2. Diophantische Gleichungen

[Teschl05, S. 91f]

2.1. Was ist eine diophantische Gleichung und wozu braucht man sie?

Def D2-1: Eine **diophantische Gleichung** ist eine Polynomfunktion in x,y,z,… , bei der als Lösungen nur ganze Zahlen erlaubt sind:

$$ax^{n_1}y^{m_1}z^{p_1} + bx^{n_2}y^{m_2}z^{p_2} + \ldots = d$$

mit nicht-negativen Potenzen $n_i,m_i,p_i \in \mathbf{N_0}$ und ganzzahligen Koeffizienten $a,b,d \in \mathbf{Z}$.

Eine **lineare diophantische Gleichung** enthält in jedem Term nur eine der Variablen in der ersten (linearen) Potenz:

$$ax + by + cz + \ldots = d$$

Beispiele:

- Fermat'sche Zahlentripel: $x^n + y^n = z^n$ für geg. $n \in N$ mit gesuchten Lösungen $x,y,z \in Z$. (Fermatsche Vermutung: Es gibt keine ganzzahlige Lösung für n>2. Bewiesen 1993 von Wiles & Taylor). Für n=2 gibt es unendlich viele Lösungen, die sog. pythagoräischen Zahlentripel.
- Die lineare diophantische Gl. 3x+4y=1 hat als ganzzahlige Lösung z.B. (x,y)=(3,-2).

Anti-Beispiele:

- sin(x)=1 (keine Polynomfunktion),
- 3.4x+2.5y=3 (keine ganzzahligen Koeffizienten)

Wozu braucht man diophantische Gleichungen?

- **Produktionsplanung**: Wenn ich 10000 Einheiten eines Rohstoffes habe und meine Produkte X und Y je Einheit 75 bzw. 38 Rohstoffeinheiten verbrauchen, wieviele von welchen Produkten muss ich herstellen, um die Rohstoffmenge genau aufzubrauchen? Gesucht ist eine Lösung der diophantischen Gleichung

  $$75x + 38y = 10000$$

  mit der zusätzlichen Anforderung, dass x und y **nichtnegativ** sein müssen. Wir werden hierzu in Kap. 2.2 eine Lösung entwickeln.

- Das **Briefmarkenproblem**:

  1. Kann ich mit 5c- und 2c-Briefmarken JEDES Porto >3c darstellen?
  2. Wieviele Arten gibt es, einen Brief mit Porto Z mit 5c-, 3c- und 2c-Briefmarken zu bekleben?

- Berechnung des **multiplikativen Inversen** zu a modulo m, das beim **RSA-Algorithmus** gebraucht wird: Welches $x \in \mathbf{Z}$ erfüllt

  $$ax = 1 \pmod m$$

  ? Die Antwort kann auch so formuliert werden: x ist genau dann das multiplikative Inverse zu a modulo m, wenn ein $y \in \mathbf{Z}$ existiert, so dass

  $ax = 1 - my$ (Die Zahl ax ist ein Vielfaches von m von der Zahl 1 entfernt)

  $ax + my = 1$ (lineare diophantische Gleichung mit b=m und d=1)

2.2. Wie löst man diophantische Gleichungen?

Wir betrachten im Folgenden nur **lineare** diophantische Gleichungen, die für die Anwendung die größte Rolle spielen.

Satz S2-1: Lösbarkeit einer diophantischen Gleichung (Existenz)

Eine lineare diophantische Gleichung

$$ax + by = c$$

für $a,b \in \mathbf{Z}$ besitzt genau dann ganzzahlige Lösungen $x,y \in \mathbf{Z}$, wenn

$$c = n \cdot ggT(a,b)$$

wenn also c ein ganzzahliges Vielfaches des größten gemeinsamen Teilers von a und b ist.

Beweis: Wir können den Beweis in drei Fälle zerlegen:

Fall 1: **c ist kein Vielfaches von ggT(a,b)**: Es kann keine Lösung geben, denn die linke Seite ist wg. a = a'·ggT(a,b) und b = b'·ggT(a,b) bei ganzzahligem x und y sicher ein Vielfaches von ggT(a,b).

Fall 2: **c = ggT(a,b)**: Der Algorithmus ErweiterterEuklid (Satz S1-8) liefert zumindest eine ganzzahlige Lösung (x,y).

Fall 3: **c ist Vielfaches von ggT(a,b)**: Wenn c = k·ggT(a,b), dann können wir für

$$ax+by = ggT(a,b)$$

mit Algo Erweiterter Euklid eine Lösung (x',y') ermitteln. Multiplizieren mit k liefert

$$a\cdot kx' + b\cdot ky' = k\cdot ggT(a,b) = c$$

also ist (x,y) = (kx', ky') eine Lösung der linearen diophantischen Gleichung, q.e.d.

Folgerung: Wenn a und b teilerfremd sind (gilt sicher für Primzahlen a,b, aber auch für Zahlen a=6, b=7), dann ist ggT(a,b)=1, mithin ist die lin. diophantische Gleichung **für alle** $c \in \mathbf{Z}$ lösbar.

Für den Fall 2 können wir eine Lösung mittels Satz S1-8 ermitteln. Alternativ geben wir hier noch eine andere, logisch äquivalente, aber nichtrekursive Variante des Algorithmus Erweiterter Euklid an:

Sei o.B.d.A. $a \le b$. Startend mit Zahlen $r_0=a$ und $r_1=b$ finden wir die Zahlen q_{k+1} und r_{k+2} derart, dass

$$r_k = q_{k+1}\, r_{k+1} + r_{k+2}$$

gilt. r_{k+2} ist also nichts anderes als der Rest r_k mod r_{k+1} und q_{k+1} = floor(r_k/r_{k+1}). Der Algorithmus terminiert, wenn $r_{k+2}=0$ ist. Das r_{k+1} ist dann der ggT(a,b). Mit dem jeweiligen q_{k+1} können wir eine Berechnung für x_k und y_k fortsetzen. Die konkreten Gleichungen stehen in der untenstehenden Tabelle, wir zeigen es gleich an einem konkreten Beispiel

$$5x + 3y = 1$$

	$r_0 = a$	$r_1 = b$		$x_0=1$	$y_0=0$
	$r_0 = 5$	$r_1 = 3$		$x_1=0$	$y_1=1$

k	$r_k = q_{k+1}\, r_{k+1} + r_{k+2}$	r_{k+1}	q_{k+1}	$x_{k+2}=x_k - q_{k+1}\, x_{k+1}$	$y_{k+2}=y_k - q_{k+1}\, y_{k+1}$
0	5 = 1·3 + 2	3	1	1	-1
1	3 = 1·2 + 1	2	1	**-1**	**2**
2	2 = 2·1 + 0	0	2		

Hier ging in der Zeile k=2 die Division r_k erstmalig ohne Rest auf. In der Zeile davor – hier also bei k=1 – können wir in der x- und y-Spalte die Lösung (x,y) = (-1,2) ablesen:

$$5\cdot(-1) + 3\cdot 2 = 1$$

ist eine zutreffende Aussage.

Satz S2-2: Alle Lösungen einer diophantischen Gleichung (Vollständigkeit)

Sei (x,y) eine spezielle Lösung der linearen diophantischen Gleichung

(§) $ax + by = n\cdot ggT(a,b)$

für $a,b \in \mathbf{Z}$, die nach Satz S2-1 existiert und mit dem Algorithmus Erweiterter Euklid (Satz S1-8) ermittelt werden kann. Dann haben alle weiteren ganzzahligen Lösungen $(\tilde{x},\tilde{y})$ von (§) die Form

$$\tilde{x} = x + \frac{kb}{ggT(a,b)}, \qquad \tilde{y} = y - \frac{ka}{ggT(a,b)}$$

worin $k \in \mathbf{Z}$ eine beliebige ganze Zahl ist.

Beweis in Vorlesung.

Wir haben nun alles beisammen, um unsere Aufgabe Produktionsplanung aus der Einleitung zu lösen: Gegeben:

$$ax+by = c = n\cdot ggT(a,b)$$

Welche nichtnegativen, ganzzahligen Paare (x,y) lösen diese Gleichung?

Lösungsweg:

1. Mit Algorithmus Erweiterter Euklid bestimmt man spezielle Lösung (x_s,y_s) zu
   $$ax+by = ggT(a,b)$$

2. Wenn c = n·ggT(a,b), d.h. die rechte Seite ist ein Vielfaches von ggT(a,b), dann ist (x,y) = ($n\cdot x_s$, $n\cdot y_s$) eine spezielle Lösung zu ax+by=c

3. Jede weitere Lösung $(\tilde{x},\tilde{y})$ zu ax+by=c erfüllt nach Satz S2-2

$$\tilde{x} = x + \frac{kb}{ggT(a,b)}, \qquad \tilde{y} = y - \frac{ka}{ggT(a,b)} \qquad \text{mit} \quad k \in Z$$

Man versucht dann, solche k zu finden, die $(\tilde{x},\tilde{y})$ nicht negativ werden lassen (zwei einfache Ungleichungen).

Beispiel: Welches nichtnegative, ganzzahlige Paar (x,y) erfüllt

$$75x + 38y = 10000 \quad ?$$

Lösung: Zunächst stellen wir fest, ob 10000 ein Vielfaches von ggT(75,38)=ggT(3·5·5,2·19) ist. Da beide Zahlen teilerfremd sind, also ggT(75,38)=1, ist dies gegeben.

1. Mit Algorithmus Erweiterter Euklid löst man

   75x + 38y = 1:

	r_0 = 75	r_1 = 38		x_0=1	y_0=0
				x_1=0	y_1=1
k	**$r_k = q_{k+1}\, r_{k+1} + r_{k+2}$**	**r_{k+1}**	**q_{k+1}**	**$x_{k+2}=x_k - q_{k+1}\, x_{k+1}$**	**$y_{k+2}=y_k - q_{k+1}\, y_{k+1}$**
0	75 = 1·38 + 37	38	1	1	-1
1	38 = 1·37 + 1	1	1	**-1**	**2**
2	37 = 37·1 + 0	0	37		

   und man rechnet nach:

   75·(-1) + 38·2 = 1

   also stimmt die Probe, (x_s,y_s)=(-1,2) ist eine Lösung der ggT-Gleichung.

2. Dann ist (x,y) = (-10 000, 20 000) eine spezielle Lösung der Produktionsgleichung.

3. Für nichtnegative Lösungen stellt Satz S2-2 zwei Forderungen an $k \in \mathbf{Z}$ auf:

$$\tilde{x} = -10000 + \frac{k\cdot 38}{1} \geq 0, \qquad \tilde{y} = 20000 - \frac{k\cdot 75}{1} \geq 0$$

$$\Rightarrow \quad k \geq \frac{10000}{38} = 263.15, \qquad \frac{20000}{75} = 266.66 \geq k$$

4. Es kommen also die ganzen Zahlen k = 264, 265, 266 in Betracht. Dies führt auf die Lösungen:
   $(\tilde{x}_1, \tilde{y}_1) = (32{,}200)$ und $(\tilde{x}_2, \tilde{y}_2) = (70{,}125)$ und $(\tilde{x}_3, \tilde{y}_3) = (108{,}50)$

Übung: Gibt es nichtnegative ganze Zahlen, die die Gleichung

$5x+3y=17$

lösen? Auch wenn man hier eine Lösung schnell durch Probieren finden kann, lösen Sie die diophantische Gleichung nach dem oben beschriebenen Verfahren.

Weitere Übungen