Inhalt

Ein wesentlicher Bestandteil der **Kryptografie** ist die s.g. **Zahlentheorie**. Dabei stellt die Zahlentheorie ein Teilgebiet der Mathematik dar, in dem es, vereinfacht dargestellt, um die Eigenschaften von Zahlen geht.

Primzahlen sind hier von fundamentaler Bedeutung. Immer wieder begegnet man diesen Sonderlingen der natürlichen Zahlen. Wer den Artikel Symmetrie vs. Asymmetrie gelesen hat, weiß, dass **Primzahlen** unter anderem bei dem asymmetrischen Verschlüsselungsverfahren **RSA** eine Hauptrolle spielen.

Es handelt sich bei den Primzahlen um natürliche Zahlen größer als 1, die nur durch 1 und sich selbst ohne Rest teilbar sind. Man muss kein großer Mathematiker sein, um sich durch die Eigenheiten dieser Primzahlen angezogen zu fühlen.

Beispiele für Primzahlen:
2,3,5,7,11,13

Keine Primzahlen:
1,4,6,15,96,102

Eine Vermutung ist kein Beweis *

Jedem leuchtet ein, dass man jede natürliche Zahl (>1) als Summe zweier anderer Zahlen (>0) darstellen kann.

2 = 1 + 1

3 = 1 + 2

11 = 3 + 8

Wie sieht es mit Primzahlen als Summanden aus. Kann man jede Zahl (>3) als Summe zweier Primzahlen darstellen?

4 = 2 + 2

5 = 2 + 3

6 = 3 + 3

…

10 = 3 + 7 = 5 + 5

Sieht gut aus!

Aber bei 11 ist dann Schluss, auch 17 macht Schwierigkeiten. Mit den geraden Zahlen sieht es bisher gut aus.

Wir schränken jetzt ein und verlangen einfach, da es sich bei unseren Problemkindern ja um ungerade Zahlen handelt, **dass wir nur gerade natürliche Zahlen >= 4 als Summe zweier Primzahlen darstellen wollen**.

Das scheint tatsächlich zu funktionieren. Man hat bisher ca. 4 * 10 ^14 (**400 Billionen**) aufeinanderfolgende Zahlen gefunden, für die diese spezielle Summendarstellung funktioniert. Aber in der Mathematik ist Vorsicht angesagt. Nur, weil etwas 400 Billionen Mal funktioniert, muss es noch lange nicht bedeuten, dass es auch bei der 500 billionsten Zahl stimmt. Wir haben höchstens die Vermutung, dass es so ist.

Was fehlt ist ein Beweis!

Dabei würde es auch genügen, eine Zahl in der Folge zu finden, für die die Vermutung nicht mehr stimmt. Wir hätten dann durch ein Gegenbeispiel bewiesen, dass die Vermutung falsch ist.

Die angesprochene Vermutung wurde erstmals im Jahr **1742** in einem Brief von Christian Goldbach an Leonard Euler als Randnotiz geäußert und ist als **Goldbach’sche Vermutung** in die Geschichte eingegangen.

Der Eine-Million-Dollar Beweis *

Bis heute wiedersetzt sich diese recht einfach anmutende Vermutung jedem Beweisversuch. Auch Preisgelder halfen nicht. Selbst als der Verlag Faber und Faber im Rahmen einer Werbekampagne 1 Million Dollar aussetzte, fand sich kein Genie, welches in der Lage war, die Vermutung zu beweisen. Jörg Richtstein, ein Mathematiker (*unter anderem Mitautor des Buches Die Welt der Primzahlen*) nutzte die Rechenzeit im Leerlauf befindlicher Rechner. Dabei untersuchte er die oben angesprochenen 400 Billionen Fälle. Beweisen lässt sich damit die Vermutung niemals, höchstens durch das Auffinden eines Gegenbeispiels wiederlegen.

Es gibt nicht einmal einen Ansatz für einen Beweis, den man weiter verfolgen könnte. Im Jahr 1966 gelang es dem Chinesen Chen, zu zeigen, dass sich jede natürliche Zahl als Summe einer Primzahl und dem Produkt zweier Primzahlen darstellen lässt. Also zum Beispiel 22 = 13 + 3 X 3. Hört sich bereits ziemlich ähnlich an, ist dennoch meilenweit von Goldbach’s Vermutung entfernt.

Buchtipp für die Wartezeit bis zum Frühling *

Eine ähnlich harte Nuss der Zahlentheorie war
Fermat’s letzter Satz. 350 Jahre bissen sich die namhaftesten Zahlentheoretiker und Mathematiker die Zähne daran aus. 1997 gelang es dann dem Briten Andrew Wiles, diese Randbemerkung (auch hier ging es um eine Randnotiz) in einem Buch zu beweisen. Das wirklich spannend geschriebene und auch für uns NICHT-Zahlentheoretiker geeignete Buch „Fermat’s letzter Satz: Die abenteuerliche Geschichte eines mathematischen Rätsels“ zieht einen sofort in seinen Bann. Wer das Buch in die Hand nimmt, legt es so schnell nicht wieder zur Seite. Hochspannung einmal ohne Splattereffekte.

Das Witzige: Auch hier spielen Primzahlen eine Rolle.

http://www.mathematik.ch/mathematiker/Goldbachsche_Vermutung.php

http://de.wikipedia.org/wiki/Gro%C3%9Fer_fermatscher_Satz

http://de.wikipedia.org/wiki/Goldbachsche_Vermutung