ggT – eine Eigenschaft

Steffen Solyga*

30. Januar - 4. Februar 2010

Das erneute Programmieren treibt mich zu unerwarteten Entdeckungen: Seit dreißig Jahren (oder mehr) habe ich mit dem größten gemeinsamen Teiler zu tun. Ich habe ihn über Jahre in der linearen Algebra und der Analysis „verwendet“, und ich habe Studenten erklärt, wie man ihn berechnet. Ich dachte, das Wesentliche daran verstanden zu haben.

Aber schon das erste Beispiel in WIRTHS Modula-2-Buch [1] belehrte mich jüngst eines Besseren. Sein Algorithmus zur Berechnung des größten gemeinsamen Teilers basiert auf dem folgenden

Satz 0 *Für alle natürlicher Zahlen x, y mit $x > y$ ($y \geq 1$) gilt:*

$$\mathrm{ggT}(x, y) \quad = \quad \mathrm{ggT}(x - y, y). \tag{1}$$

Wie läßt sich diese - mir bislang unbekannte - Eigenschaft beweisen? Mein erster Gedanke war Primfaktorzerlegung, jedoch kam ich damit zu keinem Ergebnis. Also mußte ich geordneter vorgehen.

1 Definition

Was ist der größte gemeinsame Teiler zweier Zahlen[1] überhaupt?

Definition 1 *Die Zahl t heißt Teiler der Zahl x, wenn eine Zahl a existiert, so daß $at = x$ gilt:*

$$t \backslash x \quad :\Leftrightarrow \quad \exists a \,:\, at = x. \tag{2}$$

Mit der – zugegebenermaßen saloppen – Begründung, daß für jedes geordnete Paar (t, x) entscheidbar ist, ob $t \backslash x$ gilt oder nicht, betrachte ich diese Relation als wohldefiniert. Offenbar gilt für alle t, x

$$1 \backslash x, \tag{3}$$

$$x \backslash x, \tag{4}$$

$$t \backslash x \quad \Rightarrow \quad t \leq x. \tag{5}$$

Mit obiger Relation ist auch die Teilermenge wohldefiniert:

*solyga@gmx.de

[1] Es werden im folgenden nur natürliche Zahlen (≥ 1) betrachtet.

Definition 2 *Die Menge T aller Teiler einer Zahl x heißt Teilermenge von x:*

$$T(x) \;:=\; \{\, t \mid t\backslash x \,\}. \tag{6}$$

Es ist also für alle t und x

$$t\backslash x \;\Leftrightarrow\; t \in T(x), \tag{7}$$

und zu (3) bis (5) sind die folgenden Aussagen (über alle x) äquivalent

$$1 \;\in\; T(x), \tag{8}$$
$$x \;\in\; T(x), \tag{9}$$
$$T(x) \;\subseteq\; |1, x|. \tag{10}$$

$T(x)$ besitzt also ein größtes Element, und dieses Element ist x

$$\max[T(x)] \;=\; x. \tag{11}$$

Definition 3 *Die Zahl t heißt gemeinsamer Teiler der Zahlen x und y, wenn t sowohl Teiler von x als auch von y ist:*

$$t\backslash(x, y) \;:\Leftrightarrow\; t\backslash x \;\wedge\; t\backslash y. \tag{12}$$

Die Relation ist also symmetrisch

$$t\backslash(x, y) \;\Leftrightarrow\; t\backslash(y, x), \tag{13}$$

und wegen (3) und (5) gilt für alle t, x, y

$$1\backslash(x, y), \tag{14}$$
$$t\backslash(x, y) \qquad \Rightarrow \qquad t \le \min(x, y). \tag{15}$$

Definition 4 *Die Menge G aller gemeinsamen Teiler von x und y heißt Teilermenge von x, y:*

$$G(x, y) \;:=\; \{\, t \mid t\backslash(x, y) \,\}. \tag{16}$$

Es ist also für alle t, x, y

$$t\backslash(x, y) \;\Leftrightarrow\; t \in G(x, y), \tag{17}$$
$$G(x, y) \;=\; G(y, x), \tag{18}$$
$$G(x, y) \;=\; T(x) \cap T(y), \tag{19}$$
$$G(x, x) \;=\; T(x), \tag{20}$$

und aus (8) und (10) folgt für alle x, y in Äquivalenz zu (14) und (15)

$$1 \;\in\; G(x, y), \tag{21}$$
$$G(x, y) \;\subseteq\; |1, \min(x, y)|, \tag{22}$$

G besitzt also für jedes Paar (x, y) ein größtes Element, d.h. für alle (x, y) existiert $\max[G(x, y)]$.

Definition 5 *Das größte Element von $G(x, y)$ heißt größter gemeinsamer Teiler von x und y:*

$$\mathrm{ggT}(x, y) \;:=\; \max[G(x, y)]. \tag{23}$$

2 Eigenschaften

Aus der Definition ergeben sich wegen (11), (18) und (20) sofort zwei wichtige Eigenschaften des größten gemeinsamen Teilers zweier Zahlen

$$\mathrm{ggT}(x,y) = \mathrm{ggT}(y,x), \tag{24}$$
$$\mathrm{ggT}(x,x) = x. \tag{25}$$

Zum Beweis der mit Satz 0 in Frage stehenden Eigenschaft des ggT benötige ich weitere Eigenschaften der Teilerrelation. Um dem Ausdruck $x-y$ Sinn zu verleihen, wird im folgenden $x > y$ angenommen, was wegen der Symmetrien (13), (18) und (24) keine Beschränkung der Allgemeinheit darstellt.

Satz 1 *Jeder gemeinsame Teiler von x und y ist auch Teiler von $x + y$:*

$$t\backslash(x,y) \Rightarrow t\backslash(x+y). \tag{26}$$

Beweis: Sei t ein gemeinsamer Teiler von x und y. Gemäß den Definitionen 1 und 3 existiert also ein Paar (a,b) mit $x = at$ und $y = bt$, woraus $x+y = at+bt = (a+b)t$ folgt, d.h. t ist gemäß Definition 1 ein Teiler von $x + y$. □

Satz 2 *Jeder gemeinsame Teiler von x und y ist auch Teiler von $x - y$:*

$$t\backslash(x,y) \Rightarrow t\backslash(x-y). \tag{27}$$

Beweis: Wie oben mit schematischem Ersetzen von + durch −. Die Terme $a + b$ bzw. $a - b$ existieren gemäß Distributivgesetz. □

3 Beweis

Damit gestaltet sich der Beweis von Satz 0 recht einfach: Die Konjugation von (27) mit $t\backslash y$ liefert zunächsteinmal

$$t\backslash x \wedge t\backslash y \Rightarrow t\backslash(x-y) \wedge t\backslash y. \tag{28}$$

Ersetzt man in (26) x durch $x - y$ (jede Zahl kann durch eine Differenz dargestellt werden), hat man $t\backslash(x-y,y) \Rightarrow t\backslash(x)$, und die Konjugation mit $t\backslash y$ liefert

$$t\backslash(x-y) \wedge t\backslash y \Rightarrow t\backslash x \wedge t\backslash y. \tag{29}$$

Mithin besteht für alle t, x, y mit $x > y$ die Äquivalenz

$$t\backslash x \wedge t\backslash y \Leftrightarrow t\backslash(x-y) \wedge t\backslash y \tag{30}$$

oder – äquivalent dazu –

$$G(x,y) = G(x-y,y). \tag{31}$$

so daß mit Definition 5 der Beweis vollendet ist. □

4 Bestimmung

Die Eigenschaften (1), (24) und (25) sichern wegen $x - y < x$ den Halt und die Korrektheit des folgenden Algorithmus:

```
PROCEDURE ggT( x,y: CARDINAL ): CARDINAL;
BEGIN
  IF x = y THEN
    RETURN x;
  ELSIF x > y THEN
    ggT( x-y, y );
  ELSE
    ggT( x, y-x );
  END;
END ggT;
```

5 Diskussion

Es gibt mir zu denken, daß meine Definition des Teilers die Multiplikation, die Berechnung des größten gemeinsamen Teilers jedoch „lediglich“ die Subtraktion voraussetzt. Insofern stellt sich die Frage, ob man den ggT nicht einfacher induktiv definieren sollte.

Literatur

[1] Niklaus Wirth:
Programmieren in Modula-2.
Springer-Verlag, 2. Auflage, 1991
ISBN 3-540-51689-1 (Berlin ..), 0-387-51689-1 (New York ..)