Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Fachbereich Mathematik
Algebra und Zahlentheorie
Christian Curilla

Grundlagen der Mathematik (LPSI/LS-M1)

Lösungen Blatt 7 WiSe 2010/11 - Curilla/Koch/Ziegenhagen

Präsenzaufgaben

(P24) (a) Es ist

$$\begin{aligned}
[a] &= \{x \in \mathbb{Z} : a \equiv x \mod m\} \\
&= \{x \in \mathbb{Z} : m|(x-a)\} \\
&= \{x \in \mathbb{Z} : \exists k \in \mathbb{Z} : km = x - a\} \\
&= \{x \in \mathbb{Z} : \exists k \in \mathbb{Z} : x = km + a\} \\
&= \{km + a \in \mathbb{Z} : k \in \mathbb{Z}\}.
\end{aligned}$$

(b) Es gibt m verschiedene Äquivalenzklassen, nämlich

$$\begin{aligned}
[0] &= \{\ldots, -2m, -m, 0, m, 2m, \ldots\}\ , \\
[1] &= \{\ldots, -2m+1, -m+1, 1, m+1, 2m+1, \ldots\}\ , \\
&\vdots \\
[m-2] &= \{\ldots, -m-2, -2, m-2, 2m-2, 3m-2, \ldots\}\ , \\
[m-1] &= \{\ldots, -m-1, -1, m-1, 2m-1, 3m-1, \ldots\}\ .
\end{aligned}$$

Wir wollen diese Behauptung beweisen:
Zunächst halten wir fest, dass für $a, b \in \mathbb{Z}$ gilt:

$$[a] = [b] \Longleftrightarrow a \equiv b \mod m\,.$$

Für beide Implikationen benutzen wir, dass $x \in [x]$ gilt für alle $x \in \mathbb{Z}$. Wir zeigen zuerst „$\Rightarrow$“: Aus $b \in [b]$ folgt $b \in [a]$. Nach Definition der Äquivalenzklassen ist dann aber $a \equiv b \mod m$. Als nächstes zeigen wir „$\Leftarrow$“: Sei $x \in [a]$, also $a \equiv x \mod m$. Weil die Modulo-Relation symmetrisch ist, gilt $x \equiv a \mod m$. Aus der Transitivität der Relation folgt nun - zusammen mit $a \equiv b \mod m$ - dass $x \equiv b \mod m$ ist. Mit der Symmetrie erhält man dann $b \equiv x \mod m$ und somit $x \in [b]$. Sei umgekehrt $x \in [b]$ gegeben, d.h. insbesondere $b \equiv x \mod m$. Hieraus - zusammen mit $a \equiv b \mod m$ - folgt $a \equiv x \mod m$, wegen der Transitivität der Relation R_m. Es folgt also $x \in [a]$. Insgesamt haben wir gezeigt, dass $[a] = [b]$ gilt.
Sei nun $[a]$ eine beliebige Äquivalenzklasse. Divison mit Rest liefert uns $a = q \cdot m + r$, wobei $0 \leq r < m$ ist (Satz 6.4 bzw. Kiechle-Skript (4.6)). Aus $(-q) \cdot m = r - a$ folgt $a \equiv r \mod m$ und somit $[r] = [a]$.
Zur Verschiedenheit von $[0], [1], ..., [m-1]$: Seien $[i]$ und $[j]$ zwei dieser Klassen. Wenn $[i] = [j]$ ist, so folgt $i \equiv j \mod m$. Aus Satz 6.5 (Kiechle (4.7)) folgt dann allerdings $i = j$, weil bei der Division von i (bzw. j) durch m der Rest gerade i (bzw. j) ist.

(c) Ja, das haben wir in der Vorlesung bewiesen. Wir überlegen es uns aber nochmal an diesem Beispiel: Es ist zu beweisen, dass $[0] \cup [1] \cup ... \cup [m-1] = \mathbb{Z}$ gilt, und dass für $0 \leq i, j \leq m-1$ aus $[i] \neq [j]$ folgt, dass $[i] \cap [j] = \emptyset$ ist.
Die erste Aussage haben wir bereits in (P24b) bewiesen: Jedes $x \in \mathbb{Z}$ liegt in einer der Äquivalenzklassen $[0], [1], ..., [m-1]$. Die zweite Aussage zeigen wir, indem wir die Kontraposition beweisen, also zeigen, dass aus $[i] \cap [j] \neq \emptyset$ folgt, dass $[i] = [j]$ ist. Ist $x \in [i] \cap [j]$, so folgt $i \equiv x \mod m$ und $j \equiv x \mod m$. Wegen der Symmetrie gilt $x \equiv j \mod m$. Die Transitivität liefert jetzt $i \equiv j \mod m$ und somit $[i] = [j]$ nach (b).

(P25) Wir zeigen die Behauptung durch Induktion nach n:
Induktionsanfang: Für $n = 1$ ist $n^2 + n = 1 + 1 = 2$ gerade.
Induktionsvoraussetzung: Sei $m^2 + m$ gerade für ein beliebiges, aber fest gewähltes $m \in \mathbb{N}$.
Induktionsschluss: Wir wollen zeigen, dass unter der Induktionsvoraussetzung auch $(m+1)^2 + m + 1$ gerade ist: Es ist

$$(m+1)^2 + m + 1 = m^2 + 2m + 1 + m + 1 = m^2 + m + 2m + 2.$$

Nach Induktionsvoraussetzung gibt es ein $k \in \mathbb{Z}$ mit $m^2 + m = 2k$. Folglich ist

$$m^2 + m + 2m + 2 = 2k + 2m + 2 = 2(k + m + 1).$$

Also gilt unter der Induktionsvoraussetzung $2 | (m+1)^2 + m + 1$, das heißt $(m+1)^2 + m + 1$ ist gerade.
Damit ist die Behauptung gezeigt.

(P26) Es gilt $2010 = 2 \cdot 1005 = 2 \cdot 3 \cdot 335 = 2 \cdot 3 \cdot 5 \cdot 67$. Da $2, 3, 5$ und 67 Primzahlen sind, ist dies die Primfaktorzerlegung von 2010.

Hausaufgaben

(H25) Die Formel gilt für alle $n \in \mathbb{N}$, wir beweisen dies durch Induktion nach n:
Induktionsanfang: Für $n = 1$ ist

$$\sum_{k=1}^{1} k! \cdot k = 1! \cdot 1 = 1 = 2 - 1 = (1+1)! - 1.$$

Induktionsvoraussetzung: Sei $\sum_{k=1}^{m} k! \cdot k = (m+1)! - 1$ für ein beliebiges, aber fest gewähltes $m \in \mathbb{N}$.
Induktionsschluss: Wir wollen zeigen, dass unter der Induktionsvoraussetzung auch $\sum_{k=1}^{m+1} k! \cdot k = (m+2)! - 1$ gilt. Dazu nutzen wir, dass sich $\sum_{k=1}^{m} k! \cdot k$ und $\sum_{k=1}^{m+1} k! \cdot k$ nur um einen Summanden unterscheiden: Es ist

$$\begin{aligned} \sum_{k=1}^{m+1} k! \cdot k &= \sum_{k=1}^{m} k! \cdot k + (m+1)! \cdot (m+1) \\ &= (m+1)! - 1 + (m+1)! \cdot (m+1) \\ &= (m+1)! \cdot (1 + m + 1) - 1 \\ &= (m+2)! - 1. \end{aligned}$$

Dabei haben wir die Induktionsvoraussetzung beim Übergang von der ersten zur zweiten Zeile benutzt.
Damit ist die Behauptung gezeigt.

(H26) Wir beweisen zunächst die Ungleichung aus dem Hinweis: Für $n \geq 5$ ist $\frac{3}{n} < 1$ und $\frac{1}{n^2} < 1$. Damit ist $n \geq 5 = 3 + 1 + 1 > 3 + \frac{3}{n} + \frac{1}{n^2}$.

Durch Einsetzen finden wir heraus: Die Ungleichung $2^n > n^3$ gilt für $n = 1$, für $n \in \{2, ..., 9\}$ gilt sie nicht. Für $n \in \mathbb{N}$ mit $n \geq 10$ gilt sie wieder. Wir beweisen die Gültigkeit der Ungleichung für $n \geq 10$ durch vollständige Induktion nach n:
Induktionsanfang: Für $n = 10$ ist $1024 = 2^{10} > 10^3 = 1000$.
Induktionsvoraussetzung: Sei $2^m > m^3$ für ein beliebiges, aber fest gewähltes $m \in \mathbb{N}$ mit $m \geq 10$.
Induktionsschluss: Wir wollen zeigen, dass unter der Induktionsvoraussetzung auch $2^{m+1} > (m+1)^3$ gilt. Wegen $2^{m+1} = 2 \cdot 2^m$ lässt sich die linke Seite der zu beweisenden Ungleichung mithilfe der linken Seite der Ungleichung aus der Induktionsvoraussetzung ausdrücken. Wir wenden die Induktionsvoraussetzung an und erhalten

$$2^{m+1} = 2 \cdot 2^m > 2 \cdot m^3 = m^3 + m^3.$$

Wir haben die Hinweisungleichung noch nicht benutzt und betrachten diese: Multipliziert man die Ungleichung $m > 3 + \frac{3}{m} + \frac{1}{m^2}$ mit m^2, so erhält man $m^3 > 3m^2 + 3m + 1$. Damit ist

$$2^{m+1} > m^3 + m^3 > m^3 + 3m^2 + 3m + 1.$$

Die rechte Seite der zu beweisenden Ungleichung ist aber gerade $(m+1)^3 = m^3 + 3m^2 + 3m + 1$ - wir erhalten also $2^{m+1} > (m+1)^3$ und haben den Induktionsschluss vollzogen.
Damit ist die Behauptung gezeigt.

(H27) Wir berechnen zuerst die Primfaktorzerlegung von a, b und c. Es ist

$$a = 2^3 \cdot 3^2 \cdot 7^2 \cdot 11, \quad b = 2 \cdot 3^2 \cdot 7 \cdot 13^2, \quad c = 2 \cdot 3^2 \cdot 5.$$

(a) Natürliche Teiler von a sind nach der Bemerkung aus der Vorlesung genau die Zahlen m, in deren Primfaktorzerlegung dieselben Primzahlen (oder weniger, falls es β_j mit $\beta_j = 0$ gibt) wie in der von a vorkommen, aber eventuell mit kleinerem Exponenten. Dasselbe gilt für Teiler von b. In der Primfaktorzerlegung eines m, das a und b teilt, darf also die 2 höchstens einmal vorkommen, die 3 darf höchstens Exponenten 2 haben, die 7 darf nur einmal oder keinmal vorkommen. Die 11 und 13 dürfen gar nicht in der Primfaktorzerlegung von m vorkommen, da die 11 kein Teiler von b ist und die 13 kein Teiler von a. Wählen wir die Exponenten so groß wie maximal erlaubt, so erhalten wir den größten gemeinsamen Teiler: Es ist $\mathrm{ggT}(a, b) = 2 \cdot 3^2 \cdot 7 = 126$.

(b) Damit a eine Zahl n teilt, müssen die Exponenten der einzelnen Primzahlen (die auch bei a vorkommen) in der Primfaktorzerlegung von n mindestens so groß sein wie in der von a. Positive Vielfache von a und b, also Zahlen aus $\mathbb{N}$, die von a und b geteilt werden, sind Zahlen von der Form

$$2^{\beta_1} \cdot 3^{\beta_2} \cdot 7^{\beta_3} \cdot 11^{\beta_4} \cdot 13^{\beta_5} \cdot c$$

mit $\beta_1 \geq 3, \beta_2, \beta_3 \geq 2, \beta_4 \geq 1, \beta_5 \geq 2$ und $c \in \mathbb{N}$. Das kleinste gemeinsame Vielfache ist also $\mathrm{kgV}(a, b) = 2^3 \cdot 3^2 \cdot 7^2 \cdot 11 \cdot 13^2 = 6558552$.

(c) Nach der Bemerkung aus der Vorlesung müssen wir lediglich die natürlichen Zahlen m finden, deren Primfaktorzerlegung aus denselben (oder weniger) Primzahlen wie bei c mit höchstens so großem Exponenten besteht. Teiler von c sind also

$$\begin{aligned}
2^0 \cdot 3^0 \cdot 5^0 = 1, \quad 2^1 \cdot 3^0 \cdot 5^0 = 2, \quad 2^0 \cdot 3^1 \cdot 5^0 = 3, \\
2^0 \cdot 3^0 \cdot 5^1 = 5, \quad 2^1 \cdot 3^1 \cdot 5^0 = 6, \quad 2^1 \cdot 3^0 \cdot 5^1 = 10, \\
2^0 \cdot 3^2 \cdot 5^0 = 9, \quad 2^0 \cdot 3^1 \cdot 5^1 = 15, \quad 2^1 \cdot 3^2 \cdot 5^0 = 18, \\
2^1 \cdot 3^1 \cdot 5^1 = 30, \quad 2^0 \cdot 3^2 \cdot 5^1 = 45 \quad 2^1 \cdot 3^2 \cdot 5^1 = 90.
\end{aligned}$$

(d) Wie in (c) müssen wir uns nur die verschiedenen Möglichkeiten (bzw. deren Anzahl) überlegen, Exponenten zu wählen, die höchstens so groß sind wie in der angegebenen Zahl. Es gibt drei Möglichkeiten, den Exponenten von p_1 zu wählen (nämlich $0, 1, 2$), vier Möglichkeiten für den zweiten Exponenten, drei für den dritten und sechs für den letzten. Da die Primfaktorzerlegung einer Zahl eindeutig ist, haben wir keinen Teiler doppelt gezählt und erhalten insgesamt $3 \cdot 4 \cdot 3 \cdot 6 = 216$ verschiedene Teiler.

(e) Seien die Bezeichnungen wie in der Bemerkung. Wir zeigen zuerst, dass n von m geteilt wird, falls $m = \prod_{j=1}^{k} p_j^{\beta_j}$ mit $\beta_j \in \{0, ..., \alpha_j\}$ ist. Wir wollen also ein $l \in \mathbb{Z}$ finden, so dass $lm = n$ ist. Wir können dieses l hier direkt angeben: Die Primfaktoren von l und m sollen miteinander multipliziert die von n ergeben, wir setzen also $l := \prod_{j=1}^{k} p_j^{\alpha_j - \beta_j}$. Da $\alpha_j - \beta_j \geq 0$ ist, ist dies eine ganze Zahl. Mit dieser Definition von l rechnen wir

$$\begin{aligned} lm &= \prod_{j=1}^{k} p_j^{\alpha_j - \beta_j} \cdot \prod_{j=1}^{k} p_j^{\beta_j} \\ &= p_1^{\alpha_1 - \beta_1} ... p_k^{\alpha_k - \beta_k} p_1^{\beta_1} ... p_k^{\beta_k} \\ &= p_1^{\alpha_1 - \beta_1} p_1^{\beta_1} ... p_k^{\alpha_k - \beta_k} p_k^{\beta_k} \\ &= p_1^{\alpha_1 - \beta_1 + \beta_1} ... p_k^{\alpha_k - \beta_k + \beta_k} \\ &= p_1^{\alpha_1} ... p_k^{\alpha_k} \\ &= n. \end{aligned}$$

Also teilt m die Zahl n, und die Richtung „$\Leftarrow$“ ist bewiesen.

Zur anderen Richtung: Wir nehmen an, dass $m|n$ gilt, die Primfaktorzerlegung von n sei wie in der Bemerkung angegeben. Ist $m = n$, so ist die Behauptung klar. Wir können uns also auf die Situation $m \neq n$ konzentrieren. Die Zahl m hat ebenfalls eine Primfaktorzerlegung $m = \prod_{j=1}^{s} \hat{p}_j^{\delta_j}$, deren Form wir nun genauer bestimmen wollen.
Wir schreiben aus, was unsere Annahme $m|n$ bedeutet: $\exists l \in \mathbb{N} : lm = n$. Dabei ist l positiv, da m und n positiv sind. Sei $l = \prod_{j=1}^{r} \tilde{p}_j^{\gamma_j}$ die Primfaktorzerlegung von l, die $\tilde{p}_j$ sind also Primzahlen und $\gamma_j \in \mathbb{N}$ die Vielfachheiten, mit denen sie in l auftreten. Setzen wir dies in unsere Voraussetzung $ml = n$ ein, erhalten wir

$$\tilde{p}_1^{\gamma_1} ... \tilde{p}_r^{\gamma_r} \hat{p}_1^{\delta_1} ... \hat{p}_s^{\delta_s} = p_1^{\alpha_1} ... p_k^{\alpha_k}.$$

Es steht auf der linken und auf der rechten Seite der obigen Gleichung ein Produkt von Primzahlen, das n ergibt. Da Primfaktorzerlegungen eindeutig sind, muss jede Primzahl im Produkt auf der linken Seite genau so oft vorkommen wie im Produkt auf der rechten Seite. Was heißt das für m? Es heißt für jedes $\hat{p}_i^{\delta_i}$, dass auf der rechten Seite ebenfalls δ_i-mal ein $\hat{p}_i$ steht. Da die p_i untereinander verschieden sind, muss es sogar genau ein p_j auf der rechten Seite geben, dass mit dem $\hat{p}_i$ übereinstimmt. Dass dieses $\hat{p}_i$ links mindestens δ_i-mal vorkommt, heißt dann, dass das p_j rechts auch mindestens δ_i-mal vorkommt. Wie oft das p_j vorkommt, ist aber durch α_j vorgegeben. Es muss also $\delta_i \leq \alpha_j$ sein.
Insgesamt ergibt sich: Die $\hat{p}_i$ sind aus der Menge $\{p_1, \ldots, p_k\}$, und eine Prim-

zahl kommt in der Primfaktorzerlegung von m höchstens so oft vor wie in der von n. Dies beweist die Richtung „⇒“.

(H28) (a) Wir müssen uns überlegen, ob aus $a \equiv b \mod m$ folgt, dass $a^2 \equiv b^2 \mod m$ gilt. Wir behaupten, dass dies stimmt und beweisen es: Setze $a \equiv b \mod m$ voraus. Dies bedeutet $m|(a-b)$, also gibt es ein $k \in \mathbb{Z}$ mit $mk = a - b$. Wir wollen zeigen, dass $a^2 \equiv b^2 \mod m$ gilt, dass es also ein $l \in \mathbb{Z}$ mit $ml = a^2 - b^2$ gibt.

Erinnern wir uns an die binomischen Formeln: Multiplizieren wir $a - b$ mit $a + b$, so erhalten wir die gewünschte rechte Seite $a^2 - b^2$. Also multiplizieren wir die Gleichung $mk = a - b$, die wir als gültig angenommen hatten, mit $a + b$, und erhalten

$$mk(a + b) = a^2 - b^2.$$

Wir können also $l = k(a + b)$ setzen und erhalten $m|a^2 - b^2$, also $a^2 \equiv b^2 \mod m$.

(b) Wir müssen uns nun überlegen, ob aus $a^2 \equiv b^2 \mod m$ folgt, dass $a \equiv b \mod m$ gilt. Die Aussage ist falsch, wir geben ein Gegenbeispiel an: Setze $m = 4, a = 2$ und $b = 0$. Dann gilt $a^2 \equiv b^2 \mod m$, denn $m = 4$ teilt $4 - 0 = a^2 - b^2$. Aber $m = 4$ teilt offenbar nicht $a - b = 2$, also gilt $a \equiv b \mod m$ nicht.