{0\}$. Eine Zahl $n\in\mathbb{Z}$ heißt **gemeinsames Vielfaches** von m_1 und m_2, falls gilt: $m_1|n$ und $m_2|n$. (Ein solches n existiert immer: $n_1\cdot n_2$ ist ein gemeinsames Vielfaches). Das kleinste positive Vielfache von m_1 und m_2 heißt **kleinstes gemeinsames Vielfaches (kgV)** von m_1 und m_2 und wird mit $[m_1,m_2]$ bezeichnet. Analog definiert man den Begriff für endlich viele Zahlen $m_1,\ldots,m_k,$ die alle $\neq 0$ sind.

Die Berechnung von $[m_1,m_2]$ erfolgt über den Satz von der Primfaktorzerlegung, den wir im nächsten Abschnitt beweisen:

§ 2 Primzahlen

Definition:

(i) Die zahlentheoretische Funktion $d(n)$ sei definiert über

$$d(n) := \sum_{d|n,\ d\in\mathbb{N}} 1.$$

$d(n)$ ist also die Anzahl der positiven Teiler von n.

(ii) Jede Zahl $n > 1$ mit $d(n) = 2$ heißt **Primzahl.** Jede andere Zahl heißt eine **zusammengesetzte Zahl.** Die Menge aller Primzahlen bezeichnen wir mit $\mathcal{P}$.

Bemerkungen:

(i) Ist $n \geq 2$, so ist sicherlich $1|n$ und $n|n \Rightarrow d(n) \geq 2$.

(ii) Für $m \in \mathbb{Z},\ p \in \mathcal{P}$ ist

$$(m,p) = \begin{cases} p & p|m \\ 1 & \text{sonst} \end{cases}$$

(denn: d positiver Teiler von m und $p \Rightarrow d|p \Rightarrow d = 1$ oder $d = p$)

Satz 5:

Für $n \in \mathbb{N},\ n \geq 2$ sei $d_1(n)$ der kleinste positive echte Teiler von n, (also > 1). Dann gilt:

(i) $d_1(n)$ ist eine Primzahl.

(ii) Ist darüberhinaus n keine Primzahl, so ist $d_1(n) \leq \sqrt{n}$.

Beweis:

(i) Angenommen, es sei $d_1(n) \notin \mathcal{P} \Rightarrow \exists\, d \in \mathbb{N}$ mit $1 < d < d_1(n) \Rightarrow d|n$. Also war d doch nicht der kleinste Teiler von n, der > 1 ist.

(ii) $n \notin \mathcal{P} \Rightarrow \exists\, d,\ 1 < d < n$ mit: $d|n$ und $\frac{n}{d}\Big|n \Rightarrow d$ und $\frac{n}{d}$ sind nicht beide $> \sqrt{n}$, denn sonst wäre $n = \underbrace{d}_{>\sqrt{n}} \cdot \underbrace{\frac{n}{d}}_{>\sqrt{n}} > n$, ein Widerspruch.

Bemerkungen:

(i) Aus (ii) ergibt sich ein erster primitiver Primzahltest. Man braucht für eine Zahl n nur die Primteiler bis $\sqrt{n}$ zu untersuchen. Teilt keiner von ihnen n, so ist n Primzahl. Beispiel: 107 ist Primzahl, denn $\sqrt{107} < 11$, und 107 ist nicht durch $2, 3, 5$ und 7 teilbar.

(ii) Auf (ii) beruht auch das Siebverfahren von Erathostenes: Man beginnt mit der Liste der natürlichen Zahlen von 2 bis N. Die kleinste auftretende Zahl ist die 2. Man streicht dann alle durch 2 teilbaren Zahlen. Von den restlichen ist die kleinste (hier die 3) wieder eine Primzahl. Man streicht dann alle verbliebenen, noch durch 3 teilbaren Zahlen heraus. Dieses Aussieben braucht man dann nur bis $\sqrt{N}$ durchzuführen. Die übriggebliebene Liste ist dann die Liste aller Primzahlen bis N.

Satz 6 (Primfaktorzerlegung):

Jede ganze Zahl $n > 1$ kann als ein Produkt von Primzahlen dargestellt werden, wobei ein solches Produkt auch nur aus einem einzigen Faktor bestehen kann.

Beweis:

Ist n eine Primzahl, so steht sie selbst als Produkt mit einem einzigen Faktor. Andernfalls kann n in Faktoren zerlegt werden, etwa in $n = n_1 n_2$, wobei $1 < n_1 < n$ ubnd $1 < n_2 < n$ gilt. Ist n_1 eine Primzahl, so brauchen wir sie nicht weiter zu betrachten. Andernfalls stellen wir n_1 als Produkt $n_1 = n_3 n_4$ dar mit $1 < n_3 < n_1,\ 1 < n_4 < n_1$. In analoger Weise behandeln wir n_2. Das Verfahren bricht nach endlich vielen Schritten ab, denn die so konstruierten ganzen Zahlen sind alle > 1 und $< n$.

Bemerkungen:

(i) Da die im Beweis zu Satz 6 konstruierten Primteiler nicht notwendig voneinander verschieden sind, kann man präziser formulieren:

Zu jedem $n \in \mathbb{N},\ n > 1$ gibt es $r \in \mathbb{N}$, Primzahlen $p_1, \ldots, p_r$ mit $p_1 < p_2 < \ldots < p_r$ und natürliche Zahlen $\alpha_1, \ldots, \alpha_r$ mit

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$$

Das die sogenannte **Primfaktorzerlegung** von n.

(ii) In der Formulierung von (i) kann man zeigen, dass die Primfaktorzerlegung eindeutig ist.

Satz 7 (Anwendungen der Primfaktorzerlegung):

(i) Es sei $n \in \mathbb{N},\ n > 1$ mit Primfaktorzerlegung $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$. Dann sind alle positiven Teiler d von n gegeben durch

$$d = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r} \text{ mit } k_\nu \in \mathbb{N}_0,\ 0 \le k_\nu \le \alpha_\nu,\ 1 \le \nu \le r.$$

(ii) Seien $m, n \in \mathbb{N},\ m, n > 1$ mit $m = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r},\ n = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$, p_ν Primzahlen, $\alpha_1, \ldots, \alpha_r,\ \beta_1, \ldots, \beta_r \in \mathbb{N}_0$ (also nicht unbedingt die Primfaktorzerlegungen: Ein auftretender Primfaktor p_ν soll in wenigstens einer der Primfaktorzerlegungen von m bzw. n vorkommen). Dann gilt:

- $(m, n) = p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$ mit $\gamma_\nu = \min\{\alpha_\nu, \beta_\nu\},\ 1 \leq \nu \leq r$;
- $[m, n] = p_1^{\delta_1} \cdot \ldots \cdot p_r^{\delta_r}$ mit $\delta_\nu = \max\{\alpha_\nu, \beta_\nu\},\ 1 \leq \nu \leq r$;
- Ist $p \in \mathcal{P}$ und $p|mn$, so gilt $p|m$ oder $p|n$.

Beweis:

Das ist an der Primfaktorzerlegung ablesbar, z.B. die dritte Aussage in (ii):

$p|mn = p_1^{\alpha_1+\beta_1} \cdot \ldots \cdot p_r^{\alpha_r+\beta_r} \Rightarrow p = p_\nu$ für ein ν. Ist dann $\alpha_\mu > 0$, so gilt $p|m$. Ist aber $\alpha_\nu = 0$, so ist $\beta_\nu > 0$, also $p|n$. (Sind α_ν und β_ν beide > 0, so gilt $p|m$ und $p|n$.)

Beispiel:

$72 = 2^3 \cdot 3^2 \Rightarrow$ Teiler von $72:\ 2^0 \cdot 3^0 = 1,\ 2^1 \cdot 3^0 = 2, \ldots, 2^3 \cdot 3^2 = 72.$

$42 = 2 \cdot 3 \cdot 7 \Rightarrow\ (42, 72) = 2 \cdot 3 = 6;\ [42, 72] = 2^3 \cdot 3^2 \cdot 7 = 504.$

Satz 8 (Euklid):

Es gibt unendlich viele Primzahlen.

Beweis:

Angenommen, es gebe nur endlich viele Primzahlen, etwa $p_1, \ldots, p_r$. Bilde dann

$$n = 1 + p_1 \cdot p_2 \cdot \ldots \cdot p_r.$$

Dann ist offenbar n durch keine der Primzahlen $p_1, \ldots, p_r$ teilbar. Damit ist n entweder selbst eine Primzahl oder besitzt einen Primteiler, der nicht unter den $p_1, \ldots, p_r$ vorkommt. In beiden Fällen gibt es aber eine weitere Primzahl, so dass $p_1, \ldots, p_r$ nicht die komplette Auflistung aller Primzahlen sein kann.