Faktorisieren mit Dreieckszahlen

von Benjamin Wolff, Graßdorfer Str. 16, 04315 Leipzig, und

Dr. W. Quapp, Mathematisches Institut, Universität Leipzig

PF 10 09 20, 04009 Leipzig

in: $\sqrt[Die]{Wurzel}$ Zeitschrift für Mathematik **46**, No 2 (2012) S. 45-50

1 Einleitung

Wir wollen eine ungerade, natürliche Zahl a faktorisieren, d.h. in Teiler zerlegen. Sei etwa $a = 27$, so ist eine Zerlegung 27=3·9. Der naive Test für die Zerlegung von a ist das Probedividieren: man prüft a auf Teilbarkeit durch alle möglichen Primteiler. Wenn a sehr groß ist, muss man eventuell sehr lange probieren. Aber man braucht nicht alle Primzahlen kleiner als a zu testen, sondern nur diejenigen, die kleiner oder gleich $\sqrt{a}$ sind. Größere Teiler kann es nicht geben.

In diesem Beitrag stellen wir eine Methode zur Faktorisierung vor, die nur Additionen als Testoperation verwendet, aber keine Divisionen (höchstens eine durch 2). Dies mag verwundern. Das Mittel ist die Nutzung von Dreieckszahlen.

Abbildung 1: Ein Dreieck aus 10 Steinen

Dreieckszahlen wurden schon von Mathematikern in der Antike betrachtet. Z.B. war 10 die heilige Zehnzahl (Tetraktys) der Anzahl der Steine im Dreieck von Abbildung 1 [1]. Dreieckszahlen $d(n)$ zur Kantenlänge n entstehen,

wenn Steine aufeinanderfolgend immer vollständig an einer Seite eines Dreiecks angelegt werden. Folglich hat man $d(1) = 1,\ d(2) = 1 + 2 = 3,\ d(3) = 1 + 2 + 3 = 6,\ d(4) = 1 + 2 + 3 + 4 = 10$ Steine, u.s.w. Eine allgemeine Formel ist $d(n) = \sum_{i=1}^{n} i$. Damit ist sofort eine rekursive Definition von $d(n)$ gegeben:

$$d(n+1) = d(n) + (n+1). \tag{1}$$

Die Summenformel für $d(n)$ ist (Übungsaufgabe!)

$$d(n) = \frac{n(n+1)}{2}. \tag{2}$$

Dreieckszahlen haben vielfältige Beziehungen zu anderen Zahlenfolgen, als auch geometrischen Strukturen. Auf der web-page [2] findet man unter A000217 eine umfangreiche Zusammenstellung.

2 Methode der Faktorisierung einer ungeraden Zahl a

Die Dreieckszahlen selbst sind ab $d(3) = 6$ immer zerlegbar; wenn also a gleich einer Dreieckszahl ist, sind wir fertig. (Übungsaufgabe!) Ist a keine Dreieckszahl, so können wir seine Zerlegbarkeit in 3 Schritten testen.

1. **Schritt:** Wir suchen das n mit $d(n+1) > a$. Dann können wir an ein volles Dreieck aus n Reihen eine unvollständige Reihe anfügen, die bei a Steinen endet. Beispiel: sei $a = 25$ Dann ist $d(6+1) = 28$ größer als a. An ein Dreieck aus 6 Zeilen mit 21 Steinen fügen wir 4 Steine hinzu, um $a = 25$ Steine zu erreichen.

2. **Schritt:** Wir ergänzen die a-Reihe durch fortlaufende Dreieckszahlen $d(x)$ solange, bis ein neues, komplettes Dreieck entsteht. Dazu müssen eventuell noch weitere Zeilen angefügt werden. Wenn ein volles Dreieck erreicht ist, gibt es ein kleinstes x und ein kleinstes y mit $x < y$, $y > n$, die die Bedingung

   $$a + d(x) = d(y) \tag{3}$$

   erfüllen.

3. **Schritt:** Gilt Gleichung (3), so gibt es 3 Möglichkeiten für die Differenz $f = y - x$. Es ist

   $$f \begin{cases} > 2\ , & \text{ungerade, dann ist } \ f \mid a\ , \\ > 2\ , & \text{gerade, dann ist } \ \frac{f}{2} \mid a\ , \\ = 2\ , & \text{dann war a eine Primzahl.} \end{cases} \tag{4}$$

Anhand von drei Beispielen wollen wir die Möglichkeit dieser drei Fälle einsehen, siehe die Abbildungen 2 und 3.

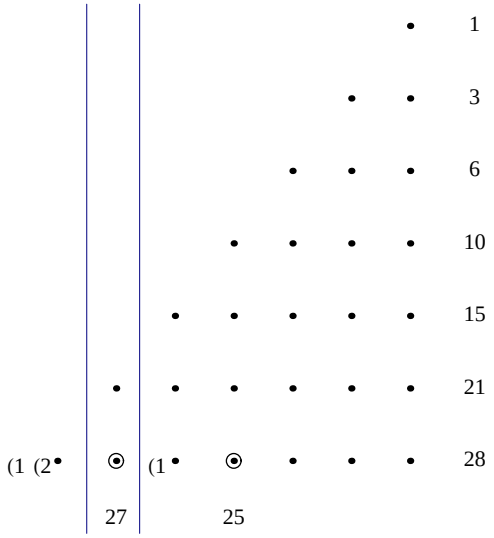

Abbildung 2: Zerlege $a = 25$ und $a = 27$. Es ist $n = 6$, zu 25 in der 7. Reihe ist $x = 2$, zu 27 ist $x = 1$, also entsprechend sind 1+2 Steine, oder 1 Stein zu addieren. In beiden Fällen ist schon für $y = 7$ die Reihe voll. Die senkrechten Schnitte deuten ein Abtrennen von je $d(x)$ Steinen an.

Sei im **1. Fall** $a = 25$, $d(6) = 21$, $d(7) = 28$, d.h. $n = 6$, siehe Figur 2. An 21 Steine werden 4 angelegt, um $a = 25$ zu erhalten. Nun müssen weitere 1+2=3 Steine angelegt werden, um $d(7) = 28$ zu erreichen. Also ist $d(x) = 3$, mit $x = 2$ und $y = 7$, folglich $f = y - x = 5$. Bekanntermaßen ist 5 ein Teiler von 25.
Als **2. Fall** betrachten wir $a = 27$. Dies liegt wieder in Reihe $n + 1 = 7$. Es ist nur nötig $d(1) = 1$ anzulegen, damit $d(7) = 28$ erreicht wird. Somit ist $f = 7 - 1 = 6$, also gerade. Dann ist $f/2 = 3$ der gesuchte Teiler.
Sei nun im **3. Fall** $a = 23$ eine Primzahl, siehe Abbildung 3. Dann kann es keinen Teiler geben. Obige Aufspaltung darf also nicht funktionieren. Um ein volles Dreieck zu erhalten, müssen wir 10 Dreieckszahlen Steine anlegen, mit $d(10) = 55$. Dann haben wir ein Dreieck zu $d(y) = d(12) = 78$, also 23+55=78 Steinen. Damit ist in der Tat $f = 12 - 10 = 2$, und wir erhalten die gewünschte Aussage, daß a eine Primzahl ist.

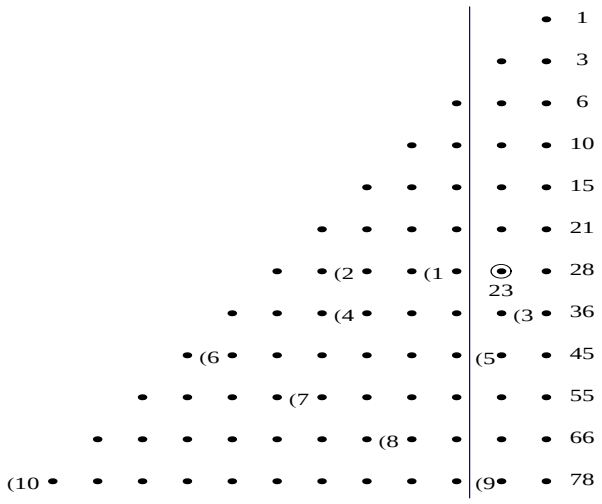

Abbildung 3: Primtest bei $a = 23$. Es ist wieder $n = 6$, aber man muß bis $x = 10$ weiterzählen, damit die 12. Reihe mit $d(12) = 78$ aufgeht. Numerierte Klammern geben die benötigten Dreickszahlen $d(x)$ an.

Um einzusehen, daß die Entscheidung (4) immer funktioniert, ist folgende Überlegung wichtig:
Wenn man vom vollen Dreieck zur Zeilenzahl y mit der Dreieckszahl $d(y)$ Steinen die Anzahl $d(x)$ Steine abzieht, ergibt sich mit Gleichung (3) die Anzahl a der zu zerlegenden Zahl. Dieses Abziehen kann in der Figur von $d(y)$ so geschehen, daß man ein volles Dreieck $d(x)$ links abschneidet. In den Figuren 2 und 3 ist die Schnittgerade durch senkrechte Striche angedeutet.
Im **Fall 1** bei $a = 25$ bleiben als Basislinie 5 Steine übrig, der Teiler von a. Der verbleibende Rest der Steine bildet ein Trapez. Die in der Abbildung senkrechten Seiten sind 3 und 7 Steine lang. Die Schräge ist 4 Zeilen hoch. Die Steine der Schräge können nun so auf 2 Zeilen umverteilt werden, das insgesamt aus dem Trapez ein Rechteck (im allgemeinen Fall) entsteht. Dessen Höhe (hier 5 Steine) ist ein weiterer Teiler von a.
Im **Fall 2** bei $a = 27$ bleiben als Basislinie 6 Steine übrig, eine gerade Zahl. Der verbleibende Rest der Steine bildet wieder ein Trapez. Die senkrechten Seiten sind nun 2 und 7 Steine lang. Die Schräge ist 5 Zeilen hoch. Aber hier geht ein Umverteilen noch nicht auf. Erst wenn wir die Spalten noch einmal teilen, kann ein Rechteck durch Umverteilung erzeugt werden. Dessen Höhe (hier 9 Steine) ist der weitere Teiler von a.

Im **Fall 3** bei $a = 23$ in Figur 3 kann mit $d(y) - d(x)$ Steinen kein Rechteck entstehen, da a als Primzahl nicht so zerlegbar ist. Im Beispiel entsteht mit $y = 12$ und $x = 10$ ein Trapez aus 2 Spalten, mit den Höhen 11 und 12, deren Summe gerade a ist.

Die Methode (4) ist folglich auch ein Primzahltest, allerdings ein umständlicher. Denn für ein primes $a = p$ benötigt man immer das maximale $x = (p-1)/2$ zum zugehörigen $y = (p+1)/2$. Mit einer Binomischen Formel kann man sich sofort überzeugen, daß dann in Formel (3) gilt

$$p + \frac{1}{2}\frac{p-1}{2}\frac{p+1}{2} = \frac{1}{2}\frac{p+1}{2}\frac{p+3}{2}.$$

Ein Faktorisierungsprogramm, welches den Test (3) ausnutzt, ist:

1 a, n, dx, dy, und f seien Integer.
Suche zu a das größte n mit $d(n) = \frac{1}{2}n(n+1) < a$

2 Setze $dx = 0,\ y = n,\ dy = d(n)$

3 Prüfe in einer Schleife:
Do $x = 1, (a-1)/2$
$dx = dx + x$
If$(a + dx = dy)$ Then $f = y - x$, Sprung zu **4**
If$(a + dx > dy)$ Then $dy = dy + y, y = y + 1$
Enddo

4 Verwende f wie in Formel (4).

3 Einschätzung

Dieses Verfahren probiert eventuell auch viele Dreieckszahlen $d(x)$ aus, bis die Bedingung (3) erfüllt ist. Gegenüber der Probedivision gibt es zwei Unterschiede: Statt zu dividieren muß man nur addieren, und statt alle Primzahlen bis $\sqrt{a}$ zu kennen muß man nur die Iterationsformel (1) für fortlaufende Dreieckszahlen $d(x)$ und $d(y)$ anwenden. Aber für große Zahlen wird auch das sehr aufwendig. Mit einem normalen PC kann man bis zu 12-stellige Zahlen aber problemlos untersuchen.

In der Verschlüsselungstechnik ist es wichtig, daß man sehr, sehr große Zahlen (dabei hat a etwa 200 Stellen) nicht in menschlichen Zeiten zerlegen kann. Moderne Verfahren verwenden zahlentheoretische Ansätze für diese Aufgabe, und können sie trotzdem nicht lösen. Der Primzahltest selbst wird

mit dem kleinen Satz von Fermat leicht bewältigt, die Faktorisierung verwendet neben Primzahlsieben Methoden, die auch auf dem kleinen Satz von Fermat beruhen. Sie sind etwa in dem Buch [3] beschrieben.

Literatur

[1] H. Wußing: *Vorlesungen zur Geschichte der Mathematik*. VEB Deutscher Verlag der Wissenschaften, Berlin, 1989.

[2] http://oeis.org/

[3] M. Hüttenhofer, M. Lesch, N. Peyerimhoff: *Mathematik in Anwendung mit C++*. Quelle & Meyer Verlag, Heidelberg, 1994.