Reichsstadt – Gymnasium
Rothenburg o.d.T.

Kollegstufe 2001/2003

Leistungskurs Mathematik

Facharbeit

Thema: Primzahlen

Verfasser: Raimund Schilder

Kursleiter: OStR Tomann

Bewertung:

Schriftliche Facharbeit: …… Punkte
(einfache Wertung)

Mündliche Prüfung: …… Punkte

Gesamtbewertung der Facharbeit: …… Punkte
(schriftl. FA dreifach + mdl. Prüfung)/4

……
Unterschrift des Kursleiters

Inhaltsverzeichnis

Klassifizierungen der natürlichen Zahlen

Natürliche Zahlen lassen sich auf unterschiedlichste Weise klassifizieren. Beispielsweise können sie in gerade (2, 4, 6, 8, …) und ungerade (1, 3, 5, 7, …) Zahlen aufgeteilt werden. So ist die Klasse der geraden Zahlen durch Zwei teilbar, die restlichen natürlichen Zahlen sind dies nicht. Wird, wie hier, von einer Zahl a gesprochen, die durch eine andere Zahl b teilbar ist, so geht man davon aus, dass die Division aufgeht, also kein Rest bleibt. In diesem Verständnis gilt: $a \bmod b = 0$, falls a durch b teilbar ist. Ebenfalls könnte man die natürlichen Zahlen nach der Teilbarkeit durch 5 klassifizieren, also $n \bmod 5 = 0$, $n \in N$. Im Gegensatz zur Einteilung in gerade und ungerade Zahlen hat dies aber keine besondere Bedeutung. Wichtiger ist die Klassifizierung der natürlichen Zahlen nach Quadratzahlen (1, 4, 9, …) und Zahlen, die diese Eigenschaft nicht besitzen (2, 3, 5, 6, 7, 8, …). Am Bedeutensten ist jedoch die Klassifizierung der natürlichen Zahlen nach Primzahlen (2, 3, 5, 7, …) und nicht primen Zahlen, den zerlegbaren, zusammengesetzten Zahlen (4=2*2, 6=2*3, 8=2*2*2, 10=2*5, 12=2*2*3, …).

Definition der Primzahlen

Eine natürliche Zahl n wird dann als Primzahl bezeichnet, wenn sie nur durch sich selbst und 1 ohne Rest teilbar ist. Die Zahl 1 stellt einen Spezialfall dar und wird nicht als Primzahl angesehen.

n ist prim, falls gilt: $n \bmod x \neq 0 \qquad n \in N \setminus \{1\} \qquad x \in N \setminus \{1 ; n\}$

Zusammengesetzte Zahlen

Natürliche Zahlen, die keine Primzahlen sind, werden als *zusammengesetzte* oder *zerlegbare Zahlen* bezeichnet. Sie können auf eindeutige Weise als Produkt von Primzahlen geschrieben werden. So ist die Zahl 3960 das Produkt aus 7 Primzahlen: $3960 = 2 * 2 * 2 * 3 * 3 * 5 * 11$. Eine solche Zerlegung einer natürlichen Zahl wird *Primfaktorzerlegung* genannt.

Bereits der griechische Mathematiker Euklid erkannte die wichtige Bedeutung der Primzahlen und bewies in seinem IX. Buch der Elemente einen Satz, der heute unter dem Namen *Fundamentalsatz der Arithmetik* bekannt ist, und wie folgt lautet:

Jede natürliche Zahl größer 1 ist entweder eine Primzahl oder kann auf eindeutige Weise als Produkt von Primzahlen geschrieben werden.

So stellen die Primzahlen die fundamentalen Bausteine der natürlichen Zahlen dar, vergleichbar mit den Elementen in der Chemie oder den Elementarteilchen in der Physik.

Primzahlenverteilung

Chemiker haben ein System in der Anordnung der Elemente erkannt, wie das Periodensystem der Elemente, um noch nicht entdeckte Elemente zu finden oder deren Eigenschaften vorherzusagen. Genau so bemühen sich Mathematiker, eine Regelmäßigkeit in der Verteilung der Primzahlen aufzuspüren. Dies ist jedoch bis heute nicht gelungen. Somit wird nur die Verteilung der Primzahlen betrachtet, ohne aber allgemeingültige Aussagen darüber machen zu können. Wenn man das Intervall [2; 11] untersucht, scheint es, als wären Primzahlen sehr verbreitet, da hier immerhin die Hälfte aller natürlichen Zahlen prim sind. Jedoch nimmt die Häufigkeit der Primzahlen ab, je größer die Zahlen werden. Sehr deutlich wird dies, wenn man die Primzahlverteilung anhand einer geeigneten Tabelle betrachtet, welche die Anzahl der Primzahlen $\pi(n)$ kleiner n und die Primzahlendichte $\pi(n)/n$ angibt.

n	$\pi(n)$	$\pi(n)/n$
10	4	0,4
100	25	0,25
1 000	168	0,168
10 000	1 229	0,1225
100 000	9 592	0,09592
1 000 000	78 498	0,078498

„Größte Primzahl“

Nachdem die Primzahlen bei immer größer werdenden Zahlen seltener werden, könnte man nun vermuten, dass sie irgendwann ganz verschwinden und es folglich eine größte Primzahl gibt. Dass dies nicht so ist, bewies schon Euklid mit einer musterhaften, eleganten mathematischen Beweisführung:

$p_1, p_2, p_3, \ldots, p_n$ seien die Primzahlen der Größe nach aufgelistet. Zu zeigen ist nun, dass zu jeder beliebigen Liste eine Primzahl existieren muss, die größer p_n ist.

Man betrachtet dazu die Zahl N, das Produkt aller Primzahlen einer Liste plus 1:

$$N = p_1 * p_2 * p_3 * \ldots * p_n + 1$$

Unübersehbar ist N größer p_n. Ist N zufälligerweise prim, so ist bereits bewiesen, dass es eine größere Primzahl als p_n gibt. Wenn N dagegen keine Primzahl ist, so muss sie durch eine Primzahl p teilbar sein. N ist aber durch keine der Primzahlen p_1, p_2, p_3, bis p_n teilbar, da stets der Rest 1 bleibt, der zu dem Produkt addiert wurde. Folglich ist die List $p_1, p_2, p_3, \ldots, p_n$ unvollständig und es muss, da die Primzahlen der Größe nach ohne Lücken aufgelistet sind, eine Primzahl p existieren, die größer p_n ist.

Erstaunlicherweise ist N nicht zwingend eine Primzahl. So sind N_1 bis N_5 prim, jedoch können N_6 bis N_9 in Primfaktoren zerlegt werden.

$N_1 = 2 + 1 = 3$ $N_2 = 2 * 3 + 1 = 7$

$N_3 = 2 * 3 * 5 + 1 = 31$ $N_4 = 2 * 3 * 5 * 7 + 1 = 211$

$N_5 = 2 * 3 * 5 * 7 * 11 + 1 = 2311$

$N_6 = 2 * 3 * 5 * 7 * 11 * 13 + 1 = 30\,031 = 59 * 509$

$N_7 = 2 * 3 * 5 * 7 * 11 * 13 * 17 + 1 = 510\,511 = 19 * 97 * 277$

$N_8 = 2 * 3 * 5 * 7 * 11 * 13 * 17 * 19 + 1 = 9\,699\,691 = 347 * 27953$

$N_9 = 2 * 3 * 5 * 7 * 11 * 13 * 17 * 19 * 23 + 1 = 223\,092\,871 = 317 * 703\,763$

Bis heute ist jedoch nicht geklärt, ob durch den Ausdruck

$$N = p_1 * p_2 * p_3 * \ldots * p_n + 1$$

unendlich viele Primzahlen oder unendlich viele zerlegbare Zahlen generiert werden, wobei auch beides zutreffen kann.

Goldbachsche Vermutung

Ein ebenfalls ungelöstes Problem, betreffend der Primzahlen, ist die Goldbachsche Vermutung. Christian Goldbach stellte sie 1742 in einem Brief an Leonhard Euler auf, indem er behauptete, dass jede gerade Zahl größer als 2 die Summe genau zweier Primzahlen ist.

$4 = 2 + 2$ $6 = 3 + 3$ $8 = 5 + 3$ $10 = 5 + 5$

$12 = 5 + 7$ …. $20 = 7 + 13$ …. $32 = 3 + 29$ …. $112 = 11 + 101$ ….

Mit Hochleistungsrechenmaschinen konnte die Goldbachsche Vermutung für alle geraden Zahlen bis 100 000 000 verifiziert werden, jedoch fehlt bis jetzt eine allgemeine mathematische Lösung, die diese Vermutung entweder bestätigt oder widerlegt.

Primzahlentests

Das schwierigste, weitaus wichtigste und immer noch ungelöste Problem im Zusammenhang mit Primzahlen, stellt deren Verteilung dar. So konnte bis heute noch keine mathematische Gesetzmäßigkeit erkannt werden, die es ermöglicht, die Primzahlverteilung allgemein anzugeben und jeweils eine beliebige Primzahl zu ermitteln. Darum bleibt nichts anderes übrig, als Primzahlen mit Tests zu bestimmen.

Probedivisionen

Den einfachsten Weg stellen Probedivisionen dar. Ob eine beliebige Zahl n eine Primzahl ist oder nicht, wird bei diesem Test festgestellt, indem man die Zahl n durch alle Primzahlen bis einschließlich $\sqrt{n}$ teilt. $\sqrt{n}$ ist als Grenze gewählt, da eine zerlegbare Zahl n entweder aus mindestens einem Faktor kleiner $\sqrt{n}$ und einem größer $\sqrt{n}$ besteht oder eine Quadratzahl ist, die aus $\sqrt{n} * \sqrt{n}$ besteht. Das Prüfen bis $\sqrt{n}$ stellt also sicher, dass ein Primfaktor gefunden wird, sofern n nicht prim ist. Sollte eine Primzahl Teiler von n sein, so ist n ein Produkt und der Test kann damit beendet werden. Ist jedoch keine Primzahl bis $\sqrt{n}$ ein Teiler von n, muss n prim sein.

Beispiele für Probedivisionen:

91: $\sqrt{91} \approx 9{,}5$

$91 \bmod 2 \neq 0$ $91 \bmod 3 \neq 0$ $91 \bmod 5 \neq 0$

$91 \bmod 7 = 0 \Rightarrow$ 91 ist keine Primzahl, da 7 ein Teiler von 91 ist.

61: $\sqrt{61} \approx 7{,}8$

$61 \bmod 2 \neq 0$ $61 \bmod 3 \neq 0$ $61 \bmod 5 \neq 0$

$61 \bmod 7 \neq 0 \Rightarrow$ 61 ist eine Primzahl, da keine Primzahl bis $\sqrt{61}$ ein Teiler von 61 ist.

Fermatsche Gesetz

So einfach und überschaubar diese Methode wirkt, so unzulänglich ist sie für größere Zahlen. Zum Beispiel würde das Überprüfen einer 20-stelligen Zahl mit einer Hochleistungsrechenmaschine über 1 Stunde dauern, bei einer Primzahl mit 100 Stellen sogar 10^{36} Jahre. Dagegen werden mit dem derzeit besten Verfahren zur Primzahlerkennung, dem *ARCL-Test*, nur 20 bzw. 40 Sekunden benötigt. Es wurde 1980 von den Mathematikern L.M. Adleman, R.S. Rumely, H. Cohen, und H.W. Lenstra Jr. entwickelt und mit den Initialen der Erfinder benannt. Die zu Grunde liegende, hochentwickelte Mathematik ist viel zu komplex, um den ARCL-Test hier zu erklären, jedoch lässt sich der zentrale Gedanke leicht darstellen:
Pierre de Fermat (1601-1665), von Beruf Jurist, beschäftigte sich „nur“ in seiner Freizeit mit Mathematik. Es gelang ihm aber, einige der bewundernswertesten Gesetze der Mathematik zu entdecken. Unter anderem dieses:
Ist p eine Primzahl, dann ist $a^{p-1} - 1$ für alle $a \in N$ kleiner p durch p teilbar.

In Zeichenschreibweise gilt für alle Primzahlen p: $(a^{p-1} - 1) \bmod p = 0$ mit $a \in N$, $a < p$
Nicht ausgeschlossen ist jedoch, dass diese Gleichung auch durch eine Zahl p erfüllt wird, die nicht prim ist, welche dann als Pseudo-Primzahl bezeichnet wird. Im Gegensatz zu den echten Primzahlen treten Pseudo-Primzahlen, von denen es ebenfalls unendlich viele gibt, äußerst selten auf. Die nachfolgende Tabelle veranschaulicht dies:

n	$\pi(n)$	$\pi_p(n)$	$\pi(n) / n$	$\pi_p(n) / n$	$\pi_p(n) / \pi(n)$
1 000	168	2	0,168	0,002	0,011905
1000 000	78 498	245	0,078498	0,000245	0,003121

$\pi(n)$ ist die Anzahl der Primzahlen kleiner n, $\pi_p(n)$ die der Pseudo-Primzahlen.

$\pi(n)/n$ gibt die Primzahlendichte, $\pi_p(n)/n$ die Pseudo-Primzahlendichte an.

$\pi_p(n) / \pi(n)$ stellt das Verhältnis von Pseudo-Primzahlen zu Primzahlen dar.

Folgende frei gewählte Beispiele sollen zur Verständlichkeit beitragen:
Da 7 eine Primzahl ist, müsste $(a^{7-1} - 1) \bmod 7 = 0$ sein:

Für a = 2 : $(2^{7-1} - 1) \bmod 7 = (2^6 - 1) \bmod 7 = (64 - 1) \bmod 7 = 63 \bmod 7 = 0$ q.e.d.

Für a = 3: $(3^{7-1} - 1) \bmod 7 = (3^6 - 1) \bmod 7 = (729 - 1) \bmod 7 = 728 \bmod 7 = 0$ q.e.d.

Wie bereits erwähnt, ist dieses System auch für weitaus größere Primzahlen geeignet. Man stellt jedoch zur einfacheren Bearbeitung das Fermatsche Gesetz um:

$$(a^{p-1} - 1) \bmod p = 0 \quad \Leftrightarrow \quad (a^{p-1}) \bmod p = 1$$

Der Primzahlenbeweis für p = 71 mit a = 2:

$(2^{71-1}) \bmod 71 = 2^{70} \bmod 71 = ((2^7 \bmod 71)^2 \bmod 71)^5 \bmod 71 =$

$= (57^2 \bmod 71)^5 \bmod 71 = 54^5 \bmod 71 = 1$ q.e.d.

Der Versuch zu beweisen, dass 3 * 7 = 21 prim ist (p = 21 ; a = 2):

$(2^{21-1}) \bmod 21 = 2^{20} \bmod 21 = (2^{10} \bmod 21)^2 \bmod 21 = 4 \neq 1 \quad \Rightarrow$ 21 ist nicht prim.

Der Primzahlenbeweis für eine zerlegbare Zahl p = 341 = 11 * 31 mit a = 2:

$(2^{341-1}) \bmod 341 = 2^{340} \bmod 341 = (2^{10} \bmod 341)^{34} \bmod 341 = 1^{34} \bmod 341 = 1$ q.e.d.

$\Rightarrow$ 341 ist prim oder pseudo-prim. Hier handelt es sich um eine Pseudoprimzahl, da 341 das Produkt aus 11 und 31 ist und somit laut Definition keine Primzahl sein kann.

Der bereits erwähnte ARCL-Test modifiziert diese Anwendung des Fermatschen Gesetzes soweit, dass Pseudo-Primzahlen erkannt und ausgeschlossen werden können. Zum Verstehen des ARCL-Tests sind jedoch enorme Kenntnisse der höheren Mathematik notwendig. Daher würde eine Erläuterung jener Vorgehensweise den vorgegebenen Rahmen dieser Facharbeit sprengen.

Strukturierte Primzahlen

Es ist jedoch nicht nur interessant, Primzahlen zu erkennen, sondern auch, sie zu erstellen. So werden bei der Datenverschlüsselung sehr große Primzahlen benötigt, die dann eine Art Code bilden. Zur Erstellung solcher riesiger Primzahlen nutzt man die strukturellen Eigenschaften bestimmter Primzahlen.

Mersennesche Primzahlen

Im Jahre 1664 schrieb der französische Mönch Marin Mersenne im Vorwort seines publizierten Buchs *Cogitata Physica-Mathematica*, dass die Zahl $M_n = 2^n - 1$ für $n \in \{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$ prim sei, während für alle anderen n kleiner 257 dies nicht zutreffe. Niemand weiß, wie er auf dieses erstaunliche Ergebnis kam, jedoch irrte er sich bei M_{67} und M_{257}, da diese zerlegbar sind. Außerdem vergaß er M_{61}, M_{89} und M_{107}, die prim sind.

Nach ihrem Entdecker werden Zahlen der Form $M_n = 2^n - 1$ als Mersennesche Zahlen bezeichnet. Diejenigen Mersenneschen Zahlen, die zusätzlich zu dieser Struktur auch noch prim sind, heißen Mersennesche Primzahlen.

Durch das schnelle Wachstum des Terms 2^n werden die Mersenneschen Zahlen rasch extrem groß. Entscheidend, im Zusammenhang mit Primzahlen, sind die Zahlen n, für die M_n prim ist. Es lassen sich bereits alle zerlegbaren Zahlen ausschließen, weil für eine zusammengesetzte Zahl $n = a * b$ M_n nicht prim sein kann, da gilt:

$$M_n = 2^n - 1 = 2^{a*b} - 1 = (2^a - 1)*(2^{(b-1)*a} + 2^{(b-2)*a} + \ldots + 2^a + 1)$$

Beispiel für n = 6:

$$M_6 = 2^6 - 1 = 2^{2*3} - 1 = (2^2 - 1)*(2^{(3-1)*2} + 2^{(3-2)*2} + 2^{(3-3)*2}) =$$
$$= (4 - 1)*(16 + 4 + 1) = 3 * 21$$

Man könnte nun schließen, dass M_n für alle primen n ebenfalls eine Primzahl ist. Jedoch ist M_{11} bereits ein Gegenbeispiel hierfür:

$M_2 = 2^2 - 1 = 4 - 1 = 3$ prim

$M_3 = 2^3 - 1 = 8 - 1 = 7$ prim

$M_5 = 2^5 - 1 = 32 - 1 = 31$ prim

$M_7 = 2^7 - 1 = 128 - 1 = 127$ prim

$M_{11} = 2^{11} - 1 = 2\,048 - 1 = 2\,047 = 23 * 89$ nicht prim

$M_{13} = 2^{13} - 1 = 8\,192 - 1 = 8\,191$ prim

$M_{17} = 2^{17} - 1 = 131\,072 - 1 = 131\,071$ prim

$M_{19} = 2^{19} - 1 = 524\,288 - 1 = 524\,287$ prim

Hier erscheint es, als könne durch nahezu jede Primzahl wieder eine Primzahl erstellt werden. Dies wird jedoch zunehmend schwieriger und die nächsten Werte für n, die eine Mersennesche Primzahl generieren, sind 31, 61, 89, 127, 521, 607, 1279, 2203, … Um eine Vorstellung von der Größenordnung der Mersenneschen Primzahlen zu erhalten, ist zu erwähnen, dass bereits $M_{2\,203}$ 664 Dezimalstellen hat. Die momentan größte Mersennesche Primzahl $M_{13\,466\,917}$ besitzt unvorstellbare 4 053 946 Dezimalstellen (Stand: Januar 2003).

Lucas-Lehmer-Test

Wie jedoch ist es möglich zu erkennen, ob solch eine riesige Zahl prim ist oder sich doch in sehr große Primfaktoren zerlegen lässt?

Edouard Lucas entwickelte 1876 ein Testverfahren auf Grund höchst komplexer Überlegungen, das trotzdem einfach anzuwenden ist. 1930 verbesserte Derrick Lehmer diese Methode zur Erkennung Mersennescher Primzahlen. Heutzutage ist dieses Verfahren unter dem Namen *Lucas-Lehmer-Test* bekannt.

Um zu erfahren, ob M_n (n hat prim zu sein) eine Primzahl ist, berechnet man die Zahlen U(0), U(1), U(2), …, U(n-2) wie folgt:

$U(0) = 4$

$U(k + 1) = [U(k)^2 - 2] \bmod M_n$

Falls $U(n-2) = 0$, dann ist M_n eine Primzahl. Wenn $U(n-2) \neq 0$ ist, kann M_n nicht prim sein.

Als Beispiel hierfür dienen die Mersennesche Primzahl $M_7 = 127$ und die nicht prime Mersennesche Zahl $M_{11} = 2047 = 23 * 89$:

$M_7 = 127$:

$U(0) = 4$ $\qquad$ $U(1) = [4^2 - 2] \bmod 127 = 14$

$U(2) = [14^2 - 2] \bmod 127 = 67$ $\qquad$ $U(3) = [67^2 - 2] \bmod 127 = 42$

$U(4) = [42^2 - 2] \bmod 127 = 111$ $\qquad$ $U(5) = [111^2 - 2] \bmod 127 = 0$

$\Rightarrow M_7 = 127$ ist prim.

$M_{11} = 2047$:

$U(0) = 4$ $\qquad$ $U(1) = [4^2 - 2] \bmod 2047 = 14$

$U(2) = [14^2 - 2] \bmod 2047 = 194$ $\qquad$ $U(3) = [194^2 - 2] \bmod 2047 = 788$

$U(4) = [788^2 - 2] \bmod 2047 = 111$ $\qquad$ $U(5) = [111^2 - 2] \bmod 2047 = 119$

$U(6) = [119^2 - 2] \bmod 2047 = 1877$ $\qquad$ $U(7) = [1877^2 - 2] \bmod 2047 = 240$

$U(8) = [240^2 - 2] \bmod 2047 = 282$ $\qquad$ $U(9) = [282^2 - 2] \bmod 2047 = 1736 \neq 0$

$\Rightarrow M_{11} = 2047 = 23 * 89$ ist nicht prim.

Faktorisierung von großen Zahlen

Zwar lässt sich durch den Lucas-Lehmer-Test ermitteln, ob eine Mersennesche Zahl M_n prim ist oder nicht, aber es werden keinerlei Aussagen über Faktoren getroffen. So könnte man durch simples Probieren versuchen, die Primfaktoren einer erwiesenermaßen zerlegbaren Zahl zu finden. Dies ist aber nur begrenzt möglich, da bei sehr großen Zahlen viel zu viel Zeit dafür benötigt würde. Bereits Fermat beschäftigte sich mit diesem Problem und entwickelte eine Methode, um sehr große Zahlen in Faktoren, die nicht zwingend prim sein müssen, zerlegen zu können. Hierbei ist n eine sehr große Zahl, die sich in die Faktoren u und v zerlegen lässt. Dabei sind u und v große ungerade Zahlen, für die gilt $u \geq v$.

Es seien nun $x = (u + v) / 2$ und $y = (u - v) / 2$.

Dann gilt: $0 \leq y < x \leq n$ und $u = x + y$, $v = x - y$

$\Rightarrow n = u * v = (x + y) * (x - y) = x^2 - y^2$

$\Rightarrow y^2 = x^2 - n$

Wenn x und y diese Gleichung erfüllen, dann ist $n = (x + y) * (x - y) = u * v$ und u bzw. v können leicht errechnet werden.

Um die Gleichung $y^2 = x^2 - n$ zu lösen, setzt man $x = k \geq \sqrt{n}$, $k \in N$, $x = k, k + 1, ...$ und beginnt mit der kleinsten ganzen Zahl, die größer $\sqrt{n}$ ist. Sobald $x^2 - n$ eine Quadratzahl ergibt, ist die Faktorisierung erfolgreich abgeschlossen, da das gefundene x nun erlaubt, y zu errechnen und aus diesen beiden Zahlen wiederum die Faktoren u und v berechnet werden können. Um die Primfaktorzerlegung einer sehr großen Zahl zu finden, wendet man dieses Verfahren auf die gefundenen Faktoren u und v an, bis schließlich nur noch Primfaktoren existieren. Hilfreich ist bei dieser Methode zu wissen, dass Quadratzahlen niemals auf 2, 3, 7 und 8 enden. Denn dadurch kann jedes Ergebnis von $x^2 - n$ ignoriert werden, das auf eine der obigen Ziffern endet.

Fermat selbst verwendete dieses Verfahren, um 2 027 651 281 in 44 021 * 46 061 zu zerlegen.

Die Faktorisierung der Zahl 10 379 dient zum einfacheren Verständnis dieser Methode. Im Anschluss daran wird die bewiesenermaßen zerlegbare Mersennesche Zahl M_{11} faktorisiert.

Zur Zahl 10 379 :

$\sqrt{10379} \approx 101{,}88 \Rightarrow x_1 = 102 \Rightarrow y^2 = 102^2 - 10\,379 = 25$

$\Rightarrow y = 5$; $x = x_1 = 102$ $\Rightarrow n = u * v = (x + y) * (x - y) = 107 * 97 = 10\,379$

Zu $M_{11} = 2^{11} - 1 = 2\,047$:

$\sqrt{2047} \approx 45{,}24$

$\Rightarrow x_1 = 46 \Rightarrow y^2 = 46^2 - 2047 = 69 \Rightarrow y \approx 8{,}3 \Rightarrow y \notin N$

$\Rightarrow x_2 = 47 \Rightarrow y^2 = 16\underline{2}$ aus der letzten Ziffer folgt: $y \notin N$

$\Rightarrow x_3 = 48 \Rightarrow y^2 = 25\underline{7} \Rightarrow y \notin N \quad \Rightarrow x_4 = 49 \Rightarrow y^2 = 354 \Rightarrow y \approx 18{,}8 \Rightarrow y \notin N$

$\Rightarrow x_5 = 50 \Rightarrow y^2 = 45\underline{3} \Rightarrow y \notin N \quad \Rightarrow x_6 = 51 \Rightarrow y^2 = 554 \Rightarrow y \approx 23{,}5 \Rightarrow y \notin N$

$\Rightarrow x_7 = 52 \Rightarrow y^2 = 65\underline{7} \Rightarrow y \notin N \quad \Rightarrow x_8 = 53 \Rightarrow y^2 = 76\underline{2} \Rightarrow y \notin N$

$\Rightarrow x_9 = 54 \Rightarrow y^2 = 869 \Rightarrow y \approx 29{,}48 \Rightarrow y \notin N \quad \Rightarrow x_{10} = 55 \Rightarrow y^2 = 97\underline{8} \Rightarrow y \notin N$

$\Rightarrow x_{11} = 56 \Rightarrow y^2 = 1089 \Rightarrow y = 33 \; ; \; x = x_{11} = 56$

$\Rightarrow n = u * v = (x + y) * (x - y) = 89 * 23 = 2047$

Da 89 und 23 prim sind, ist somit die Primfaktorzerlegung für M_{11} gefunden.

Fermatsche Primzahlen

Anno 1604 behauptete Fermat in einem Brief an Mersenne kühn, dass alle Zahlen der Form

$$F_n = 2^{2^n} + 1 \qquad \text{mit } n \in N$$

prim seien. Man bildet also die n - te Potenz von 2, potenziert dann 2 mit der erhaltenen Zahl und addiert schließlich 1 zu dem Ergebnis. Fermat ließ sich durch die Beobachtung, dass F_0 bis F_4 prim sind, zu diesem Fehlschluss verleiten, denn vermutlich sind die Fermatschen Zahlen nur für n = 0, 1, 2, 3, 4 prim.

$F_0 = 3$ $\qquad$ $F_1 = 5$ $\qquad$ $F_2 = 17$

$F_3 = 257$ $\qquad$ $F_4 = 65537$

Ein Beweis steht jedoch noch aus. Mit Sicherheit ist F_n aber für alle n größer 4 bis einschließlich 21 zerlegbar. Als erstes gelang es dem Schweizer Mathematiker Leonard Euler, Fermatsches These schlüssig zu widerlegen, indem er bewies, dass $F_5 = 4\,294\,967\,297$ keine Primzahl ist. Erstaunlich ist, dass Fermat nur seinen selbst erfundenen Test hätte anwenden müssen, um selbst festzustellen, dass nicht alle F_n prim sein können, da bereits F_5 keine Primzahl ist. Denn p kann laut Fermat nur dann prim sein, wenn gilt: $3^{p-1} \bmod p = 1$. Für $p = F_5$ ergibt sich jedoch 3 029 026 160.

Prothsches Theorem

Heutzutage existiert eine einfache Methode, um die immens großen Fermatschen Zahlen auf ihre Primeigenschaften zu testen. Sie beruht auf dem Prothschen Theorem, welches besagt, dass die Fermatsche Zahl F_n genau dann prim ist, wenn gilt:

$$3^{(Fn-1)/2} \bmod F_n = -1$$

Demonstriert wird dieses Verfahren an der Fermatschen Primzahl $F_3 = 2^{2^3} + 1 = 257$:

$3^{(257-1)/2} \bmod 257 = 3^{128} \bmod 257 = (3^{16} \bmod 257)^8 \bmod 257 = 249^8 \bmod 257 =$

$= (249^2 \bmod 257)^4 \bmod 257 = 64^4 \bmod 257 =$

$= 16\,777\,216 \bmod 257 = 256 \bmod 257 = -1$ q.e.d.

Es ist jedoch leider nicht möglich, ein Gegenbeispiel aufzuführen, da bereits bei F_5, der kleinsten nicht primen Fermatschen Zahl, unvermeidbar 19-stellige Zahlen auftreten und insgesamt 16 Rechenschritte notwendig wären.

Primzahlen aus Fakultäten

Eine andere Möglichkeit, strukturierte Primzahlen zu generieren, stellt folgende Formel dar:

$$F_n = n! \pm 1$$

Man berechnet also die Fakultät einer beliebigen natürlichen Zahl n, zu welcher dann entweder 1 addiert oder von der 1 subtrahiert wird. Man erhält dann scheinbar zufällig bis zu 2 Primzahlen. Folgende Tabelle veranschaulicht dies bis n = 10:

n	**F_n**	**Primeigenschaften**
1	$F_1 = 1 \pm 1 \rightarrow 0; 2$	nicht prim ; **prim**
2	$F_2 = 2 \pm 1 \rightarrow 1; 3$	nicht prim ; **prim**
3	$F_3 = 6 \pm 1 \rightarrow 5; 7$	**prim** ; **prim**
4	$F_4 = 24 \pm 1 \rightarrow 23; 25$	**prim** ; nicht prim
5	$F_5 = 120 \pm 1 \rightarrow 119; 121$	nicht prim ; nicht prim
6	$F_6 = 720 \pm 1 \rightarrow 719; 721$	**prim** ; nicht prim
7	$F_7 = 5040 \pm 1 \rightarrow 5039; 5041$	**prim** ; nicht prim
8	$F_8 = 40320 \pm 1 \rightarrow 40319; 40321$	nicht prim ; nicht prim
9	$F_9 = 362880 \pm 1 \rightarrow 362879; 362881$	nicht prim ; nicht prim
10	$F_{10} = 3628800 \pm 1 \rightarrow 3628799; 3628801$	nicht prim ; nicht prim

Auch hier ist, wie bei den Mersenneschen und Fermatschen Primzahlen, nicht klar, ob unendlich viele Primzahlen generiert werden können, oder aber, ob 5039 unter Umständen schon die größte, durch Fakultäten erzeugbare Primzahl darstellt.

Primzahlzwillinge

Im Gegensatz zu den vorhergehenden Bereichen stellen Primzahlzwillinge einen wesentlich bekannteren Teil der Primzahlen dar. So werden zwei Primzahlen, die folgende Gleichung erfüllen, als Primzahlzwillinge bezeichnet:

$$p_1 + 2 = p_2$$

Als Beispiel dazu können 3 und 5 genommen werden, aber auch das Zahlenpaar 5 und 7 oder 11 und 13 erfüllen diese Gleichung. Die Anzahl der Primzahlzwillinge endet jedoch keinesfalls in diesem Bereich, sondern 659 und 661 sind ebenso wie 1487 und 1489 Primzahlzwillinge. Trotz alledem ist ungewiss, ob es endlich viele Primzahlzwillinge gibt. Die Vermutung, dass dies nicht so ist und unendlich viele Primzahlzwillinge existieren, liegt aber wesentlich näher. Der Beweis steht aber noch aus!

Primzahldrillinge

Es gibt bewiesenermaßen aber nur ein Primzahltripel, nämlich die Zahlen 3, 5 und 7. Sie erfüllen die Gleichungen, die für alle Primzahldrillinge gelten müssen:

$$p_1 + 2 = p_2 \;\; ; \;\; p_1 + 4 = p_3$$

Es ist jedoch ausgeschlossen, ein weiteres Primzahltripel zu finden, da von diesen immer eine Zahl durch 3 teilbar ist.

Anwendung von Primzahlen

Mathematik und insbesondere die Zahlentheorie erscheinen meist absolut unnütz. Sogar der von der Fachwelt anerkannte britische Mathematiker G.H. Hardy äußerte sich im Jahre 1940 entsprechend in seinem Buch „A Mathematician's Apology". Dass dies aber nicht zutrifft und gerade seine Arbeit als Zahlentheoretiker sehr wohl enorm wichtig und nützlich wurde, stellte sich jedoch erst Jahre später heraus. So wurde die „nutzloseste" Sparte der Mathematik, die Zahlentheorie, durch die Weiterentwicklung der Computer rasend schnell zu einem der wichtigsten Teilbereiche. Sämtliche Sicherheitssysteme und die gesamte Datenverschlüsselung entwickelten nämlich Zahlentheoretiker und nur durch die Zahlentheorie kann eine ausreichende Sicherheit garantiert werden.

Zwar verwendete bereits Julius Cäsar geheime Codes zur Übermittlung seiner Befehle, jedoch bestanden diese aus einfachen Substitutionen. Zum Beispiel wurde A durch B ersetzt und C durch D, also der jeweilige Buchstabe durch den nächsten im Alphabet substituiert. Diese Art der Chiffrierung würde sogar ein einfaches Stochastikprogramm in kürzester Zeit knacken, da durch die Häufigkeit der verwendeten Buchstaben auf den wirklichen Buchstaben geschlossen werden kann. Selbst bei weitaus komplizierteren Substitutionsregeln würde die

Dechiffrierung durch ein leistungsstarkes Stochastikprogramm innerhalb kürzester Zeit erfolgen.
Es darf daher keine erkennbare Struktur vorhanden sein, da ansonsten durch Stochastikprogramme der Code sofort geknackt werden kann. Andererseits ist ein Muster notwendig, da sonst der Empfänger der chiffrierten Nachricht diese nicht entschlüsseln kann. Es muss also die ursprüngliche Struktur der Botschaft so geschickt verändert werden, dass keinerlei Ordnung mehr erkennbar ist und selbst eine Analyse durch leistungsstarke Rechenmaschinen keinen Erfolg bringt.

DES-System

Ein System zum Senden und Empfangen codierter Nachrichten besteht aus zwei Komponenten. Zum Einen ist ein Programm oder sogar ein spezieller Computer notwendig, der sowohl chiffrieren als auch dechiffrieren kann und zum Anderen ein Schlüssel. Es kann also das gleiche Programm von vielen benutzt werden. Obwohl nun alle dasselbe Verschlüsselungssystem verwenden, kann die Nachricht nur mit dem passenden Schlüssel dechiffriert werden. Empfänger und Sender der Nachricht müssen logischerweise denselben Schlüssel besitzen, was aber ein Problem darstellt, denn wie soll ein Schlüssel sicher übermittelt werden? Es ist zwar kein Problem, militärische Kommunikationseinrichtungen damit auszustatten, da ein Beauftragter alle Einrichtungen besuchen könnte. Im Regelfall sind sich aber Empfänger und Sender der Nachrichten noch nie begegnet und kennen sich nicht. Es ist also nicht möglich, einen gemeinsamen Schlüssel sicher zu übergeben. Folglich taugt dieses System nur bedingt, da zum Beispiel große Bankinstitute oder Wirtschaftsunternehmen nicht in der Lage sind, sämtliche Nachrichtenempfänger und -sender mit dem entsprechenden Schlüssel auszustatten. Dies ist rein praktisch nicht durchführbar.
Das bekannteste Beispiel für dieses System dürfte der amerikanische „Data Encryption Standard“ (DES) sein. Als Schlüssel dient dabei eine binäre Zahl mit 56 Stellen, also eine Zahl, die 56 bits benötigt. Insgesamt gibt es deshalb 2^{56} Möglichkeiten. Um den Code zu knacken, könnte man nun theoretisch über $7{,}2 * 10^{16}$ mögliche Schlüssel ausprobieren. In der Praxis aber war dies bis vor kurzem nicht möglich. Mittlerweile gelingt es aber Hochleistungsrechenmaschinen, eine solche Nachricht innerhalb von 3 Tagen zu entschlüsseln. Trotz aller Nachteile ist dieses System noch relativ weit verbreitet, da der Schlüssel durch einen vertrauenswürdigen Kurier übermittelt werden kann und die gesendeten Nachrichten nicht so wichtig sind, dass ein Dechiffrieren durch eine

Hochleistungsrechenmaschine zu befürchten ist. Außerdem sind die meisten Nachrichten schon veraltet, wenn sie erst nach 2 oder 3 Tagen geknackt wurden.

RSA-Verfahren

Um die Nachteile dieses Systems auszuschalten, entwickelten Whitfield Diffie und Martin Hellman im Jahre 1975 die sogenannte „public key cryptography“. Ronald Rivest, Adi Shamir und Leonard Adleman vom Massachusetts Institute of Technology brachten dieses System zur Serienreife, daher ist es nach ihren Initialen als RSA-Verfahren benannt worden. Der Grundaufbau ist mit dem DES-System identisch, jedoch ist der Schlüsselgedanke grundlegend verändert worden. Wie der Name schon sagt, existiert ein öffentlicher Schlüssel, der jedem bekannt sein darf. Es handelt sich dabei um das Produkt zweier mindestens 100-stelliger Primzahlen, also einer 200-stelligen Zahl. Allerdings kennt alleine der Empfänger die beiden Primfaktoren dieser Zahl und somit kann nur er die Nachricht entschlüsseln. Es werden dabei bewusst zwei riesige Primfaktoren gewählt, da eine 200-stellige Zahl, die sich zum Beispiel lediglich aus vielen ein- oder zweistelligen Primzahlen zusammensetzt, sehr schnell faktorisiert werden kann. So ist die Zahl 6000 schneller und leichter in $2^4 * 3 * 5^3$ zerlegt, als 3431 in 47 und 73.

Bei diesem System der geheimen Übertragung von Daten macht man sich das grundlegende Problem der Faktorisierung von großen Zahlen zu Eigen. Zum Beispiel kann die Zahl 323 sehr schnell in 17 * 19 zerlegt werden, doch die Zerlegung von 355 207 in 359 und 599 ist bereits nicht mehr so leicht zu bewerkstelligen. Und selbst mit Hochleistungs-rechenmaschinen ist es unmöglich, eine 200-stellige Zahl in ihre beiden 100-stelligen Primfaktoren zu zerlegen.

Trotz dieser scheinbar unüberwindbaren Hürde kann selbst dieses System keine absolute Sicherheit bieten. Die Erfinder mussten dies 1982 erfahren, als der Hochleistungsrechner CRAY-1 unerwartet bis zu 70-stellige Zahlen mit Leichtigkeit faktorisieren konnte und die damals nur 100-stelligen Schlüssel unsicher wurden. Der Ausweg war die Einführung von 200-stelligen Zahlen als Schlüssel. Es blieb jedoch die Unsicherheit, dass durch noch leistungsstärkere Computer selbst diese riesigen Zahlen eines Tages keine ausreichende Sicherheit mehr garantieren könnten.

Handytechnik als explizites Beispiel

Es denkt gewiss niemand an Mathematik, wenn er mit einem Handy telefoniert. Doch gerade hier wird durch komplizierteste Systeme versucht, die SIM-Karten (SIM = subscriber identity module) vor unerlaubtem Benutzen zu schützen. Bei der PIN-Eingabe (PIN = personal identity number) wird nicht nur die Geheimzahl geprüft, sondern gleichzeitig werden zufallsgenerierte Ströme durch die SIM-Karte geschickt. Dies soll verhindern, dass durch Messungen von Spannungen und Strömen Rückschlüsse auf den richtigen PIN gezogen werden können. Es zeigt sich auch hier wieder die Problematik der absoluten Sicherheit, denn diese kann trotz kompliziertester und ausgeklügelster Systeme niemals und nirgendwo gewährleistet werden.

Literaturverzeichnis

Bücher:

Athen, Hermann
und Bruhn, Jörn: Lexikon der Schulmathematik. Köln 1977

Devlin, Keith: Sternstunden der modernen Mathematik.
Aus dem Englischen von Doris Gerstner. Basel 1990

Trost, Ernst: Primzahlen. Zweite, überarbeitete Auflage. Basel 1968.

Zagier, Prof. Dr. D.: Die ersten 50 Millionen Primzahlen. Erste Auflage. Basel 1977.

Internetbeiträge:

http://www.primzahlen.de/files/theorie/beweise.htm aufgerufen am 10.01.03
(siehe Anhang I)

http://www.primzahlen.de/files/theorie/fakultaet.htm aufgerufen am 10.01.03
(siehe Anhang II)

http://www.primzahlen.de/files/theorie/index.htm aufgerufen am 10.01.03
(siehe Anhang III)

http://www.primzahlen.de/files/theorie/mersenne.htm aufgerufen am 24.07.02
(siehe Anhang IV)

Sonstige Hilfsmittel

Programm:

QBasic mit 2 selbst geschriebenen Programmen (primtest.bas und generat.bas)
(siehe Anlage V)

Ich erkläre hiermit,

dass ich die Facharbeit ohne fremde Hilfe angefertigt und nur die im Literaturverzeichnis angeführten Quellen und Hilfsmittel benützt habe.

Neusitz, den 11.01.03 ……

Raimund Schilder