Frank Klinker

Zahlentheorie

Teil 1: Teilbarkeit, Primzahlen, ggT und der euklidische Algorithmus

1 Teilbarkeit, Teiler und Primzahlen

Sind a und b zwei positive natürliche Zahlen, dann gilt

$$\boxed{a \textbf{ ist Teiler } b \iff \text{Es gibt eine natürliche Zahl } k, \text{ sodass } b = k \cdot a}$$

Statt a **ist Teiler von** b sagt man auch b **wird von** a **geteilt** oder a **teilt** b und schreibt $a|b$.

Beispiel 1. 3 teilt 102, denn $102 = 34 \cdot 3$. Deswegen teilt auch 34 die Zahl 102.

Fakt 2. 1. Ist a ein Teiler von b, dann ist $a \leq b$.

2. Ist a ein Teiler von b, dann gibt es einen weiteren Teiler a' von b mit $a \cdot a' = b$, sodass Teiler immer in "Paaren" vorkommen. Ist keiner der beiden Teiler die Zahl 1, dann sind beide $\leq \frac{b}{2}$.
3. Ist a ein Teiler von b und b ein Teiler von a, dann ist $a = b$.
4. Ist a ein Teiler von b, dann ist a auch Teiler von jedem Produkt $b \cdot c$.
5. Die Umkehrung von 4. ist im Allgemeinen falsch, wie man an folgendem Beispiel sieht:

   12 teilt zwar $40 \cdot 30 = 1200$, aber 12 teilt weder 40 noch 30.

   Die Umkehrung von 4. kann aber richtig sein, wie das folgende Beispiel zeigt:

   12 teilt $24 \cdot 50 = 1200$, und 12 teilt den Faktor 24.

   Ob die Umkehrung gilt, hängt hier von der Zerlegung von 1200 in ein Produkt ab.

   Wir werden später einen Situation kennenlernen, wo die Umkehrung unabhängig von der Zerlegung gilt!
6. Ist a kein Teiler von $b \cdot c$, dann teilt a weder b noch c.

Fakt 3. 1. Jede Zahl hat mindestens zwei Teiler, nämlich 1 und sich selbst.

2. Eine Zahl kann viele oder wenig Teiler haben:

   - 60 hat viele Teiler: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 und 60
   - 65 hat wenig Teiler: 1, 5, 13, 65

Adresse: Eduard-Spranger-Berufskolleg, 59067 Hamm
E-Mail: mail@frank-klinker.de
Version: 26. März 2024

- 71 hat nur zwei Teiler: 1, 71

Die Zahlen mit der minimalen Anzahl an Teilern werden eine wichtige Rolle spielen:

Eine Zahl p, die nur die zwei Teiler 1 und p hat, heißt **Primzahl**

Fakt 4.
- 1 ist keine Primzahl, da sie keine zwei Teiler hat.
- 2 ist die kleinste Primzahl.
- Außer 2 sind alle Primzahlen ungerade.
- Die Primzahlen zwischen 1 und 100 sind:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$$
$$43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

- Der **Sieb des Eratosthenes** ist ein Verfahren, wie man die Primzahlen herausfiltern kann, die kleiner als eine vorgegebene Zahl sind: Wikipedia: Der Sieb des Eratosthenes.

Man kann die Teiler einer Zahl a der Größe sortieren und wir haben:

Fakt 5. Der kleinste Teiler $\neq 1$ einer Zahl ist eine Primzahl.

Wäre der kleinste Teiler einer Zahl a keine Primzahl, so ließe er sich in ein Produkt zerlegen und jeder Faktor selbst wäre ein Teiler von a und noch kleiner als der Teiler mit dem wir gestartet sind. Da wir aber mit dem kleinsten gestartet sind, kann es die Zerlegung nicht geben und der kleinste Teiler muss eine Primzahl sein.

Auch wenn eine Zahl kein Teiler einer anderen ist, dann gibt es eine sehr natürliche Zerlegung:

Fakt 6 (Teilbarkeit mit Rest)**.** Ist $a \leq b$, dann gibt es Zahlen k und r mit $0 \leq r < b - 1$, sodass

$$b = k \cdot a + r$$

Die Zahl r heißt **Rest von b beim Teilen durch a** und dieser ist genau dann Null, wenn a ein Teiler von b ist.

Bemerkung 7.
- Praktisch erhalten wir den Rest r, indem wir die Zahl a so lange von b abziehen, bis wir eine Zahl zwischen Null und b erreichen.
- Mit dem Taschenrechner berechnen wir $b : a$ und nehmen vom Ergebnis nur den Teil vor dem Komma. Das ist dann k in der Zerlegung und r ist dann $b - k \cdot a$.

Folgerung 8. Es gibt unendlich viele Primzahlen.

2 Der ggT und die Primfaktorzerlegung

Man kann die Teiler zweier Zahlen a und b vergleichen und untersuchen, ob es gemeinsame Teiler gibt. Diese gemeinsamen Teiler kann man dann der Größe nach sortieren und bekommt so den größten gemeinsamen Teiler von a und b. Diesen bezeichnet man mit

$$\boxed{\text{ggT}(a,b) = \textbf{größter gemeinsamer Teiler} \text{ von } a \text{ und } b}$$

Zwei Zahlen a und b heißen **teilerfremd**, wenn sie nur 1 als gemeinsamen Teiler haben. Das ist dann auch gleichzeitig ihr größter gemeinsamer Teiler, also:

$$\boxed{a \text{ und } b \text{ sind } \textbf{teilerfremd} \iff \text{ggT}(a,b) = 1}$$

Fakt 9. 1. Ist p eine Primzahl, welche die Zahl b nicht teilt, dann gilt $\text{ggT}(p,b) = 1$.

2. Die Aussage in Punkt 1. ist so nicht unbedingt korrekt, wenn p keine Primzahl ist: 4 teilt zwar 10 nicht, aber $\text{ggT}(4,10) = 2$ ist trotzdem nicht 1.
3. Ist $\text{ggT}(a,b) = g$, dann ist $\text{ggT}\left(\frac{a}{g}, \frac{b}{g}\right) = 1$

Man kann den ggT zweier Zahlen a und b auch rechnerisch bestimmen und erhält dann eine eindeutige Darstellung von $\text{ggT}(a,b)$ durch die Zahlen a und b:

Fakt 10 (Erweiterter euklidischer Algorithmus)**.** Sind a und b ganze Zahlen, dann gibt es ganze Zahlen k und ℓ, sodass

$$a \cdot k + b \cdot \ell = \text{ggT}(a,b)\,.$$

Die folgenden Aussagen im Zusammenhang mit Primzahlen sind sehr natürlich aber auch sehr nützlich:

Fakt 11. Ist p eine Primzahl und a eine natürliche Zahl mit $\text{ggT}(a,p) = 1$, dann sind nur die Vielfachen

$$a \cdot p, \quad a \cdot 2 \cdot p, \quad a \cdot 3 \cdot p, \quad \ldots$$

durch p teilbar.

Diese Tatsache gibt uns die Möglichkeit, die Teilbarkeitseigenschaft von Produkten auch umzukehren:

Folgerung 12. Ist p eine Primzahl, dann gilt:

$$p \text{ ist Teiler von } a \cdot b, \text{ dann ist } p \text{ Teiler von } a \text{ oder Teiler von } b$$

Die Primzahlen und ihre Eigenschaften ermöglichen uns nun, jede Zahl in "minimale" Faktoren zu zerlegen

Fakt 13 (Primfaktorzerlegung)**.** Ist a eine natürliche Zahl, dann gibt es eine eindeutige Zerlegung

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$$

in ein Produkt von n Primzahlen $p_1, p_2, \ldots, p_n$. Diese müssen nicht unterschiedlich sein.

Beispiel 14. $60 = 2 \cdot 2 \cdot 3 \cdot 5$, $184 = 2 \cdot 2 \cdot 2 \cdot 23$, $1002 = 2 \cdot 3 \cdot 167$, $32 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$

Folgerung 15. Ist die Primfaktorzerlegung einer Zahl bekannt, dann erhalten wir alle Teiler der Zahl, indem wir die Primzahlen geeignet zu Produkten kombinieren.

3 Der euklidische Algorithmus

Den größten gemeinsamen Teiler zweier Zahlen zu bestimmen, indem zunächst für beide Zahlen alle Teiler bestimmt und dann den größten heraussucht, ist keine sonderlich effiziente Methode. Wünschenswert wäre eine Methode, mit der man den ggT berechnen kann.

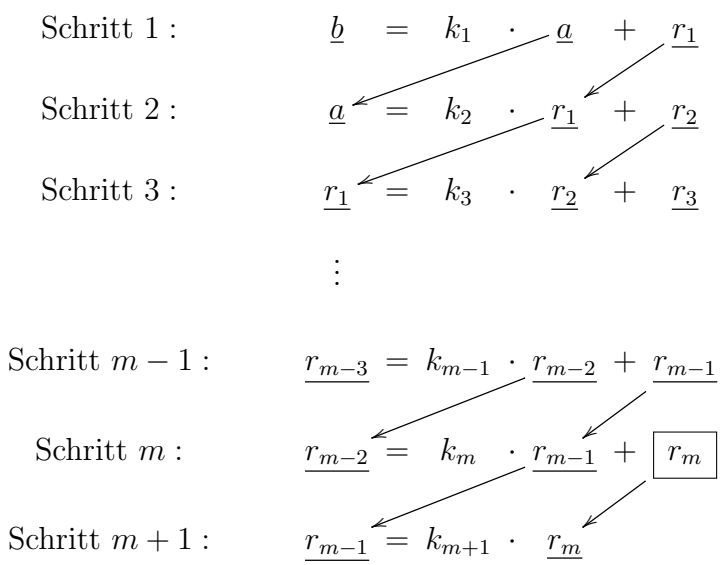
Das kann man mit Hilfe des euklidischen Algorithmus, denn dieser erlaubt uns:

1. den größten gemeinsamen Teiler $\mathrm{ggT}(a, b)$ zweier positiver, ganzen Zahlen a, b zu berechnen und
2. die Zahlen k und ℓ in der Zerlegung $k \cdot a + \ell \cdot b = \mathrm{ggT}(a, b)$ berechnen.

Im Punkt 2. spricht man auch vom erweiterten euklidischen Algorithmus.

3.1 Die Berechnung des größten gemeinsamen Teilers

Das Schema des euklidischen Algorithmus



- Schritt 1: Wir stellen b als Vielfaches von a mit Rest dar: Rest ist r_1
- Schritt 2: Wir stellen a als Vielfaches von r_1 mit Rest dar: Rest ist r_2
- Schritt 3: Wir stellen r_1 als Vielfaches von r_2 mit Rest dar: Rest ist r_3
- Wir wiederholen dies so lange, bis es keinen Rest mehr gibt (das klappt, da in jedem Schritt der positive Rest kleiner wird)
- Im vorletzten m-ten Schritt haben wir dann als Rest $r_m = \mathrm{ggT}(a, b)$ stehen

3.2 Der erweiterte euklidische Algorithmus

Neben dem Wert $ggT(a,b)$ liefert der euklidische Algorithmus auch die oben beschriebene Zerlegung dieser Zahl:

Sind a und b ganze Zahlen, dann gibt es ganze Zahlen k und ℓ, sodass

$$\mathrm{ggT}(a,b) = k \cdot a + \ell \cdot b\,.$$

Um diese Zerlegung zu erhalten nehmen wir uns die Rechnung aus dem euklidischen Algorithmus her und gehen wie folgt vor:

- Wir lösen Schritt 1 des Algorithmus nach dem Rest r_1 auf
- Wir lösen Schritt 2 nach r_2 auf und ersetzen dort r_1 durch das vorige Ergebnis.
- Wir lösen Schritt 3 nach r_3 auf und ersetzen dort r_1 und r_2 durch die zwei vorigen Ergebnisse.
- Diesen letzten Punkt wiederholen wir nun für Schritt 4 bis Schritt m.

Beispiel 16. Wir führen den erweiterten euklidischen Algorithmus für die Zahlen $a = 158$ und $b = 288$ durch.
Dabei finden wir links die Berechnung von $\mathrm{ggT}(a,b)$ und rechts die Berechnung der Zerlegung $\mathrm{ggT}(a,b) = k \cdot a + \ell \cdot b$:

$$\begin{array}{l|l}
\underline{288} = 1 \cdot \underline{158} + \underline{130} & \rightarrow \underline{130} = 1 \cdot \underline{288} - 1 \cdot \underline{158} \\
\underline{158} = 1 \cdot \underline{130} + \underline{28} & \rightarrow \underline{28} = \underline{158} - 1 \cdot \underline{130} \\
 & \quad = \underline{158} - 1 \cdot (1 \cdot \underline{288} - 1 \cdot \underline{158}) \\
 & \quad = 2 \cdot \underline{158} - 1 \cdot \underline{288} \\
\underline{130} = 4 \cdot \underline{28} + \underline{18} & \rightarrow \underline{18} = \underline{130} - 4 \cdot \underline{28} \\
 & \quad = (1 \cdot \underline{288} - 1 \cdot \underline{158}) - 4 \cdot (2 \cdot \underline{158} - 1 \cdot \underline{288}) \\
 & \quad = 5 \cdot \underline{288} - 9 \cdot \underline{158} \\
\underline{28} = 1 \cdot \underline{18} + \underline{10} & \rightarrow \underline{10} = \underline{28} - 1 \cdot \underline{18} \\
 & \quad = (2 \cdot \underline{158} - 1 \cdot \underline{288}) - 1 \cdot (5 \cdot \underline{288} - 9 \cdot \underline{158}) \\
 & \quad = 11 \cdot \underline{158} - 6 \cdot \underline{288} \\
\underline{18} = 1 \cdot \underline{10} + \underline{8} & \rightarrow \underline{8} = \underline{18} - 1 \cdot \underline{10} \\
 & \quad = (5 \cdot \underline{288} - 9 \cdot \underline{158}) - 1 \cdot (11 \cdot \underline{158} - 6 \cdot \underline{288}) \\
 & \quad = 11 \cdot \underline{288} - 20 \cdot \underline{158} \\
\underline{10} = 1 \cdot \underline{8} + \boxed{2} & \rightarrow \boxed{2} = \underline{10} - 1 \cdot \underline{8} \\
 & \quad = (11 \cdot \underline{158} - 6 \cdot \underline{288}) - 1 \cdot (11 \cdot \underline{288} - 20 \cdot \underline{158}) \\
 & \quad = 31 \cdot \underline{158} - 17 \cdot \underline{288} \\
\underline{8} = 4 \cdot \underline{2} &
\end{array}$$

Wir haben damit schließlich

$$\text{ggT}(288, 158) = 2 \quad \text{und} \quad 2 = 31 \cdot 158 - 17 \cdot 288\,.$$

4 Die Begründungen für einige der Aussagen

4.1 Die Begründung für Folgerung 8

Es gibt unendlich viele Primzahlen

Wir zeigen, dass es zu einer endlichen, lückenlos aufsteigenden Menge an Primzahlen immer eine weitere weitere Primzahl geben muss, die dann größer ist als alle bisherigen.

Wir nehmen also alle die ersten n Primzahlen her: $p_1 = 2, p_2 = 3, \ldots, p_n$. Die neue Zahl, die wir berechnen ist

$$q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1\,.$$

Diese Zahl ist durch keine der vorigen vielen Primzahlen teilbar, da sie beim Teilen jeweils den Rest 1 hat, siehe Fakt 6.

Wegen Fakt 5 ist der kleinste Teiler von q ungleich 1 eine Primzahl. Diese ist entweder q selbst oder eine neue Primzahl. In beiden Fällen muss diese aber größer als p_n sein, da es bei $p_1, \ldots, p_n$ ja keine Lücke gab.

4.2 Die Begründung für Fakt 11

Ist p eine Primzahl und a eine natürliche Zahl mit $\text{ggT}(a, p) = 1$, dann sind nur die Vielfachen

$$a \cdot p, \quad a \cdot 2 \cdot p, \quad a \cdot 3 \cdot p, \quad \ldots$$

durch p teilbar.

Zunächst sieht man direkt, dass alle Zahlen in der Liste durch p teilbar sind. Wir müssen also noch begründen, dass es keine weiteren Zahlen gibt, die zwar durch p teilbar sind aber nicht von der speziellen Form.

Die Begründung erfolgt in mehreren Schritten:

1. Wir suchen uns das kleinste Vielfache von a heraus, dass durch p teilbar ist. Diese Zahl ist dann von der Form $a \cdot m$. Dabei muss $1 < m \leq p$ gelten, denn 1 ist ausgeschlossen, da a nicht durch p teilbar sein soll, und $m > p$ ist ausgeschlossen, da dann $a \cdot p$ kleiner als $a \cdot m$ wäre.
2. Wir nehmen uns jetzt ein weiteres Vielfaches von a her, dass ebenfalls durch p teilbar ist. Das können wir als $a \cdot h$ schreiben. Es muss $h \geq m$ gelten, da $a \cdot m$ das kleinste durch p teilbare Vielfache war.

3. Für die beiden Vielfachen aus 1. und 2. gibt es wegen $h \geq m$ Zahlen k und r mit $h = k \cdot m + r$ und $0 \leq r < m$, siehe Fakt 6.
4. Damit ist $a \cdot r = a \cdot h - a \cdot k \cdot m$ ebenfalls durch p teilbar, weil $a \cdot h$ und $a \cdot k \cdot m$ durch p teilbar sind.

   Weil aber $a \cdot r < a \cdot m$ ist und $a \cdot m$ das kleinste Vielfache war, dass durch p teilbar war, muss $r = 0$ sein.
5. Wegen 4. ist $h = k \cdot m$ und das beliebige(!) Vielfache $a \cdot h$, das durch p teilbar ist, ist von der Form $a \cdot k \cdot m$.

Bis jetzt haben wir: Alle Vielfachen von a, die von p geteilt werden, sind von der Form $a \cdot k \cdot m$. Dabei ist $a \cdot m$ das kleinste aller Vielfachen, die durch p teilbar sind.

Jetzt bleibt nur noch zu begründen, warum m selber p ist:

6. Auf alle Fälle wird $a \cdot p$ von p geteilt. Daher muss $a \cdot p$ auch von der Form $a \cdot p = a \cdot k \cdot m$ sein und damit $p = k \cdot m$. das heißt, m ist ein Teiler von p, also $m = 1$ oder $m = p$, weil p eine Primzahl ist. Wegen $m > 1$ aus Punkt 1. ist damit $m = p$.

4.3 Begründung für Fakt 13

Ist a eine natürliche Zahl, dann gibt es eine eindeutige Zerlegung

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$$

in ein Produkt von n Primzahlen $p_1, p_2, \ldots, p_n$. Diese müssen nicht unterschiedlich sein.

Der Zusatz, dass die Primzahlen unterschiedlich sein dürfen, haben wir bereits an den Beispielen gesehen.

Dass es so eine Zerlegung immer gibt, sieht man, indem man beschreibt, wie man sie erhält. Dazu wendet man den folgenden Algorithmus an:

i. Ist a eine Primzahl, dann ist man fertig.
ii. Ist a keine Primzahl, dann gibt es Zahlen b und c, die nicht 1 sind und die a zerlegen: $a = b \cdot c$.
iii. Mit b und c startet man nun neu mit Schritt i. und ii.
iv. Das Verfahren endet, wenn man in Schritt iii. nur noch Primzahlen hat.

Wir müssen jetzt noch begründen, warum es keine zwei unterschiedlichen Zerlegungen geben kann. das tun wir in mehreren Schritten:

1. Wir tun so, als gäbe es zwei Zerlegungen für a, nämlich

   $$p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_m \,.$$

   Darin sollen die Primzahlen der Größe nach sortiert sein und es soll $n \leq m$ sein.

2. Da p_1 die Zahl $q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_m$ teilt, muss diese von der Form $p_1 \cdot k$ sein. Das heißt, p_1 muss unter den ganzen Primzahlen $q_1, \ldots, q_m$ vorkommen, etwa $p_1 = q_1$. Wir können diese Primzahl jetzt auf beiden Seiten dividieren und behalten

$$p_2 \cdot p_3 \cdot \ldots \cdot p_n = q_2 \cdot q_3 \cdot \ldots \cdot q_m \,.$$

3. Den Schritt aus 2. wiederholen wir jetzt n mal und bekommen $p_1 = q_1, p_2 = q_2, \ldots, p_n = q_n$. Die Gleichung, die nach Division übrig bleibt, ist

$$1 = q_{n+1} \cdot \ldots \cdot \ldots \cdot q_m \,.$$

Diese Gleichung darf auf der rechten Seite aber keine weiteren Faktoren haben. Das geht jedoch nur, wenn $n = m$ ist und damit beide Zerlegung von vornherein gleich.