Karlhorst Meyer

# Teilbarkeiten, Kongruenzen, DIOPHANTische Gleichungen

Die folgende Abhandlung war früher Teil des Oberseminars im Trainingslager für die bayerische Mannschaft bei der Bundesrunde der Mathematik-Olympiaden. Das Seminar wurde 1996 bis 2014 hinsichtlich zahlentheoretischer Aufgaben des Bundeswettbewerbs Mathematik und der Mathematik-Olympiade von Begabtenförderung Mathematik e. V. angeboten. Vorarbeiten zum Folgenden hat ROLAND GIRGENSON (1999 bis 2001, unveröffentlicht) geleistet. Hierfür gilt es zu danken. Diese Abhandlung übersteigt die Möglichkeiten eines „normalen" Unterrichts am Gymnasium.

## 1. Teiler

**Definition 1.1:** $a \neq 0$ und $b$ seien ganze Zahlen. Man sagt $a$ teilt $b$, in Zeichen $a \mid b$ genau dann, wenn es eine ganze Zahl $q$ mit $b = aq$ gibt. Gibt es eine solche Zahl $q$ nicht, sagt man $a$ teilt $b$ nicht.
Im Folgenden wird die Menge der **ganzen Zahlen** bezeichnet mit $Z = \{\ldots. -3, -2, -1, 0, 1, 2, 3 \ \ldots.\}$. Die Menge der **natürlichen Zahlen** sei $N = \{1, 2, 3, 4, \ldots..\}$; die Menge der natürlichen Zahlen samt der **Zahl null** sei $N_0 = \{0, 1, 2, 3, \ldots..\}$.

*Beispiele 1.1:* $2 \mid 6,\ 5 \mid -10,\ -3 \mid 12$, dagegen: 6 teilt 10 nicht.

Die folgenden Sätzchen können leicht bewiesen werden:

**Satz 1.2:** Alle verwendeten Buchstaben sind beliebige ganze Zahlen:

a) Mit jedem Teiler einer Zahl $a$ hat man stets auch einen zweiten Teiler dieser Zahl gefunden.
b) Will man alle Teiler einer Zahl $a$ finden, muss man nur solche natürlichen Zahlen $n$ mit $n < \sqrt{a}$ prüfen.
c) Das Teilzeichen ist reflexiv, d. h. $a \mid a$ für alle $a$. Insbesondere gilt: $a \mid 0$ falls $a \neq 0$ und $1 \mid a$.
d) Das Teilzeichen ist nicht symmetrisch. Es gilt *nicht*: $a \mid b \Rightarrow b \mid a$.
e) Das Teilzeichen ist transitiv, d. h.: Aus $a \mid b$ *und* $b \mid c$ folgt $a \mid c$.
f) Für beliebige $c \neq 0$ gilt $a \mid b$ genau dann, wenn $ac \mid bc$.
g) Aus $ab \mid c$ folgt $a \mid c$ *und* $b \mid c$.
h) Aus $a \mid b$ *und* $a \mid c$ folgt für beliebige ganze Zahlen $n$ und $m$: $a \mid mb + nc$
i) Aus $a \mid b$ *und* $a \mid mb + c$ für eine ganze Zahl $m$ folgt $a \mid c$.
j) Aus $a \mid b$ *und* $a \mid b + 1$ folgt $a = 1$ *oder* $a = -1$.
k) Aus $a \mid b$ *und* $c \mid d$ folgt $ac \mid bd$.

*Aufgabe 1.1:* a) Weshalb ist die Umkehrung von 1.2g), h) und k) falsch?
b) Beweise 1.2h).
c) Beweise 1.2i).

Ohne Beweis benutzen wir:

**Satz 1.3 (Dezimaldarstellung):** Zu jeder natürlichen Zahl $n$ gibt es Ziffern (das sind die Zahlen 0, 1, 2, 3, 4, 5, 6, 7, 8, 9) $a_0, a_1, \ldots.., a_n$ mit $n \in N_0$ und $a_n \neq 0$ und $a = a_n 10^n + a_{n-1}10^{n-1} + \ldots. + a_1 10 + a_0 10^0$. Hierfür schreiben wir vorübergehend $a = a_n a_{n-1} \ldots.. a_1 a_0$.

*Beispiel 1.2:* $102030 = 1 \cdot 10^5 + 0 \cdot 10^4 + 2 \cdot 10^3 + 0 \cdot 10^2 + 3 \cdot 10 + 0 \cdot 10^0$

**Satz 1.4 (einige Teilbarkeitsregeln): *a* ist durch**

a) 2 teilbar genau dann, wenn $a$ gerade ist, also genau dann, wenn $a_0$ gerade ist.
b) 3 teilbar genau dann, wenn die **Quersumme** von $a$ durch 3 teilbar ist, also wenn gilt $3 \mid a_n + a_{n-1} + .... + a_1 + a_0$.
c) 4 teilbar genau dann, wenn $a_1a_0$ durch 4 teilbar ist.
d) 5 teilbar genau dann, wenn $a_0 = 0$ oder $a_0 = 5$ ist.
e) 6 teilbar genau dann, wenn $a$ durch 2 *und* 3 teilbar ist.
f) 8 teilbar genau dann, wenn $a_2a_1a_0$ durch 8 teilbar ist.
g) 9 teilbar genau dann, wenn die Quersumme durch 9 teilbar ist.
h) 10 teilbar genau dann, wenn $a_0 = 0$ ist.
i) 11 teilbar genau dann, wenn $a_0 - a_1 + a_2 - a_3 + .... \pm a_{n-1} \mp a_n$ durch 11 teilbar ist.

Es gibt weitere Teilbarkeitsregeln, die allerdings wesentlich schwieriger sind.

**Erinnerung:** $(a + b)^n$ heißt **Binom** für beliebige Zahlen $a$, $b$ und einem natürlichen $n$.
Ohne Beweis gilt: $(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$ (1)
mit $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ und $n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n$, wobei $0 \le k \le n$ mit einem natürlichen $k$.

*Beweis zu 1.4i):* An Beispielen findet man rasch die Zwischenbehauptung $10^n \equiv \pm 1 \bmod 11$, die man mit (1) durch vollständige Induktion leicht beweisen kann. Hieraus folgt für jede natürliche Zahl $n$ die Behauptung.

*Aufgabe 1.2:* Beweise die Regeln 1.4b) und g).

**Definition 1.5:** Eine natürliche Zahl $p > 1$ heißt **Primzahl**, wenn sie nur die natürlichen Teiler 1 und $p$ besitzt. Ein Teiler einer Zahl heißt **Primteiler**, wenn er Primzahl und Teiler der Zahl ist.

*Beispiel 1.3:* Die ersten elf Primzahlen sind 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.

*Aufgabe 1.3:* Finde alle Primteiler der Zahl 978. Ist 4567 eine Primzahl?

Ohne Beweis verwenden wir:

**Satz 1.6 (Eindeutige Primfaktorzerlegung):** Jede natürliche Zahl ist Produkt von Primzahlen. Diese Zerlegung ist abgesehen von der Reihenfolge der Faktoren eindeutig.

*Beispiele 1.4:* $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$, $48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$, $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$

**Satz 1.7:** Es gibt unendlich viele Primzahlen.

*Beweis:*
Man betrachte die ersten $n$ Primzahlen $p_1 < p_2 < ..... < p_n$ geordnet nach ihrer Größe und bildet $q = p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Dann muss die Zahl $q + 1$ ein $r$ als kleinsten wesentlichen Teiler haben. Dieses $r$ muss eine Primzahl größer als $p_n$ sein, weil kein Teiler $p_i$ von $q$ nach Satz 1.2j) auch Teiler von $q + 1$ sein kann. Damit hat man eine weitere Primzahl gefunden.

**Satz 1.8:** Für Primzahlen $p$, $q$ gelten:

a) $p \mid ab$ genau dann, wenn $p \mid a$ *oder/und* $p \mid b$.
b) $p \mid b$ *und* $q \mid b$ dann und nur dann, wenn $p \cdot q \mid b$.

# 2. Kongruenzen

**Satz 2.1 (Division mit Rest):** Es seien $a$ und $b$ ganze Zahlen, $q$ eine natürliche Zahl, $a = cq + r$ und $b = dq + s$ mit $0 \le r < q$ und $0 \le s < q$. Dann gilt: $r = s$ genau dann, wenn gilt $q \mid b - a$.

*Beweis:*
1. $r = s$, also $a - cq = b - dq$, also $b - a = (c - d)q$ und damit $q \mid b - a$.
2. Aus $a = cq + s$ und $b = dq + r$ mit $s$ und $r$ kleiner als $q$, also auch $0 < s - r < q$ und der Annahme $q \mid b - a$ folgt $b - a = q(d - c) + (s - r)$; also ist $s = r$.

*Aufgabe 2.1:* Berechne $r$ und $s$ aus Satz 2.1 für $a = 31$, $b = 27$ und $q = 4$

**Definition 2.2:** $a$ und $b$ seien ganze Zahlen, $m$ eine natürliche Zahl (d. h. ungleich null). Man schreibt $a \equiv b \bmod m$ oder $a \equiv b(m)$, gesprochen ***a* kongruent *b* modulo *m*,** genau dann, wenn $m \mid a - b$.

**Definition 2.3:** $\underline{a}_m = \underline{a}(m) = \underline{a}: = \{b: a \equiv b \bmod m\} = \{b: b = a - m \cdot n \text{ für alle } n \in Z\} = \{a + m \cdot n \text{ für alle } n \in Z\}$

$b$ ist hierbei nicht eindeutig bestimmt, z. B.: $10^n \equiv 10^{n-1} \equiv 10^{n-2} \equiv .... \equiv 10 \equiv 0 \bmod 10$. Es gibt also eine Menge $\underline{a}_m$ von ganzen Zahlen b, die modulo $m$ zu einem gegebenen $a$ gehören. Man nennt diese Menge die **Restklasse** $\underline{a}_m$ modulo $m$. In jeder dieser Restklassen liegt ein $b$ mit kleinstem $|b|$, d. h. mit $|b| <$ m. Dieses $b$ erhält man, wenn man die Division $a : m$ bis auf diesen kleinsten Rest $b$ durchführt.

*Aufgabe 2.2:* a) Es seien $a = 31$, $b = 27$ und $m = 4$. Zeige $a \equiv b \bmod m$ und $m \mid a - b$.
b) Finde alle $a$ mit $a \equiv 3 \bmod 4$.

*Aufgabe 2.3:* Konstruiere die Restklasse $\underline{1}_4$ und gib alle weiteren Restklassen für $m = 4$ an.

**Sätze 2.4:**

a) $a \mid c \Leftrightarrow c \equiv 0 \bmod a$.
b) $a \equiv a \bmod m$ (Reflexivität des Kongruenzzeichens).
c) $a \equiv b \bmod m \Leftrightarrow b \equiv a \bmod m$ (Symmetrie des Kongruenzzeichens).
d) Aus $a \equiv b \bmod m$ *und* $b \equiv c \bmod m$ folgt $a \equiv c \bmod m$ (Transitivität des Kongruenzzeichens).
e) Aus $a \equiv b \bmod m$ *und* $c \equiv d \bmod m$ folgt $a \pm c \equiv (b \pm d) \bmod m$.
f) Aus $a \equiv b \bmod m$ *und* $c \equiv d \bmod m$ folgt $a \cdot c \equiv (b \cdot d) \bmod m$.
g) b), c) und d) kann man zusammenfassen: Das Kongruenzzeichen definiert eine Äquivalenzrelation.
h) Ist $p(x)$ ein Polynom mit ganzen Koeffizienten *und* $c \equiv d \bmod m$, so ist $p(c) \equiv p(d) \bmod m$.

*Aufgabe 2.4:* Beweise alle Sätze von 2.4 und finde Beispiele für diese Sätze.

**Definition 2.5:** In der Menge aller Äquivalenzklassen modulo m führt man eine algebraische Struktur ein:
$\underline{a} + \underline{b}: = \underline{a + b}$ und $\underline{a} \cdot \underline{b}: = \underline{a \cdot b}$

**Hinweis:** In einem kommutativen Ring mit 1 (1 ist das neutrale Element der Multiplikation) gelten alle aus dem Unterricht bekannten Rechenregeln der Addition und der Multiplikation einschließlich Distributivgesetz außer dem Dividieren.

**Satz 2.6:** Die Menge $\mathfrak{R}_m$ aller Äquivalenzklassen modulo $m$ bildet einen kommutativen Ring mit der Eins $\underline{1}_m$.

*Aufgabe 2.5:* Beweise Satz 2.6.

Die „Division“ in $\mathfrak{R}_m$ zeigt Besonderheiten; z. B. gilt $2 \cdot 3 \equiv 0 \bmod 6$. Hieraus folgt $\underline{2} \cdot \underline{3} = \underline{0}$, obwohl $\underline{2} \neq \underline{0}$ *und* $\underline{3} \neq \underline{0}$. Man sagt $\mathfrak{R}_6$ hat **Nullteiler**, weil z. B. $\underline{2}$ und $\underline{3}$ die Restklasse $\underline{0}$ teilen. Es gibt deshalb keine Division in $\mathfrak{R}_6$ (siehe in Beispiel 2.1 die unterlegten Felder in der Multiplikationstafel von $\mathfrak{R}_6$).

*Beispiel 2.1:* mod 6

| · | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

| a:b | b | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| a | | | | | | |
| 1 | | 1 | - | - | - | 5 |
| 2 | | 2 | 1?4? | - | 2?5? | 4 |
| 3 | | 3 | - | 1?3?5? | - | 3 |
| 4 | | 4 | 2?5? | - | 1?4? | 2 |
| 5 | | 5 | - | - | - | 1 |

*Beispiel 2.2:* mod 5

| · | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

| a:b | b | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| a | | | | | |
| 1 | | 1 | 3 | 2 | 4 |
| 2 | | 2 | 1 | 4 | 3 |
| 3 | | 3 | 4 | 1 | 2 |
| 4 | | 4 | 2 | 3 | 1 |

*Aufgabe 2.6:* a) Vergleiche die Multiplikationstafeln der Beispiele 2.1 und 2.2:
Was fällt in den Zeilen auf,
was fällt in den Spalten auf,
welche Symmetrien stellt man fest?
b) Weshalb gibt es in $\mathfrak{R}_6$ keine Division?

**Satz 2.7:** Wenn $a = b$ ist, gilt $a \equiv b \bmod m$ für alle $m$ aus Z.

Die Umkehrung dieses Satzes gilt nicht; z. B. Es gilt zwar $6 \equiv 2 \bmod 4$, aber trotzdem ist $6 \neq 2$.

*Beispiel 2.3:* Beweise: 8007 kann nicht Summe von 3 Quadraten sein.

*Beweis:* Wegen Satz 2.7 genügt es 8007 z. b. modulo 8 zu untersuchen: $8007 \equiv 7 \bmod 8$.

| n | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $n^2$ | 0 | 1 | 4 | 1 | 0 | 1 | 4 | 1 |

Man muss nun einige Fälle untersuchen und stellt fest: Die Summe von drei beliebigen Klassen von $n^2$ ist niemals $\underline{7}$.

*Beispiel 2.4:* Zeige $9^n + 1$ mit natürlichem $n$ wird für kein $n$ von 100 geteilt.

*Beweis:* Wenn 100 teilen würde, müsste auch 4 Teiler sein, was aber für kein $n$ möglich ist, da $9 \equiv 1 \bmod 4$ und deshalb $9^n + 1 \equiv 2 \bmod 4$ gilt und damit $9^n + 1$ nicht durch 4 teilbar ist.

**Definition 2.8:** $t$ heißt gemeinsamer Teiler von $a$ und $b$, wenn $t$ beide ganzen Zahlen teilt. Da man alle gemeinsamen Teiler zweier Zahlen kennt, wenn man den **größten gemeinsamen Teiler**, abgekürzt $ggT(a,b)$, kennt, interessiert man sich für $ggT(a,b)$. Haben zwei Zahlen $a$ und $b$ außer 1 (bzw. – 1) keine weiteren gemeinsamen Teiler, so nennt man sie **teilerfremd** und schreibt $ggT(a,b) = 1$.

**Satz 2.9:** Aus $ax \equiv ac \bmod m$ mit $ggT(a,m) = 1$ folgt $x \equiv c \bmod m$.

*Aufgabe 2.7:* Beweise Satz 2.9.

# 3. Satz von EULER – FERMAT[1]

Es seien $a$ und $c$ teilerfremde natürliche Zahlen, außerdem $n \in \mathbb{N}$. Will man den Rest von $a^n$ bei Division durch $c$ bestimmen und ist $n$ recht groß, so ist es nützlich, einen Exponenten $m$ zu kennen mit $a^m \equiv 1 \bmod c$, denn für $n > m$ ist dann $a^n \equiv a^m a^{n-m} \equiv a^{n-m} \bmod c$. Auf diese Weise kann man den Exponenten von $a$ oft stark verkleinern und sich die Aufgabe erleichtern. Nehmen wir einmal an, es gebe einen kleinsten natürlichen Exponenten $m$ mit $a^m \equiv 1 \bmod c$. Dann sind alle natürlichen Exponenten $k$ mit $a^k \equiv 1 \bmod c$ Vielfache von $m$, denn wenn man $k$ mit Rest durch $m$ dividiert, erhält man $k = tm + r$, $r < m$, also ist dann

$$1 \equiv a^k \equiv a^{tm+r} \equiv (a^m)^t a^r \equiv a^r \bmod c.$$

Da $m$ die kleinste natürliche Zahl ist mit $a^m \equiv 1 \bmod c$, kann dies also nur gelten für $r = 0$. Mit dem Satz von EULER-FERMAT kann man ziemlich leicht ein für viele Anwendungen genügend kleines Vielfaches von $m$ erhalten. Hierzu muss zunächst noch die sogenannte EULERsche $\phi$-Funktion eingeführt werden:

**Definition 3.1:** Für gegebenes $n \in \mathbb{N}$ sei die EULERsche $\phi$-Funktion die **Anzahl** der zu $n$ teilerfremden Zahlen $c$ mit $1 \le c \le n$.

*Beispiel 3.1:* $\phi(6) = 2$ (nämlich die Zahlen 1 und 5).

**Satz 3.2:** Ist $p$ Primzahl, so gilt $\phi(p) = p - 1$.

*Beweis:* Die $p - 1$ Zahlen 1, 2, ... , $p - 1$ sind zu $p$ teilerfremd.

Es sei $n = p_1^{a_1} p_2^{a_2} \ldots\ldots p_r^{a_r}$ die Zerlegung einer natürlichen Zahl $n$ in Primfaktoren, wobei die Faktoren $p_1, \ldots, p_r$ Primzahlen sind und $a_1, \ldots, a_r$ natürliche Zahlen. Bestimme $\phi(n)$, ausgehend von der Menge $\{1; 2; \ldots; n\}$ mit $n$ Elementen. Alle Vielfachen von $p_1$ sind nicht teilerfremd zu $n$, dies schließt genau $n/p_1$ Zahlen aus. Alle Vielfachen von $p_2$ sind auch nicht teilerfremd zu $n$, müssen also auch ausgeschlossen werden usw. Hierbei sind offenbar einige Zahlen zuviel ausgeschlossen worden, nämlich z. B. die Vielfachen von $p_1 p_2$ einmal zu viel; sie müssen also wieder eingerechnet werden, also $\frac{n}{p_1 p_2}$ Zahlen, ebenso die Vielfachen der anderen Produkte zweier Primfaktoren. Die Vielfachen der Produkte dreier Primfaktoren sind zunächst dreimal ausgeschlossen, dann wieder dreimal eingerechnet worden, müssen also nochmals ausgeschlossen werden usw. Schließlich erhält man:

**Satz 3.3:**

$$\phi(n) = n - \frac{n}{p_1} - \ldots - \frac{n}{p_r} + \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \ldots + \frac{n}{p_{r-1} p_r} - \frac{n}{p_1 p_2 p_3} - \ldots + \frac{(-1)^r n}{p_1 p_2 \cdots p_r} =$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\ldots\left(1 - \frac{1}{p_r}\right).$$

**Satz 3.4 von EULER – FERMAT:** Es seien $a$ und $c$ teilerfremde natürliche Zahlen. Dann gilt $a^{\phi(c)} \equiv 1 \bmod c$.

*Beweis:*
Es seien $d_1, \ldots, d_{\phi(c)}$ die zu $c$ teilerfremden Zahlen in $\{1, \ldots, c\}$. Dann sind auch die Zahlen $ad_1, \ldots, ad_{\phi(c)}$ teilerfremd zu $c$ und haben paarweise verschiedene Reste bei Division durch $c$;

[1] LEONHARD EULER *15. 4. 1707 Basel, †18. 9. 1783 (gregorianisch) St. Petersburg
PIERRE DE FERMAT *1607, † 12. 1. 1665 in Castres

denn sind $k$ und $m$ Indices mit $ad_k \equiv ad_m \bmod c$, folgt $c \mid a(d_k - d_m)$ und $c \mid d_k - d_m$ und $d_k = d_m$, da $a$ und $c$ teilerfremd sind. Daher haben auch $ad_1, ..., ad_{\phi(c)}$ alle möglichen Reste bei Division durch $c$, die bei zu $c$ teilerfremden Zahlen auftreten können, somit ist

$d_1....d_{\phi(c)} \equiv \mathrm{ad}_1...\mathrm{ad}_{\phi(c)} \bmod c \Rightarrow$

$\mathrm{d}_1....d_{\phi(c)} \equiv a^{\phi(c)}d_1...d_{\phi(c)} \bmod c \Rightarrow$

$c \mid (a^{\phi(c)} - 1)\, d_1....d_{\phi(c)} \Rightarrow c \mid (a^{\phi(c)} - 1) \Rightarrow a^{\phi(c)} \equiv 1 \bmod c$

*Beispiel 3.2:* Welchen Rest hat $15337^{15338}$ bei Division durch 6?

*Lösung:* 15337 ist teilerfremd zu 6, also ist $15337^{\phi(6)} \equiv 1 \bmod 6$. Wegen $\phi(6) = 2$ ist $15337^2 \equiv 1 \bmod 6$, also auch $15337^{15338} \equiv 1 \bmod 6$.

*Beispiel 3.3:* Zeige $7 \mid 2222^{5555} + 5555^{2222}$.

*Lösung:*
Es ist $2222 \equiv 3 \bmod 7$, $5555 \equiv 4 \bmod 7$, weiter ist $\phi(7) = 6$, $2222 \equiv 2 \bmod 6$ und $5555 \equiv 5 \bmod 6$. Damit folgt $2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \equiv 3^{925\cdot 6 + 5} + 2^{370\cdot 6 + 2} \equiv 3^5 + 4^2 \equiv 259 \equiv 0 \bmod 7$.

# 4. EUKLIDischer[2] Algorithmus

Zur Bestimmung des größten gemeinsamen Teilers zweier nicht negativen ganzen Zahlen zerlegt man oft diese in Primfaktoren und sieht nach, welche Faktoren bei beiden Zahlen vorkommen. Man kann den größten gemeinsamen Teiler aber auch ohne Primfaktorzerlegung bestimmen:

*Beispiel 4.1:* Gesucht wird *ggT* (525, 231):

1. Lösung:

$525 = 2\cdot 231 + \mathbf{63}$

$231 = 3\cdot\mathbf{63} + \underline{42}$

$\mathbf{63} = 1\cdot\underline{42} + \underline{\underline{21}}$

$\underline{42} = 2\cdot\underline{\underline{21}} + 0$

$\underline{\underline{21}} = ggT(525, 231)$

oder 2. Lösung:

$525 - 2\cdot 231 = \mathbf{63}$

$231 - 3\cdot\mathbf{63} = \underline{42}$

$\mathbf{63} - \underline{42} = \underline{\underline{21}}$

$\underline{42} - 2\cdot\underline{\underline{21}} = 0$

oder:

3. Lösung

$525 = 2\cdot 231 + \mathbf{63} =$

$= 2\cdot(3\cdot\mathbf{63} + \underline{42}) + \mathbf{63} =$

$= 2\cdot(3\cdot 3\cdot\underline{\underline{21}} + 2\cdot\underline{\underline{21}}) + 3\cdot\underline{\underline{21}} =$

$= 2\cdot 11\cdot\underline{\underline{21}} + 3\cdot\underline{\underline{21}} =$ also $231 = 11\cdot\underline{\underline{21}}$

$= 25\cdot\underline{\underline{21}}$ deshalb ist ggT(525, 231) = 21

*Allgemein:* Für die natürlichen Zahlen $a$ und $b$ wird der $ggT(a, b)$ gesucht. Da trivial $ggT(a,a) = a$ ist, kann ohne Beschränkung der Allgemeinheit $a > b$ angenommen werden. Für alle natürlichen $s$ mit $sb \le a$ gilt: $t$ ist gemeinsamer Teiler von $a$ und $b$ genau dann, wenn $t \mid a - sb$ *und* $t \mid b$. Bei diesem Reduktionsschritt bleibt auch der größte gemeinsame Teiler unverändert, nur die zu betrachtenden Zahlen werden kleiner. Diese Reduktion setzt man so lange fort, bis eine der jeweils beteiligten Zahlen 0 ist. Da dann $ggT(a, b) = ggT(x, 0) = x$ ist, hat man damit $ggT(a, b)$ gefunden.

Man kann Beispiel 4.1 auch noch anders interpretieren:

[2] EUKLID VON ALEXANDRIA * um 300 v. Chr.

*Beispiel 4.1 Fortsetzung (so genannter **erweiterter EUKLIDischer Algorihmus**):*
Die 4. Lösung erhält man, wenn man die 2. Rechnung von unten nach oben liest:
$\underline{21} = \mathbf{63} - 42 =$
$= \mathbf{63} - (231 - 3\cdot\mathbf{63}) =$
$= \mathbf{63} + 3\cdot\mathbf{63} - 231 =$
$= 4\cdot\mathbf{63} - 231 =$
$= 4\cdot(525 - 2\cdot 231) - 231 =$
$= 4\cdot 525 - 9\cdot 231$

Damit hat man den folgenden Satz gefunden:

**Satz 4.1:** Für alle natürlichen Zahlen $a$ und $b$ gibt es ganze Zahlen $k$ und $m$ so, dass $ka + mb = ggT(a, b)$ ist.

**Satz 4.2:** Es seien $a$, $b$ teilerfremde natürliche Zahlen. Dann gibt es eine Zahl $k \in \mathbb{Z}$ mit $ka \equiv 1 \bmod b$.

*Beweis:*

1. Möglichkeit: Da $a$ und $b$ teilerfremd sind, gibt es nach Satz 4.1 ganzzahlige Vielfache $ka$ und $km$ mit $ka + mb = ggT(a, b) = 1$. Dann ist aber $ka \equiv 1 \bmod b$.
2. Möglichkeit: Nach dem Satz von EULER-FERMAT ist mit $k$: $= a^{\phi(b)-1}$ auch $ka \equiv a^{\phi(b)} \equiv 1 \bmod b$.

*Beispiel 4.2:* Bestimme die kleinste natürliche Zahl, die auf 1986 endet und durch 1987 teilbar ist.

*Lösung:*
Die Zahl hat die Darstellung $10000x + 1986$ mit $x \in \mathbb{N}_0$. Gilt $1987 \mid 10000x + 1986$, gibt es $n \in \mathbb{N}$ mit $1987n = 10000x + 1986$ bzw. $10000x - 1987(n - 1) = 1$.
Bestimmen wir zunächst einmal mit dem euklidischen Algorithmus das $ggT(10000, 1987)$:

$10\,000 = 1987\cdot 5 + 65$ (1)
$1987 = 65\cdot 30 + \mathbf{37}$ (2)
$65 = \mathbf{37}\cdot 1 + \underline{28}$ (3)
$\mathbf{37} = \underline{28}\cdot 1 + \underline{9}$ (4)
$\underline{28} = \underline{9}\cdot 3 + 1$ (5)
$\underline{9} = 9\cdot 1 + 0$, d. h. $ggT(10\,000, 1987) = 1$

Mit dem erweiterten euklidischen Algorithmus erhält man hieraus (*Vorsicht: Die markierten Zahlen haben hier eine andere Bedeutung als oben*):

$1 = \mathbf{28} - 9\cdot 3 =$
$= \mathbf{(37 - 9)} - 9\cdot 3 = 37 - \mathbf{9}\cdot 4 =$
$= 37 - \mathbf{(37 - 28)}\cdot 4 = -37\cdot 3 + \mathbf{28}\cdot 4 =$
$= -37\cdot 3 + \mathbf{(65 - 37)}\cdot 4 = 65\cdot 4 - \mathbf{37}\cdot 7 =$
$= 65\cdot 4 - \mathbf{(1987 - 65\cdot 30)}\cdot 7 = \mathbf{65}\cdot 214 - 1987\cdot 7 =$
$= \mathbf{(10\,000 - 5\cdot 1987)}\cdot 214 - 1987\cdot 7 = 10\,000\cdot 214 - 1987\cdot 1077.$

Zum Verfahren:
Man beginnt bei (5) und arbeitet sich „nach oben“ durch. Jeweils die fetten Zahlen werden im nächsten Schritt durch die vorhergehende Gleichung mit dem Ziel ersetzt, die Zahlen immer größer werden zu lassen. Also ist $x = 214$ und $n = 1078$. Die Zahl lautet 2141986.

# 5. DIOPHANTische[3] Gleichungen

Eine Gleichung z. B. in den Unbekannten *x* und *y* lautet $ax + my = b$ mit Zahlen *a*, *b* und *m* mit
$a^2 + m^2 \neq 0$. (1)
Alle ihre Lösungen $(x \mid y)$ stellt man z. B. dar als $\left\{(x \mid y) \text{ und } y = \frac{b-ax}{m} \text{ für alle } x\right\}$ falls $m \neq 0$. Ansonsten wählt man eine analoge Beziehung mit *y* als Parameter; dies ist wegen (1) möglich. Die gegebene Gleichung definiert in einem Koordinatensystem in *x* und *y* eine Gerade, hat also für jedes reelle *x* oder *y* einen Punkt.

Dgg:
DIOPHANTische Gleichungen sind lineare Gleichungen in mehreren Unbekannten mit ganzzahligen Parametern; man sucht **ganzzahlige Lösungen** für die Gleichung. Im einfachsten Fall hat man für $m \neq 0$ die Gleichung $ax + my = b$ oder – falls auch $m \neq \pm 1$ – die Beziehung $ax \equiv b \bmod m$.

**Satz 5.1:** Für die natürliche Zahl $m \neq 1$ und ganze Zahlen *a* und *b* hat $ax \equiv b \bmod m$ oder $ax + my = b$ genau dann ganzzahlige Lösungen $(x \mid y)$, wenn $ggT(a,m) \mid b$ gilt.

*Beweis:*
1. $ggT(a,m) \mid b$:
1a) Ist $ggT(a,m) = 1$, dann hat $ax \equiv b \bmod m$ nach Satz 4.1 ganzzahlige Lösungen; es gibt eine ganze Zahl *d* aus der Restklasse $\underline{b}_m$ mit $d = ac$. Damit ist $ax \equiv ac \bmod m$ und wegen $ggT(a,m) = 1$ kann Satz 2.9 angewendet werden und es gilt $x \equiv c \bmod m$.

1b) Ist $ggT(a,m) = e > 1$ und $e \mid b$, also gibt es ein *b'* mit $b = eb'$; wegen $ggT(a,m) = e$ gibt es *a'* und *m'* mit $a = ea'$ und $m = em'$. Damit folgt aus $ax \equiv b \bmod m$ die Kongruenz $a'x \equiv b' \bmod m'$ mit $ggT(a',m') = 1$ und man fährt nach 1) mit der Konstruktion der Lösung fort.

2. Die Gleichung $ax + my = b$ mit $e = ggT(a,m)$ hat eine ganzzahlige Lösung $(x \mid y)$:
Es gibt dann ein ganzes *k* so, dass $ax + my = ke = b$. Wegen der eindeutigen Primfaktorzerlegung muss dann $e \mid b$ gelten.

*Beispiel 5.1:* $3x + 5y = 2$ mit $ggT(3,5) = 1$
$3x \equiv 2 \bmod 5$
$3x \equiv 12 \bmod 5$, wegen $ggT(3,5) = 1$ folgt:
$x \equiv 4 \bmod 5$
$x = 5k + 4$ für alle ganzen *k*, d. h.
$5y = 2 - 3x = 2 - 15k - 12 = -10 - 15k$ oder
$y = -2 - 3k$
$L = \{(5k + 4 \mid -2 - 3k) \text{ für alle ganzen } k\}$.

*Beispiel 5.2:* $6x + 10y = 4$ mit $ggT(6,10) = 2 \mid 4$; deshalb bekommt man
$3x + 5y = 2$ mit $ggT(3,5) = 1$
Die weitere Lösung geschieht wie bei Beispiel 1.

**Reduktionsverfahren von EULER:**
*Beispiel 5.3:* Bestimme alle ganzzahligen Lösungen von $179x + 234y = 251$

[3] DIOPHANTOS VON ALEXANDRIA * zwischen 150 v. Chr. bis 364 n. Chr.

*Lösung:*

| Divisionsalgorithmus | Reduktionsverfahren nach EULER |
|---|---|
| 234 = 179 + **55** führt zu ⇒ | $x = \frac{-234y + 251}{179} = \frac{(-179 - 55)y + (179 + 55)}{179}$ also<br>$x = -y + 1 + u$ (1)<br>mit $u := \frac{-55y + 72}{179}$ äquivalent zu:<br>$-179u = 55y - 72$ äquivalent zu: |
| 179 = 3·**55** + 14 führt zu ⇒ | $y = \frac{-179u + 72}{55} = \frac{-(3 \cdot 55 + 14)u + (55 + 17)}{55}$ also<br>$y = 3u + 1 + v$ (2)<br>mit $v := \frac{-14u + 17}{55}$ äquivalent zu:<br>$14u - 17 = -55v$ äquivalent zu: |
| **55** = 3·14 + 13 führt zu ⇒ | $u = \frac{-55v + 17}{14} = \frac{-4 \cdot 14v + 14 + v + 3}{14}$ also<br>$u = -4v + 1 + k$ (3)<br>mit $w := \frac{v + 3}{14}$ äquivalent zu:<br>$v + 3 = 14w$ äquivalent zu<br>$v = -3 + 14w$ (4) |
| 14 = 13 + 1<br>13 = 1·13 + *0* folgt<br>*ggT*(179, 234) = 1; damit ist die Lösungsmenge L nicht leer. | (4) eingesetzt in (3) gibt:<br>$u = -4(-3 + 14w) + 1 + w$ also<br>$u = 13 - 55w$ (5)<br>(4) und (5) eingesetzt in (2):<br>$y = -3(13 - 55w) + 1 + (-3 + 14w)$ also<br>$y = -41 + 179w$ (6)<br>(5) und (6) eingesetzt in (1):<br>$x = -(-41 + 179w) + 1 + (13 - 55w)$ also<br>$x = 55 - 234w$ |
| Probe | $179(55 - 234w) + 234(-41 + 179w) = 251$ |
| Ergebnis nach (5) und (6) | L = {$(x \mid y) = (55 - 234w \mid -41 + 179w$ für alle ganzen $w$] |

**Hinweis:** | hat in der Mathematik mindestens zwei Verwendungsmöglichkeiten:

a) $a \mid b$ bedeutet *a* teilt *b*

b) $(x \mid y)$ sind ein Paar, z. B. Koordinaten.

*Aufgabe 5.1:* Finde alle Lösungen von $411x + 379y = 371$

# 6. Lösungen

**Aufgabe 1.1:**

a) Man bildet formal eine Umkehrung U und sucht ein Beispiel, das zeigt, dass die Umkehrung U nicht existiert:

U2.1g): Aus $a \mid c$ und $b \mid c$ folgt $ab \mid c$, ist falsch, weil es ein Gegenbeispiel gibt:

$6 \mid 12$ und $4 \mid 12$, aber $6 \cdot 4 = 24$ teilt 12 nicht.

U2.1h): Aus $a \mid mb + nc$ folgt $a \mid c$ und $a \mid c$ ist falsch, weil es ein Gegenbeispiel gibt:

$5 \mid 1 \cdot 2 + 1 \cdot 3$, aber 5 teilt weder 2 noch 3.

U2.1k): Aus $ac \mid bd$ folgt $a \mid b$ und $c \mid d$ ist falsch, weil es ein Gegenbeispiel gibt:
$6 \cdot 15 \mid 18 \cdot 10$, aber 6 teilt zwar 18 aber 15 nicht 10.

b) Aus $a \mid b$ also $a \cdot b_1 = b$ und $a \mid c$ also $a \cdot c_1 = c$ folgt $mb + nc = mab_1 + nac_1 = a(mb_1 + nc_1)$ folgt $a \mid mb + nc$.

c) $a \mid b$ und $a \mid mb + c$ folgt nach Satz 1.1h): $a \mid (-m)b + 1 \cdot (mb + c) \Rightarrow a \mid c$.

**Aufgabe 1.2:** Beweis zu den Aufgaben 1.4b) und 1.4g):
Aus Satz 1.2h) folgt: Teilt c zwei Zahlen, so teilt c auch deren Summe oder Differenz.
Aus $a = \sum_{k=1}^{n} a_k 10^k$ und 10 = 9 + 1, 100 = 99 + 1, 1000 = 999 + 1 usw. folgt:
$a = a_0 + a_1(9 + 1) + a_2(99 + 1) + a_3(999 + 1) + \ \ldots + a_n(99999 \ldots 9 + 1) =$
$= 9 \cdot z + q$ mit $q = a_0 + a_1 + a_2 + a_3 + \ldots + a_n$ mit $z = a_1 + 11a_2 + \cdots + 111 \ldots 1a_n$
$9 \cdot z$ ist durch 3 und 9 teilbar. Wenn 3 oder 9 Teiler von a ist, dann auch von $q = a - 9 \cdot z$. Wenn 3 oder 9 Teiler von $q$ ist, dann auch von $a = 9 \cdot z + q$.

**Aufgabe 1.3:**
a) Nach 1.4a) gilt $2 \mid 978$ und nach 1.4b) gilt $3 \mid 978$, weil $3 \mid 24$. Nach 1.4e folgt hieraus $6 \mid 978 = 6 \cdot 163$. Deshalb muss man nach Satz 1.2b) nur noch die Teiler von 163 finden. Da $\sqrt{163} = 12{,}7..$, muss man nur noch Teiler bis 12 untersuchen. 163 ist ungerade und deshalb nach Satz 1.4a durch 2, 4, 8, 10 und 12 nicht teilbar. Man muss also nun noch untersuchen, ob 5, 7 oder 9 Teiler sein können:
Nach Satz 1.4h) scheidet 5 als Teiler aus.
Nach Satz 1.4g) scheidet 9 als Teiler aus, weil die Quersumme von 163 den Wert 10 hat. 7 ist kein Teiler, weil 163:7 = 23,2.. beträgt. 163 ist demnach Primzahl und $978 = 2 \cdot 3 \cdot 163$. 978 hat also drei Primteiler.
b) Nach Satz 1.2b) untersucht man die Primteiler bis $\sqrt{4567} = 67{,}5..$ also bis 67; dies ist eine Primzahl. Da die Quersumme der ungeraden Zahl 4567 den Wert 22 hat, erkennt man, auch anhand der letzten Ziffer, dass 2, 3 und 5 keine Primteiler sein können.
Man muss noch mehrere Divisionen 4567 : $a = b$ für Primzahlen $a$ durchführen; stellt es sich heraus, dass kein $b$ eine ganze Zahl ist, dann ist 4567 selbst prim. Man findet die folgenden Ergebnisse:

| $a$ | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 |
|---|---|---|---|---|---|---|---|---|---|---|
| $b$ | 652,4.. | 415,1.. | 351,3.. | 268,6.. | 240,3.. | 198,5.. | 157.4.. | 147,3.. | 123,4.. | 111,3.. |

| $a$ | 43 | 47 | 53 | 59 | 61 | 67 |
|---|---|---|---|---|---|---|
| $b$ | 106,2.. | 97,1.. | 86,1.. | 77,4.. | 74,8.. | 68,1.. |

**Aufgabe 2.1:**
Da $31 = 7 \cdot 4 + 3$ und $27 = 6 \cdot 4 + 3$ sind, gilt r = s = 3.

**Aufgabe 2.2:**
a) $31 \equiv 3 \bmod 4 \equiv 27$, also gilt $31 \equiv 27 \bmod 4$ und $4 \mid 31 - 27 = 4$.
b) …., –4, –1, 3, 7, 11, 15, 19, 23, 27, 31, …. Genauer: $\underline{3}_4 = \{4k + 3 \text{ für alle } k \in \mathrm{Z}\}$

**Aufgabe 2.3:**
Die Division durch 4 hat die Reste 0, 1, 2 oder 3; deshalb gibt es die Restklassen
$\underline{0} = \{4k \text{ mit } k \in Z\}$, $\underline{1} = \{4k + 1 \text{ mit } k \in Z\}$,
$\underline{2} = \{4k + 2 \text{ mit } k \in Z\}$ und $\underline{3} = \{4k + 3 \text{ mit } k \in Z\}$.

**Aufgabe 2.4:**
a) Aus $a \mid c$ folgt $a \mid c - 0$ und mit Definition 2.2 gilt: $c \equiv 0 \bmod a$. Umgekehrt ist Letzteres nach Definition 2.2 äquivalent mit $a \mid c - 0 = c$.
b) Jede Zahl $m \neq 0$ teilt $0 = a - a$, was nach Definition 2.2 äquivalent mit $a \equiv a \bmod m$ ist.

c) Nach Definition 2.2 ist $a \equiv b \bmod m$ äquivalent zu $m \mid a - b$, was äquivalent zu $m \mid -(a - b) = b - a$ ist und damit abermals nach Definition 2.2 äquivalent zu $b \equiv a \bmod m$.
d) Nach Definition 2.2 folgt aus $a \equiv b \bmod m$, dass $m \mid a - b$. (1)
Nach Definition 2.2 folgt aus $b \equiv c \bmod m$, dass $m \mid b - c$. (2)
Aus (1) und (2) folgt nach Satz 1.2h) $m \mid (a - b) + (b - c) = a - c$ also $a \equiv c \bmod m$.
e) Nach Definition 2.2 folgt aus $a \equiv b \bmod m$, dass $m \mid a - b$. (3)
Nach Definition 2.2 folgt aus $c \equiv d \bmod m$, dass $m \mid c - d$. (4)
Aus (3) und (4) folgt nach Satz 1.2h) $m \mid (a - b) \pm (c - d) = (a \pm c) - (b \pm d)$ also $a \pm c \equiv (b \pm d) \bmod m$.
f) Aus $a \equiv b \bmod m$ und $c \equiv d \bmod m$ folgt $m \mid a - b$ und $m \mid c - d$. Mit den Sätzen 1.2f) und g) folgt $m \mid ca - cb$ und $m \mid bc - bd$ und mit Satz 1.2h) $m \mid ca - cb + bc - bd = ac - bd$, also $ac \equiv bd \bmod m$.
g) ist eine Definition.
h) Es sei $p(x) = \sum_{i=0}^{n} a_i x^i$. Für alle $i$ aus $c \equiv d \bmod m$ mit Satz 2.4f): $a_i c^i \equiv a_i d^i \bmod m$. So erhält man aus Satz 2.4e): $p(c) \equiv p(d) \bmod m$.

Beispiele:
a) $3 \mid 12$ also $3 \cdot 4 = 12$ also $12 \equiv 0 \bmod 3$; umgekehrt $12 \equiv 0 \bmod 3$ hat zur Folge $12 = 3 \cdot 4 + 0$, also $3 \mid 12$.
b) $3 \equiv 3 \bmod 4$ bedeutet $3 \mid 3 - 0 = 3$.
c) $3 \equiv 7 \bmod 4$, also $4 \mid 3 - 7 = -4$. Dann ist auch $4 \mid 7 - 3$ wahr und damit $7 \equiv 3 \bmod 4$.
d) Aus $3 \equiv 7 \bmod 4$ und $7 \equiv 15 \bmod 4$ folgt $4 \mid 3 - 7 = -4$ und $4 \mid 7 - 15 = -8$. Hieraus folgt nach Satz 1.2h) $4 \mid -8 + (-4) = -12 = 3 - 15$, also $3 \equiv 15 \bmod 3$.
e) $7 \equiv 3 \bmod 4$ und $6 \equiv 2 \bmod 4$ folgt $4 \mid 7 - 3$ und $4 \mid 6 - 2$ und damit $4 \mid (7 - 3) \pm (6 - 2) = (7 \pm 6) - (3 \pm 2)$, also $7 \pm 6 \equiv (3 \pm 2) \bmod 4$ nach Satz 1.2h).
f) Aus $7 \equiv 3 \bmod 4$ und $10 \equiv 2 \bmod 4$ folgt:
$70 \equiv 7 \cdot 10 \equiv 3 \cdot 2 \equiv 6 \equiv 2 \bmod 4$, weil $70 = 4 \cdot 17 + 2$ und $6 = 4 \cdot 1 + 2$
h) Es seien $p(x) = 3x^2 + 4x - 1$ und $7 \equiv 1 \bmod 3$; dann gilt: $p(7) = 3 \cdot 7^2 + 4 \cdot 7 - 1 = 174 \equiv 0 \bmod 3$ und $p(1) = 3 + 4 - 1 = 6 \equiv 0 \bmod 3$, also $p(7) \equiv p(1) \bmod 3$.

**Aufgabe 2.5:**
Da die Addition wie auch die Multiplikation von Restklassen auf die Addition und die Multiplikation der die Klasse definierenden Zahlen zurückgeführt wird, gelten die Rechengesetze der Zahlen. Man muss also nur noch die Existenzen der Null und der Eins bzw. der Inversen nachweisen:
Nach Definition 2.5 gelten: $\underline{0} + \underline{a} = \underline{0 + a} = \underline{a + 0} = \underline{a}$ und damit auch $\underline{0} + \underline{a} = \underline{a} + \underline{0} = \underline{a}$ für alle $\underline{a}$.
$\underline{1} \cdot \underline{a} = \underline{1 \cdot a} = \underline{a \cdot 1} = \underline{a} = \underline{a \cdot 1} = \underline{a} \cdot \underline{1}$ für alle $\underline{a}$.
Zu jedem $\underline{a}$ gibt es ein $\underline{-a}$ mit $\underline{a} + \underline{-a} = \underline{a + (-a)} = \underline{a - a} = \underline{0}$. Hierfür schreibt man auch $\underline{a} - \underline{a} = \underline{0}$; man bekommt damit auch die dazugehörigen Vorzeichenregeln.
Die Existenz eines Inversen der Multiplikation, also die Existenz einer Division kann man wegen Beispiel 2.1 nicht nachweisen.

**Aufgabe 2.6:**
a) Bei Beispiel 2.1 kommen in der Multiplikationstafel alle Restklassen nur in der zweiten und letzten Zeile vor. Manche „Divisionen“ sind anhand der Multiplikationstafel gar nicht vorhanden oder nicht eindeutig. Wohingegen in Beispiel 2.2 bei der Multiplikationstafel – abgesehen von der ersten Zeile – in jeder weiteren *alle* Restklassen zu finden sind. Alle Multiplikationstabellen sind wegen des Kommutativgesetzes symmetrisch zu ihrer Hauptdiagonalen (von oben links nach unten rechts) und deshalb gilt die vorher beschriebene Eigenschaft für Zeilen entsprechend für Spalten.
b) In Beispiel 2.2 gibt es eine Division; man kann zeigen, dass dies in Restklassenringen immer so ist, falls der Modul eine Primzahl ist. In Beispiel 2.1 zeigt die „Divisionstabelle“ Löcher und viele Mehrdeutigkeiten wegen der vorhandenen Nullteiler bei $\underline{2} \cdot \underline{3} = \underline{3} \cdot \underline{4} = \underline{0}$; $\underline{2}$, $\underline{3}$ und $\underline{4}$ können keine Divisoren sein.

**Aufgabe 2.7:**
Aus $ax \equiv ac \bmod m$ folgt nach Def. 2.2 die Gültigkeit von $m \mid ax - ac = a(x - c)$. Weil nach Voraussetzung $a$ und $m$ teilerfremd sind, folgt hieraus $x \equiv c \bmod m$. Man kann also in einem solchen Fall mit $a$ dividieren.

**Aufgabe 5.1:**
Wir suchen die Lösungen von $379y + 411x = 371$:

| Divisionsalgorithmus | Reduktionsverfahren nach EULER |
|---|---|
| | |
| $411 = 379 + \mathbf{32} \quad \Rightarrow$ | $y = \frac{-411x+371}{379} = \frac{(-379-32)x+379-8}{379} = -x + 1 + u$ mit (1)<br>$u = \frac{-32x-8}{379} \quad \Rightarrow -379u = 32x + 8$ (2) |
| $379 = 11\cdot \mathbf{32} + 27 \quad \Rightarrow$ | $x = \frac{-379u-8}{32} = \frac{(-11\cdot 32-27)u-8}{32} = -11u + v$ mit<br>$v = \frac{-27u-8}{32} \quad \Rightarrow 32v = -27u - 8$ (3) |
| $\mathbf{32} = 1\cdot 27 + 5 \quad \Rightarrow$ | $u = \frac{-32v-8}{27} = \frac{(-27-5)v-8}{27} = -v + w$ mit<br>$w = \frac{-5v-8}{27} \quad \Rightarrow 27w = -5v - 8$ (4) |
| $27 = 5\cdot 5 + 2 \quad \Rightarrow$ | $v = \frac{-27w-8}{5} = \frac{(-5\cdot 5-2)w-5-3}{5} = -5w - 1 + k$ mit<br>$k = \frac{-2w-3}{5} \quad \Rightarrow 5k = -2w - 3$ (5) |
| $5 = 2\cdot 2 + 1 \quad \Rightarrow$ | $w = \frac{-5k-3}{2} = \frac{(-2\cdot 2-1)k-2-1}{2} = -2k - 1 + s$ mit<br>$s = \frac{-k-1}{2} \quad \Rightarrow 2s = -k - 1 \quad \Rightarrow \quad k = -2s - 1$ (6) |
| $2 = 2\cdot 1 + 0 \quad \Rightarrow$<br>$ggT(379, 411) = 1$ und damit ist die Lösungsmenge $L \neq \varnothing$ | (6) in (5) ergibt: $5(-2s - 1) = -2w - 3$, d. h.: $w = 5s + 1$<br>eingesetzt in (4): $27(5s + 1) = -5v - 8$ d. h.: $v = -27s - 7$<br>eingesetzt in (3): $32(-27s - 7) = -27u - 8$ d. h.: $u = 32s + 8$ (7)<br>eingesetzt in (2): $-379(32s + 8) = 32x + 8$ d. h.: $x = -379s - 95$<br>eingesetzt in (1) mit (7): $y = 379s + 95 + 1 + 32s + 8 = 411s + 104$ |
| Probe | $379(411s + 104) + 411(-379s - 95) = 371$ |
| Lösungsmenge | $\{(x \mid y) = (-379s - 95 \mid 411s + 104)$ für alle $s \in \mathbb{Z}\}$ |

# 7. Literatur

Die hier dargestellten Inhalte findet man in jedem Buch über elementare Zahlentheorie; es werden deshalb nur 2 solche Bücher angegeben:


| | |
|---|---|
| Burton D., Dalkowski H. | Handbuch der elementaren Zahlentheorie mit über 1000 Übungsaufgaben und ihre Lösungen, Heldermann, Lemgo 2005 |
| Scholz A., Schoeneberg B. | Einführung in die Zahlentheorie, Walter de Gruyter & Co, Berlin 1973 |


Der Autor bedankt sich bei Herrn Gustav Vogl, Bad Aibling für das Lesen von Korrekturen.

Anschrift des Autors:
Dr. Karlhorst Meyer
Kyffhäuserstra0e 20
85579 Neubiberg
e-mail: karlhorst@meyer-muc.de

Eingereicht am 1. 12. 2017