Dr. Silke Hartlieb, Prof. Dr. Luise Unger

Modul 61113

Elementare Zahlentheorie mit MAPLE

LESEPROBE

Fakultät für
Mathematik und Informatik

FernUniversität in Hagen

Inhaltsverzeichnis

1 Kurseinheit 1 5

1 Teilbarkeit 11
1.1 Verwendete Maple-Befehle 11
1.2 Division mit Rest 11
1.3 Der größte gemeinsame Teiler 17
1.4 Das kleinste gemeinsame Vielfache 25
1.5 Lineare Diophantische Gleichungen 31

2 Kurseinheit 2 47

2 Primzahlen 53
2.1 Verwendete Maple Befehle 53
2.2 Grundlagen 53
2.3 Das Sieb des Eratosthenes 56
2.4 Primzahlverteilung 63
2.5 Mersenne'sche Primzahlen 69
2.6 Eindeutige Primfaktorzerlegung 71
2.7 Noch einmal ggT und kgV 75

3 Kurseinheit 3 87

3 Kongruenzen 91
3.1 Verwendete Maple-Befehle 91
3.2 Kongruenzen – erste Eigenschaften 91
3.3 Lineare Kongruenzen 96
3.4 Systeme linearer Kongruenzen 101
3.5 Der Kleine Satz von Fermat 104
3.6 Der Satz von Wilson 109

4 Kurseinheit 4 123

4 Zahlentheoretische Funktionen 127
4.1 Verwendete Maple-Befehle . . . 127
4.2 Die Anzahl der Teiler einer Zahl . . . 127
4.3 Die Summe der Teiler einer Zahl . . . 130
4.4 Multiplikative Funktionen . . . 132
4.5 Vollkommene Zahlen . . . 134
4.6 Die Anzahl der zu einer Zahl teilerfremden Zahlen . . . 136
4.6.1 Einschub: Abbildungen zwischen endlichen Mengen . . . 136
4.6.2 Die Euler'sche φ-Funktion . . . 139
4.6.3 Der Satz von Euler . . . 144

5 Kurseinheit 5 155

5 Ganzzahlige Lösungen von $X^n + Y^n = Z^n$ 159
5.1 Verwendete Maple-Befehle . . . 159
5.2 Lösungen von $X^2 + Y^2 = Z^2$ . . . 159
5.2.1 Pythagoreische Dreiecke und pythagoreische Tripel . . . 159
5.2.2 Einige Reduktionen . . . 161
5.2.3 Euklids Klassifikationssatz . . . 163
5.3 Die Fermat'sche Vermutung . . . 167
5.3.1 Zur Geschichte des Problems . . . 168
5.3.2 Die Methode des unendlichen Abstiegs . . . 171
5.3.3 Die Gleichung $X^4 + Y^4 = Z^4$ . . . 171
5.4 Die so genannte Pell'sche Gleichung . . . 175
5.4.1 Definition und erste Beispiele . . . 176
5.4.2 Irrationale Zahlen . . . 177
5.4.3 Der Dirichlet'sche Approximationssatz . . . 178
5.4.4 Über die Existenz von Lösungen . . . 181
5.4.5 Struktur der Lösungsmenge der Pell'schen Gleichung . . . 183

6 Kurseinheit 6 197

6 Summe von Quadraten 201
6.1 Verwendete Maple-Befehle . . . 201
6.2 Summe von zwei Quadraten . . . 201
6.2.1 Die Kongruenz $X^2 \equiv -1 (\mathrm{mod} p)$ . . . 201
6.2.2 Primzahlen als Summe von zwei Quadraten . . . 204

6.2.3 Der allgemeine Fall 210
6.3 Summe von vier Quadraten 213
6.3.1 Zur Geschichte des Problems 213
6.3.2 Eulers Teilergebnisse 213
6.3.3 Primzahlen als Summe von vier Quadraten 217
6.4 Das Waring'sche Problem 221

7 Kurseinheit 7 235

7 Gauß'sche Zahlen 239
7.1 Verwendete Maple-Befehle 239
7.2 Komplexe Zahlen 239
7.2.1 Rechnen mit komplexen Zahlen 239
7.2.2 Komplexe Zahlen mit Maple 244
7.2.3 Die Norm einer komplexen Zahl 245
7.3 Einheiten in $\mathbb{Z}[i]$ 246
7.4 Division mit Rest und ggT in $\mathbb{Z}[i]$ 248
7.5 Gauß'sche Primzahlen 251
7.6 Noch einmal der Zwei-Quadrate-Satz 255

Anhang 271

Studierhinweise

Bevor es losgeht, sollten wir vielleicht erklären, worum es in diesem Kurs geht. Zahlentheorie beschäftigt sich mit Phänomenen der ganzen Zahlen. Neben der Geometrie ist die Zahlentheorie vermutlich eine der ältesten mathematischen Disziplinen. Schon die frühesten Kulturen benötigten Zahlen um Handel zu treiben oder das Erbe gerecht zu teilen. Zahlen und Zahlendarstellungen sind eng verbunden mit unserer Kulturgeschichte, und Zahlen haben Menschen von jeher fasziniert. Vor mehr als 3500 Jahren hielten die Babylonier die Zahlentripel

$$\begin{array}{lll} 120, & 119, & 169 \\ 4800, & 4601, & 6649 \\ 360, & 319, & 481 \\ 6480, & 4961, & 8161 \\ 2400, & 1679, & 2929 \\ 2700, & 1771, & 3229. \end{array}$$

für so wichtig, dass sie sie auf Tontafeln notierten. Wozu sie sie brauchten, ist nicht bekannt, aber all diese Tripel a, b, c haben die Eigenschaft, dass $a^2+b^2 = c^2$ ist. Gibt es unendlich viele solcher Tripel? Wenn ja, gibt es ein Bildungsgesetz, wie wir sie alle konstruieren können? Eine Antwort auf diese Frage hat Euklid von Alexandria (etwa 325 – 265 vor unserer Zeitrechnung) gegeben, und wir werden uns dieser Frage in Kurseinheit 5 stellen. Aber spinnen wir unsere Gedanken weiter. Wie ist es mit Tripeln (a, b, c) natürlicher Zahlen, die die Gleichung $a^3 + b^3 = c^3$ erfüllen? Wie viele kann es davon geben? Schon 1637 wusste der französische Mathematiker Fermat, dass es keine solcher Zahlentripel geben kann, und er wusste auch, dass dies für den Exponenten 4 der Fall war, dass es also kein Tripel (a, b, c) natürlicher Zahlen gibt, für dass $a^4 + b^4 = c^4$ gilt. Mehr noch, Fermat behauptete, dass er beweisen könne, dass es für alle $n \geq 3$ keine natürlichen Zahlen a, b, c so gibt, dass $a^n + b^n = c^n$ ist. Diese Äußerung hat die mathematische Welt über 350 Jahre lang in Atem gehalten, denn niemand sah sich bis 1995 in der Lage, Fermats Beweis zu reproduzieren. Auch dazu mehr in Kurseinheit 5.

Der hier angerissene Fragenkreis zeigt schon ein faszinierendes Phänomen der Zah-

lentheorie. Viele Probleme sind so einfach zu formulieren, dass sie ein Schulkind versteht, aber die Lösungen sind so schwierig, dass sie Generationen von Mathematikerinnen und Mathematikern beschäftigen und dass neue Gebiete der Mathematik für ihre Lösung entwickelt werden müssen.

Und das bringt uns zu dem weiteren Zusatz zum Titel dieses Kurses. „Elementar“ bezieht sich nicht auf den Schwierigkeitsgrad des Kurses. Die Elementare Zahlentheorie ist die Teildisziplin der Zahlentheorie, die ohne weiteren Input aus anderen mathematischen Disziplinen auskommt. Weitere Teilbereiche der Zahlentheorie sind etwa die Analytische Zahlentheorie (mit Input aus der Analysis), die Algebraische Zahlentheorie (mit Input aus der Algebra) oder die Algorithmische Zahlentheorie. Letztere ist eine relativ junge Disziplin, die sich unter anderem damit beschäftigt, wie man Algorithmen der Zahlentheorie so optimieren kann, dass sie vom Rechner schnell durchgeführt werden können. Dass dies eine wichtige Frage ist, liegt daran, dass Teile der Zahlentheorie, die über Jahrtausende als eine intellektuelle Spielerei angesehen werden konnten, heute Anwendungen in der Angewandten Mathematik, etwa in der Kryptografie oder Computeralgebra finden.

Neben einer Einführung in die Elementare Zahlentheorie ist dieser Kurs auch eine Einführung in den Gebrauch des Computeralgebrasystems Maple. Den Rechner in einem Kurs zur Elementaren Zahlentheorie zu verwenden, ist nahe liegend. Um einen Zahlentheoretiker zu zitieren, ist Elementare Zahlentheorie ohne Computer etwa so, wie Astronomie ohne Teleskop. Natürlich kann man das machen, aber warum sollte man sich um das Vergnügen bringen, die im Kurs bewiesenen Resultate in Beispielen anzusehen oder mit Zahlen zu experimentieren und eigene Vermutungen aufzustellen? All das ist mit Maple möglich, ohne fehleranfällige Rechnungen mit der Hand durchführen zu müssen. Sie bekommen in diesem Kurs zwar nur einen Ausschnitt dessen zu sehen, was Maple zu leisten vermag, aber nach Durcharbeiten dieses Kurses sollten Sie in der Lage sein, sich auch in andere Maple-Programmbibliotheken einzuarbeiten um Maple dann auch in anderen Kontexten einzusetzen.

Kommen wir nun zu einem Überblick dessen, was Sie in Kurseinheit 1 erwarten wird. Kurseinheit 1 widmet sich dem Thema der Teilbarkeit ganzer Zahlen. Vieles davon werden Sie aus Schulzeiten kennen, allerdings werden da in der Regel keine Beweise geliefert.

In Abschnitt 1.2 geht es um Division mit Rest. Wir zeigen, dass für ganze Zahlen a und b mit $b \neq 0$ stets eindeutig bestimmte ganze Zahlen q und r existieren, sodass $a = qb + r$ ist. Dabei gilt $0 \leq r < |b|$, wobei $|b|$ der Betrag von b ist, also $|b| = b$, wenn $b \geq 0$ ist, und $|b| = -b$, wenn $b < 0$ ist.

In Abschnitt 1.3 behandeln wir größte gemeinsame Teiler ganzer Zahlen. Mit dem

Euklidischen Algorithmus stellen wir ein Verfahren vor, wie der größte gemeinsame Teiler $\mathrm{ggT}(a, b)$ zu ganzen Zahlen a und b berechnet werden kann. Analysiert man den Euklidischen Algorithmus genauer, so stellt man fest, dass mit seiner Hilfe ganze Zahlen s und t so berechnet werden können, dass $\mathrm{ggT}(a, b) = sa + tb$ ist (das geschieht im so genannten erweiterten Euklidischen Algorithmus). Dieses Ergebnis werden wir im Folgenden immer wieder verwenden. Außer den Zahlen s und t, die der erweiterte Euklidische Algorithmus liefert, gibt es weitere ganze Zahlen s' und t', die die Gleichung $\mathrm{ggT}(a, b) = s'a + t'b$ erfüllen. Warum das so ist? Damit beschäftigen wir uns detaillierter in Abschnitt 1.5.

In Abschnitt 1.4 geht es aber zunächst um kleinste gemeinsame Vielfache ganzer Zahlen. Das wichtigste Ergebnis in diesem Abschnitt ist Satz 1.4.6, der kleinste gemeinsame Vielfache und größte gemeinsame Teiler in Zusammenhang stellt. Dies führt dazu, dass man auch kleinste gemeinsame Vielfache mit Hilfe des Euklidischen Algorithmus berechnen kann. In Abschnitt 1.4 werden Sie auch Ihre erste Maple-Prozedur schreiben, das heißt, Sie lernen, wie man mit Maple programmieren kann.

In Abschnitt 1.5 kommen wir dann zu den so genannten linearen Diophantischen Gleichungen, die nach dem griechischen Mathematiker Diophantos von Alexandrien, der vermutlich zwischen 200 und 284 gelebt hat, benannt sind. Diese haben die Form $aX + bY = c$, wobei a, b und c ganze Zahlen sind. Ein Paar (x, y) ganzer Zahlen wird eine Lösung von $aX + bY = c$ genannt, wenn $ax + by = c$ ist. Der erweiterte Euklidische Algorithmus liefert beispielsweise eine Lösung (s, t) der linearen Diophantischen Gleichung $aX + bY = \mathrm{ggT}(a, b)$. Lineare Diophantische Gleichungen müssen keine Lösungen besitzen. Als Beispiel, für die Gleichung $2X + 2Y = 1$ gibt es keine Lösung in den ganzen Zahlen, denn $2x + 2y$ ist immer eine gerade Zahl. Unter welchen Umständen eine lineare Diophantische Gleichung lösbar ist, wie viele Lösungen es gibt, und wie man alle Lösungen finden kann, werden wir in Abschnitt 1.5 klären.

Kapitel 1

Teilbarkeit

Mit $\mathbb{Z}$ bezeichnen wir die ganzen Zahlen, also $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$, mit $\mathbb{N}$ die natürlichen Zahlen, also $\mathbb{N} = \{1, 2, 3, \dots\}$, und mit $\mathbb{N}_0$ die Menge $\mathbb{N} \cup \{0\}$, also $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$.

1.1 Verwendete Maple-Befehle

In diesem Kapitel werden wir die Maple-Befehle `iquo()`, `irem()`, `mod`, `igcd()`, `igcdex()`, `ilcm()`, `proc()`, `local`, `end`, `#`, `save()`, `read()`, `abs()`, `for`, `do`, `od`, `print()` und `isolve()` verwenden.

Warten Sie ab, bis wir im Text zu ihnen kommen. Mehr erfahren Sie dann über diese Befehle, wenn Sie im Maple-Worksheet `?befehl`, also zum Beispiel `?irem`, eingeben.

1.2 Division mit Rest

Ein zentraler Begriff in der Elementaren Zahlentheorie ist der Begriff der Teilbarkeit ganzer Zahlen, der im Folgenden definiert wird.

1.2.1 Definition: Seien a und b in $\mathbb{Z}$, und sei $a \neq 0$. Die Zahl a heißt **Teiler** von b, wenn es ein $x \in \mathbb{Z}$ so gibt, dass $ax = b$ ist.

1.2.2 Beispiele: Es ist 12 ein Teiler von 60, denn für $x = 5$ gilt $12x = 60$. Weiter ist 8 ein Teiler von -24, denn für $x = -3$ gilt $8x = -24$.

1.2.3 Notation: Wenn a ein Teiler von b ist, so schreiben wir $a \mid b$ (gesprochen „a teilt b“), anderenfalls $a \nmid b$ (gesprochen „a teilt nicht b“).

1.2.4 Aufgabe:
1. Gilt $2|6$, $4|2$, $-5|50$?
2. Welche ganzen Zahlen a erfüllen $a|0$?
3. Es gibt zwei ganze Zahlen, die alle ganzen Zahlen teilen. Welche sind das?
4. Bestimmen Sie alle Teiler von 6.

Wir werden jetzt die ersten Rechenregeln für Teiler herleiten.

1.2.5 Proposition: (Rechenregeln für Teilbarkeit)

Seien a, b und c ganze Zahlen. Dann gilt:

1. Gilt $a|b$ und $b|c$, so folgt $a|c$.
2. Gilt $a|b$ und $a|c$, so folgt $a|(b+c)$.
3. Gilt $a|b$, so folgt $a|bc$ für alle $c \in \mathbb{Z}$.
4. Sind $b_1, \ldots, b_n$ ganze Zahlen, und gilt $a|b_1, \ldots, a|b_n$, so gilt
$$a|(b_1c_1 + \cdots + b_nc_n)$$
für alle $c_1, \ldots, c_n \in \mathbb{Z}$.
5. (Kürzungsregel) Gilt $ab = ac$ und ist $a \neq 0$, so folgt $b = c$.

Beweis:

1. Da $a|b$, gibt es ein $x_1 \in \mathbb{Z}$ mit $ax_1 = b$. Analog, da $b|c$, gibt es ein $x_2 \in \mathbb{Z}$ mit $bx_2 = c$. Wir setzen $ax_1 = b$ in die zweite Gleichung ein und erhalten $ax_1x_2 = c$. Dies zeigt, dass es ein $x \in \mathbb{Z}$, nämlich $x = x_1x_2$, so gibt, dass $ax = c$ ist. Es folgt $a|c$.
2. Da $a|b$, gibt es ein $x_1 \in \mathbb{Z}$ mit $ax_1 = b$. Da $a|c$, gibt es ein $x_2 \in \mathbb{Z}$ mit $ax_2 = c$. Dann gilt
$$b + c = ax_1 + ax_2 = a(x_1 + x_2).$$
Es gibt also ein $x \in \mathbb{Z}$, nämlich $x = x_1 + x_2$, mit $ax = b + c$. Es folgt $a|(b+c)$.
3. Sei a ein Teiler von b, und sei c eine beliebige ganze Zahl. Dann gilt $ax_1 = b$ für ein $x_1 \in \mathbb{Z}$. Es folgt $ax_1c = bc$. Für $x = x_1c$ ist dann $ax = bc$, also $a|bc$.

4. Es gelte $a|b_1$, $a|b_2$, $\ldots$, $a|b_n$. Mit dem, was in 3. bewiesen wurde, folgt $a|c_1b_1$, $a|c_2b_2$, $\ldots$, $a|c_nb_n$ für alle $c_1, \ldots c_n \in \mathbb{Z}$.

   Mit 2. gilt: $a|(c_1b_1 + c_2b_2)$
   Mit 2. gilt: $a|((c_1b_1 + c_2b_2) + c_3b_3)$, also $a|c_1b_1 + c_2b_2 + c_3b_3$
   $\vdots$
   Mit 2. gilt: $a|((c_1b_1 + \cdots + c_{n-1}b_{n-1}) + c_nb_n)$, also $a|(c_1b_1 + \cdots + c_nb_n)$.

5. Sei $ab = ac$ und $a \neq 0$. Es folgt $ab - ac = a(b - c) = 0$. Da $a \neq 0$, folgt $b - c = 0$, also $b = c$.

□

1.2.6 Aufgabe: Geben Sie für jede der Aussagen in Proposition 1.2.5 (bis auf die letzte) ein konkretes Zahlenbeispiel.

Das folgende Ergebnis kennen Sie vermutlich bereits aus der Schule, allerdings wird dort nicht bewiesen, dass alles gut geht. Das holen wir an dieser Stelle nach.

1.2.7 Proposition: (Division mit Rest – Spezialfall)

Seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ gegeben. Dann gibt es eindeutig bestimmte ganze Zahlen q und r, sodass $a = qb + r$ und $0 \leq r < b$ ist.

Beweis: Wir denken uns die Folge von Zahlen

$$\ldots, a - 3b, a - 2b, a - b, a, a + b, a + 2b, a + 3b, \ldots$$

nach beiden Richtungen unbegrenzt fortgesetzt. Wähle aus dieser Folge die kleinste Zahl ≥ 0 und bezeichne sie mit r. Es gilt also $r = a - qb$ für ein $q \in \mathbb{Z}$. Wir formen um und erhalten

$$a = qb + r, \text{ mit } q \in \mathbb{Z} \text{ und } 0 \leq r.$$

Wir müssen noch zeigen, dass $r < b$ ist.

Angenommen, $r \geq b$. Dann ist $r - b \geq 0$, und Einsetzen von $a - qb$ für r liefert

$$r - b = a - qb - b = a - (q + 1)b \geq 0.$$

Damit taucht $r - b$ in unserer Folge von Zahlen auf und ist ≥ 0, sowie $b > 0$ nach Voraussetzung. Das kann aber nicht sein, denn wir hatten r so klein wie möglich gewählt. Dieser Widerspruch zeigt, dass die Annahme $r \geq b$ falsch ist, und dass damit $r < b$ gelten muss.

Bis jetzt haben wir gezeigt, dass es ganze Zahlen q und r so gibt, dass $a = qb + r$ und $0 \leq r < b$ ist. Es bleibt zu zeigen, dass diese Zahlen eindeutig sind.

Dazu seien q' und r' weitere Zahlen mit $a = q'b + r'$ und $0 \leq r' < b$. Wir müssen zeigen, dass $r = r'$ und $q = q'$ ist. Wir zeigen zunächst, dass $r = r'$ gilt.

Wäre $r \neq r'$, dann gilt $r' > r$, denn r war so klein wie möglich gewählt. Also gilt $0 < r' - r < b$. Einsetzen für r und r' liefert

$$0 < r' - r = a - q'b - a + qb = (q - q')b.$$

Damit ist b ein Teiler von $r' - r$, was aber unmöglich ist, weil $b > r' - r > 0$ ist. Also war die Annahme $r \neq r'$ falsch, und es folgt $r = r'$.

Es gilt also $a = qb + r = q'b + r$. Durch Umformung erhalten wir $q = q'$. Damit sind die oben konstruierten Zahlen eindeutig. □

Machen wir ein konkretes Zahlenbeispiel zum Beweis von Proposition 1.2.7:

1.2.8 Beispiel: Seien $b = 17$ und $a = -58$. Die konstruierte Folge von Zahlen ist

$$\ldots, \underbrace{a - 3b}_{=-109}, \underbrace{a - 2b}_{=-92}, \underbrace{a - b}_{=-75}, \underbrace{a}_{=-58}, \underbrace{a + b}_{=-41}, \underbrace{a + 2b}_{=-24}, \underbrace{a + 3b}_{=-7}, \underbrace{a + 4b}_{=10}, \underbrace{a + 5b}_{=27}, \ldots$$

Die kleinste Zahl ≥ 0 in dieser Folge ist 10, also $a + 4b = 10 = r$. Weiter ist $q = -4$, denn $a = \underbrace{-4}_{=q} b + \underbrace{10}_{=r}$.

1.2.9 Aufgabe: Finden Sie q und r für $a = 75$ und $b = 24$.

In Proposition 1.2.7 hatten wir vorausgesetzt, dass $b \in \mathbb{N}$, also $b > 0$ ist. Man möchte aber auch die Division mit Rest bei negativem b durchführen. Das ist auch leicht möglich, wie der folgende Satz zeigen wird. Allerdings brauchen wir noch einen Begriff:

1.2.10 Definition: Sei b eine reelle Zahl. Der **Betrag** $|b|$ von b wird definiert durch

$$|b| = \begin{cases} b, & \text{falls } b \geq 0, \\ -b, & \text{falls } b < 0. \end{cases}$$

Der allgemeine Fall der Division mit Rest lautet jetzt:

1.2.11 Satz: (Division mit Rest)

Seien $a, b \in \mathbb{Z}$, und sei $b \neq 0$. Dann gibt es eindeutig bestimmte ganze Zahlen q und r, sodass $a = qb + r$ und $0 \leq r < |b|$ ist.

Beweis: Ist $b \in \mathbb{N}$, also $b > 0$, so wurde die Aussage in Proposition 1.2.7 bewiesen. Wir können also annehmen, dass $b < 0$ ist. Dann ist $-b = |b| > 0$, und mit 1.2.7 gibt es eindeutig bestimmte ganze Zahlen q und r, sodass

$$a = q(-b) + r = (-q)b + r \text{ mit } 0 \leq r < (-b) = |b| \text{ ist.}$$

In beiden Fällen gilt die Behauptung. □

1.2.12 Definition: (Division mit Rest)

Seien $a, b \in \mathbb{Z}$, und sei $b \neq 0$. Sei $a = qb + r$ mit $0 \leq r < |b|$ und $q, r \in \mathbb{Z}$. Wir sagen, dass a durch b **mit Rest geteilt** wurde. Die Zahl q heißt der **Quotient** und die Zahl r der **Rest** der Division.

1.2.13 Notation: Den (kleinsten) Rest einer Division von a durch b mit Rest bezeichnen wir mit $a \bmod b$.

Die Maple-Befehle für die Division mit Rest sind `iquo` (wie integer quotient, also ganzzahliger Quotient) für q und `irem` (für integer remainder, also ganzzahliger Rest) für den Rest r.

Beide Befehle brauchen zwei ganze Zahlen (nämlich a und b) als Eingabe, die durch ein Komma getrennt werden. Eine mögliche Abfrage könnte also lauten:

```
> iquo(987346524,1234532);
```

$$799$$

```
> irem(987346524,1234532);
```

$$955456$$

Etwas eleganter ist es, Variablen a und b einzuführen, und diesen die Werte 987346524 und 1234532 zuzuweisen. Eine mögliche Abfrage könnte dann wie folgt aussehen:

```
> a:=987346524;
```

$$a := 987346524$$

```
> b:=1234532;
```

$$b := 1234532$$

```
> iquo(a,b);
```

$$799$$

```
> irem(a,b);
```

955456

Wenn Sie die Hilfe `?iquo` beziehungsweise `?irem` zu `iquo` und `irem` aufrufen, werden Sie feststellen, dass Sie, wenn Sie möchten, in `iquo` und `irem` noch ein drittes Argument eingeben können. Dieses ist ein Variablenname, den Sie beliebig wählen dürfen, den Sie allerdings in Hochkommata einschließen müssen. Bei der Ausführung von `iquo()` wird dieser Variablen der Wert des Restes r bei der Division mit Rest zugewiesen, und bei der Ausführung von `irem()` der Wert des Quotienten. Wenn Sie diese Option auswählen, könnte Ihre Abfrage wie folgt aussehen:

```
> a:=987346524; b:=1234532;
```

$$a := 987346524$$
$$b := 1234532$$

```
> iquo(a,b,'r');
```

799

```
> r;
```

955456

```
> irem(a,b,'q');
```

955456

```
> q;
```

799

Wenn Sie die Hilfeseiten zu `irem` aufmerksam gelesen haben, ist Ihnen vielleicht aufgefallen, dass sich die Definition des Befehls `irem` an einer Stelle von unserer Definition des Restes unterscheidet.

1.2.14 Aufgabe: Finden Sie zwei ganze Zahlen a und b, sodass der Rest der Division von a durch b nicht gleich dem Wert von `irem`(a, b) in Maple ist. Wann genau gibt `irem` nicht das gewünschte Ergebnis aus?

Der Befehl in Maple, der exakt den Rest liefert, den wir hier im Kurs definiert haben, ist `mod`.

1.2.15 Aufgabe: Rufen Sie Maple auf und informieren Sie sich über den Maple Befehl `mod`. Berechnen Sie mit diesem Befehl und mit `irem` den Rest bei der Division von $a = -987346524$ durch $b = -1234532$ mit Rest.

Welchen der beiden Befehle `irem` und `mod` Sie letztendlich benutzen, bleibt Ihnen überlassen. Die Befehle `iquo` und `irem` sind handlicher, weil Sie dort zwei Befehle in einem verpackt haben. Sie sollten sich aber immer bewusst sein, dass es zu einem Unterschied zu `mod` und damit zu 1.2.12 kommt, wenn $a < 0$ gilt.

1.3 Der größte gemeinsame Teiler

Wir beginnen mit einer Definition.

1.3.1 Definition: Eine ganze Zahl d heißt ein **gemeinsamer Teiler** von zwei ganzen Zahlen a und b, falls $d|a$ und $d|b$ gilt.

Beispielsweise ist -2 ein gemeinsamer Teiler von 6 und -8.

1.3.2 Definition: Seien a und b ganze Zahlen, die nicht beide 0 sind. Eine ganze Zahl d heißt **größter gemeinsamer Teiler** von a und b (abgekürzt $\mathrm{ggT}(a, b)$), falls die beiden folgenden Bedingungen gelten.

1. $d|a$ und $d|b$, und
2. wenn $c \in \mathbb{Z}$ ein gemeinsamer Teiler von a und b ist, dann ist $c \leq d$.

Die erste Bedingung von Definition 1.3.2 besagt, dass d ein gemeinsamer Teiler von a und b ist. Die zweite besagt, dass d der größte unter allen gemeinsamen Teilern von a und b ist. Damit ist d eindeutig festgelegt, das heißt, $\mathrm{ggT}(a, b)$ bezeichnet genau eine Zahl.

1.3.3 Warnung: Beachten Sie, dass $\mathrm{ggT}(0, 0)$ nicht definiert ist.

Da 1 jede ganze Zahl teilt, gilt immer $\mathrm{ggT}(a, b) \geq 1$.

1.3.4 Aufgabe: Sei $n \in \mathbb{N}$. Beweisen Sie, dass $\mathrm{ggT}(n, n + 1) = 1$ ist.

1.3.5 Definition: Ganze Zahlen a und b, deren größter gemeinsamer Teiler 1 ist, werden **teilerfremd** genannt.

1.3.6 Proposition: (Rechenregeln für ggT)

Seien a und b ganze Zahlen, die nicht beide 0 sind. Dann gilt:

1. $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a)$.
2. $\mathrm{ggT}(a, b) = \mathrm{ggT}(-a, b)$

3. $\mathrm{ggT}(a, b) = \mathrm{ggT}(a - b, b)$
4. Wenn $d = \mathrm{ggT}(a, b)$ ist, dann ist $\mathrm{ggT}(\frac{a}{d}, \frac{b}{d}) = 1$.
5. $\mathrm{ggT}(a, b) = \mathrm{ggT}(a \bmod b, b)$.

Beweis:

1. Die Behauptung ist klar, denn a und b haben dieselben Teiler wie b und a.
2. Die Behauptung folgt, da die Menge der Teiler von a und die Menge der Teiler von $-a$ gleich sind.
3. Sei $d = \mathrm{ggT}(a, b)$. Da $d|a$ und $d|b$, folgt mit Proposition 1.2.5, dass d ein Teiler von $(a - b)$ ist. Somit ist d ein gemeinsamer Teiler von $a - b$ und b. Sei $c \in \mathbb{N}$ ein weiterer gemeinsamer Teiler von $a - b$ und b. Wieder mit Proposition 1.2.5 folgt $c|((a - b) + b)$, also $c|a$. Also ist c ein gemeinsamer Teiler von a und b, das heißt $c \leq d$.
4. Sei $c = \mathrm{ggT}(\frac{a}{d}, \frac{b}{d})$. Es ist $c \geq 1$, und wir müssen zeigen, dass $c = 1$ ist.

   Da c ein Teiler von $\frac{a}{d}$ ist, gibt es ein $x_1 \in \mathbb{Z}$ mit $cx_1 = \frac{a}{d}$, also $cdx_1 = a$.

   Da c ein Teiler von $\frac{b}{d}$ ist, gibt es ein $x_2 \in \mathbb{Z}$ mit $cx_2 = \frac{b}{d}$, also $cdx_2 = b$.

   Es folgt, dass cd ein gemeinsamer Teiler von a und b ist, und da d der größte gemeinsame Teiler ist, folgt $cd \leq d$. Da c und d positive Zahlen sind, folgt $c = 1$.
5. Sei $d = \mathrm{ggT}(a, b)$. Sei $a = kb + (a \bmod b)$ für ein $k \in \mathbb{Z}$. Da d ein Teiler von a und b ist, ist d ein Teiler von $a - kb$, also ein Teiler von $a \bmod b$. Sei c ein weiterer positiver Teiler von $a \bmod b$ und b. Dann gilt $c|a$, also $c|a$ und $c|b$. Da d der größte gemeinsame Teiler ist, folgt $c \leq d$, und dies zeigt $d = \mathrm{ggT}(a \bmod b, b)$.

□

Wie berechnet man größte gemeinsame Teiler? Was ist zum Beispiel $\mathrm{ggT}(5767, 4453)$? Bei der Beantwortung dieser Frage hilft folgendes Lemma.

1.3.7 Lemma: Seien a und b natürliche Zahlen, die nicht beide 0 sind. Sei $a = qb + r$ die Division von a durch b mit Rest. Dann gilt

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r).$$

Beweis: Mit Proposition 1.3.6 und $r = a \bmod b$ gilt

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a \bmod b, b) = \mathrm{ggT}(b, a \bmod b) = \mathrm{ggT}(b, r).$$

□

1.3.8 Aufgabe: Überzeugen Sie sich davon, dass das Lemma für $a = 16$ und $b = 6$ richtig ist.

Jetzt sind wir ein gutes Stück weiter. Da nämlich $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a)$ ist, können wir annehmen, dass $a > b$ ist (im Fall $a = b$ wären wir fertig, denn dann ist $\mathrm{ggT}(a, a) = a$). Das Lemma besagt, dass $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$ ist, und es ist $a > b > r \geq 0$. Wir müssen also den größten gemeinsamen Teiler für kleinere Zahlen ausrechnen. Und wir können dieses Verfahren fortsetzen, wie wir im folgenden Beispiel sehen werden.

1.3.9 Beispiel: Wir möchten $\mathrm{ggT}(5767, 4453)$ berechnen. Dazu verwenden wir wiederholt Division mit Rest und das Lemma.

$$\begin{aligned}
&\text{Division mit Rest:} && 5767 = 1 \cdot 4453 + 1314\\
&\text{Division mit Rest:} && 4453 = 3 \cdot 1314 + 511\\
&\text{Division mit Rest:} && 1314 = 2 \cdot 511 + 292\\
&\text{Division mit Rest:} && 511 = 1 \cdot 292 + 219\\
&\text{Division mit Rest:} && 292 = 1 \cdot 219 + 73\\
&\text{Division mit Rest:} && 219 = 3 \cdot 73 + 0
\end{aligned}$$

Mit Lemma 1.3.7 folgt

$$\begin{aligned}
&\mathrm{ggT}(5767, 4453) = \mathrm{ggT}(4453, 1314) = \mathrm{ggT}(1314, 511) = \mathrm{ggT}(511, 292)\\
&= \mathrm{ggT}(292, 219) = \mathrm{ggT}(219, 73) = \mathrm{ggT}(73, 0) = 73.
\end{aligned}$$

Bei den wiederholten Divisionen mit Rest wurden die Reste immer kleiner. Da es zwischen 0 und dem größten Rest (in unserem Beispiel 1314) aber nur endlich viele natürliche Zahlen gibt, musste die Kette der kleiner werdenden Reste irgendwann abbrechen, also 0 werden. Der gesuchte ggT war dann der Rest in dieser Kette, der unmittelbar vor dem Rest 0 ausgerechnet wurde. Und das hängt nicht von der speziellen Wahl unserer Zahlen ab, sondern gilt allgemein. Und schon sind wir mitten in einem der wohl wichtigsten Algorithmen der Elementaren Zahlentheorie, dem Euklidischen Algorithmus, der auch viele Anwendungen in der Computeralgebra und Kryptografie hat.

1.3.10 Algorithmus: (Euklidischer Algorithmus)

Die Eingabe sind zwei natürliche Zahlen a und b, und die Ausgabe ist $\mathrm{ggT}(a, b)$.

1. (Initialisierung:) Setze $x = a$ und $y = b$.
2. (Sind wir fertig?) Wenn $y = 0$ ist, so gib $\mathrm{ggT}(a, b) = x$ aus.
3. (Nimm den Rest:) Setze $r = x \bmod y$, $x = y$, $y = r$ und gehe zurück zu Schritt 2.

Bei jeder Durchführung von Schritt 3 des Algorithmus wird r kleiner, und es gilt $r \geq 0$. Da es nur endlich viele positive Zahlen zwischen $(a \bmod b)$ und 0 gibt, muss der Algorithmus abbrechen. Er bricht ab, wenn $y = r = 0$ ist, und dann ist $\mathrm{ggT}(x, y) = x$. Mit Lemma 1.3.7 gilt aber nach jeder Ausführung von Schritt 3 $\mathrm{ggT}(a, b) = \mathrm{ggT}(x, y)$, der Algorithmus berechnet also in der Tat den größten gemeinsamen Teiler von a und b.

Der Euklidische Algorithmus wurde für natürliche Zahlen formuliert, aber das ist keine Einschränkung. Ist eine der Zahlen 0 (es dürfen ja nicht beide Zahlen 0 sein) und die andere positiv, dann ist der ggT gerade diese positive Zahl. Da die gemeinsamen Teiler von a und b und von $|a|$ und $|b|$ für alle $a, b \in \mathbb{Z}$ gleich sind, gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|)$. Zur Berechnung von größten gemeinsamen Teilern reicht es also aus, sich auf positive Zahlen zu beschränken.

1.3.11 Aufgabe: Berechnen Sie $\mathrm{ggT}(299, 247)$ und $\mathrm{ggT}(578, -442)$.

Der Euklidische Algorithmus ist so wichtig, dass er natürlich auch in Maple enthalten ist. Der Maple-Befehl lautet `igcd`, das ist eine Abkürzung von „integer greatest common divisor“, also ganzzahliger größter gemeinsamer Teiler. Als Eingabe verlangt `igcd()` zwei ganze Zahlen a und b. Wenn Sie das gleich ausprobieren, setzen Sie doch auch mal $a = 0$ und $b = 0$ ein. Das führt nicht zu einer Fehlermeldung, und das ist auch kein Bug in Maple. Der Grund ist, dass manchmal $\mathrm{ggT}(0, 0) = 0$ definiert wird. In diesem Kurs tun wir das nicht, hier gilt weiterhin die Regel, dass $\mathrm{ggT}(0, 0)$ nicht definiert ist.

1.3.12 Aufgabe: Überprüfen Sie Ihre Rechnungen in Aufgabe 1.3.11 mit Maple.

Seien nun $a, b \in \mathbb{N}$, und sei $d = \mathrm{ggT}(a, b)$. Das nächste Ergebnis wird sein, dass es ganze Zahlen s und t so gibt, dass $d = s \cdot a + t \cdot b$ ist. Die Idee bei dem Beweis von diesem Ergebnis ist, den Euklidischen Algorithmus nochmal zu durchlaufen. Machen wir das einfach mal in einem Beispiel.

1.3.13 Beispiel: In Beispiel 1.3.9 haben wir berechnet, dass $\mathrm{ggT}(5767, 4453) = 73$ ist. Das haben wir durch wiederholte Division mit Rest gemacht, die einzelnen

Divisionen waren

$$\begin{aligned} 5767 &= 1 \cdot 4453 + 1314 \\ 4453 &= 3 \cdot 1314 + 511 \\ 1314 &= 2 \cdot 511 + 292 \\ 511 &= 1 \cdot 292 + 219 \\ 292 &= 1 \cdot 219 + 73 \\ 219 &= 3 \cdot 73 + 0. \end{aligned}$$

Wir suchen ganze Zahlen s und t, sodass $73 = s5767 + t4453$ ist.

Dazu stellen wir nach den Resten um und erhalten

$$\begin{aligned} 1314 &= 5767 - 4453 \\ 511 &= 4453 - 3 \cdot 1314 \\ 292 &= 1314 - 2 \cdot 511 \\ 219 &= 511 - 292 \\ 73 &= 292 - 219. \end{aligned}$$

Jetzt ersetzen wir 1314 in der zweiten und dritten Zeile durch $5767 - 4453$ und erhalten

$$\begin{aligned} 511 &= 4453 - 3(5767 - 4453) = 4 \cdot 4453 - 3 \cdot 5767 \\ 292 &= 5767 - 4453 - 2 \cdot 511 \\ 219 &= 511 - 292 \\ 73 &= 292 - 219. \end{aligned}$$

Jetzt ersetzen wir 511 in der (neuen) zweiten und dritten Zeile durch $4 \cdot 4453 - 3 \cdot 5767$ und erhalten

$$\begin{aligned} 292 &= 5767 - 4453 - 2(4 \cdot 4453 - 3 \cdot 5767) = 7 \cdot 5767 - 9 \cdot 4453 \\ 219 &= 4 \cdot 4453 - 3 \cdot 5767 - 292 \\ 73 &= 292 - 219. \end{aligned}$$

Jetzt ersetzen wir 292 in der zweiten und dritten Zeile durch $7 \cdot 5767 - 9 \cdot 4453$. Dies ergibt

$$\begin{aligned} 219 &= 4 \cdot 4453 - 3 \cdot 5767 - (7 \cdot 5767 - 9 \cdot 4453) = -10 \cdot 5767 + 13 \cdot 4452 \\ 73 &= 7 \cdot 5767 - 9 \cdot 4453 - 219. \end{aligned}$$

Zum Schluss ersetzen wir 219 in der letzten Zeile durch $-10 \cdot 5767 + 13 \cdot 4452$ und erhalten

$$73 = 7 \cdot 5767 - 9 \cdot 4453 - (-10 \cdot 5767 + 13 \cdot 4452) = 17 \cdot 5767 - 22 \cdot 4453.$$

Für die Zahlen $s = 17$ und $t = -22$ gilt dann

$$\mathrm{ggT}(5767, 4453) = s5767 + t4453.$$

1.3.14 Aufgabe: Finden Sie ganze Zahlen s und t, sodass $\mathrm{ggT}(578, -442) = s578 + t(-442)$ ist. Die nötige Vorarbeit haben Sie in Aufgabe 1.3.11 bereits geleistet.

1.3.15 Satz: Seien a und b ganze Zahlen, die nicht beide 0 sind. Dann gibt es ganze Zahlen s und t, sodass gilt

$$\mathrm{ggT}(a, b) = sa + tb.$$

Beweis: (Erweiterter Euklidischer Algorithmus)

Ist $a = 0$, so ist $\mathrm{ggT}(a, b) = |b|$, und es ist $s = 0$ und $t = \pm 1$. Analog, wenn $b = 0$ ist, so ist $\mathrm{ggT}(a, b) = |a|$ und $s = \pm 1$ und $t = 0$. In diesen Fällen ist der Satz also richtig, und wir nehmen im Folgenden an, dass $a \neq 0$ und $b \neq 0$ ist. Zunächst nehmen wir darüber hinaus an, dass $a, b \in \mathbb{N}$ gilt.

Wir berechnen $\mathrm{ggT}(a, b)$ mit Hilfe des Euklidischen Algorithmus'. Dabei führen wir Divisionen mit Rest der folgenden Form aus:

$$\begin{array}{lcll}
a & = & q_1 b + r_1, & 0 < r_1 < b \\
b & = & q_2 r_1 + r_2, & 0 < r_2 < r_1 \\
r_1 & = & q_3 r_2 + r_3, & 0 < r_3 < r_2 \\
\vdots & & \vdots & \vdots \\
r_{n-3} & = & q_{n-1} r_{n-2} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\
r_{n-2} & = & q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} & = & q_{n+1} r_n + 0. &
\end{array}$$

Es ist $\mathrm{ggT}(a, b) = r_n$. Diese Gleichungen stellen wir nach den Resten um und erhalten

$$\begin{array}{lcl}
r_1 & = & a - q_1 b \\
r_2 & = & b - q_2 r_1 \\
r_3 & = & r_1 - q_3 r_2 \\
\vdots & & \vdots \\
r_{n-1} & = & r_{n-3} - q_{n-1} r_{n-2} \\
r_n & = & r_{n-2} - q_n r_{n-1}.
\end{array}$$

Jetzt setzen wir für r_1 in der zweiten und dritten Zeile $a - q_1 b$ ein, dann ersetzen wir r_2 in der dritten und vierten Zeile durch die neue zweite Zeile und so weiter. Die jeweils folgende Zeile ist von der Form $xa + yb$ mit $x, y \in \mathbb{Z}$. Wenn wir r_{n-2} und r_{n-1} in der letzten Zeile durch Ausdrücke der Form $xa + yb$ ersetzt haben, erhalten wir

$$\mathrm{ggT}(a, b) = r_n = sa + tb \text{ mit } s, t \in \mathbb{Z}.$$

Seien $a, b \in \mathbb{Z}$ und nicht beide 0. Da $\mathrm{ggT}(a,b) = \mathrm{ggT}(|a|,|b|)$ gibt es ganze Zahlen s und t mit

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(|a|,|b|) = s|a| + t|b|.$$

Es folgt

$$\mathrm{ggT}(a,b) = \pm sa \pm tb,$$

die Behauptung. □

1.3.16 Definition: Das Verfahren, mit dem s und t im Beweis dieses Satzes konstruiert wurden, wird der **erweiterte Euklidische Algorithmus** genannt.

Auch der erweiterte Euklidische Algorithmus ist in Maple enthalten. Der Befehl lautet `igcdex`, wie „integer greatest common divisor, extended“. Als Eingabe erwartet der Befehl zwei ganze Zahlen a und b. Außerdem kann man noch zwei Variablennamen in Hochkommata angeben, also etwa `igcdex`$(a, b,' s',' t')$. Die Ausgabe ist dann der ggT von a und b, und die Variablen s und t enthalten Werte, sodass $sa + tb = \mathrm{ggT}(a,b)$ gilt.

```
> igcdex(123452345,8765432345,'s','t');s;t;
```

$$5$$
$$-828143950$$
$$11663579$$

```
> s*123452345+t*8765432345;
```

$$5$$

1.3.17 Aufgabe: Berechnen Sie mit Maple $\mathrm{ggT}(12,21)$ und ganze Zahlen s und t, für die $12s+21t = \mathrm{ggT}(12,21)$ gilt. Berechnen Sie außerdem – nicht unbedingt mit Maple – ganze Zahlen $s' \neq s$ und $t' \neq t$, für die ebenfalls $12s' + 21t' = \mathrm{ggT}(12,21)$ gilt.

Satz 1.3.15 hat viele Folgerungen, von denen wir einige jetzt zusammenstellen werden.

1.3.18 Korollar: Seien $a, b, d \in \mathbb{Z}$.

Ist d ein Teiler von ab, und ist $\mathrm{ggT}(d,a) = 1$, so ist d ein Teiler von b.

Beweis: Satz 1.3.15 besagt, dass es ganze Zahlen s und t so gibt, dass $sd+ta = 1$ ist. Wir multiplizieren diese Gleichung mit b und erhalten

$$bsd + bta = b.$$

Da d ein Teiler von bsd und ein Teiler von $bta(= abt)$ ist, folgt mit Proposition 1.2.5, dass d ein Teiler von $bsd + bta = b$ ist. Es gilt also $d|b$, die Behauptung. □

1.3.19 Aufgabe: Es gilt $6|8 \cdot 9$, aber $6 \nmid 8$ und $6 \nmid 9$. Warum ist das kein Widerspruch zu Korollar 1.3.18?

1.3.20 Korollar: Seien $a, b, c \in \mathbb{Z}$. Gilt $a \mid c$, $b \mid c$ und $\mathrm{ggT}(a, b) = 1$, dann folgt $ab \mid c$.

Beweis: Da $a \mid c$ gilt, gibt es ein $x \in \mathbb{Z}$ mit $c = ax$. Es gilt also $b \mid ax$ und $\mathrm{ggT}(a, b) = 1$. Mit Korollar 1.3.18 folgt $b \mid x$, also $x = yb$ für ein $y \in \mathbb{Z}$. Damit ist $c = aby$, also $ab \mid c$. □

1.3.21 Korollar: Seien $a, b \in \mathbb{Z}$, und sei $d = \mathrm{ggT}(a, b)$. Sei c ein gemeinsamer Teiler von a und b. Dann ist c ein Teiler von d.

Beweis: Seien s und t in $\mathbb{Z}$, sodass $sa + tb = d$ gilt. Nach Annahme gilt $c|a$ und $c|b$. Mit Proposition 1.2.5 folgt $c|(sa + tb)$, also $c|d$. □

1.3.22 Korollar: Sei $m \in \mathbb{N}$, seien $a, b \in \mathbb{Z}$, und sei $d = \mathrm{ggT}(a, b)$.

Dann gilt $\mathrm{ggT}(ma, mb) = md$.

Beweis: Sei $z = \mathrm{ggT}(ma, mb)$.

Nach Annahme gilt $d|a$ und $d|b$, also gilt $md|ma$ und $md|mb$. Damit ist md ein gemeinsamer Teiler von ma und mb.

Mit Korollar 1.3.21 ist md ein Teiler von z, es gibt also ein $x \in \mathbb{Z}$ mit $mdx = z$. Da m, d und z positive Zahlen sind, ist auch x positiv.

Da $\mathrm{ggT}(ma, mb) = z = mdx$, folgt $mdx|ma$ und $mdx|mb$, also $dx|a$ und $dx|b$ (denn wir können in $\mathbb{Z}$ kürzen). Wieder mit Korollar 1.3.21 gilt $dx|d$, also $x = 1$, denn $x > 0$. Es folgt $z = md = \mathrm{ggT}(ma, mb)$, die Behauptung. □

1.3.23 Korollar: Sei $m \in \mathbb{N}$, und seien $a, b \in \mathbb{Z}$. Seien a und b nicht beide 0. Sei m ein gemeinsamer Teiler von a und b. Dann gilt

$$\mathrm{ggT}(\frac{a}{m}, \frac{b}{m}) = \frac{1}{m} \cdot \mathrm{ggT}(a, b).$$

Beweis: Mit Korollar 1.3.22 gilt

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(\frac{a}{m} \cdot m, \frac{b}{m} \cdot m) = m \cdot \mathrm{ggT}(\frac{a}{m}, \frac{b}{m}).$$

Wir teilen durch m und erhalten $\frac{1}{m} \cdot \mathrm{ggT}(a,b) = \mathrm{ggT}(\frac{a}{m}, \frac{b}{m})$, die Behauptung. □

Euklid von Alexandria (etwa 325 – 265 vor unserer Zeitrechnung) ist der bekannteste Mathematiker des Altertums. Sein mathematisches Werk „Die Elemente“ ist vermutlich nach der Bibel das am häufigsten gedruckte Werk der westlichen Kultur. Mehr zu Euklid erfahren Sie auf dem hervorragenden Server zur Mathematikgeschichte http://turnbull.mcs.st-and.ac.uk/history/, hier unter http://www-groups.dcs.st-and.ac.uk/history/Biographies/Euclid.html.

1.4 Das kleinste gemeinsame Vielfache

Wieder beginnen wir mit einer Definition.

1.4.1 Definition: Seien $a, b \in \mathbb{Z}$ mit $a \neq 0$ und $b \neq 0$. Eine Zahl $c \in \mathbb{Z}$ heißt **gemeinsames Vielfaches** von a und b, falls a und b Teiler von c sind. Die kleinste positive Zahl, die ein gemeinsames Vielfaches von a und b ist, wird das **kleinste gemeinsame Vielfache** von a und b genannt und mit $\mathrm{kgV}(a,b)$ bezeichnet.

1.4.2 Beispiel: Es ist $\mathrm{kgV}(12,8) = 24$, denn $2 \cdot 12 = 24 = 3 \cdot 8$. Somit gilt $12|24$ und $8|24$. Da es keine kleinere positive Zahl gibt, die 12 und 8 als Teiler hat, ist 24 das kleinste gemeinsame Vielfache von 12 und 8.

Der Maple-Befehl zur Berechnung kleinster gemeinsamer Vielfacher lautet `ilcm` wie „integer least common multiple“, also „ganzzahliges kleinstes gemeinsames Vielfaches“.

1.4.3 Aufgabe: Berechnen Sie $\mathrm{kgV}(12345654, -987654)$ mit Maple. Wie ist in Maple $\mathrm{kgV}(0,0)$ definiert?

Die gemeinsamen Vielfachen zweier Zahlen a und b sind gerade die Vielfachen des kleinsten gemeinsamen Vielfachen von a und b. Das ist die Aussage der folgenden Proposition.

1.4.4 Proposition: Seien $a, b \in \mathbb{Z}$ mit $a \neq 0$ und $b \neq 0$. Sei $h = \mathrm{kgV}(a,b)$.

Genau dann ist $m \in \mathbb{Z}$ ein gemeinsames Vielfaches von a und b, wenn $m = kh$ für ein $k \in \mathbb{Z}$ ist.

Vorbemerkung zum Beweis: Hier ist eine Äquivalenz von Aussagen zu beweisen, genauer, wir müssen zeigen:

$m \in \mathbb{Z}$ ist ein gemeinsames Vielfaches von a und $b \Leftrightarrow m = kh$ für ein $k \in \mathbb{Z}$.

Den Beweis zerlegen wir in zwei Schritte. Zunächst werden wir zeigen: Wenn m ein gemeinsames Vielfaches von a und b ist, dann ist $m = kh$ für ein $k \in \mathbb{Z}$. Danach zeigen wir: Wenn $m = kh$ für ein $k \in \mathbb{Z}$ ist, dann ist m ein gemeinsames Vielfaches von a und b. Für Beweismethoden vergleichen Sie auch mit der Kurseinheit 1 der Mathematischen Grundlagen (Kurs 1141).

Beweis: Sei m ein beliebiges gemeinsames Vielfaches von a und b. Wir dividieren m durch h mit Rest und erhalten

$$m = qh + r \text{ mit } 0 \leq r < h.$$

Wir sind fertig, wenn wir zeigen können, dass $r = 0$ ist, denn dann ist m ein Vielfaches von h.

Angenommen, $r \neq 0$. Es ist $r = m - qh$. Weiter gilt $a|m$ und $a|h$, also $a|r$, und analog $b|m$ und $b|h$, also $b|r$.

Damit ist r ein gemeinsames Vielfaches von a und b, welches positiv ist und kleiner als h. Das ist ein Widerspruch, denn wir hatten angenommen, dass h das kleinste gemeinsame Vielfache von a und b ist. Dieser Widerspruch zeigt, dass die Annahme $r \neq 0$ falsch ist, es gilt also $r = 0$.

Sei umgekehrt $k \in \mathbb{Z}$ und sei $m = kh$. Da $a|h$ und $b|h$, gilt $a|kh$ und $b|kh$. Somit ist m ein gemeinsames Vielfaches von a und b. □

Das folgende Ergebnis besagt, dass wir gemeinsame Teiler von a und b aus dem kleinsten gemeinsamen Vielfachen von a und b ausklammern können.

1.4.5 Proposition: Seien $a, b \in \mathbb{Z}$ mit $a \neq 0$ und $b \neq 0$. Sei $m \in \mathbb{N}$. Dann gilt $\text{kgV}(ma, mb) = m\text{kgV}(a, b)$.

Beweis: Es ist $\text{kgV}(ma, mb)$ ein Vielfaches von m. Es gibt also ein $x \in \mathbb{Z}$ mit $mx = \text{kgV}(ma, mb)$. Da m und $\text{kgV}(ma, mb)$ positiv sind, ist auch x positiv. Wir müssen zeigen, dass $x = \text{kgV}(a, b)$ ist.

Sei $h = \text{kgV}(a, b)$.

Es gilt

$$\left.\begin{array}{rcl} ma|mx & \Rightarrow & a|x \\ mb|mx & \Rightarrow & b|x \end{array}\right\} \Rightarrow x \text{ ist gemeinsames Vielfaches von } a \text{ und } b.$$

Mit Proposition 1.4.4 folgt $h|x$.

Andererseits gilt

$$\left.\begin{array}{rcl} a|h & \Rightarrow & ma|mh \\ b|h & \Rightarrow & mb|mh \end{array}\right\} \Rightarrow mh \text{ ist gemeinsames Vielfaches von } am \text{ und } bm.$$

Wieder mit Proposition 1.4.4 – jetzt angewendet auf $mx = \mathrm{kgV}(ma, mb)$ – folgt $mx|mh$, also $x|h$.

Wir haben also $x|h$ und $h|x$, und da beide Zahlen positiv sind, folgt $x = h$.

Es gilt also $m\mathrm{kgV}(a, b) = \mathrm{kgV}(ma, mb)$, die Behauptung. □

Der Euklidische Algorithmus ist ein sehr effizienter Algorithmus zur Berechnung größter gemeinsamer Teiler, das heißt, er hat eine geringe Laufzeit und verbraucht wenig Speicherplatz. Auch kleinste gemeinsame Vielfache lassen sich schnell berechnen – der Grund dafür ist der folgende Zusammenhang zwischen ggT und kgV.

1.4.6 Satz: (Zusammenhang zwischen ggT und kgV)

Seien $a, b \in \mathbb{N}$. Dann gilt $\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = ab$.

Beweis: Wir betrachten zunächst den Spezialfall, dass $\mathrm{ggT}(a, b) = 1$ ist.

Es ist $\mathrm{kgV}(a, b)$ ein Vielfaches von a, also $\mathrm{kgV}(a, b) = ma$ für ein $m \in \mathbb{N}$. Nun ist b ein Teiler von $\mathrm{kgV}(a, b)$, es gilt also $b|ma$. Jetzt kommt unsere Annahme, dass $\mathrm{ggT}(a, b) = 1$ ist, ins Spiel: Mit Korollar 1.3.18 folgt jetzt nämlich, dass b ein Teiler von m ist. Da b und m natürliche Zahlen sind, impliziert dies, dass $b \leq m$ ist, also

$$ab \leq am = \mathrm{kgV}(a, b).$$

Nun ist ab aber ein positives gemeinsames Vielfaches von a und b, und ma ist das kleinste gemeinsame Vielfache von a und b. Es folgt $ab = am$. Dann gilt

$$ab = \mathrm{kgV}(a, b) = \mathrm{kgV}(a, b) \cdot \underbrace{\mathrm{ggT}(a, b)}_{=1 \text{ nach Annahme}}.$$

Im Spezialfall $\mathrm{ggT}(a, b) = 1$ gilt also die Aussage des Satzes.

Nehmen wir nun an, dass $\mathrm{ggT}(a, b) = d > 1$ ist. Mit Proposition 1.3.6 gilt $\mathrm{ggT}(\frac{a}{d}, \frac{b}{d}) = 1$. Wie wir gerade gezeigt haben gilt dann

$$\frac{a}{d} \cdot \frac{b}{d} = \mathrm{kgV}(\frac{a}{d}, \frac{b}{d}) \cdot \mathrm{ggT}(\frac{a}{d}, \frac{b}{d}),$$

also

$$ab = d\left(\mathrm{kgV}(\frac{a}{d},\frac{b}{d})\right)\cdot d\left(\mathrm{ggT}(\frac{a}{d},\frac{b}{d})\right).$$

Mit Proposition 1.4.5 gilt

$$d\left(\mathrm{kgV}(\frac{a}{d},\frac{b}{d})\right) = \mathrm{kgV}(\frac{a}{d}d,\frac{b}{d}d) = \mathrm{kgV}(a,b),$$

und mit Korollar 1.3.23 gilt

$$d\left(\mathrm{ggT}(\frac{a}{d},\frac{b}{d})\right) = \frac{d}{d}\mathrm{ggT}(a,b) = \mathrm{ggT}(a,b).$$

Es folgt $ab = \mathrm{ggT}(a,b)\cdot\mathrm{kgV}(a,b)$, die Behauptung. □

Da größte gemeinsame Teiler und kleinste gemeinsame Vielfache unabhängig von den Vorzeichen von a und b sind, gilt auch:

1.4.7 Korollar: Seien $a,b\in\mathbb{Z}$, und seien $a\neq 0$ und $b\neq 0$. Dann gilt

$$\mathrm{ggT}(a,b)\cdot\mathrm{kgV}(a,b) = \mathrm{ggT}(|a|,|b|)\cdot\mathrm{kgV}(|a|,|b|) = |a|\cdot|b|.$$

□

Satz 1.4.6 beziehungsweise Korollar 1.4.7 ermöglichen es, kleinste gemeinsame Vielfache schnell zu berechnen. Mit dem Euklidischen Algorithmus wird $\mathrm{ggT}(|a|,|b|)$ berechnet, und dann ist $\mathrm{kgV}(a,b) = \dfrac{|a|\cdot|b|}{\mathrm{ggT}(|a|,|b|)}$.

An dieser Stelle werden wir unsere erste kleine Prozedur in Maple schreiben. Das Programmieren mit Maple ist sehr intuitiv, und wir werden einfach Schritt für Schritt in kleinen Prozeduren alle Elemente eines Mapleprogramms kennen lernen. Die Syntax einer Prozedur sieht in etwa folgendermaßen aus:

```
name:=proc(Parameter1,Parameter2,...)
  local LokaleVariable1, ...;
  Berechnungen, Zuweisungen etc.;
  end:
```

Am besten schauen wir uns dazu ein Beispiel an:

1.4.8 Beispiel: Es folgt eine Prozedur, die das kleinste gemeinsame Vielfache von zwei natürlichen Zahlen berechnet.

```
> kgVnat:=proc(a,b) #berechnet kgV(a,b), wobei a und b
natürlicheZahlen sind
    local kgV;
    kgV:=a*b/igcd(a,b);
    end:
> kgVnat(27,6);
```

54

Jede Prozedur fängt an, indem man ihr einen Namen gibt (in diesem Fall `kgVnat`) und diesem dann `proc` zuweist. Die Zuweisung erfolgt durch die beiden Zeichen `:=`. (Bitte achten Sie darauf, dass sich zwischen `:` und `=` kein Leerzeichen befindet.) In diesem Beispiel erwartet die Prozedur als Eingabe zwei Werte a und b, deshalb schreibt man `proc(a,b)`. Es gibt aber auch Prozeduren, denen keine Parameter übergeben werden. In einem solchen Fall schreibt man einfach `proc()`. Man kann auch bei der Eingabe schon eine Abfrage einbauen, ob die eingegebenen Werte vom korrekten Format sind, aber das verschieben wir auf später. Wir gehen hier davon aus, dass a und b natürliche Zahlen sind.

In der zweiten Zeile stehen dann hinter `local` die lokalen Variablen. Das sind Variablen, die während der Prozedur benötigt werden. In diesem Beispiel ist die lokale Variable kgV gar nicht unbedingt nötig, aber zum Verdeutlichen des Prinzips haben wir sie eingebaut. Mehrere lokale Variablen werden durch Kommata getrennt. Ja, und dann geht es mit der eigentlichen Prozedur los. Hier ist das für den Anfang nur eine Zuweisung. Achten Sie bitte darauf, jede Zuweisung mit einem `;` zu beenden. Wichtig ist dann noch, die Prozedur durch ein `end`, gefolgt von einem Doppelpunkt, abzuschließen.

In der ersten Zeile befindet sich hinter dem `#` außerdem noch ein Kommentar. Das heißt, Maple übersieht alles, was hinter dem `#` steht. Sie sollten sich gleich von Anfang an angewöhnen, Ihre Prozeduren ausreichend zu kommentieren. Dazu gehört neben dem obligatorischen Kommentar nach dem Befehl `proc(...)` immer dann eine Kommentierung, wenn Variablen oder Anweisungen verwendet werden, die nicht ohne weiteres für den Leser verständlich sind oder die Prozedur sehr umfangreich ist. `#` leitet einen einzeiligen Kommentar ein. Für einen mehrzeiligen Kommentar benutzen Sie `(*` und `*)`. Innerhalb dieser Klammern schreiben Sie den Kommentar.

Bevor Sie jetzt gleich eine ganz ähnlich Prozedur schreiben sollen, noch zwei Tipps. Der erste bezieht sich auf das Schreiben von Prozeduren im Maple Worksheet. Da sich eine Prozedur ja meistens über mehrere Zeilen hinzieht, sollten Sie, um in

die nächste Zeile zu wechseln, gleichzeitig mit der Returntaste auch die Shifttaste drücken. Dies bewirkt, dass die bis dahin geschriebene Prozedur noch nicht ausgeführt wird. Um dies zu vereinfachen können Sie aber stattdessen auch die Code Edit Region verwenden. Diese finden Sie in Maple unter „Insert -> Code Edit Region“. In dem Rahmen, der erscheint, können Sie Ihre Prozeduren eingeben ohne beim Zeilenwechsel die Shifttaste drücken zu müssen. Außerdem werden in der Code Edit Region die Schlüsselwörter hervorgehoben und das Einrücken funktioniert automatisch. Um die Prozedur ausführen zu lassen, bewegen Sie den Mauszeiger in den Rahmen der Code Edit Region und klicken mit der rechten Maustaste. Aus dem sich öffnenden Kontextmenü wählen Sie den Punkt „Execute Code“ oder Sie verwenden die dort angezeigte Tastenkombination Strg+E.

Sie können Prozeduren so speichern, dass Sie sie in jedes andere Worksheet einlesen und dort benutzen können. Dazu werden die Befehle `save` und `read` benutzt. Mit der Endung .m werden die Prozeduren in einem komprimierten Maple-internen Format abgespeichert. Bei Problemen mit diesen Befehlen schauen Sie bitte in die „Einführung in Maple“, die Sie im Virtuellen Studienplatz finden.

```
> kgVnat:=proc(a,b) #berechnet kgV(a,b), wobei a und b
natürlicheZahlen sind
    local kgV;
    kgV:=a*b/igcd(a,b);
    end:

> save(kgVnat,"kgVnatproc.m"):
```

Wenn Sie nun ein neues Worksheet starten, können Sie die Prozedur wieder einlesen:

```
> read("kgVnatproc.m");

> kgVnat(100,175);
```

700

1.4.9 Aufgabe: Schreiben Sie eine Maple-Prozedur, die als Eingabe zwei ganze Zahlen a und b hat und als Ausgabe $\mathrm{kgV}(a, b)$. Die Maple-Funktion `igcd` dürfen Sie dabei benutzen, nicht aber die Funktion `ilcm`. (Hinweis: Der Befehl für den Betrag ist `abs`.)

1.5 Lineare Diophantische Gleichungen

Diophantos von Alexandrien war ein griechischer Mathematiker, der vermutlich zwischen 200 und 284 gelebt hat. Über sein Leben ist wenig bekannt, wenn Sie jedoch mehr über ihn wissen wollen, so schauen Sie doch einmal unter http://www-history.mcs.st-andrews.ac.uk/Biographies/Diophantus.html nach.

1.5.1 Definition: Eine **lineare Diophantische Gleichung** ist von der Form $aX + bY = c$, wobei $a, b, c \in \mathbb{Z}$ sind. Eine **Lösung** einer linearen Diophantischen Gleichung ist ein Paar (x, y) mit $x, y \in \mathbb{Z}$, für das $ax + by = c$ gilt.

Das Adjektiv „linear“ bezieht sich darauf, dass die Variablen X und Y ohne Potenzen > 1 auftreten.

Ist $b \neq 0$, so können wir eine lineare Diophantische Gleichung umformen und erhalten $Y = -\frac{a}{b}X + \frac{c}{b}$, eine Geradengleichung. Lösungen sind dann gerade die Punkte mit ganzzahligen Koordinaten auf dieser Gerade.

Eine lineare Diophantische Gleichung muss keine Lösungen haben. Betrachten wir beispielsweise die Gleichung

$$2X + 2Y = c.$$

Wenn c ungerade ist, dann hat diese Gleichung keine Lösung (zur Erinnerung, Lösungen müssen ganze Zahlen sein), und wenn c gerade ist, dann gibt es unendlich viele Lösungen.

Wir haben schon Beispiele für lineare Diophantische Gleichungen gesehen. Sind a und b in $\mathbb{Z}$, nicht beide 0, und ist $d = \mathrm{ggT}(a, b)$, so haben wir in Satz 1.3.15 gesehen, dass es ganze Zahlen s und t so gibt, dass $d = as + bt$ ist. Also ist (s, t) eine Lösung der linearen Diophantischen Gleichung $aX + bY = d$. Eine solche Lösung können wir mit dem erweiterten Euklidischen Algorithmus auch schnell konstruieren.

Die Fragen, denen wir uns in diesem Abschnitt widmen werden, lauten:

1.5.2 Fragen:
1. Wie können wir entscheiden, ob eine lineare Diophantische Gleichung eine Lösung besitzt?
2. Falls es Lösungen gibt, wie viele Lösungen gibt es?
3. Falls es Lösungen gibt, wie können wir alle Lösungen konstruieren?

Bevor wir uns an die Untersuchung dieser Fragen machen, sollten wir noch einen pathologischen Fall aus der Welt schaffen. Wenn $aX + bY = c$ die lineare Diophantische Gleichung mit Koeffizienten $a = 0$ und $b = 0$ ist, dann gibt es zwei

Möglichkeiten. Ist auch $c = 0$, so sind alle $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ Lösungen. Ist $c \neq 0$, so gibt es keine Lösungen. Wir werden also im Folgenden immer annehmen, dass a und b nicht beide 0 sind.

Die erste Frage in 1.5.2 beantwortet die folgende Proposition.

1.5.3 Proposition: (Existenz von Lösungen)

Sei $aX + bY = c$ eine lineare Diophantische Gleichung, wobei a und b nicht beide 0 sind. Sei $d = \text{ggT}(a, b)$. Dann gilt:

1. Wenn d ein Teiler von c ist, dann hat die lineare Diophantische Gleichung (mindestens) eine Lösung.
2. Wenn d kein Teiler von c ist, dann hat die lineare Diophantische Gleichung keine Lösung.

Beweis:

1. Sei d ein Teiler von c. Dann gibt es ein $m \in \mathbb{Z}$ mit $md = c$.

   Mit dem erweiterten Euklidischen Algorithmus gibt es ganze Zahlen s und t, sodass $as+bt = d$ ist. Wir multiplizieren diese Gleichung mit m und erhalten

   $$a(ms) + b(mt) = md = c.$$

   Mit $x_0 = ms$ und $y_0 = mt$ ist (x_0, y_0) eine Lösung von $aX + bY = c$.

2. Sei d kein Teiler von c. Angenommen,wir hätten eine Lösung $(x_0, y_0) \in \mathbb{Z}\times\mathbb{Z}$. Es gilt $d|ax_0$ und $d|by_0$, also $d|(ax_0 + by_0)$, das heißt $d|c$. Das hatten wir aber gerade ausgeschlossen, und dieser Widerspruch zeigt, dass es keine Lösung von $aX + bY = c$ gibt.

□

1.5.4 Aufgabe: Welche der folgenden linearen Diophantischen Gleichungen hat eine Lösung?

(a) $874394X - 27364Y = 539762$.

(b) $874396X - 27364Y = 539762$.

(c) $214866X + 305900Y = 419336$.

Proposition 1.5.3 klärt also völlig, welche linearen Diophantischen Gleichungen eine Lösung haben und welche nicht. Der ggT von a und b muss c teilen. Falls dies

der Fall ist, werden wir im Folgenden die Gleichung $aX + bY = c$ vereinfachen, indem wir zu der so genannten reduzierten Form übergehen, die wir jetzt definieren werden.

1.5.5 Definition: Sei $aX + bY = c$ eine lineare Diophantische Gleichung, und seien a und b nicht beide 0. Sei $d = \mathrm{ggT}(a, b)$, und sei d ein Teiler von c.

Seien $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ und $c' = \frac{c}{d}$. Dann wird

$$a'X + b'Y = c'$$

die zu $aX + bY = c$ **reduzierte** lineare Diophantische Gleichung genannt.

1.5.6 Bemerkung: Seien $a, b \in \mathbb{Z}$, nicht beide 0. Sei $d = \mathrm{ggT}(a, b)$. Sei $aX+bY = c$ eine lineare Diophantische Gleichung, und sei $d = \mathrm{ggT}(a, b)$ ein Teiler von c. Sei $a'X + b'Y = c'$ die zu $aX + bY = c$ reduzierte Gleichung. Dann gilt

1. $\mathrm{ggT}(a', b') = 1$.
2. $aX + bY = c$ und $a'X + b'Y = c'$ haben dieselben Lösungen.

Beweis:

1. Das ist gerade die vierte Aussage von Proposition 1.3.6.
2. Sei $\mathcal{L}$ die Menge der Lösungen von $aX + bY = c$, und sei $\mathcal{L}'$ die Menge der Lösungen von $a'X + b'Y = c'$. Sei $(x_0, y_0) \in \mathcal{L}$. Dann gilt $ax_0 + by_0 = c$. Division durch d liefert $a'x_0 + b'y_0 = c'$. Also ist (x_0, y_0) eine Lösung der reduzierten Gleichung, und es gilt $\mathcal{L} \subseteq \mathcal{L}'$.

   Sei (x_0', y_0') eine Lösung von $a'X+b'Y = c'$, also $a'x_0'+b'y_0' = c'$. Multiplikation mit d liefert $ax_0' + by_0' = c$, also ist (x_0', y_0') eine Lösung von $aX + bY = c$. Es folgt $\mathcal{L}' \subseteq \mathcal{L}$, also $\mathcal{L} = \mathcal{L}'$.

□

Um eine lineare Diophantische Gleichung auf Lösungen zu untersuchen, reicht es also aus, sich auf reduzierte lineare Diophantische Gleichungen zu beschränken. Wenn aber die vollständige Lösungsmenge gesucht wird, hilft Punkt 2 der folgenden Proposition weiter.

1.5.7 Proposition: (Struktur der Lösungsmenge)

Sei $aX + bY = c$ eine lineare Diophantische Gleichung, die eine Lösung (x_0, y_0) besitzt. Seien a und b nicht beide 0. Dann gilt:

1. Für alle $t \in \mathbb{Z}$ ist auch $(x_0 + bt, y_0 - at)$ eine Lösung von $aX + bY = c$.
2. Die Tupel der Form $(x_0 + b't, y_0 - a't)$ für ein $t \in \mathbb{Z}$, wobei $a'X + b'Y = c'$ die zu $aX + bY = c$ reduzierte lineare Diophantische Gleichung ist, sind genau alle Lösungen der Diophantischen Gleichung $aX + bY = c$.

Beweis:

1. Wir wissen, dass $ax_0 + by_0 = c$ ist. Dann gilt für alle $t \in \mathbb{Z}$

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + abt + by_0 - abt = ax_0 + by_0 = c.$$

   Es folgt, dass auch $(x_0 + bt, y_0 - at)$ eine Lösung von $aX + bY = c$ ist.

2. Laut Annahme sind nicht beide Koeffizienten a und b von $aX + bY = c$ Null. Wir nehmen an, dass $a \neq 0$ gilt, anderenfalls benennen wir die Variablen X und Y einfach um.

   Sei $a'X + b'Y = c'$ die zu $aX + bY = c$ reduzierte lineare Diophantische Gleichung. Sei (x, y) irgendeine Lösung von $aX + bY = c$. Dann ist (x, y) auch eine Lösung von $a'X + b'Y = c'$. Wir wollen zeigen, dass es ein $t \in \mathbb{Z}$ so gibt, dass $x = x_0 + b't$ und $y = y_0 - a't$ sind. Dabei ist (x_0, y_0) unsere vorgegebene Lösung.

   Laut Annahme gilt $a'x_0 + b'y_0 = c'$ und $a'x + b'y = c'$. Wir subtrahieren diese Gleichungen und erhalten

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

   Es folgt $a'(x_0 - x) = -b'(y_0 - y)$, das heißt, $a' | b'(y_0 - y)$. Da $\mathrm{ggT}(a', b') = 1$, folgt mit Korollar 1.3.18, dass a' ein Teiler von $y_0 - y$ ist. Es gibt also ein $t \in \mathbb{Z}$ mit $a't = y_0 - y$, also $y = y_0 - a't$. Wir setzen $a't$ für $y_0 - y$ in die Gleichung $0 = a'(x_0 - x) + b'(y_0 - y)$ ein und erhalten $a'(x_0 - x) + b'a't = 0$. Da $a' \neq 0$ ist, können wir kürzen und erhalten $x_0 - x + b't = 0$, also $x = x_0 + b't$.

□

Bevor wir zur nächsten Übungsaufgabe kommen, möchten wir Ihnen einen weiteren Baustein für Maple-Prozeduren vorstellen, die `for`-Schleife. Formal sehen diese Schleifen immer in etwa so aus:

```
for Variable from Anfang by Schrittweite to Ende
 do
   ...
 od;
```

Den Wert `Schrittweite` kann man auch weglassen, dann wird der Wert von `Variable` in jedem Schritt um eins erhöht bis der Wert `Ende` erreicht ist. Also, was passiert in der `for`-Schleife? Zuerst wird die Variable auf den Wert `Anfang` gesetzt und die Anweisungen zwischen `do` und `od` werden ausgeführt. Anschließend wird der Wert von `Variable` um `Schrittweite` verändert, und die Anweisungen werden wieder ausgeführt. Die Anweisungen werden ein letztes Mal ausgeführt, wenn der Wert von `Variable` den Wert von `Ende` erreicht hat. Hier ein Beispiel für eine Prozedur mit `for`-Schleife:

```
> Quadrate:=proc() #berechnet alle Quadrate von 1 bis 10 und
schreibt  diese auf den Bildschirm
    local i;
    for i from 1 to 10 do
     print(i^2);
    od;
   end:

> Quadrate();
```

1
4
9
16
25
36
49
64
81
100

Die Variable i wird hier in jedem Schritt um 1 erhöht, bis der Wert 10 erreicht ist. Dabei wird jeweils i^2 berechnet. Der Befehl `print` bewirkt, dass die Elemente auf den Bildschirm ausgegeben werden.

1.5.8 Aufgabe: Die Lineare Diophantische Gleichung $2X+3Y = 5$ hat die Lösung $(1, 1)$. Schreiben Sie eine Maple-Prozedur, die mit Eingabe a weitere a Lösungen der Gleichung produziert und berechnen Sie so 20 Lösungen der Gleichung.

Kommen wir jetzt noch einmal zu unseren Fragen 1.5.2 zu Beginn dieses Abschnitts zurück. Die erste Frage, wann es Lösungen von $aX + bY = c$ geben kann, wird mit Proposition 1.5.3 umfassend beantwortet. Es gibt genau dann mindestens eine

Lösung, wenn $\mathrm{ggT}(a,b)$ ein Teiler von c ist. Die zweite Frage, wie viele Lösungen es gibt, wird von Proposition 1.5.7 beantwortet. Wenn es überhaupt eine Lösung gibt (wenn also $\mathrm{ggT}(a,b)$ ein Teiler von c ist), dann gibt es unendlich viele Lösungen. Auch die dritte Frage können wir beantworten. Wenn (x_0, y_0) irgendeine Lösung ist, dann sind alle Lösungen von der Form $(x_0 + b't, y_0 - a't)$ mit $t \in \mathbb{Z}$, wobei $a'X + b'Y = c'$ die zu $aX + bY = c$ reduzierte lineare Diophantische Gleichung ist.

Die einzige Frage, die bleibt, ist die, wie wir irgendeine Lösung von $aX + bY = c$ finden können. Aber auch das haben wir im Beweis von Proposition 1.5.3 schon erledigt. Zur Erinnerung:

1.5.9 Algorithmus: (Bestimmung einer Lösung von $aX + bY = c$)

Sei $aX + bY = c$ eine lineare Diophantische Gleichung, für die $\mathrm{ggT}(a,b)|c$ gilt.

1. Bilde $m = \dfrac{c}{\mathrm{ggT}(a,b)}$.
2. Konstruiere mit dem erweiterten Euklidischen Algorithmus ganze Zahlen s und t, sodass $as + bt = \mathrm{ggT}(a,b)$ ist.
3. Bilde $x_0 = ms$ und $y_0 = mt$. Dann ist (x_0, y_0) eine Lösung von $aX + bY = c$.

1.5.10 Beispiel: Wir suchen alle Lösungen von $2X + 6Y = 18$. Es ist $\mathrm{ggT}(2,6) = 2$, und $2|18$. Also hat diese lineare Diophantische Gleichung unendlich viele Lösungen. Sei nun $m = \frac{18}{\mathrm{ggT}(2,6)} = 9$. Nun sind $s, t \in \mathbb{Z}$ gesucht mit $as+bt = \mathrm{ggT}(a,b) = 2$. Da können wir natürlich $s = 1$ und $t = 0$ nehmen. Nun ist $x_0 = ms = 9$ und $y_0 = mt = 0$. Eine Lösung ist also $(9, 0)$. Die Menge aller Lösungen ist dann

$$\mathcal{L} = \{(9 + 3t, -t) \mid t \in \mathbb{Z}\},$$

denn die zu $2X+6Y = 18$ reduzierte lineare Diophantische Gleichung ist $X+3Y = 9$.

1.5.11 Aufgabe: Finden Sie alle Lösungen von $2X + 6Y = 20$.

Der Maple Befehl zum Lösen linearer Diophantischer Gleichungen lautet `isolve` wie „integer solve“, ganzzahliges Lösen. Als Eingabe verlangt Maple eine Gleichung, die allerdings in Maple-Syntax gegeben sein muss. Etwa: $3x$ wird nicht verstanden, Sie müssen statt dessen $3 * x$ schreiben. Ein zweites Argument ist optional, Sie können auf die Eingabe verzichten. Es bezeichnet den Namen des Parameters, der in der Lösungsmenge auftritt; wir haben ihn oben t genannt. Mehr erfahren Sie, wenn Sie `?isolve` eingeben.

1.5.12 Aufgabe: Lösen Sie Aufgabe 1.5.11 mit Maple. Warum sind beide Lösungen richtig?

1.5.13 Aufgabe: Schreiben Sie eine Maple-Prozedur `LDG(a,b,c)`, die mit der Eingabe der ganzen Zahlen a, b, c eine Lösung (x_0, y_0) der linearen Diophantischen Gleichung $aX + bY = c$ berechnet, falls $\mathrm{ggT}(a, b) \mid c$ gilt. Benutzen dürfen Sie den Maple-Befehl `igcdex`, nicht jedoch den Befehl `isolve`. Berechnen Sie mit dieser Prozedur eine Lösung von $1234X - 5678Y = 736$.

Lösungen der Aufgaben

Lösungen der Aufgaben in 1.2

Aufgabe 1.2.4

1. Es gilt $2|6$, denn $2 \cdot 3 = 6$. Es gilt $4 \nmid 2$, denn es gibt keine ganze Zahl x mit $4x = 2$. Es gilt $-5|50$, denn mit $x = -10$ gilt $(-5)x = 50$.
2. Für alle Zahlen $a \in \mathbb{Z}$ gibt es ein $x \in \mathbb{Z}$ (nämlich $x = 0$), sodass $ax = 0$ ist. Somit sind alle $a \in \mathbb{Z}$, $a \neq 0$, Teiler von 0. Der Fall $a = 0$ ist nach Definition eines Teilers ausgeschlossen, denn Teiler sind immer $\neq 0$.
3. Die Zahlen 1 und -1 sind Teiler aller ganzen Zahlen.
4. Die Teiler von 6 sind $-6, -3, -2, -1, 1, 2, 3, 6$.

Aufgabe 1.2.6

1. Sei $a = 2$, $b = 6$ und $c = 12$. Dann gilt $2|6$, $6|12$, und es gilt $2|12$.
2. Sei $a = 2$, $b = 4$ und $c = 12$. Dann gilt $2|4$, $2|12$ und $2|(4 + 12) = 16$.
3. Sei $a = 2$, $b = 6$ und $c = -7$. Dann gilt $2|6$ und $2| - 42$.
4. Sei $n = 3$, sei $a = 2$, und seien $b_1 = -2$, $b_2 = 6$ und $b_3 = -2$. Seien $c_1 = 7$, $c_2 = -3$ und $c_3 = 5$. Dann gilt $2|(-14 - 18 - 10) = -42$.

Aufgabe 1.2.9

Es gilt $75 = 3 \cdot 24 + 3$. Es folgt $q = 3$ und $r = 3$.

Aufgabe 1.2.14

```
> irem(-23,5);
```

$$-3$$

Auf den Hilfeseiten zu `irem` steht, dass r=`irem(m,n)` folgende Bedingungen erfüllt: $m = qn + r$ mit $|r| < |n|$ und $rm \geq 0$. Es folgt, dass $r < 0$ ist, wenn $m < 0$ ist. In unserer Definition war jedoch der Rest in der Division mit Rest immer größer oder gleich 0. Ein Problem gibt es also, wenn a durch b mit Rest geteilt wird und $a < 0$ gilt.

Aufgabe 1.2.15

Informieren können Sie sich über `mod`, indem Sie `?mod` eingeben. Sie erhalten dann eine Hilfeseite, in der beispielsweise erklärt wird, wie die Syntax des Befehls lautet. Sie können auch den Links der Hilfeseiten folgen.

```
> ?mod
> -987346524 mod (-1234532);
                                279076
> irem(-987346524,-1234532);
                               -955456
```

Lösungen der Aufgaben in 1.3

Aufgabe 1.3.4

Sei $d = \text{ggT}(n, n+1)$. Dann gilt $d|n$ und $d|(n+1)$. Es folgt $d|(n+1-n)$, also $d|1$. Es folgt $d = \pm 1$, und da größte gemeinsame Teiler positiv sind, folgt $d = 1$.

Aufgabe 1.3.8

Es ist $\text{ggT}(16, 6) = 2$. Weiter gilt $\text{ggT}(6, 4) = 2$.

Aufgabe 1.3.11

Es ist

$$\begin{aligned} 299 &= 1 \cdot 247 + 52 \\ 247 &= 4 \cdot 52 + 39 \\ 52 &= 1 \cdot 39 + 13 \\ 39 &= 3 \cdot 13 + 0. \end{aligned}$$

Es folgt $\text{ggT}(299, 247) = 13$.

Es gilt $\mathrm{ggT}(578, -442) = \mathrm{ggT}(578, 442)$. Es ist

$$\begin{aligned} 578 &= 442 + 136 \\ 442 &= 3 \cdot 136 + 34 \\ 136 &= 4 \cdot 34 + 0. \end{aligned}$$

Es folgt $\mathrm{ggT}(578, -442) = 34$.

Aufgabe 1.3.12

```
> igcd(299,247);
                                13
> igcd(578,-442);
                                34
```

Aufgabe 1.3.14

Wir stellen unsere Rechnungen aus Aufgabe 1.3.11 nach den Resten um und erhalten

$$\begin{aligned} 136 &= 578 - 442 \\ 34 &= 442 - 3 \cdot 136. \end{aligned}$$

Jetzt setzen für 136 in der zweiten Zeile ein und erhalten

$$34 = 442 - 3(578 - 442) = -3 \cdot 578 + 4 \cdot 442 = -3 \cdot 578 - 4(-442).$$

Es folgt $s = -3$ und $t = -4$.

Aufgabe 1.3.17

```
> igcdex(12,21,'s','t');s;t;
                                3
                                2
                               -1
```

Um nun s' und t' zu finden, benutzen wir folgende Überlegung: Wenn $12s + 21t = \mathrm{ggT}(12, 21) = 3$ gilt, dann ist auch $12(s + 21) + 21(t - 12) = 3$. Wir können also $s' = 2 + 21 = 23$ und $t' = -1 - 12 = -13$ setzen. Dann ist $23 \cdot 12 - 13 \cdot 21 = 3$.

Aufgabe 1.3.19

Weder 6 und 8 noch 6 und 9 sind teilerfremd.

Lösungen der Aufgabe in 1.4

Aufgabe 1.4.3

```
> ilcm(12345654,-987654);
```

$$2032205759286$$

```
> ilcm(0,0);
```

$$0$$

Aufgabe 1.4.9

Im Vergleich zur Prozedur aus dem Beispiel muss nur noch der Betrag von a und b verwendet werden. Der Maple-Befehl dazu ist `abs`. Wir haben hier außerdem einmal eine Version der Prozedur benutzt, die ohne lokale Variablen auskommt.

```
> kgV:=proc(a,b) # berechnet kgV(a,b)
    abs(a)*abs(b)/igcd(a,b);
  end:
> kgV(24,36);
```

$$72$$

Lösungen der Aufgaben in 1.5

Aufgabe 1.5.4 Wie in Proposition 1.5.3 müssen wir prüfen, ob $\mathrm{ggT}(a,b) \mid c$ gilt.

1. Ihr Maple-Worksheet zu dieser Teilaufgabe könnte folgendermaßen aussehen:

   ```
   > igcd(874394,-27364);
   ```

   $$2$$

   Da 539762 gerade ist, ist also $\mathrm{ggT}(a,b)$ ein Teiler von c, und die lineare Diophantische Gleichung hat eine Lösung.

2. Ihr Maple-Worksheet zu dieser Teilaufgabe könnte folgendermaßen aussehen:

```
> igcd(874396,-27364);
                              4
> igcd(539762,4);
                              2
```

Wir sehen, dass $\mathrm{ggT}(a, b)$ kein Teiler von c ist, das heißt, die lineare Diophantische Gleichung besitzt keine Lösung.

3. Ihr Maple-Worksheet zu dieser Teilaufgabe könnte folgendermaßen aussehen:

```
> igcd(214866,305900);
                             46
> igcd(419336,46);
                             46
```

Hier existiert eine Lösung, denn $46 = \mathrm{ggT}(a, b)$ ist ein Teiler von $c = 419336$.

Aufgabe 1.5.8 Eine Prozedur wie in der Aufgabe gefordert, könnte folgendermaßen aussehen:

```
> Lösungen:=proc(a) #produziert a Lösungen der LDG 2X+3Y=5
   local t;
   for t from 1 to a do
     print(1+3*t,1-2*t);
   od;
  end:
> Lösungen(20);
```

$$
\begin{gathered}
4, -1 \\
7, -3 \\
10, -5 \\
13, -7 \\
16, -9 \\
19, -11 \\
22, -13 \\
25, -15 \\
28, -17 \\
31, -19 \\
34, -21
\end{gathered}
$$

$$37,\ -23$$
$$40,\ -25$$
$$43,\ -27$$
$$46,\ -29$$
$$49,\ -31$$
$$52,\ -33$$
$$55,\ -35$$
$$58,\ -37$$
$$61,\ -39$$

Aufgabe 1.5.11

Es ist $\mathrm{ggT}(2,6) = 2$ und $2|20$. Somit hat die lineare Diopphantische Gleichung Lösungen. Wir überführen sie in reduzierte Form und erhalten $X + 3Y = 10$. Mit scharfem Hinsehen stellen wir fest,dass $(1,3)$ eine Lösung ist. Dann ist

$$\mathcal{L} = \{(1 + 3t, 3 - t) \mid t \in \mathbb{Z}\}$$

die Menge aller Lösungen von $2X + 6Y = 20$.

Aufgabe 1.5.12 Ihr Worksheet könnte wie folgt aussehen:

```
> isolve(2*X+6*Y=20, t);
```

$$\{Y = t,\ X = 10 - 3\,t\}$$

Maple hat als Lösung (x_0, y_0) offenbar $(10, 0)$ gefunden. Gut, das hätten wir natürlich auch finden können. Mit $(x_0, y_0) = (10, 0)$ hätten wir als Lösungsmenge $\mathcal{L} = \{(10+3t, -t) \mid t \in \mathbb{Z}\}$ herausgefunden. Maple findet $\mathcal{L}' = \{(10-3t, t) \mid t \in \mathbb{Z}\}$. Da t aber die ganzen Zahlen durchläuft, sind beide Mengen gleich.

Aufgabe 1.5.13 Die Prozedur setzt einfach Algorithmus 1.5.9 um:

```
> LDG:=proc(a,b,c) #berechnet eine Lösung von aX+bY=c
   local m,s,t;
   m:=c/igcdex(a,b,'s','t');
   print(m*s,m*t);
  end:
> LDG(1234,-5678,736);
```

$$259072,\ 56304$$

```
> 259072*1234-56304*5678;
```

736