# KAP 2

# DER EUKLIDISCHE ALGORITHMUS

## 2.1 Diophantische Gleichungen (1)

Wir beginnen mit einem (klassischen) Beispiel: Ein Bauer bekommt die Aufgabe, auf dem Markt für 1000 Taler Ferkel, Enten und Tauben zu kaufen; und zwar genau 1000 Tiere. Ein Ferkel kostet 10 Taler, eine Ente 3 Taler und eine Taube einen halben Taler. Bestimme alle Möglichkeiten - natürlich sollen die Tier lebendig und vollständig sein.

Mit Einführung der Variablen f, e und t erhalten wir das folgende mathematische Modell:

$$\begin{array}{l} 10f+3e+0{,}5t=1000 \quad |\cdot 2 \\ \underline{\;\;f+\;\;e+\;\;\;t=1000\;\;} \\ 19f+5e\qquad\;\; =1000 \end{array} \qquad (*)$$

Wir suchen nun alle ganzzahligen positive Lösungen dieser Gleichung (*). Gleichungen, deren Lösungen man nur in Z sucht, heißen nach dem griechischen Mathematiker *Diophant* (3. Jh. nach Chr.) „*diophantische Gleichungen*“ (hier speziell lineare diophantische Gleichungen). Wir stellen hier ein erstes Verfahren vor, solche Gleichungen zu lösen. Zur Unterscheidung von späteren Verfahren sprechen wir vom D-Algorithmus (auch Eulersches Reduktionsverfahren).

Der Trick besteht darin, die Gleichung immer wieder nach dem Glied mit dem kleinsten Koeffizienten aufzulösen:

$$(*) \quad \Leftrightarrow \quad e = \frac{1000-19f}{5} = 200-3f-\frac{4}{5}f \qquad (**)$$

Damit e ganzzahlig ist, muss f Vielfaches von 5 sein. Wir setzen also f=5k.

und setzen dies in (**) ein: e=200-15k-4k=200-19k

Diese Gleichung macht es aber nun einfach, alle Lösungen des Problems zu überschauen:

| **k** | **1** | **2** | **3** | **4** | **5** | **....** | **10** |
|---|---|---|---|---|---|---|---|
| **f** | 5 | 10 | 15 | 20 | 25 | .... | 50 |
| **e** | 181 | 162 | 143 | 124 | 105 | .... | 10 |
| **t** | 814 | 828 | 842 | 856 | 870 | .... | 940 |

Es gibt also 10 korrekte Lösungen des Problems!

***AUFGABE 2.1*** Löse das Marktproblem für 100 Taler und 100 Tiere (dieselben Preise).

***AUFGABE 2.2*** Löse in Z und gib jeweils drei Lösungen an:
a) 29x-13y=17 b) 187x-104y=41 c) 47x+24y=79
d) 111x+5y=433 e) 67x-33y=547 f) 401x+101y=-301

Übrigens sind nicht alle linearen diophantischen Gleichungen lösbar! Ein Lösbarkeitskriterium wird in 2.3 erarbeitet.

Einen ganz anderen Zugang zum Problem erhält man, wenn man die Gleichung (*) als Gerade interpretiert.

g: $e=-\frac{19}{5}f+200$ - gesucht alle Punkte $P\in Z^2$ mit $P\in g$.

Einfacher erkennt man die linearen Funktionen, wenn man e in y und f in x umbenennt. Dann wird die Gleichung zu g: $y=-\frac{19}{5}x+200$

Ist $P_0(x_0|y_0)$ ein Punkt von g, so liegen sicher auch alle Punkte $P_k(x_0-5k|y_0+19k)$ auf g, denn
$-\frac{19}{5}\cdot(x_0-5k)+200=-\frac{19}{5}x_0+19k+200=(-\frac{19}{5}x_0+200)+19k=y_0+19k$ (Steigungsdreieck: Man geht von einem Gitterpunkt um 5 Einheiten nach links und um 19 Einheiten nach oben.). Andererseits ist mit $k\in Z$ auch $P_k\in Z^2$, so daß sich das Problem darauf reduziert, eine einzige konkrete Lösung von (*) anzugeben. Diese findet man aber sicherlich mit f=5 und damit e=181. Auf diese Art erhält man die Lösungsmenge also mit den Paaren $(5-5k|181+19k)$ für $k\in Z$. Für k=0, -1, -2,..., -9 erhält man so ebenfalls die Lösungen aus der oben angegebenen Tabelle.

***AUFGABE 2.3*** Versuche, die Aufgabe 2.2 mit diesem Verfahren zu lösen.

Schwieriger wird's, wenn man es mit mehr Variablen zu tun hat. Starten wir auch hier mit einem Beispiel:

2x+3y+4z=9 soll in ganzen Zahlen gelöst werden. Wir lösen auf:

(1) $x=-y-2z+4+\frac{-y+1}{2}$ und setzen $x_1:=\frac{-y+1}{2}$ $\Leftrightarrow$ $y=-2x_1+1$

Dies liefert für alle $x_1\in Z$ ganzzahlige y. Wir ersetzen wieder $x_1$ durch k und erhalten:
y=-2k+1 in (1): x=3k-2z+3 und damit die zweiparametrige Lösungsmenge:
$L=\{(x|y|z)|x=3k-2z+3 \text{ und } y=-2k+1 \text{ und } z\in Z\}$ . Einige Lösungen

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **k** | 0 | 0 | 0 | 1 | 1 | 7 | -5 |
| **z** | 0 | 1 | -1 | 0 | 1 | -5 | 3 |
| **x** | 3 | 1 | 5 | 6 | 4 | 34 | -18 |
| **y** | 1 | 1 | 1 | -1 | -1 | 13 | 11 |

***AUFGABE 2.4*** Löse die folgenden linearen diophantischen Gleichungen allgemein und gib jeweils 5 verschiedenen Lösungen an:
a) $3x-\frac{1}{2}y+\frac{1}{3}z=26$ b) 135x-22y+89z=100 c) 12x-5y+7z=1

***AUFGABE 2.5*** a) Bestimme Zahlen x und y mit: $\frac{x}{11}+\frac{y}{13}=\frac{1}{11\cdot 13}$

(ebenso: $\frac{x}{28}+\frac{y}{33}=\frac{1}{28\cdot 33}$)

b) Ein Betrieb kauft in unterschiedlicher Stückzahl drei verschiedene Einzelteile, die 52 DM, 29 DM bzw. 3 DM kosten. Es wurden insgesamt 100 Einzelteile gekauft, die Gesamtkosten betrugen 2500 DM. Wieviel Stücke wurden von jedem Teil gekauft.

## 2.2 DER EUKLIDISCHE ALGORITHMUS

Der „*Euklidische Algorithmus*“ (EA) ist ein Verfahren zur Bestimmung des ggT zweier Zahlen, welches schon Euklid vor 2200 Jahren in seinem bekannten Mathematikwerk beschreibt. Dieses Rechtsverfahren erwies sich als sehr tiefgehend und praktisch. Beginnen wir wieder mit einem Beispiel:

| | |
|---|---|
| gesucht sei ggT(969,627) | 969=1·627+342 |
| | 627=1·342+285 |
| | 342=1·285+57 |
| | 285=5·57+0 |
| Damit ist man fertig: | ggT(969,627)=57 |

Warum funktioniert dieses Verfahren? Worauf beruht es? Eigentlich ist dafür nur eine einfache, bereits bekannte Regel verantwortlich:
(T6) $a|b$ und $a|b\pm c \Rightarrow a|c$ (Kapitel 1; Satz 1.1 (T6))
Ist nun d der ggT von 969 und 627=969−342, so ist d nach (T6) auch ein Teiler von 342. Da aber d schon der größte gemeinsame Teiler von 969 und 627 ist, muß er auch der größte gemeinsame Teiler von 627 und 342 sein. Mit demselben Schluß ist dann aber d auch der ggT Teiler von 285, da ja d gemeinsamer Teiler von 627 und 342 ist. So schließt man weiter, bis der Rest r 0 wird (was ja notwendig einmal eintreten muß). d muß also auch ein gemeinsamer Teiler von 57 und 0 sein. Welches ist aber der größte gemeinsame Teiler von 57 und 0 - natürlich 57. Also ist rückwärts geschlossen 57 auch der größte gemeinsame Teiler von 969 und 627.

Es gilt also ggT(a,b)=ggT(a-b,b).
Wenden wir auf den Ausdruck rechts dieselbe Regel an, so ergibt sich
ggT(a-b,b)=ggT((a-b)-b),b)=ggT(((a-b)-b)-b,b)=...=ggT(r,b),
wobei r der Rest von a bei Division durch b ist ($a=k\cdot b+r$ mit $0\le r<b$). Wir können als auch direkt schreiben ggT(a,b)=ggT(a-k·b,b)=ggT(r,b)=ggT(b,r)

Beschreiben wir nun den EA noch einmal allgemein:

gesucht ggT(a,b):
$a=k_1\cdot b+r_1 \quad ,r_1<b$
$b=k_2\cdot r_1+r_2 \quad ,r_2<r_1$
$r_1=k_3\cdot r_2+r_3 \quad ,r_3<r_2$
.....
$r_{n-2}=k_n\cdot r_{n-1}+r_n \quad ,r_n<r_{n-1}$
$r_{n-1}=k_{n+1}\cdot r_n+0 \quad \Rightarrow \ ggT(a,b)=r_n$

Dieses Verfahren ist endlich, da die Zahlen a, b, $r_1$ usw. immer kleiner werden.

Und noch ein Beispiel: ggT(130900,33957):

130900=3·33957+29029
33957=1·29029+4928
29029=5·4928+4389
4928=1·4389+539
4389=8·539+77
539=7·77+0 ⇒ ggT(130900,33957)=77

Übrigens gibt es eine merkwürdige Abschätzung für die Anzahl der Schritte beim EA: Ist b die kleinere der beiden Zahlen, so ist die Anzahl der Schritte immer kleiner als das Fünffache der Anzahl der Ziffern von b. Vergleiche dies mal bei den folgenden Aufgaben

***AUFGABE 2.6*** Berechne den ggT der folgenden Zahlen mit dem EA:
a) 3059; 646 b) 4081; 2585 c) 2112; 836 d) 1597; 987

Ein für uns sehr wichtiges Ergebnis liefert der folgende Satz 2.1. Vorher wollen wir aber noch eine Bezeichnung einführen, die der Vektoralgebra entlehnt ist: Sind x und y zwei Zahlen oder Variable, so heißt rx+sy eine „*Linearkombination*“ von x und y.

**SATZ 2.1** (Lemma von Bachet)
Ist d=ggT(a,b), so gibt es $k,l\in Z$ mit ka+lb=d.

Beweis: Zum Beweis benutzen wir :
Sind sa+tb=c und ua+vb=d zwei Linearkombinationen von a und b, so ist auch die Summe c+d=(s+u)a+(t+v)b wieder eine Linearkombination von a und b. Beginnen wir nun mit
a=1·a+0·b und
b=0·a+1·b und wenden auf die linke Seite den EA an, so endet dieser mit dem ggT(a,b), während rechts eine Linearkombination von a und b steht.

Wir demonstrieren dies am ersten Beispiel:

969= 1·627+342
627= 1.342+285
342= 1·285+57
285=5·57+0

969= 1·969+0·627
627= 0·969+1·627
342= 1·969- 1·627
285=-1·969+2·627
57= 2·969- 3·627

Damit haben wir zwei Zahlen k und l gefunden mit k·969+l·627=ggT(969,627).

Als weiteres Beispiel führen wir das zweite von oben an:

130900= 1·130900+0·33957
33957= 0·130900+1·33957 |·3
29029= 1·130900- 3·33957
4928=-1·130900+4·33957 |·5
4389= 6·130900-23·33957
539=-7·130900+27·33957 |·8
77=62·130900-239·33957 Der nächste Schritt führt auf
0=..... , also ist der EA beendet.

Wir haben also die Zahlen k=62 und l=-239 gefunden, mit denen gilt
k·130900+l·33957=ggT(130900,33957)=77

Eine Formalisierung dieses Verfahrens ist unter dem Namen Berlekamp-Algorithmus (BA) bekannt.

Wir definieren vier Folgen $a_n$, $x_n$, $y_n$ und $q_n$ nach folgendem Schema ([r] bedeutet im Folgenden die sogenannte Gaußklammer, also den ganzzahligen Anteil von r):

| | | | |
|---|---|---|---|
| $a_1=a$ | $x_1=1$ | $y_1=0$ | $q_1=0$ |
| $a_2=b$ | $x_2=0$ | $y_2=1$ | $q_2=[a_1/a_2]$ |
| $a_3=a_1-q_2\cdot a_2$ | $x_3=x_1-q_2\cdot x_2$ | $y_3=y_1-q_2\cdot y_2$ | $q_3=[a_2/a_3]$ |
| ..... | ..... | ..... | ..... |
| $a_{i+1}=a_{i-1}-q_i\cdot a_i$ | $x_{i+1}=x_{i-1}-q_i\cdot x_i$ | $y_{i+1}=y_{i-1}-q_i\cdot y_i$ | $q_{i+1}=[a_i/a_{i+1}]$ für i>2 |

bis $a_k\neq 0$ und $a_{k+1}=0$.

Beispiele: a=91; b=56

| i | $a_i$ | $x_i$ | $y_i$ | $q_i$ |
|---|---|---|---|---|
| **1** | 91 | 1 | 0 | 0 |
| **2** | 56 | 0 | 1 | 1 |
| **3** | 35 | 1 | -1 | 1 |
| **4** | 21 | -1 | 2 | 1 |
| **5** | 14 | 2 | -3 | 1 |
| **6** | 7 | -3 | 5 | 2 |
| **7** | 0 | - | - | - |

also: -3·91+5·56=7=ggT(891,56)

a=9111, b=47

| i | $a_i$ | $x_i$ | $y_i$ | $q_i$ |
|---|---|---|---|---|
| **1** | 9111 | 1 | 0 | 0 |
| **2** | 47 | 0 | 1 | 193 |
| **3** | 40 | 1 | -193 | 1 |
| **4** | 7 | -1 | 194 | 5 |
| **5** | 5 | 6 | -1163 | 1 |
| **6** | 2 | -7 | 1357 | 2 |
| **7** | 1 | 20 | -3877 | 2 |
| **8** | 0 | - | - | - |

also:20·9111-3877·47=1=ggT(9111,47)

***AUFGABE 2.7*** Bestimme mit dem Berlekamp-Algorithmus die Zahlen k und l in k·a+l·b=ggT(a,b):

a) a=286, b=121 b) a=9111, b=47 c) a=391, b=153
d) a=235, b= 3567 e) a=257, b=267 f) a=322, b=199
g) a=7989, b=1233 h) a=567, b=568

***AUFGABE 2.8*** Zeige, daß man in Satz 2.1 k durch k+rb ersetzen kann, wenn man gleichzeitig l durch l-ra ersetzt. Gib dann zu jeder der Aufgaben aus Aufgabe 2.7 drei neue Lösungen an.

***AUFGABE 2.9*** Zeige, daß man jede ganze Zahl c als Linearkombination von teilerfremden Zahlen a und b angeben kann.
Löse dieses Problem speziell für a=7, b=11 und c=15 sowie für a=33, b= 29 und c=100.

# 2.3 DIOPHANTISCHE GLEICHUNGEN (2)

Gut vorbereitet können wir nun wieder das Problem der (linearen) Diohantischen Gleichungen ax+by=c angehen. Wir wollen zunächst einmal den Fall c=1 behandeln.

(I) ax+by=1 (*)

Wie man leicht einsieht, ist ax+by=1 nur dann lösbar, wenn a und b teilerfremd sind. Ist nämlich doch t>1 ein gemeinsamer Teiler von a und b, so gilt z.B. a=t·A und b=t·B, also ax+by=t(Ax+By)=1. Dann steht links ein Produkt ganzer Zahlen, bei dem zumindest der Faktor t>1 ist; das Produkt kann also nie 1 werden. Wir können also im Weiteren von teilerfremden Zahlen a und b ausgehen. Dann ist ggT(a,b)=1. Wir finden also mindestens eine Lösung von (*) mit dem Berlekamp-Algorithmus. Diese Lösung sei $(x_0|y_0)$. Dann sind auch $(x_0+kb|y_0-ka)$, $k\in Z$, Lösungen von (*) (Überprüfen durch Nachrechnen!). Das sind aber auch schon alle ganzzahligen Lösungen von (*). Denn ist $(x_1|y_1)$ irgendeine Lösung von (*), so gilt (1) $ax_1+by_1=1$ und (2) $ax_0+by_0=1$. Subtrahieren dieser beiden Gleichungen liefert: $a(x_0-x_1)+b(y_0-y_1)=0$, also $\frac{x_1-x_0}{y_0-y_1}=\frac{b}{a}$. Da rechts ein gekürzter Bruch steht, muß gelten $x_1-x_0=kb$ und $y_0-y_1=ka$, was aber auf $x_1=x_0+kb$ und $y_1=y_0-ka$ führt. Also ist die Lösung $(x_1|y_1)$ von der angegebenen Art.

Beispiel: 47x-33y=1 Der Berlekamp-Algorithmus liefert

| i | $a_i$ | $x_i$ | $y_i$ | $q_i$ |
|---|---|---|---|---|
| **1** | 47 | 1 | 0 | 0 |
| **2** | 33 | 0 | 1 | 1 |
| **3** | 14 | 1 | -1 | 2 |
| **4** | 5 | -2 | 3 | 2 |
| **5** | 4 | 5 | -7 | 1 |
| **6** | 1 | -7 | 10 | 4 |
| **7** | 0 | - | - | - |

Damit haben wir eine spezielle Lösung mit $x_0=-7$ und $y_0=-10$. Alle Lösungen finden wir also durch x=–7+k·(-33) und y=–10–k·47, also z.B.

| k | -2 | -1 | 1 | 2 |
|---|---|---|---|---|
| x | 59 | 26 | -40 | -73 |
| y | 84 | 37 | -57 | -104 |

(II) ax+by=c

Dieser Fall ist schnell erledigt, wenn wie oben die Zahlen a und b teilerfremd sind. Bleiben wir bei dem Beispiel 47x-33y=5. Wir haben die spezielle Lösung (-7|-10) gefunden. Wenn aber 47·(-7)-33(-10)=1 ist , so muß man mit dem 5-fachen der Lösungen, also mit (-35|-50) ja 5 erhalten. Probe: 47(-35)-33(-50)=5. Die anderen Lösungen der Gleichung erhält man wie oben durch x=-35+k(-33) und y=-50-k·47, wie man durch Einsetzen leicht nachprüft:
47(-35-33k)-33(-50-47k)=47·(-35)-33·47k+33·50+33·47k=47·(-35)-33·(-50)=5.

*Wir fassen zusammen: Gilt ggT(a,b)=1, so findet man alle Lösungen der Gleichung ax+by=c durch $x_r=x_0+r\cdot b$ und $y_r=y_0-r\cdot a$. Dabei ist $x_0=c\cdot x^*$ und $y_0=c\cdot y^*$. $x^*$ und $y^*$ sind spezielle Lösungen der Gleichung ax+by=1, die man z.B. mit dem Berlekamp-Algorithmus erhält.*

Wir geben ein Beispiel an:
151x+118y=60 liefert mit dem BA die Lösungen $x^*=-25$ und $y^*=32$. Damit ist $x_0=-1500$ und $y_0=1920$, was auf $x_r=-1500+r\cdot 118$ und $y_r=1920-r\cdot 151$ führt. Damit könnte man zufrieden sein, jedoch hat man als Anfangslösungen lieber „in der Nähe“ von Null liegende Zahlen. Wir berechnen deshalb 1500 DIV 118=12 und ersetzen r in beiden Lösungen durch 12+k:

$x_k=-1500+(12+k)\cdot 118=-84+118k$ und $y_k=1920-(12+k)\cdot 151=108-151k$

***AUFGABE 2.10*** Löse die folgenden diophantischen Gleichungen. Gib jeweils 3 Lösungen an:
a) 17x-21y=22 b) 55x+91y=100 c) 100x-99y=81
d) -35x-17y=99 e) 234x+457y=23
f) 1234x+2345y=3456 g) -455x-223y=1000

Wir kommen nun zur Gleichung

(*) ax+by=c mit $g=ggT(a,b)\neq 1$.

Klammert man g aus, so erkennt man aus $g(Ax+By)=c \Leftrightarrow Ax+By=c/g$, daß die Gleichung in Z nur dann lösbar ist, wenn auch c durch g teilbar ist. Dann ist aber die Gleichung ax+by=c äquivalent zu der Gleichung

(**) Ax+By=C,

die man erhält, wenn man die Ausgangsgleichung durch g teilt. Da g der ggT von a und b ist, gilt ggT(A,B)=1. Aus dem letzten Abschnitt wissen wir aber bereits, wie man (**) löst!
Wir fassen zusammen:

**SATZ 2.2** Die Gleichung ax+by=c mit $a,b,c\in Z$ ist dann und nur dann in Z lösbar, wenn c durch g=ggT(a,b) teilbar ist. Es sei $a=A\cdot g$, $b=B\cdot g$ und $c=C\cdot g$. Ist $(\tilde{x}_0|\tilde{y}_0)$ irgendeine Lösung von Ax+By=1, so erhält man alle Lösungen von ax+by=c durch $x_k=C\tilde{x}_0+k\cdot B$ und $y_k=C\tilde{y}_0-k\cdot A$.

Beispiel: 345x+525y=330 - ggT(345,525)=15 ; $15\mid 330$
$\Leftrightarrow$ 23x + 35y=22 A=23; B=35; C=22
mit dem BA erhält man: $\tilde{x}_0=-3$ und $\tilde{y}_0=2$
also $x_k=-66+35k$ und $y_k=44-23k$

Nun sind die „Anfangslösungen“ −66 und 44 schon relativ groß. Mit k=2 erhält man als „neue Anfangslösungen“ die Zahlen 4 und −2 und damit

$x_k=4+35k$ und $y_k=-2-23k$

Für einige k erhält man damit:

| k | -1 | 0 | 1 | 2 |
|---|---|---|---|---|
| x | -31 | 4 | 39 | 74 |
| y | 21 | −2 | −25 | −48 |

Wir führen ein weiteres Beispiel vor: 1491x+2059y=12567

Wendet man den BA auf die Zahlen 2059 und 1491 an, so erhält man als letzte wesentliche Zeile: 71 8 −11 2, was uns zunächst verrät, daß ggt(2059;1491) = 71 ist und weiterhin $-11\cdot1491+8\cdot2059=71$ (*) ist, Da auch 12567 durch 71 teilbar ist, können wir zu der reduzierten Gleichung 21x+29y=177 übergehen. Nun müssen wir den BA nicht etwa nochmals auf 29 und 21 anwenden, um unsere Anfangslösungen zu bekommen: teilt man nämlich (*) durch 71, so erhält man: $-11\cdot21+8\cdot29=1$; d.h., die Löungen von (*) sind bereits die ersten Lösungen. Nun geht´s wie folgt weiter:

$\tilde{x}_0=-11$ $\tilde{y}_0=8$

$\bar{x}_0=-11\cdot177=-1947$ $\bar{y}_0=8\cdot177=1416$

$\bar{x}_k=-1947+k\cdot29$ $\bar{y}_0=1416-k\cdot21$

Wir gehen zu kleineren „Anfangslösungen“ über (1416 div 21 =67)

$\bar{x}_{67}=-4$ $\bar{y}_{67}=9$

und damit endlich $x_k=-4+29k$ $y_k=9-21k$

***AUFGABE 2.11*** Gib jeweils drei Lösungen der folgenden Gleichungen an:

a) 4914x+9597y=483 b) 897x-23y=457

c) 57x+36y=18 d) 2468x+4690y=6912

e) -6370x-3122y=14000 f) 48x+32y=160

***AUFGABE 2.12*** a) Löse die diophantische Gleichung 3x+5y=c für c=7,15,20. Zeige, daß es nur für c=20 Lösungen (x|y) gibt, die beide gleichzeitig positiv sind.

b) Verfahre wie bei a) mit der Gleichung 9x+13y=c für c=50, 117,118.

Es ist schwer zu sagen, für welche Wahl der Parameter es Lösungen gibt, die gleichzeitig positiv sind - z.B. gibt es bei der Gleichung aus 2.12 b) für c=116 die Lösung (10|2). Allerdings läßt sich die folgende Behauptung beweisen:

Ist für $a,b\in N$ mit ggT(a,b)=1 c>ab, so hat die Gleichung ax+by=c immer auch Lösungen x und y, die beide positv sind.

Beweis: Es seien $x=x_0+kb$ und $y=y_0-ka$ die (nach Satz 2.2 sicher existenten) Lösungen der Gleichung. Dann gilt $x>0 \Leftrightarrow k>-x_0/b$. Es sei $k^*$ das kleinste k, das diese Ungleichung genügt, also $x_0+k^*b>0$ und $x_0+(k^*-1)b\leq0$. Dann ist $x_0\leq b-k^*b$ (*). Die Ausgangsgleichung läßt sich in by=c-ax umformen. Damit gilt dann weiter:

$by=c-ax=c-a(x_0+k^*b)\geq c-(b-k^*b+k^*b)=c-ab$ ($\geq$ gilt, da $x_0$ nach (*) durch einen größeren Term ersetzt wird, man also mehr abzieht)

Nun ist zu klären, wann $by\geq c-ab>0$ ist. Dies ist sicher der Fall, wenn c>ab ist. Ist aber by>0, so ist wegen $b\in N$ auch y>0.

***AUFGABE 2.13*** Bestimme x,y>0 in 13x+9y=1994 so, daß x+y minimal wird.
Berechne die minimale Summe.
Bestimme x,y>0 in 23x+53y=5000 so, daß x+y maximal wird.
Berechne die maximale Summe.

Ein Beispiel soll demonstrieren, wie man mit dem BA auf spezielle Lösungen von linearen Diophantischen Gleichungen mit mehr als zwei Variablen erhält:
Gleichung: 5x+7y+11z=1 (*)
Der BA liefert: $-2\cdot 7+3\cdot 5=1=ggT(5;7)=u$; also $x_k=3-7k$; $y_k=-2+5k$; in (*): 1u+11z=1
Ohne BA erhält man hier sofort die spezielle Lösung; mit Satz2.2 also $u_l=-10-11l$; $z_l=1+l$
Eingesetzt in (*): $(-10-11l)[5\cdot x_k+7\cdot y_k]+(1+l)\cdot 11$
$=(-10-11l)(3-7k)\cdot 5+(-10-11l)(-2+5k)\cdot 7+(1+l)\cdot 11=1$

Mit k=l=0 erhält man als spezielle Lösung(–30 | 20 | 1); mit k=l=1 erhält man(84 | –63 | 2); mit k=0 und l=1 ergibt sich (–63 | 42 | 2) als Lösung usw. usw.

Man versuche einmal, einige Lösungen von 6x+9y–5z–10u=7 herauszufinden.
z.B.: (28 | –14 | 7 | 0); (28 | –14 | 21 | –7); (45 | –27 | 12 | –4)

# 2.4 DER CHINESISCHE RESTSATZ (1)

In vielen Mathematikbüchern aus alten Zeiten, angefangen bei über 2000 Jahre alten chinesischen Mathematikbüchern (Handbuch der Arithmetik von Sun-Tzun Suan-Ching), aber auch in berühmten „Liber abaci“ der Leonardo von Pisa (Fibonacci), finden sich Aufgaben, in denen Zahlen gesucht werden, die bei Division durch verschiedenen andere Zahlen vorgegebene Reste lassen. Fangen wir zur Demonstration mit einem Beispiel an:

> „Wie alt bist Du?“ wird Daisy von Donald gefragt. „So was fragt man eine Dame doch nicht“ antwortet diese. „Aber wenn Du mein Alter durch drei teilst, bleibt der Rest zwei.“ „Und wenn man es durch fünf teilt?“ „Dann bleibt wieder der Rest zwei. Und jetzt sage ich Dir auch noch, daß bei Division durch sieben der Rest fünf bleibt. Nun müßtest Du aber wissen, wie alt ich bin.“ Weißt der Leser es auch?

Wir wollen hier zwei Verfahren kennenlernen, mit denen man solche Probleme lösen kann.

**1. Verfahren**: Bei kleinen Zahlen wie im obigen Beispiel kann man vorteilhaft alle Zahlen durchprobieren, die der Bedingung mit dem größten Teiler gehorchen und diese dann auf ihre Eignung bezüglich der anderen Teiler überprüfen. Für die obige Aufgabe ergeben sich der Reihe nach die Zahlen: 5, 12, 19, 26, 33, 40, 47 - und da hat man bereits die gesuchte Zahl. Natürlich kommen nun auch alle Zahlen $x_k=47+k\cdot 3\cdot 5\cdot 7$ in Frage (allerdings nicht bei der obigen Situation), denn diese hinterlassen ja bei Division durch 3, 5 und 7 denselben Rest.

***AUFGABE 2.14*** a) Löse: x läßt bei Division durch 7 den Rest 4 und bei Division durch 13 den Rest 10.
b) ebenso: x läßt bei Division durch 11 den Rest 9, bei Division durch 7 den Rest 5 und bei Division durch 3 den Rest 2

Bei großen Divisoren oder mehreren Bedingungen kann das 1. Verfahren schon recht mühsehlig werden. Wir demonstrieren deshalb ein **2.Verfahren** an einigen Beispielen. Zuerst werden wir allerdings im Vorgriff auf das nächste Kapitel eine Schreibweise einführen, mit der man Aufgaben dieser Art angenehmer und übersichtlicher formulieren kann. Nehmen wir an, wir suchen die Zahlen x, die bei Division durch 13 den Rest 5 und bei Division durch 11 den Rest 6 lassen. Vom Programmieren kennen wir die Schreibweise x MOD 13 = 5. Wir wandeln in Anlehnung an Gauß die Schreibweise etwas ab (näheres im nächsten Kapitel) und schreiben: $x\equiv 5 \bmod 13$ (gelesen „x kongruent 5 modulo 13“).

> Die obige Aufgabe lautet in dieser Schreibweise: Bestimme alle $x\in Z$ mit $x\equiv 5 \bmod 13 \wedge x\equiv 6 \bmod 11$.
> Es ist also x ein Vielfaches von 13 plus 5 und x ein Vielfaches von 11 plus 6. Anders ausgedrückt: Wir suchen $a,b\in Z$ mit: $x=a\cdot 13+5=b\cdot 11+6$ (*). Durch Umformen erhalten wir: $13a-11b=1$. Das ist aber ein bekanntes Problem - mit dem BA erhalten wir $a=-5$ und $b=6$. In (*) eingesetzt bringt das $x=-60$. Nach kurzem Stutzen sieht man ein:
> $-60=-5\cdot 13+5$ und $-60=-6\cdot 11+6$ - das Ergebnis ist korrekt. Wir hätten jedoch lieber eine kleine positive Lösung. Kein Problem! Zunächst einmal können wir

uns klar machen, daß sich alle Lösungen um Vielfache von 11·13=143 unterscheiden. Sind nämlich x und y zwei Lösungen des Problems, so lassen x und y jeweils denselben Rest bei Division durch 13 und 11. Also läßt x-y bei Division durch 11 und 13 den Rest 0, ist also durch 11 teilbar und durch 13 teilbar, d.h. x-y=k·11·13 oder x=y+k·11·13. Damit erhalten wir nun alle Lösungen der Aufgabe durch $x_k$=-60+k·143=83+k·143.

***AUFGABE 2.15*** Bestimme alle x mit:

a) $x \equiv 7 \bmod 13 \wedge x \equiv 17 \bmod 23$ b) $x \equiv 2 \bmod 11 \wedge x \equiv 1 \bmod 7$
c) $x \equiv 3 \bmod 7 \wedge x \equiv 12 \bmod 13$ d) $x \equiv 48 \bmod 95 \wedge x \equiv 37 \bmod 81$
e) $x \equiv 100 \bmod 127 \wedge x \equiv 102 \bmod 113$

Ist allgemein die Aufgabe $x \equiv a \bmod s \wedge x \equiv b \bmod t$ gegeben, so führt dies wie im obigen Beispiel auf die Gleichung: x=k·s+a=l·t+b $\Leftrightarrow$ k·s-l·t=b-a. Diese ist nach Satz 2.2 dann und nur dann in Z lösbar, wenn b-a durch den ggT(s,t) teilbar ist, insbesondere also immer dann, wenn s und t relativ prim sind. Das halten wir in einem Satz fest:

**SATZ 2.3** (Chinesischer Restsatz - Satz über simultane Kongruenzen) Sind s und t teilerfremd, so existiert eine Lösung z des Systems von Kongruenzen $x \equiv a \bmod s \wedge x \equiv b \bmod t$. Man erhält dann alle Lösungen durch $x_k$=z+k·s·t

Bemerkung: Man kann durch geeignete Wahl von k immer erreichen, daß $0 \le z < s \cdot t$ ist. Darauf wollen wir bei allen Lösungen achten.

***AUFGABE 2.16*** Suche alle x mit

a) $x \equiv 217 \bmod 373 \wedge x \equiv 25 \bmod 251$
b) $x \equiv 16 \bmod 88 \wedge x \equiv 37 \bmod 55$
c) $x \equiv 281 \bmod 389 \wedge x \equiv 269 \bmod 457$
d) $x \equiv 15 \bmod 88 \wedge x \equiv 37 \bmod 55$

Für Aufgaben mit mehr als drei Bedingungen ändern wir das Verfahren etwas ab.

Gesucht sind alle Zahlen x mit $x \equiv 3 \bmod 5$, $x \equiv 7 \bmod 11$ und $x \equiv 1 \bmod 13$. Um nun eine Lösung x zu finden, starten wir mit dem Ansatz:

$$x = 11 \cdot 13 \cdot a + 5 \cdot 13 \cdot b + 5 \cdot 11 \cdot c \quad ,a,b,c \in Z \qquad (**)$$

Für diese Zahl x gilt dann: $x \equiv 143a \bmod 5$. Wir haben nun a so zu bestimmen, daß 143a den Rest 3 bei Division durch 5 läßt, also: $143a = k \cdot 5 + 3 \Leftrightarrow 143a - 5k = 3$. Hier können wir nun unser eben erworbenes Wissen über Diophantische Gleichungen ins Spiel bringen:

| i | $a_i$ | $x_i$ | $y_i$ | $q_i$ |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **1** | 143 | 1 | 0 | 0 |
| **2** | 5 | 0 | 1 | 28 |
| **3** | 3 | 1 | -28 | 1 |
| **4** | 2 | -1 | 29 | 1 |
| **5** | 1 | 2 | 57 | 2 |
| **6** | 0 | - | - | - |

Wir erhalten $a_0=2$ (k brauchen wir gar nicht) und damit a=6. Entsprechend bearbeiten wir die Gleichung (**) bez. 11 und 13. Wir erhalten x mod 11=65b. Das soll den Rest 7 bei Division durch 11 lassen, was uns auf 65b-11k=7 führt. Mit dem BA erhalten wir $b_0=-1$ und damit b=-7. Entsprechend verfahren wir mit 13. Die Gleichung 55c-13k=1 führt auf c =-4.

Eingesetzt in (**) bringt das $x=143\cdot6+65\cdot(-7)+55\cdot(-4)=183$. Tatsächlich gilt: $183\equiv3 \bmod 5$; $183\equiv7 \bmod 11$ und $183\equiv1 \bmod 13$, d.h. 183 ist eine Lösung. Wegen (*) sind damit alle Zahlen $x_k=183+715k$ Lösungen des Problems.

***AUFGABE 2.17*** Bestimme x mit:

a) $x\equiv3 \bmod 7$; $x\equiv12 \bmod 13$; $x\equiv1 \bmod 5$
b) $x\equiv3 \bmod 7$; $x\equiv5 \bmod 12$; $x\equiv10 \bmod 19$
c) $x\equiv20 \bmod 23$; $x\equiv20 \bmod 31$; $x\equiv20 \bmod 37$
d) $x\equiv10 \bmod 15$; $x\equiv12 \bmod 19$; $x\equiv20 \bmod 28$
e) $x\equiv7 \bmod 12$; $x\equiv12 \bmod 19$; $x\equiv19 \bmod 23$

Hat man mehr als drei Reste gegeben, sucht man sinnvollerweise erst mal alle Zahlen, die die ersten zwei oder drei Bedingungen erfüllen und dann diejenigen, die die weiteren Bedingungen erfüllen. Dazu ein Beispiel:

> Es sei $x\equiv1 \bmod 3$, $x\equiv3 \bmod 5$, $x\equiv5 \bmod 7$ und $x\equiv7 \bmod 11$
> Wir fangen mit der ersten und der letzten Bedingung an und finden mit dem ersten Verfahren sofort 7 als erste Lösung. Also gilt für alle Lösungen bezüglich dieser Bedingungen: $x\equiv7 \bmod 33$
> Ebenso finden wir für die „mittleren“ Bedingungen mit dem 1.Verfahren der Reihe nach:
> 5,12,19,26,33 - also $x\equiv33 \bmod 35$
> Nun setzen wir an: $x=33a+7=35b+33$. Das führt auf die diophantische Gleichung:
> $35b-33a=-26$ mit der Lösung $b_0=-16$, also b=416 und damit $x_0=14593=12\cdot1155+733$. Damit sind alle Lösungen des Problems durch $x_k=733+k\cdot1155$ gegeben.

Man hätte auch direkt nach dem 2.Verfahren vorgehen können. Wir geben deshalb das Verfahren des (nach den ersten Quellen so genannten) „Chinesischen Restsatzes“ noch allgemein an:

Es seien die paarweise teilerfremden Zahlen $a_1, a_2,...,a_n$ gegeben. Um alle Zahlen x mit
$x\equiv r_1 \bmod a_1$, $x\equiv r_2 \bmod a_2,...,x\equiv r_n \bmod a_n$ zu finden, bestimme man die Zahl $a=a_1\cdot a_2\cdots a_n$ sowie die Zahlen $b_1:=a/a_1$, $b_2:=a/a_2,...,b_n:=a/a_n$. Dann bestimme man die Zahlen $x_i$ in den Gleichungen $x_i\cdot b_i+y_i\cdot a_i=1$ für i=1,...,n. Dann gilt:
$x_k=x_1\cdot b_1\cdot r_1+...+x_n\cdot b_n\cdot r_n+k\cdot a$.

Wir kommen auf das Thema „Chinesischer Restsatz“ an späterer Stelle im Zusammenhang mit Kongruenzen noch einmal zurück.

***AUFGABE 2.18*** a) Finde x mit: $x \equiv 1 \bmod 2$; $x \equiv 2 \bmod 3$; $x \equiv 3 \bmod 5$; $x \equiv 4 \bmod 7$; $x \equiv 5 \bmod 11$; $x \equiv 6 \bmod 13$

b) ebenso: $x \equiv 3 \bmod 11$; $x \equiv 8 \bmod 13$; $x \equiv 5 \bmod 17$; $x \equiv 5 \bmod 19$

c) $x \equiv 7 \bmod 11$; $x \equiv 8 \bmod 19$; $x \equiv 15 \bmod 23$; $x \equiv 4 \bmod 29$; $x \equiv 5 \bmod 31$