Diskrete Mathematik Teilbarkeit

Christoph Dohmen Judith Coenen

17. Mai 2006

Inhaltsverzeichnis

- 1. Einleitung
- 2. Der größte gemeinsame Teiler
- 3. Division mit Rest
- 4. Der "Euklid´sche Algorithmus"
- 5. Das kleinste, gemeinsame Vielfache

1 Einleitung

• Eine Zahl d, ,teilt" eine Zahl a, wenn es eine Zahl q gibt mit

$$a=q*d$$

Hierfür schreiben wir d/a. a heißt Vielfaches von d. Die Negation (ein solches q existiert nicht) wird beschrieben durch d/a.

- Es gilt, dass jedes a die Teiler 1, -1, a und -a hat.
- Beispiel:
 - -4|12, da 12 = 4*3.

• Es gilt z.B. folgendes:

- 1. $d \mid 0 \quad \forall d$
- 2. $0 \mid a \Leftrightarrow a = 0$
- 3. $d \mid a \land a \mid b \Rightarrow d \mid b$
- 4. $d \mid a \Rightarrow db \mid ab$
- 5. $d \mid a \land e \mid b \Rightarrow de \mid ab$
- 6. $d \mid a \land d \mid b \Rightarrow d \mid ax + by \forall x, y$
- 7. $d \mid a \Rightarrow d \mid ab \quad \forall b$
- 8. $d \mid a \Rightarrow d \mid -a$
- 9. $d \mid a \Rightarrow -d \mid a$
- 10. $d \mid a \land a \neq 0 \Rightarrow 1 \leq |d| \leq |a|$
- 11. $a \mid b \land b \mid a \Leftrightarrow a = \pm b$

• Sehen wir uns Punkt 3 z.B. genauer an:

$$d \mid a \text{ und } a \mid b \Rightarrow d \mid b$$

- Beweis:
 - $-a = i*d, b = j*a \rightarrow b = j*a = (i*j)*d$
 - Hieran sieht man nun, dass d mit einem Faktor (i*j) multipliziert b ergibt.
 - Also muss d dann auch b teilen!

Aufgabe 1

• Beweisen Sie Punkt 6:

$$d \mid a \text{ und } d \mid b \Rightarrow d \mid (ax+by) \quad \forall x, y$$

und geben Sie hierfür ein Zahlenbeispiel an!

Lösung Aufgabe 1

- Da d/a und d/b, legen wir fest: a = i*d und b = j*d.
- Nun soll jedoch gezeigt werden, dass d/(ax+by).
 Setzen wir also a und b ein. Dies liefert folgendes:
 (i*d)x + (j*d)y = d*(ix + jy).
 Dies bedeutet jedoch, dass die letzte Klammer mit d multipliziert wird, also teilt d auf jeden Fall diese Klammer, also gilt auch d/(ax+by).
- Mögliches Beispiel:
 - d = 8, a = 24, b = 56, x = 3, y = 4
 - $-8|24 \text{ und } 8|56 \rightarrow 8|(72+224) \rightarrow 8|296 \rightarrow 8*37 = 296$

- Seien d, a, b ganze Zahlen mit d/a und d/b.
- Dann gilt auch d/(a+b) bzw. d/(a-b).
- Der Beweis ist ein Spezialfall von:

$$d \mid a \text{ und } d \mid b \Rightarrow d \mid (ax+by) \quad \forall x, y$$

für
$$x = 1$$
, $y = 1$ bzw. $x = 1$, $y = -1$.

Beispiel:

- Sei d eine Zahl, welche 143 und 169 teilt. Da d dann auch die Differenz teilt, muss d ein Teiler von 26 sein, also 1, 2, 13 oder 26 sein.
 - Durch Probe erhält man $d = \pm 1$ oder $d = \pm 13$.
- Andererseits erhält man, wenn man 143 und 169 miteinander addiert, 312.
 - Da gilt d/(a+b), muss d nun nicht nur 143 und 169 teilen, sondern auch 312. Da (169, 143) = 13, muss 13 auch 312 teilen. Wir wissen, dass 24*13 = 312.

• Gelte für positive Zahlen a und b, dass d a teilt (d/a), dann ist d = a oder $d \le \frac{a}{2}$.

Beweis:

- Es ist
$$a = q*d$$
. Ist $q = 1$, so ist $d = a$.
Sonst ist $q \ge 2$

und damit

$$a = qd \ge 2d$$

und damit

$$d \leq \frac{a}{2}$$

 Für beliebige, auch negative, Zahlen ergibt sich entsprechend: • Gelte $d \mid a, a \neq 0$.

Dann ist
$$|d| = |a|$$
 oder $|d| \le \left| \frac{a}{2} \right|$.

- Insgesamt gilt abgeschwächt für Zahlen $d \neq 0$, die a teilen $|d| \leq |a|$.
- Beispiel:

$$d = -13$$
, $a = 182$

$$/-13/$$

hier ist also | d | auch kleiner als $\left| \frac{a}{2} \right|$.

• Eine Zahl a, die von einem positivem d geteilt wird, liege zwischen -(d-1) und (d-1), so ist a=0.

• Annahme:

Sei $a \neq 0$: Dann ist $|a| \leq d - 1 < |d|$.

Im Widerpruch zu $|d| \le |a|$. Damit gilt a = 0.

2 Der größte gemeinsame Teiler (ggT)

- $T_a = \{d \mid a\}$ heißt die Teilermenge von a.
- Elemente aus

$$T_a \cap T_b$$

heißen gemeinsame Teiler von a und b. Für positive a und b heißt $\max(T_a \cap T_b)$

größter gemeinsamer Teiler von a und b.

Schreibweise (a,b).

Aufgabe 2

• Bestimmen Sie T_{16} !

Lösung Aufgabe 2

•
$$T_{16} = \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}$$

• Außerdem gilt:

$$T_1 = \{-1, 1\}, \quad T_0 = Z, \quad T_a = T_{-a}, \quad |T_a| < \infty \quad \text{für } a \neq 0$$

• Es gilt:

$$-(a,b) = (b,a)$$

 $-(a,0) = a$

$$- 1 \le (a,b) \le \min(a,b)$$

$$-(0,0)=0$$

- Ist (a,b) = 1, dann sind a und b teilerfremd, da sie als einzigen gemeinsamen Teiler die 1 haben.
- $(a,b) = b \rightarrow b/a$
- Beweis:
 - b ist gemeinsamer Teiler von a und b. Deswegen teilt b dann natürlich auch a.

2 Der größte gemeinsame Teiler

•
$$(a,b) = d \implies \left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

• Klar, dass $\frac{a}{d}$ bzw. $\frac{b}{d}$ ganzzahlig und positiv. Sei $c = \left(\frac{a}{d}, \frac{b}{d}\right)$

Dann ist
$$\frac{a}{d} = q_1 c$$
, $\frac{b}{d} = q_2 c$
 $a = q_1 cd$, $b = q_2 cd$

also $cd \in T_a \cap T_b$. Damit $cd \le (a,b) = d$ und somit $c \le 1$.

Da
$$c = \left(\frac{a}{d}, \frac{b}{d}\right) \ge 1$$
 ergibt sich $c = 1$.

Beispiel:

$$- a = 12, b = 8 \rightarrow d = 4.$$

Dann haben wir (12,8) = 4. Dies bedeutet dann jedoch,
 dass nach Voraussetzung gilt :

$$\left(\frac{12}{4}, \frac{8}{4}\right) = (3,2) = 1.$$

Hier sehen wir nun, dass 3 und 2 teilerfremd sind, wie es auch die Voraussetzung zeigt.

3 Division mit Rest

• Seien a und b ganze Zahlen mit b > a > 0. Dann gibt es eindeutig bestimmte Zahlen q und r mit

$$b = q * a + r \text{ und } 0 \le r < a.$$

- Eine andere für Programmierer bekanntere Schreibweise für die Division mit Rest ist "modulo".
- Hat man z.B. folgende Berechnung eines Restes:

$$15 = 1*12 + 3$$
,

so erhält man in Modulo-Schreibweise folgendes:

$$15 \equiv 3 \mod 12$$

- Der Satz sichert Existenz und Eindeutigkeit von q und r
- 1. Existenz: Sei $M = \{t \mid b ta \ge 0\}$. M ist nicht leer (wähle t "klein genug") und nach oben beschränkt. Setze $q = \max M$ und r = b qa. Damit $r \ge 0$ ist klar.

Wäre $r \ge a$, so wäre auch $b - (q+1)a = b - qa - a = r - a \ge 0$ und damit $q+1 \in M$ im Widerspruch zu $q = \max M$

- 2. Eindeutigkeit: Seien qa + r = q'a + r' mit $0 \le r$, $r' \le |a|$ (q q')a = r' r Also: a teilt r' r. r' r liegt aber zwischen -(a 1) und (a 1). Damit ist r' r = 0 und damit wiederum r' = r. Wegen $a \ne 0$ aber auch q q' = 0, also q = q'
 - q ist durch $\frac{b}{a} 1 < q \le \frac{b}{a}$ eindeutig festgelegt

• Beispiel:

- b = 15, a = 4
- Damit $M = \{t \mid b t * a \ge 0\}$ gilt, kann t höchstens 3 sein. Hier sieht M dann folgendermaßen aus $M = \{0,1,2,3\}$. In diesem Fall ist dann $q = \max M = 3$ und r = 15 - 3 * 4 = 3.

 Jeder gemeinsame Teiler von a und b ist auch Teiler vom Rest r.

• Beweis:

- Sei t Teiler von a und b. Setzen wir a = i * t und b = j * t..
- Sehen wir uns nun folgende Gleichung: b = q * a + r an und formen nach r um.
- So erhalten wir r = b q*a. Setzen wir nun für a und b ein, so erhalten wir

$$r = j * t - q * (i * t) = t * (j - i * q).$$

Die Klammer wird also mit t multipliziert, also muss t
 Teiler vom Rest r sein.

Aufgabe 3

• Beweisen Sie, dass t auch Teiler von b ist unter der Voraussetzung, dass t/a und t/r!

Lösung Aufgabe 3

- Wir gehen wie eben vor und setzen für a und r a = i*t und r = j*t ein.
- So erhalten wir

$$b = q * a + r = q * i * t + j * t = t * (i * q + j).$$

• Also ist auch t Teiler von b!

• Das gerade Bewiesene bedeutet nun jedoch, dass gilt:

$$T_a \cap T_b = T_b \cap T_r$$

- Das heißt nun, dass alle gemeinsamen Teiler von *a* und *b* auch Teiler vom Rest *r* sind.
- Der ggT bleibt nun auch erhalten, und es gilt (b,a) = (a,r).
- Das heißt, dass b und a den gleichen ggT haben wie a und r.
- Die wiederholte Anwendung davon führt zum "Euklid'schen Algorithmus"

Der "Euklid´sche Algorithmus"

- Seien a und b Zahlen mit b > a > 0.
 - -1) Berechne die Zerlegung b = q*a + r
 - -2.1) Ist r = 0, so ist (a,b) = a.
 - 2.2) Ist $r \neq 0$, so ist (b, a) = (a, r).
 - Setze b = a und a = r und gehe zu 1.
 - Führe diese Vorgehensweise solange fort, bis irgendwann die Gleichung ohne Rest aufgeht.
 - Der ggT ist also der letzte positive Rest (in der vorletzten Zeile) des Euklid'schen Algorithmus

Aufgabe 4

• Berechnen Sie (212, 112) am Beispiel des "Euklid´schen Algorithmus"!

Lösung Aufgabe 4

- Zu berechnen ist (212, 112)
- 1. 212 = 1*112 + 100
- 2. 112 = 1*100 + 12
- 3. 100 = 8*12 + 4
- 4. $12^{2} = 3*4(=12)$
- 5. Ende des Algorithmus'!
- (212, 112) = 4

Aufgabe 5

• Berechnen Sie (212, 117)!

Lösung Aufgabe 5

- Zu berechnen ist (212, 117)
- 1. 212 = 1*117 + 95
- 2. 117 = 1*95 + 22
- 3. 95 = 4*22 + 7
- 4. $\frac{22}{3} = \frac{3*7}{1} + \frac{1}{1}$
- 5. 7 = 7*1
- 212 und 117 sind also teilerfremd, da sie die 1 als einzigen gemeinsamen Teiler haben!

• Ist (a,b) = d, so existieren ganze Zahlen a und b mit d = a*a' + b*b'. Insbesondere gilt für teilerfremde Zahlen 1 = a*a' + b*b'.

• Beispiel:

- -a = 42, b = 18
- Damit haben wir (42, 18) = 6.
- Somit muss es nun zwei ganze Zahlen a' und b' geben,
 wobei dann gilt:

$$a*a' + b*b' = d,$$

in unserem Beispiel also:

$$42*a' + 18*b' = 6.$$

- Setzen wir a' = 1 und b' = -2, so erhalten wir: 42*1 + 18*(-2) = 6.

• Beweis:

- Um den Beweis zu führen, wenden wir den Euklid´schen Algorithmus an, diesmal jedoch rückwärts:
- Sehen wir uns Aufgabe 4 nochmal an.

$$-4 = 100 - 8*12$$
 und $12 = 112 - 1*100$
 $4 = 100 - 8*(112 - 1*100)$
 $4 = 212 - 112 - 8*(112 - (212 - 112))$
 $4 = 212 - 112 - 8*112 + 8*212 - 8*112$
 $4 = 9*212 - 17*112$

Aufgabe 6

• Bestimmen Sie (42,16) und zeigen Sie anhand der rückwärtigen Anwendung des Euklid´schen Algorithmus, dass gilt: d = a*a' + b*b'.

Lösung Aufgabe 6

- (42,16) = 2
- 1. 42 = 2*16 + 32. 16 = 1*10 + 63. 10 = 1*6 + 442 = 2*16 + 10
- 16 = 1*10 + 6
- 4. 6 = 1*4 + 2
- 4 = 2*2

1.
$$2 = 6 - 1*4$$
, $4 = 10 - 1*6$, $6 = 16 - 1*10$, $10 = 42 - 2*16$

- 2. 2 = 6 1*(10 1*(16 1*(42 2*16)))3. 2 = 16 1*(42 2*16) 1*((42 2*16) 1*(16 1*(42 2*16)))4. 2 = 16 42 + 2*16 1*42 + 2*16 + 1*16 1*42 + 2*162 = 16 - 1*(42 - 2*16) - 1*((42 - 2*16) - 1*(16 - 1*(42 - 2*16))
- 2 = 8*16 3*42

Diese Lösung ist nicht eindeutig. Es gibt unendlich viele Lösungen, also unendlich viele a' und b'.

• Allgemein sieht der "Euklid´sche Algorithmus" dann folgendermaßen aus:

$$\begin{array}{llll} b & = q_1 a + r_2 & & mit & 0 < r_2 < a \\ a & = q_2 r_2 + r_3 & & mit & 0 < r_3 < r_2 \\ r_2 & = q_3 r_3 + r_4 & & mit & 0 < r_4 < r_3 \\ & & \vdots & & \\ r_{n-2} & = q_{n-1} r_{n-1} + r_n & mit & 0 < r_n < r_{n-1} \\ r_{n-1} & = q_n r_n \end{array}$$

Der Abbruch erfolgt wegen

$$a > r_2 > ... > r_n > 0$$

zwingend, und es gilt

$$(b,a) = (a,r_2) = \dots = (r_{n-1},r_n) = r_n$$

oder allgemeiner

$$T_a \cap T_b = T_b \cap T_r = \dots = T_{r_n} = T_{(a,b)}.$$

- Die Anzahl der Schritte beim "Euklid´schen Algorithmus" kann beliebig groß werden
- Dies zeigt auch die Fibonacci-Folge, die den Worst-Case darstellt
- Algorithmus angewandt auf der Fibonacci-Folge:

$$f_{n+1} = f_n + f_{n-1}, \qquad f_0 = f_1 = 1$$

Berechnung von (f_{n+1}, f_n) :

 $f_{n+1} = 1 * f_n + f_{n-1}$
 $f_n = 1 * f_{n-1} + f_{n-2}$
 \vdots
 $f_2 = f_1 + f_0 = 2 * f_1 = 2 * f_0$

Es sind also stets n Schritte notwendig!

• Gilt 0 < a < b, so ist die Zahl der Schritte beim Euklid'schen Algorithmus nicht größer als das Fünffache der Ziffernzahl von a.

• Beweis:

- Per Induktion wird gezeigt : $f_{n+5} > 10 * f_n$.
- $n \rightarrow n+1$: $f_{n+6} = f_{n+5} + f_{n+4} > 10f_n + f_{n+4} > 10f_n + 10f_{n-1} = 10f_{n+1}$ Diese Induktion liefert fortgeführt :

$$f_{n+5l} > 10^l f_n$$

Ist nun n > 5l bzw. $n \ge 5l + 1$, so ist

$$a = f_{n+1} \ge f_{5l+2} > 10^l * f_2 > 10^l$$

d.h. a besitzt l + 1 Ziffern. Besitzt a umgekehrt nur l Ziffern, so muss damit $n \le 5l$ sein.

Weiterhin gilt folgendes:

1.
$$(ac,bc) = (a,b)*|c|$$

2. Ist d gemeinsamer Teiler von a und b, dann ist

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

$$- a = 27, b = 18, c = -3$$

$$- (27*(-3), 18*(-3)) = (27, 18)*/-3/$$

$$- (-81, -54) = 9*/-3/$$

$$- 27 = 27$$

• Beweis:
$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{|d|}$$

1.) Multiplikation im euklidschen Algorithmus jeder Zeile mit | c |

2.) Nach 1.) ist
$$(a,b) = \left(\frac{a}{d}d, \frac{b}{d}d\right) = \left(\frac{a}{d}, \frac{b}{d}\right)/d$$

- Ist (c,b) = 1, dann ist (ac,b) = (a,b)
- Beweis:
 - Sei d = (ac,b) und e = (a,b).
 - Dann gilt d/ac und $d/ab \rightarrow d/(ac,ab) = (c,b)/a/ = |a/a|$
 - Ebenso gilt d/b und damit d/(a,b) = e
 - Umgekehrt gilt: e/ac und $e/b \rightarrow e/(ac,b) = d$ und damit d = e.

- Beispiel:
 - -a = 6, c = 5, b = 8
 - Dann haben wir (6*5, 8) = (6, 8) = (2*3, 8) = (2, 8) = 2.

- Ist $(a,b) = 1 \implies (a^m, b^n) = 1$
- Beweis:
 - Durch Induktion über m folgt zunächst, wie eben gezeigt

$$(a^m,b) = 1.$$

Dann liefert die Induktion über n

$$(a^m,b^n)=1$$

- Gilt d/ab und $(a, d) = 1 \rightarrow d/b$.
- Beweis:
 - Es ist mit dem gerade Gezeigten (ab, d) = (b, d). Wegen d/ab ist d = (ab, d) = (b, d), und damit d/b.

- $\sqrt[n]{a}$ ist ganz oder irrational.
- Beweis:

- Sei
$$\sqrt[n]{a} = \frac{p}{q}$$
 mit $(p,q) = 1$. Dann ist

$$a = \left(\frac{p}{q}\right)^n$$

$$a*q^n = p^n$$

Insbesondere:

$$p^n/a*q^n$$

Nach vorigem Satz ist aber: $(p^n, q^n) = 1$

also:

$$p^n/a$$
 bzw. $a = l*p^n$

Damit:

$$l*q^n = 1$$

Deshalb:

$$q = 1$$

Also:

$$\sqrt[n]{a} = p \in Z$$

5 Das kleinste gemeinsame Vielfache (kgV)

- Nun bezeichne V_a die Vielfachen einer Zahl a. Es gilt damit
 - 1. $0 \in V_a$
 - 2. $V_0 = \{0\}$
 - 3. $V_a = V_{-a} = V_{|a|}$

• Es werden jetzt nicht mehr gemeinsame Teiler gesucht, sondern gemeinsame Vielfache.

- Für $a \neq 0$ und $b \neq 0$ ist $min(V_a \cap V_b \cap N)$ das kleinste, gemeinsame Vielfache von a und b.
- Notation: [a,b]

- Vereinbarung: [0,b] = [a,0] = 0
- Außerdem gilt:
 - [a,b] = [b,a] = [/a/,/b/]
 - $-[a,b] = |b| \Leftrightarrow a/b$
 - Für $a \neq 0$ und $b \neq 0$ ist $1 \leq [a,b] \leq |a| * |b|$

Aufgabe 7

• Berechnen Sie [12, 9]!

Lösung Aufgabe 7

• [12, 9] = 36, da 36 = 3*12 und 36 = 4*9 und (4, 3) = 1.

• Seien nun $a \neq 0$ und $b \neq 0$. Mit

$$a_1 = \frac{a}{(a,b)}$$
$$b_1 = \frac{b}{(a,b)}$$

ist $(a_1,b_1)=1$. Jedes gemeinsame Vielfache v von a und b ist darstellbar als v=q*a=r*b.

• Wird nun a durch $a_1 * (a,b)$ und b durch $b_1 * (a,b)$ ersetzt, so ergibt sich

$$qa_1 = rb_1$$
.

• Damit gilt $b_1 \mid qa_1$.

• Da $(a_1,b_1)=1$, gilt

$$b_1 \mid q$$

$$b_1 l = \frac{b}{(a,b)} l = q$$

- Daher gilt $v = qa = \frac{ab}{(a,b)}l$
- Jedes Vielfache ist also von der Gestalt

$$\frac{ab}{(a,b)}l, l \in Z.$$

$$a = 12, b = 9$$

$$\Rightarrow a_1 = \frac{12}{3} = 4, \quad b_1 = \frac{9}{3} = 3$$
damit ist $a_1 = 4$ und $b_1 = 3$ und es gilt: $(4,3) = 1$

$$v = q * a = r * b \Rightarrow v = 3 * 12 = 4 * 9$$

$$q * a_1 = r * b_1 \Rightarrow 3 * 4 = 4 * 3$$
Damit gilt $3 \mid 3 * 4$.
$$(a_1, b_1) = (4,3) = 1 \Rightarrow b_1 \mid 3 = 3 \mid 3$$

$$b_1 * l = \frac{9}{3} * l = q = 3 \Rightarrow 3 * l = 3$$

$$v = 3 * 12 = \frac{108}{3} l \Rightarrow l = 1, \quad l \in \mathbb{Z}.$$

- Das kleinste, gemeinsame Vielfache ergibt sich (je nach Vorzeichen von a und b) durch $l = \pm 1$.
- Also ergibt sich

$$[a,b] = \frac{|ab|}{(a,b)}.$$

• Dies liefert nun aber

$$(a,b)[a,b] = |ab|$$

$$-a = 12, b = 8:$$

 $(12, 8)*[12, 8] = |12*8| \Leftrightarrow 4*24 = 96 \Leftrightarrow 96 = 96$

• Dies wiederum eingesetzt bedeutet, dass jedes gemeinsame Vielfache von *a* und *b* die Darstellung

$$v = [a,b] * l$$

hat. Damit ist jedes gemeinsame Vielfache auch Vielfaches des kleinsten gemeinsamen Vielfachen, also

$$V_a \cap V_b = V_{[a,b]}$$

$$- [4,6] = \frac{4*6}{(4,6)} = \frac{24}{2} = 12, \quad V_4 \cap V_6 = V_{[4,6]} = \{\pm 0, \pm 12, \pm 24, \pm 36, \ldots\}$$

Aufgabe 8

• Berechnen Sie $V_{16} \cap V_{20}$

Lösung Aufgabe 8

•
$$[16,20] = \frac{16*20}{(16,20)} = \frac{320}{4} = 80, \quad V_{16} \cap V_{20} = V_{[16,20]} = \{\pm 0, \pm 80, \pm 160, \pm 320, \ldots\}$$