Lösungen zu Zettel 6

Jendrik Stelzner

4. Dezember 2016

Aufgabe 1

Es seien $\mathcal{P}$ ein Repräsentantensystem der Assoziiertheitsklassen der Primelemente von R.

Lemma 1. 1. Für alle $x, y \in R$ und $p \in \mathcal{P}$ gilt $\nu_p(xy) = \nu_p(x) + \nu_p(y)$.

2. Für alle $x, y \in R$ gilt genau dann $x \mid y$, wenn $\nu_p(x) \leq \nu_p(y)$ für alle $p \in \mathcal{P}$.

Beweis. Es gibt Primfaktorzerlegungen $x = u_1 \prod_{p \in \mathcal{P}} p^{\nu_p(x)}$ und $y = u_2 \prod_{p \in \mathcal{P}} p^{\nu_p(y)}$ mit $u_1, u_2 \in R^\times$.

1. Für das Produkt xy ergibt sich eine Primfaktorzerlegung

$$xy = u_1 \prod_{p \in \mathcal{P}} p^{\nu_p(x)} \cdot u_2 \prod_{p \in \mathcal{P}} p^{\nu_p(y)} = (u_1 u_2) \prod_{p \in \mathcal{P}} p^{\nu_p(x) + \nu_p(y)},$$

   weshalb $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ für alle $p \in \mathcal{P}$.

2. Gilt $x \mid y$, so gibt es $z \in R$ mit $y = xz$, weshalb

$$\nu_p(y) = \nu_p(xz) = \nu_p(x) + \nu_p(z) \geq \nu_p(x).$$

   Gilt andererseits $\nu_p(x) \leq \nu_p(y)$ für alle $p \in \mathcal{P}$, so ist $z \coloneqq u_1^{-1} u_2 \prod_{p \in \mathcal{P}} p^{\nu_p(y) - \nu_p(x)} \in R$ wohldefiniert, und wegen $xy = z$ gilt $x \mid y$. □

Für das Element $z \coloneqq \prod_{p \in \mathcal{P}} p^{\min(\nu_p(x), \nu_p(y))} \in R$ gilt $\nu_p(z) = \min(\nu_p(x), \nu_p(y))$ für alle $p \in \mathcal{P}$. Für jedes $z' \in R$ gilt nach Lemma 1, dass

$$\begin{aligned} z' \mid x, y &\iff \nu_p(z') \leq \nu_p(x), \nu_p(y) \text{ für alle } p \in \mathcal{P} \\ &\iff \nu_p(z') \leq \min(\nu_p(x), \nu_p(y)) \text{ für alle } p \in \mathcal{P} \\ &\iff \nu_p(z') \leq \nu_p(z) \text{ für alle } p \in \mathcal{P} \\ &\iff z' \mid z. \end{aligned}$$

Somit ist z ein größter gemeinsamer Teiler von x und y.

Aufgabe 2

Für $k, n \in \mathbb{Z}$ schreiben wir im Folgenden $[k]_n$ für die Restklasse von k in $\mathbb{Z}/n\mathbb{Z}$. Das Gleichungssystem

$$\begin{cases} 4x &\equiv& 5 &\mod 9, \\ 3x &\equiv& 10 &\mod 11, \end{cases}$$

für $x \in \mathbb{Z}$ ist mit dieser Notation äquivalent zu dem Gleichungssystem

$$\begin{cases} [4]_9\ [x]_9 &=& [5]_9, \\ [3]_{11}[x]_{11} &=& [10]_{11}. \end{cases}$$

Da 4 und 9 teilerfremd sind, ist $[4]_9 \in \mathbb{Z}/9\mathbb{Z}$ eine Einheit (siehe Übungszettel 4), und es gilt $[4]_9^{-1} = [7]_9$. Für alle $x \in \mathbb{Z}$ ist deshalb

$$[4]_9[x]_9 = [5]_9 \iff [7]_9[4]_9[x]_9 = [7]_9[5]_9 \iff [x]_9 = [8]_9.$$

Analog ergibt sich, dass $[3]_{11} \in \mathbb{Z}/11\mathbb{Z}$ eine Einheit ist, und mit $[3]_{11}^{-1} = [4]_{11}$ ergibt sich für alle $x \in \mathbb{Z}$, dass

$$[3]_{11}[x]_{11} = [10]_{11} \iff [4]_{11}[3]_{11}[x]_{11} = [4]_{11}[10]_{11} \iff [x]_{11} = [7]_{11}.$$

Es gilt also die Lösungen $x \in \mathbb{Z}$ des Gleichungssystems

$$\begin{cases} [x]_9 &=& [8]_9\ , \\ [x]_{11} &=& [7]_{11}, \end{cases}$$

zu finden, also die Urbilder von $([8]_9, [7]_{11}) \in (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z})$ bezüglich des Ringhomomorphismus

$$\mathbb{Z} \to (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}), \quad x \mapsto ([x]_9, [x]_{11}).$$

Da 9 und 11 teilerfremd sind, gibt es nach dem chinesischen Restklassensatz einen Ringisomorphismus

$$\varphi\colon \mathbb{Z}/99\mathbb{Z} \to (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}), \quad [x]_{99} \mapsto ([x]_9, [x]_{11}),$$

und da $5 \cdot 9 + (-4) \cdot 11 = 1$ ist φ^{-1} durch

$$\begin{aligned} \varphi^{-1}\colon (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}) &\to \mathbb{Z}/99\mathbb{Z}, \\ ([x]_9, [y]_{11}) &\mapsto [5 \cdot 9 \cdot y + (-4) \cdot 11 \cdot x]_{99} = [55x + 45y]_{99} \end{aligned}$$

gegeben. Der Isomorphismus φ bringt das folgende Diagram zum kommutieren:

$$\begin{array}{ccc} & \mathbb{Z} & \\ {\scriptstyle \pi_{99}}\swarrow & & \searrow{\scriptstyle (\pi_9, \pi_{11})} \\ \mathbb{Z}/99\mathbb{Z} & \xrightarrow{\quad\varphi\quad} & (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}) \end{array} \tag{1}$$

Dabei bezeichnet $\pi_n\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto [x]_n$ für alle $n \in \mathbb{Z}$ die kanonische Projektion. Zusammen mit $\varphi^{-1}([8]_9, [7]_{11}) = [755]_{99} = [62]_{99}$ erhalten wir, dass

$$(\pi_9, \pi_{11})^{-1}([8]_9, [7]_{11}) = \pi_{99}^{-1}\left(\varphi^{-1}([8]_9, [7]_{11})\right) = \pi_{99}^{-1}([62]_{99}) = 62 + 99\mathbb{Z}.$$

Dies ist die gesuchte Lösungsmenge des gegebenen Gleichungssystems.

Bemerkung 2. 1. Aus der Kommutativität der Diagrams (1) ergibt bereits, dass die gesuchte Lösungsmenge von der Form $x_0 + 99\mathbb{Z}$ ist, wobei x_0 eine spezielle Lösung ist. Um eine solche spezielle Lösung zu finden, haben wir die konkrete Berechnung von φ^{-1} genutzt, um $\varphi^{-1}([8]_9, [7]_{11}) = [62]_{99}$ zu bestimmen.

In dem konkreten Beispiel dieser Aufgabe ist es allerdings einfacher, eine spezielle Lösung zu bruteforcen, als φ^{-1} zu berechnen: Möglichen Lösungen der Gleichung $[x]_9 = [8]_9$ sind nämlich

$$8, 17, 26, 35, 44, 53, 62, 71, 80, 89, 98, \dots,$$

und mögliche Lösungen der Gleichung $[x]_{11} = [7]_{11}$ sind

$$7, 18, 29, 40, 51, 62, 73, 84, 95, \dots,$$

woraus sich durch direkten Vergleich die gemeinsame Lösung 62 ergibt.

2. Auf Ähnliche Weise lassen sich auch die Inversen $[4]_9^{-1}$ und $[3]_{11}^{-1}$ schnell durch Bruteforcen bestimmen: Mögliche $z \in \mathbb{Z}$ mit $[z]_9 = [1]_9$ sind

$$1, 10, 19, 28, \dots,$$

wobei 28 ein Vielfaches von 4 ist, nämlich das 7-fache. Folglich ist $[4]_9^{-1} = [7]_9$. Mögliche $z \in \mathbb{Z}$ mit $[z]_{11} = [1]_{11}$ sind

$$1, 12, \dots,$$

wobei 12 ein Vielfaches von 3 ist, nämlich das 4-fache. Folglich ist $[3]_{11}^{-1} = [4]_{11}$.

Für kleine n kann dieses Verfahren zum Bestimmen von Inversen in $\mathbb{Z}/n\mathbb{Z}$ von Hand einfacher und schneller sein als die Maschinerie des euklidischer Algorithmus. (Inbesondere ist weniger Nachdenken und deutlich weniger Verwalten von Zwischenschritten erforderlich).

Aufgabe 6

Wir erinnern an das folgende Resultat aus der Vorlesung:

Lemma 3. Es sei $0 \to M \xrightarrow{f} P \xrightarrow{g} N \to 0$ eine kurze exakte Sequenz von R-Moduln. Sind M und N endlich erzeugt, so ist auch P endlich erzeugt.

M und N sind noethersch $\implies$ P ist noethersch

Wir fixieren einen Untermodul $P' \subseteq P$. Es seien $M' \coloneqq f^{-1}(P')$ und $N' \coloneqq g(P')$, sowie $f' \coloneqq f|_{M'} \colon M' \to P'$, $m \mapsto f(m)$ und $g' \colon g|_{P'} \colon P' \to N'$, $p \mapsto g(p)$. Die Sequenz

$$0 \to M' \xrightarrow{f'} P' \xrightarrow{g'} N' \to 0 \tag{2}$$

ist exakt: Die Injektivität von f' folgt aus der von f, denn Restriktionen von Injektionen sind ebenfalls injektiv. Die Surjektivität von g' ergibt sich aus $\operatorname{im} g' = g'(P') = g(P') = N'$. Die Exaktheit der Sequenz (2) an P' ergibt sich aus

$$\ker g' = P' \cap \ker g = P' \cap \operatorname{im} f = f(f^{-1}(P')) = f(M') = f'(M') = \operatorname{im} f'.$$

Die Untermoduln $M' \subseteq M$ und $N' \subseteq N$ sind endlich erzeugt, da M und N noethersch sind. Zusammen mit der Exaktheit der Sequenz (2) ergibt sich nach Lemma 3, dass auch P' endlich erzeugt ist.