

# Musterlösung Serie 10

## DIOPHANTISCHE GLEICHUNGEN

Eine Gleichung der Form  $ax + by = c$  bei der  $a, b, c$  ganze Zahlen sind und ganzzahlige Lösungen für  $x$  und  $y$  gesucht werden, heisst **lineare diophantische Gleichung**.

34. (a) Zeige, dass die lineare diophantische Gleichung  $ax + by = c$  nur dann eine Lösung haben kann, wenn  $c$  ein Vielfaches ist von  $\text{ggT}(a, b)$ .
- (b) Zeige, dass wenn die lineare diophantische Gleichung  $ax + by = c$  eine Lösung hat, sie immer auch unendlich viele Lösungen hat.

*Lösung:*

- (a) Falls wir auf  $a, b$  den Euklid'schen Algorithmus anwenden, um  $d := \text{ggT}(a, b)$  zu berechnen, dann sehen wir, dass sich  $a$  und  $b$  in eine Summe von Vielfachen von  $d$  zerlegen lässt. Das heisst,  $d$  teilt sowohl  $a$  als auch  $b$  und deshalb auch  $c = ax + by$  für jedes  $x$  und  $y$ .

Bemerkung: Tatsächlich gilt auch die Umkehrung, die man nach Aufgabenstellung nicht hätte zeigen müssen: Wenn  $c$  ein Vielfaches von  $d = \text{ggT}(a, b)$  ist, dann folgt aus Lemma 8.2., dass  $d$  eine Linearkombination von  $a$  und  $b$  ist, das heisst, wir finden ganze Zahlen  $x, y$ , sodass  $ax + by = d$  gilt. Multiplizieren wir nun diese Gleichung mit  $\frac{c}{d}$ , so finden wir eine Lösung für die diophantische Gleichung  $ax + by = c$ .

- (b) Angenommen wir haben ganze Zahlen  $x_0, y_0$ , welche die diophantische Gleichung  $ax_0 + by_0 = c$  lösen, dann sehen wir schnell, dass für jede ganze Zahl  $k$  auch gilt

$$a(x_0 + kb) + b(y_0 - ka) = c.$$

Da  $d := \text{ggT}(a, b)$  wie oben gezeigt  $a$  und  $b$  teilt, gilt sogar

$$a\left(x_0 + k\frac{b}{d}\right) + b\left(y_0 - k\frac{a}{d}\right) = c$$

für jede ganze Zahl  $k$ . Wir wollen nun zusätzlich noch zeigen, dass alle Lösungen  $x, y$ , welche die Gleichung  $ax + by = c$  erfüllen, die obige Form haben. Schreibe  $a = a'd$  und  $b = b'd$ . Wir können nun bei allen Schritten des Euklid'schen Algorithmus für  $a, b$  die Summenterme durch  $d$  teilen und erhalten einen Euklid'schen Algorithmus für  $a', b'$ , wobei offenbar gilt  $\text{ggT}(a', b') = 1$ . Betrachte nun  $ax + by = c$  und subtrahiere davon  $ax_0 + by_0 = c$ . Wir erhalten

$$a(x - x_0) + b(y - y_0) = 0.$$

Subtrahieren wir nun  $b(y - y_0)$  und teilen wir dann durch  $d$ , dann erhalten wir schliesslich

$$a'(x - x_0) = -b'(y - y_0).$$

Das heisst  $a'$  teilt  $b'(y - y_0)$  und  $b'$  teilt  $a'(x - x_0)$ . Da  $\text{ggT}(a', b') = 1$ , folgt mit Lemma 8.3, dass  $a'$  sogar  $y - y_0$  teilt und  $b'$  teilt  $x - x_0$ . Das heisst, es existieren ganze Zahlen  $k, l$ , sodass gilt

$$x - x_0 = kb', \quad y - y_0 = la'.$$

Setzen wir nun  $k, l$  sowie  $x - x_0$  und  $y - y_0$  in

$$a(x - x_0) + b(y - y_0) = 0.$$

ein und teilen durch  $a'b'd$ , dann sehen wir, dass gelten muss  $k = -l$  und die Behauptung folgt.

Bemerkung: Mit analogen Argumenten lässt sich auch zeigen, dass die allgemeine Lösung einer linearen Differentialgleichung der Summe einer partikulären Lösung sowie einer homogenen Lösung entspricht.

35. (a) Finde mit Hilfe eines Näherungsbruches von  $\frac{58}{21}$  eine Lösung der linearen diophantischen Gleichung

$$58x - 21y = 1.$$

- (b) Finde die allgemeine Lösung der linearen diophantischen Gleichung

$$986x + 357y = 51.$$

*Lösung:*

- (a) Aus dem Vorlesungsskript wissen wir, dass  $[2, 1, 3, 5]$  der Kettenbruch von  $\frac{58}{21}$  ist. Wir können nun das folgende Schema des verallgemeinerten Euklid'schen Algorithmus ausfüllen:

$n$	-2	-1	0	1	2	3
$b_n$			2	1	3	5
$P_n$	0	1	2	3	11	58
$Q_n$	1	0	1	1	4	21

Nun wissen wir, dass wir die Zahlen unten rechts im obigen Schema übers Kreuz multiplizieren und die Produkte subtrahieren können, um auf  $-1$  oder  $1$  zu kommen:

$$58 \cdot 4 - 21 \cdot 11 = 1.$$

Das heisst, die Gleichung

$$58x - 21y = 1$$

wird zum Beispiel durch  $x = 4$  und  $y = 11$  gelöst.

- (b) Es gilt  $\frac{986}{357} = \frac{58}{21}$ . Das heisst, wir erhalten eine partikuläre Lösung, wenn wir die Gleichung oben mit den Lösungen  $x = 4$  und  $y = 11$  eingesetzt mit  $17 \cdot 3 = 51$  multiplizieren

$$986(3 \cdot 4) - 357(3 \cdot 11) = 51.$$

Also ist  $x_0 = 12$  und  $y_0 = -33$  eine partikuläre Lösung von  $986x + 357y = 51$ . Da  $\text{ggT}(58, 21) = 1$ , ist

$$\text{ggT}(986, 357) = \text{ggT}(17 \cdot 58, 17 \cdot 21) = 17 \cdot \text{ggT}(58, 21) = 17.$$

Nach Aufgabe 33 (b) sieht die allgemeine Lösung von  $986x + 357y = 51$  für eine ganze Zahl  $k$  wie folgt aus

$$x = 12 + k \frac{357}{17} = 12 + 21k, \quad y = -33 - k \frac{986}{17} = -33 - 58k.$$

36. Drei Schiffbrüchige haben auf einer einsamen Insel während dem ganzen Tag mehr als 4000 Kokosnüsse gesammelt und auf einen grossen Haufen gelegt. Bevor es ans Aufteilen geht, wird es dunkel und sie legen sich erst einmal Schlafen.

In der Nacht wacht einer der Schiffbrüchigen auf und da er seinen Kumpanen nicht traut, beschliesst er, sich seinen Drittel der Kokosnüsse jetzt schon zu sichern. Er verteilt die Kokosnüsse gleichmässig auf drei Haufen. Dabei bleibt eine Kokosnuss übrig, die er wegwirft. Darauf trägt er seinen Haufen beiseite, schiebt die restlichen beiden Haufen zusammen und legt sich wieder hin.

Bald darauf wacht der zweite Schiffbrüchige auf. Auch er möchte sich seinen Anteil sichern und verfährt mit dem Resthaufen wie der Erste. Auch bei ihm bleibt nach dem Teilen eine Kokosnuss übrig, die er wegwirft. Als auch der dritte Schiffbrüchige aufwacht, verfährt er mit dem Resthaufen wie die ersten beiden, und auch bei ihm bleibt nach dem Teilen eine Kokosnuss übrig, die er wegwirft.

Am nächsten Morgen gehen die drei Schiffbrüchigen zu dem, in der Nacht geschrumpften, Haufen und teilen die Kokosnüsse gleichmässig unter sich auf. Dabei bleibt eine Kokosnuss übrig, die sie wegwerfen.

Wie viele Kokosnüsse befanden sich zu Beginn *mindestens* auf dem Haufen?

*Lösung:* Sei  $x$  die Anzahl Kokosnüsse, dann soll  $x \geq 4000$  minimal sein, sodass

$$\frac{2^2 \frac{2^{\frac{x-1}{3}-1} - 1}{3} - 1}{3} = \frac{2^3 x - 2^3 - 2^2 \cdot 3 - 2 \cdot 3^2 - 3^3}{81} = \frac{8x - 65}{81}$$

eine natürliche Zahl ist. Das heisst, dass  $x$  die kleinste ganzzahlige Lösung der linearen diophantischen Gleichung

$$8x - 81y = 65$$

sein muss, sodass  $x \geq 4000$  gilt. Offenbar ist  $8 \cdot (-10) - 81 \cdot (-1) = 1$ . Da der grösste gemeinsame Teiler von 8 und 81 diese beiden Zahlen teilen muss, muss er auch 1 teilen, also muss gelten  $\text{ggT}(8, 81) = 1$ . Nun können wir eine partikuläre Lösung von  $8x - 81y = 65$  wie folgt finden: Wir multiplizieren die partikuläre Lösung der Gleichung  $8x - 81y = 1$  mit 65 und erhalten  $x_0 = 65 \cdot (-10) = -650$  sowie  $y_0 = 65 \cdot (-1) = -65$ . Die allgemeine Lösung der diophantischen Gleichung  $8x - 81y = 65$  (siehe Aufgabe 33 (b)) ist somit

$$x = -650 + 81k \quad y = -65 + 8k$$

für jedes ganze  $k$ . Gesucht ist also eine ganze Zahl  $k$ , sodass  $x = -650 + 81k \geq 4000$  minimal ist. Durch einsetzen findet man heraus, dass dies der Fall ist für  $k = 58$ , wobei dann  $x = 4048$  ist.

37.  $(\mathbb{Q}[X], 0, 1, +, \cdot)$  sei der Ring der Polynome mit rationalen Koeffizienten (vergleiche mit Aufgabe 11). Seien  $f, g \in \mathbb{Q}[X]$  die Polynome

$$f = X^3 + X + 1 \quad \text{und} \quad g = X^2 + 2.$$

Finde zwei Polynome  $h_0, h_1 \in \mathbb{Q}[X]$  sodass gilt:

$$h_0 \cdot f - h_1 \cdot g = X^2 - 1$$

*Hinweis:* Es ist  $\text{ggT}(f, g) = 1$ ; verwende den verallgemeinerten Euklid'schen Algorithmus um  $\tilde{h}_0$  und  $\tilde{h}_1$  zu finden mit  $\tilde{h}_0 \cdot f - \tilde{h}_1 \cdot g = 1$ .

*Lösung:* Wir möchten gerne den verallgemeinerten Euklid'schen Algorithmus anwenden. Deshalb müssen wir zuerst die Koeffizienten  $b_n$  berechnen

$$X^3 + X + 1 = X \cdot (X^2 + 2) + (-X + 1)$$

$$X^2 + 2 = (-X - 1)(-X + 1) + 3$$

$$-X - 1 = \left(-\frac{1}{3}X + \frac{1}{3}\right) \cdot 3.$$

Wir können nun die Tabelle unten ausfüllen wie im Vorlesungsskript beschrieben:

$n$	-2	-1	0	1	2
$b_n$			$X$	$-X - 1$	$-\frac{1}{3}X + \frac{1}{3}$
$P_n$	<b>0</b>	<b>1</b>	$X$	$-X^2 - X + 1$	$\frac{1}{3}(X^3 + X + 1)$
$Q_n$	<b>1</b>	<b>0</b>	1	$-X - 1$	$\frac{1}{3}(X^2 + 2)$

Offenbar gilt nun

$$(-X - 1) \frac{1}{3}(X^3 + X + 1) - (-X^2 - X + 1) \frac{1}{3}(X^2 + 2) = -1,$$

also können wir  $\tilde{h}_0 := \frac{1}{3}(X + 1)$  und  $\tilde{h}_1 := \frac{1}{3}(X^2 + X - 1)$  setzen. Dann haben wir  $\tilde{h}_0 \cdot f - \tilde{h}_1 \cdot g = 1$ . Setzen wir weiter

$$h_0 := \tilde{h}_0 (X^2 - 1) = \frac{1}{3}(X^3 + X^2 - X - 1)$$

$$h_1 := \tilde{h}_1 (X^2 - 1) = \frac{1}{3}(X^4 + X^3 - 2X^2 - X + 1),$$

dann gilt

$$h_0 \cdot f - h_1 \cdot g = X^2 - 1.$$