Johann Wiesenbauer

Was sind und was sollen große Primzahlen?

Als auf einer Tagung der Amerikanischen Mathematischen Gesellschaft im Oktober 1903 Professor F.N.Cole von der Universität Columbia zur Tafel ging, um seinen Vortrag mit dem Titel "On the Factorization of Large Numbers" zu beginnen, deutete noch nichts darauf hin, daß es ein in vieler Hinsicht recht ungewöhnlicher Vortrag werden sollte. Ungewöhnlich war dabei nicht nur die Präsentation - der Vortragende, welcher als sehr schweigsamer Mann bekannt war, machte seinem Ruf alle Ehre und sprach den ganzen Vortrag über kein einziges Wort - sondern auch der Inhalt: Cole berechnete zunächst 2^{67} zog dann sorgfältig 1 davon ab, um anschließend auf einem freien Teil der Tafel das Produkt

$$193\ 707\ 721 * 761\ 838\ 257\ 287$$

zu berechnen. Das Ergebnis war in beiden Fällen das gleiche. Es wird berichtet, daß sich das Auditorium spontan erhob, um dem Vortragenden im Stehen zu applaudieren - ein ebenfalls in diesem Rahmen noch nie dagewesenes Ereignis. Interessanterweise wurden auch keine Fragen im Anschluß an den Vortrag gestellt, wie um Cole nicht zu zwingen, sein Schweigen zu brechen. Immerhin aber wissen wir aus einer Bemerkung, die er Jahre später Bell gegenüber machte, daß es ihn "die Sonntage von drei Jahren" gekostet hatte, die oben angegebene Faktorisierung von $2^{67} - 1$ zu finden.

Wir haben hier einen Spezialfall eines allgemeinen Problems vor uns, von dem niemand Geringerer als Gauß in seinen "Disquisitiones Arithmeticae" sagte, daß es zu den nützlichsten der gesamten Arithmetik" gehöre, nämlich für eine gegebene natürliche Zahl n zu entscheiden, ob sie zusammengesetzt ist oder nicht, und gegebenenfalls ihre nichttrivialen Teiler zu bestimmen. Wenn Gauß ebenda weiter meinte, daß "alle bisher angegebenen Methoden entweder auf spezielle Fälle beschränkt oder so mühsam und weitläufig sind, daß sie auf größere Zahlen meistenteils kaum angewendet werden konnten", so muß aus heutiger Sicht dazu gesagt werden, daß speziell auf dem Gebiet der Primzahltests seither doch große Fortschritte erzielt werden konnten, wovon noch die Rede sein wird. Für Probleme der Faktorisierung aber haben die Worte von Gauß auch heute noch im wesentlichen Gültigkeit, wenn auch auf diesem Gebiet die Methoden seither sehr verfeinert wurden und man mit Hilfe

des Computers in unvorstellbare Höhen vorgestoßen ist. Ein Beispiel soll dies illustrieren: Um eine Zahl mit ca. 100 Stellen auf Primeigenschaft zu überprüfen braucht ein moderner Hochleistungscomputer heute weniger als eine Minute, um eine zusammengesetzte Zahl dieser Größenordnung zu faktorisieren würde er im allgemeinen Fall etwa 100 Jahre benötigen (siehe [3]).

Ganz anders liegen die Dinge, wenn die zu untersuchende Zahl eine spezielle Gestalt hat, sodaß bestimmte Sätze der Zahlentheorie darauf angewendet werden können. Das wohl bekannteste Beispiel dafür sind die Mersenneschen Zahlen M_n, worunter man Zahlen der Bauart $2^n - 1$ versteht. Diese Namensgebung kommt daher, daß M.Mersenne 1644 im Vorwort seiner "Cogitata Physica - Mathematica" versucht hatte, einer Liste aller $n \leq 257$ anzugeben, für welche M_n prim ist. Wie man leicht sieht, kann eine solche Liste nur selbst wieder Primzahlen enthalten, da ein nichttrivialer Teiler k von n sofort den nichttrivialen Teiler M_k von M_n induziert. Die von Mersenne angegebene Liste, nämlich 2,3,5,7,13,17, 19,31,67,127,257, enthielt allerdings 5 Fehler: 67 (siehe oben!) und 257 gehören nicht dazu, dafür fehlen irrtümlich 61,89 und 107. Mersenne wäre sicher sehr erstaunt gewesen, hätte er von der Berichtigung erfahren, die übrigens in allen Punkten erst 1947 abgeschlossen war. Er war nämlich der Meinung, daß, "um zu entscheiden, ob eine gegebene Zahl von 15 oder 20 Ziffern eine Primzahl ist, alle Zeit nicht zu reichen vermag, welche Hilfsmittel und welches Wissen wir auch benutzen." Was aber erst hätte er zur nachstehenden Liste gesagt, welche den derzeitigen Stand (Frühjahr 1986) der Dinge auf dem Gebiet der Mersenneschen Primzahlen widergibt?

n mit M prim	Entdecker	Computer	Jahr
2,3,5,7,13,17	N.N.		-
19	P.A.Cataldi	-	1588
31	L.Euler	-	1722
61	I.M.Perwuschin	-	1883
89	R.E.Powers	-	1911
107	R.E.Powers, E.Fauquemberge	-	1914
127	E.Lucas	-	1876
521,607,1279, 2203,2281	R.M.Robinson	SWAC	1952
3217	H.Riesel	BESK	1957
4253,4423	A.Hurwitz, J.L.Selfridge	IBM 7090	1961
9689,9941,11213	D.B.Gillies	ILLIAC 2	1963
19937	B.Tuckerman	IBM 360	1971

21701	C.Noll,L.Nickel	CYBER 174	1978
23209	C.Noll	CYBER 174	1979
44497	D.Slowinski,H.L.Nelson	CRAY-1	1979
86243	D.Slowinski	CRAY-1	1983
132049	D.Slowinski	CRAY X-MP	1983
216091	D.slowinski	CRAY X-MP	1985

Von den ersten 6 Mersenneschen Primzahlen waren zumindestens die ersten 4 bereits im Altertum bekannt. Cataldi, dem gelegentlich auch die Entdeckung der Mersenneschen Primzahl M_{17} zugeschrieben wird, nahm als erster für seine Berechnungen bereits eine Primzahltabelle mit ca. 750 Einträgen zur Hilfe. Trotzdem ging es in der Folge, wie die großen zeitlichen Abstände in der Tabelle zeigen, nur sehr zäh weiter. So wurde in den fast 3 Jahrhunderten zwischen 1588 und 1883 nur eine einzige neue Mersennesche Primzahl gefunden, und zwar - wie könnte es anders sein - von Euler. Erst mit dem Einsatz von elektronischen Rechenanlagen in der 2.Hälfte unseres Jahrhunderts ging es dann Schlag auf Schlag. Von der legendären SWAC, welche noch mit einem Kernspeicher von 256 Worten mit je 37 Bit auskommen mußte und noch eine Zykluszeit von 16 Mikrosekunden hatte, bis zu den heutigen Supercomputern vom Typ CRAY X-MP, welche über 400 Millionen Operationen pro Sekunde bewältigen und derzeit mit einer 65050-stelligen Mersenneschen Primzahl den Rekord halten, spannt sich hier ein weiter Bogen. Gelegentlich findet man sogar Meldungen über die Entdeckung von "größten" Primzahlen in Tageszeitungen. So meldete z.B. die Süddeutsche Zeitung den damaligen Weltrekord der kalifornischen Studenten C.Noll und L.Nickel mit M_{21701} unter der Überschrift:"Größte Primzahl blieb im Sieb des Eratosthenes hängen." Wie Borho in [1] sehr treffend bemerkt, entbehrt diese Meldung nicht der Komik, da "das Sieb des Eratosthenes für die Aufspürung großer Primzahlen ungefähr so gut geeignet ist wie eine Axt für die Spaltung von Atomkernen."

Damit sind wir bei der Frage angelangt, welche Methoden nun wirklich angewandt werden, um solche Zahlenriesen auf Primeigenschaft hin zu untersuchen. Die Antwort darauf läßt sich glücklicherweise sehr einfach formulieren. Es wird ein Kriterium verwendet, welches 1878 von E.Lucas in einem Spezialfall gefunden und 1930 von D.E.Lehmer auf die heutige allgemeine Form gebracht wurde. Es lautet:

Lucas-Lehmer-Test: Ist p eine ungerade Primzahl und die Folge $L_1, L_2, L_3, \ldots$ rekursiv defiert durch

$$L_1 = 4, \qquad L_{i+1} = L_i^2 - 2 \bmod M \quad \text{für } i=1,2,3,\ldots$$

so ist M_p genau dann prim, wenn $L_{p-1} \equiv 0 \bmod M_p$ ist.

Dieser Test ist in gewisser Hinsicht sogar noch einfacher, als er aussieht. Aufgrund der Beziehung

$$A*2^p + B \equiv A + B \bmod M_p$$

kann nämlich die Reduktion eines Folgenglieds mod M_p leicht so durchgeführt, daß man, etwas salopp ausgedrückt, die Binärdarstellung der Zahl nach dem p-ten Bit (von rechts gezählt) in 2 Teile teilt und den vorderen Teil zum hinteren addiert. Diese Prozedur muß gegebenenfalls wiederholt werden, falls das so erhaltene Binärwort noch nicht kleiner als M_p ist. Insbesondere sieht man sofort, daß eine Multiplikation eines Binärwortes mit 2 mod M_p nichts anderes bewirkt, als dessen zyklische Verschiebung um eine Stelle nach links (Linksrotation).

Im Falle, daß die Mersennesche Zahl zusammengesetzt ist, liefert der Lucas-Lehmer-Test leider keine Auskunft über mögliche nichttriviale Teiler. Glücklicherweise gibt es jedoch andere Sätze, welche hier weiterhelfen. So hat schon Fermat in einem Brief an Frenicle aus dem Jahre 1640 festgestellt, daß jeder Teiler q von M_p von der Form 2*k*p+1 sein muß. Euler hat gezeigt, daß darüberhinaus $q \equiv \pm 1 \bmod 8$ gelten muß, was die Anzahl der möglichen Teiler noch ein weiteres Mal um etwa die Hälfte reduziert.

Wir wollen die Anwendung dieser Sätze am Beispiel der M_{31} zeigen. Zunächst gibt es genau 46 340 Zahlen, welche kleiner sind als die Wurzel von M_{31} und wenn es einen nichttrivialen Teiler gibt, so müßte der kleinste nichttriviale Teiler sicher darunter sein. Da er außerdem sicher prim ist (sonst wäre er nicht der kleinste!), können wir uns weiter auf die Primzahlen in dieser Menge beschränken, wobei noch 4792 Zahlen übrig bleiben. Nur 157 davon erfüllen auch die Fer-Bedingung und davon nur 84 auch noch die Eulersche Bedingung. Von diesen verbleibenden Zahlen ist jedoch keine ein Teiler von $M_{31} \cdot M_{31}$ ist daher prim.

Wahrscheinlich den gleichen Weg, nur mit anderem Ergebnis hat auch Cole in dem eingangs erwähnten Beispiel beschritten. Allerdings ist dabei der Arbeitsaufwand schon bedeutend größer, wie folgende Überlegung zeigt: Es gibt, wie man aus der asymptotischen Abschätzung $\pi(x) \sim x/\ln(x)$ für die Funktion $\pi(x)$, welche die Anzahl der Primzahlen $\leq x$ angibt, ersieht, ungefähr 10 150 000 Primzahlen $< 193\,707\,721$, von diesen erfüllt etwa jede 67-te die Fermatsche Bedingung und etwa jede zweite dann auch noch die Eulersche Bedingung, womit rund 75 000 Zahlen übrig bleiben, die noch daraufhin

untersucht werden müssen, ob sie M_{31} teilen. Das sind noch sehr viele. Möglicherweise hat daher Cole noch auf anderem Wege einschränkende Bedingungen für die Teiler gewonnen, z.B. über die Theorie der quadratischen Reste, worauf wir hier nicht näher eingehen wollen.

Die einschränkenden Bedingungen von Fermat und Euler für die Teiler einer Mersenneschen Zahl M_p zeigen, daß die als Teiler in Frage kommenden Zahlen im Mittel einen Abstand von 4p haben, also relativ "dünn gesät" sind. Nimmt man nun an, so wie das Gillies in [4] gemacht hat, daß dies die einzige Einschränkung für potentielle Faktoren darstellt und daß ihre Anzahl in einem Intervall [A,B] unter geeigneten Einschränkungen für A,B Poisson-verteilt ist und zwar mit dem Mittelwert ln((ln B)/ln(max(A,2p)), so ergeben sich daraus eine Reihe von interessanten Konsequenzen für die statistische Verteilung von Mersenneschen Primzahlen. So wäre dann etwa die Anzahl von Mersenneschen Primzahlen $\leq x$ ungefähr (2/ln 2)ln ln x und die Wahrscheinlichkeit für ein M_p, daß es prim ist, wäre etwa (2 ln 2p)/(p ln 2). Ferner sollten für beliebiges x zwischen x und 2x im Mittel 2 Mersennesche Primzahlen liegen. Es sind dies alles Dinge, welche durch empirische Daten weitgehend bestätigt wurden (siehe [6]). Dies zeigt einmal mehr, daß Primzahlen zwar einzeln nicht "in den Griff" zu bekommen sind, sie aber in ihrer Gesamtheit, also "statistisch" gesehen, ein großes Wohlverhalten an den Tag legen.

Wir verlassen nun die Mersenneschen Zahlen, welche wir als Beispiel für Zahlen einer speziellen Bauart etwas ausführlicher besprochen haben und wenden uns der Frage zu, wie man für eine beliebig vorgegebene Zahl erkennen kann, ob sie prim ist oder nicht. Viele Methoden beruhen darauf, daß man die vorgegebene Zahl einem Test unterwirft, der speziell für Primzahlen in einer typischen Weise ausgeht. Verhält sich die vorgegebene Zahl beim Test wie eine Primzahl, so sagen wir, sie habe den "Test bestanden" und die Wahrscheinlichkeit, daß sie wirklich prim ist, ist größer geworden. Besteht sie den Test jedoch nicht, so ist sie mit Sicherheit nicht prim.

Als Beispiel wollen wir den Fermat-Test anführen, der sich aus dem "Kleinen Fermatschen Satz" ableitet. Dieser sagt aus, daß für eine Primzahl n und für jedes zu n teilerfremde a die Potenz $a^{n-1} \bmod n$ den Wert 1 ergibt. Eine Zahl n, welche diesen Test für ein teilerfremdes a besteht, ohne tatsächlich Primzahl zu sein, wird eine Pseudoprimzahl zur Basis a genannt.

Die alten Chinesen (und übrigens auch noch Leibniz) glaubten an die Nichtexistenz von Pseudoprimzahlen zur Basis 2.Leider

hatten sie nicht recht, da wir sonst ein überaus einfaches Primzahlkriterium zur Hand hätten. Schon P.F.Sarrus entdeckte im Jahre 1819 das kleinste Gegenbeispiel, nämlich n=341=11*31, welches den Fermat-Test zur Basis 2 erfüllt. Aber es kommt noch schlimmer: Es gibt Zahlen, welche den Fermat-Test für jede in Frage kommende Basis bestehen! Sie werden nach ihrem Entdecker Carmichael-Zahlen genannt. Die kleinste derartige Zahl ist 561=3*11*17. Allerdings muß gesagt werden, daß schon Pseudoprimzahlen sehr selten sind und Carmichael-Zahlen noch viel seltender (siehe [5]).

Glücklicherweise braucht man sich über sie nicht allzu sehr den Kopf zu zerbrechen, da es eine sehr einfache Verschärfung des Fermat-Tests gibt, welche dann auch den Carmichael-Zahlen zum Verhängnis wird. Setzt man dazu o.B.d.A. n als ungerade voraus, so läßt es sich darstellen in der Form $n = 2^s * t + 1$ mit ungeradem t. Nimmt man nun die Potenzierung in der Weise vor, daß man der Reihe nach die Potenzen

$$a^{t}, a^{2t}, a^{4t}, \ldots \bmod n$$

bezüglich der gewählten Basis a bildet, so muß so wie vorher für eine Primzahl n irgendwann in dieser Folge eine 1 vorkommen. Neu daran ist die von G.L.Miller stammende Beobachtung, daß unmittelbar vorher (außer die 1 ist gleich zu Beginn aufgetreten) das Folgenglied n - 1 kommen muß, da ja die 1 durch Quadrieren entstanden ist und die Kongruenz $x^2 \equiv 1$ modulo einer Primzahl n nur die Lösungen 1 und n - 1 besitzt. Eine zusammengesetzte Zahl, welche diesen Test besteht, wird auch starke Pseudoprimzahl genannt. Wie O.M.Rabin 1976 gezeigt hat, ist jedes n eine starke Pseudo-Primzahl für höchstens ein Viertel aller in Frage kommenden Basen. Durch eine zufällige Auswahl von genügend vielen Basen kann daher die Irrtumswahrscheinlichkeit bei diesem verschärften Fermat-Test, welcher auch Rabin-Miller-Test genannt wird, beliebig klein gemacht werden.

Kaum war dieser neue schnelle Primzahltest gefunden, fand er auch bereits Abnehmer im Bereich der Kryptographie. 1977 wurde von R.L.Rivest, A.Shamir Und L.Adleman ein neues Chiffrierverfahren vorgestellt, das heute nach seinen Erfindern RSA-Schema genannt wird und die Bereitstellung sehr großer (mindestens 100-stelliger) Primzahlen zur Voraussetzung hat. Der Grundgedanke des Verfahrens beruht nun darin, daß es sehr einfach ist, das Produkt zweier so großer Primzahlen zu bilden, aber in einer vernünftigen Zeit unmöglich, aus dem Produkt die Faktoren zu rekonstruieren (bez. Einzelheiten siehe etwa [7]). Hatte Euler noch geklagt: "Von

allen Problemen, mit denen man sich in der Mathematik beschäftigt, wird ... keines für unfruchtbarer und nutzloser

gehalten als diejenigen, die sich mit der Natur der Zahlen und der Teiler befassen", so hat sich diese Aussage heute geradezu in ihr Gegenteil verkehrt und die Zahlentheorie - ehemals eines der reinsten Teilgebiete der Mathematik - steht plötzlich mitten in den Anwendungen.

Wenn im Bereich der allgemeinen Zahlen bisher nur von Primzahltests die Rede war, welche mit einer, wenn auch noch so kleinen Irrtumswahrscheinlichkeit behaftet sind (was nur in theoretischen Überlegungen eine Rolle spielt), so soll damit nicht der Eindruck erweckt werden, als ob man bei den streng deterministischen Tests nicht weitergekommen wäre. Das Gegenteil ist der Fall: Im Jahre 1980 haben Adleman und R.S.Rumely einen Test entwickelt, der in der Folge von H.Cohen und H.W.Lenstra jun. noch verbessert wurde, so daß man heute damit 200-stellige in 10 Minuten auf einer Großrechenanlage auf Primalität testen kann, wofür man vorher noch ca. 1 Milliarde Jahre gebraucht hätte (siehe [3]). Leider verwendet der Test Hilfsmittel aus der algebraischen Zahlentheorie, die seine Darstellung hier verbieten.

Wie schon eingangs bemerkt, sind die Erfolge auf dem Gebiet der Faktorisierung großer Zahlen nicht ganz so verheißungsvoll, wenn auch hier große Fortschritte erzielt werden konnten. Einige der besten derartigen Tests verwenden eine einfache auf Legendre zurückgehende Idee. Dieser hatte bemerkt, daß es für ein zusammengesetztes n stets Zahlen a,b mit $a^2 \equiv b^2 \bmod n$, jedoch $a \not\equiv \pm b \bmod n$ geben muß. Umgekehrt kann man aus einer derartigen Darstellung sofort nichttriviale Teiler von n gewinnen, indem man die g.g.T. (a+b,n) bzw. (a-b.n) bildet. Diese Methoden unterscheiden sich alle nur in der Art, wie sie die Quadrate finden, z.B. mit Hilfe der Kettenbruchentwicklungen der Wurzel aus geeigneten Vielfachen von n oder über quadratische Reste. Leider führen auch hier wieder die Details aus dem Bereich der Schulmathematik heraus, sodaß wir uns mit diesen Andeutungen begnügen müssen. Sehr gute Übersichtsdarstellungen auf diesem Gebiet bieten [3], [8].

Eine Frage, die bisher nicht berührt wurde, soll zum Abschluß noch erörtert werden, nämlich die nach der algorithmischen Realisierung der dargestellten Verfahren. Statt weitläufiger Ausführungen möchte ich im folgenden zwei typische Beispielprogramme vorstellen, welche beide in Turbo-BASIC (siehe [9]) auf einem ATARI 800 XL geschrieben wurden. Die in den Programmen enthaltenen Kommentare sollten zu ihrem Verständnis ausreichen.

```
100 REM PRIMTEST FUER MERSENNESCHE ZAHLEN
110 CLR :CLS :DIM LL$(307):EXEC LIES_DATEN
120 PRINT :INPUT "EXPONENT DER MERSENNESCHEN ZAHL";M
130 TIME$= "000000":T=0
140 IF M<=2 THEN PRIM=(M=2):EXEC AUSGABE:GOTO 120
150 EXEC MIN_TEILER:IF MT<M THEN T=2^MT-1:T2=T:EXEC AUSGABE:GOTO 120
160 ? "TEILERSUCHE/LUCAS-LEHMER TEST(T/L)?";
170 GET A:TIME$= "000000"
180 IF A=ASC("T") THEN ? CHR$(A):GOTO 310
190 IF A=ASC("L") THEN ? CHR$(A):GOTO 510
200 GOTO 170
300 REM *** TEILERTEST FUER T<=T2 ***
310 POKE 559,0:T1=2*M+1:T2=10^9:IF M<60 THEN T2=2^(M/2)
320 OS=INT(M/3)+1:DT=2*M*(3*M MOD 4):T=1+DT:MM=8*M
330 WHILE T<=T2
340   EXEC T_TEILBAR:IF TB THEN 360
350   EXEC MERS_MOD_T:IF MSR=1 THEN EXIT
360   DT=MM-DT:T=T+DT
370 WEND
380 EXEC AUSGABE:GOTO 120
500 REM *** LUCAS-LEHMER TEST ***
510 IF M>2047 THEN PRINT "EXPONENT DARF NICHT > 2047 SEIN!":GOTO 120
520 POKE 559,0:PRIM=USR(ADR(LL$),M)
530 EXEC AUSGABE:GOTO 120
990 ------------------------------
1000 PROC MIN_TEILER
1010   IF (M MOD 2)=0 THEN MT=2:GOTO 1090
1020   IF (M MOD 3)=0 THEN MT=3:GOTO 1090
1030   MT=5:D=2
1040   WHILE MT<=M/MT
1050     IF (M MOD MT)=0 THEN EXIT
1060     MT=MT+D:D=6-D
1070   WEND
1080   IF MT>M/MT THEN MT=M
1090 ENDPROC
1990 ------------------------------
2000 PROC ZEIT
2010   Z=TIME/50:STD=INT(Z/3600):Z=Z-3600*STD
2020   MIN=INT(Z/60):SEC=Z-60*MIN:PRINT "ZEIT: ";
2030   IF STD>0 THEN PRINT STD;" STD ";
2040   IF MIN>0 THEN PRINT MIN;" MIN ";
2050   PRINT SEC;" SEC."
2060 ENDPROC
2990 ------------------------------
3000 PROC T_TEILBAR
3010   TB=1:IF (T MOD 3)=0 THEN 3080
3020   PT=5:D=2
3030   WHILE PT<=OS
3040     IF (T MOD PT)=0 THEN EXIT
3050     PT=PT+D:D=6-D
3060   WEND
```

```
3070   IF PT>0G THEN TB=0
3080 ENDPROC
3990 -------------------------------
4000 PROC MERS_MOD_T
4010   MSR=1
4020   FOR I=1 TO M
4030     MSR=MSR+MSR:IF MSR>=T THEN MSR=MSR-T
4040   NEXT I
4050 ENDPROC
4990 -------------------------------
5000 PROC LIES_DATEN
5010   FOR I=1 TO 307
5020     READ A:LL$(I)=CHR$(A)
5030   NEXT I
5040 ENDPROC
5100 REM DATEN FUER BINAERCODE IN LL$
5110 DATA 104,104,133,213,133,206,133,204,104,133,212,133,205,133,203,162
5120 DATA 3,24,102,204,102,203,202,208,248,169,7,37,212,170,169,1,10,202
5130 DATA 208,252,133,207,56,165,205,233,3,133,205,165,206,233,0,133,206
5140 DATA 162,255,169,0,232,157,0,80,228,203,48,248,169,4,157,0,80,164,203
5150 DATA 165,212,56,233,1,133,208,165,213,133,209,166,203,232,202,189,0,80
5160 DATA 157,0,81,157,0,82,169,0,157,0,80,138,208,238,24,162,0,200,126,0
5170 DATA 82,232,136,208,249,164,203,144,63,166,203,232,24,202,189,0,80,125
5180 DATA 0,81,157,0,80,138,208,243,173,0,80,37,207,240,39,77,0,80,1410,80
5190 DATA 185,0,80,24,105,1,153,0,80,144,22,166,203,240,241,202,189,0,80
5200 DATA 105,0,157,0,80,144,7,138,208,242,176,225,176,146,166,203,232,24
5210 DATA 202,62,0,81,138,208,249,173,0,81,37,207,240,14,77,0,81,141,0,81
5220 DATA 185,0,81,105,1,153,0,81,56,165,208,233,1,133,208,165,209,233,0
5230 DATA 133,209,176,131,185,0,80,56,233,2,153,0,80,176,26,166,203,240,14
5240 DATA 202,189,0,80,233,0,157,0,80,176,11,138,208,242,185,0,80,233,0,153
5250 DATA 0,80,165,205,56,233,1,133,205,165,206,233,0,133,206,176,155,162
5260 DATA 255,232,189,0,80,208,13,228,203,48,246,169,0,133,213,169,1,133
5270 DATA 212,96,169,0,133,213,133,212,96
5990 -------------------------------
6000 PROC AUSGABE
6010   POKE 559,34:PRINT "2^";M;"-1 IST ";
6020   IF (T=0 AND PRIM=1) OR (T>T2 AND T<10^9) THEN ? "PRIM!":GOTO 6060
6030   IF T>10^9 THEN PRINT "TEILERSUCHE BIS 10^9 ERFOLGLOS!":GOTO 6060
6040   IF T>0 THEN PRINT "TEILBAR DURCH ";T;".":GOTO 6060
6050   PRINT "NICHT PRIM!"
6060   EXEC ZEIT
6070 ENDPROC
```

```
0100 ;
0110 ;6502-ASSEMBLER PROGRAMM
0120 ;FUER LUCAS-LEHMER TEST
0130 ;(ATARI USR-ROUTINE)
0140 ;
0150 L=$CB
0160 I=$CD
0170 MSK=$CF
0180 M=$D4
0190 MM=$D0
0200 SM=$5000
0210 RL=$5100
0220 RR=$5200
0230              *=$4000
0240 ;
0250 ;INITIALISIERUNG
0260 ;
0270              PLA
0280              PLA
0290              STA M+1
0300              STA I+1
0310              STA L+1
0320              PLA
0330              STA M
0340              STA I
0350              STA L
0360              LDX #3
0370 L1           CLC
0380              ROR L+1
0390              ROR L
0400              DEX
0410              BNE L1
0420              LDA #7
0430              AND M
0440              TAX
0450              LDA #1
0460 L2           ASL A
0470              DEX
0480              BNE L2
0490              STA MSK
0500              SEC
0510              LDA I
0520              SBC #3
0530              STA I
0540              LDA I+1
0550              SBC #0
0560              STA I+1
0570              LDX #$FF
0580              LDA #0
0590 L3           INX
0600              STA SM,X
0610              CPX L
0620              BMI L3
0630              LDA #4
0640              STA SM,X
0650              LDY L
0660 ;
0670 ;BEGINN DER HAUPTITERATION
0680 ;
0690 LB1          LDA M
0700              SEC
0710              SBC #1
0720              STA MM
0730              LDA M+1
0740              STA MM+1
0750              LDX L
0760              INX
0770 LB2          DEX
0780              LDA SM,X
0790              STA RL,X
0800              STA RR,X
0810              LDA #0
0820              STA SM,X
0830              TXA
0840              BNE LB2
0850 ;
0860 ;RECHTSROTATION
0870 ;
0880 LR1          CLC
0890              LDX #0
0900              INY
0910 LR2          ROR RR,X
0920              INX
0930              DEY
0940              BNE LR2
0950              LDY L
0960              BCC LL1
0970 ;
0980 ;ADDITION
0990 ;
1000              LDX L
1010              INX
1020              CLC
1030 LA1          DEX
1040              LDA SM,X
1050              ADC RL,X
1060              STA SM,X
1070              TXA
1080              BNE LA1
1090              LDA SM
1100              AND MSK
1110              BEQ LL1
```

```
1120            EOR SM
1130            STA SM
1140 LA2        LDA SM,Y
1150            CLC
1160            ADC #1
1170            STA SM,Y
1180            BCC LL1
1190            LDX L
1200            BEQ LA2
1210 LA3        DEX
1220            LDA SM,X
1230            ADC #0
1240            STA SM,X
1250            BCC LL1
1260            TXA
1270            BNE LA3
1280            BCS LA2
1290 LA4        BCS LB1
1300 ;
1310 ;LINKSROTATION
1320 ;
1330 LL1        LDX L
1340            INX
1350            CLC
1360 LL2        DEX
1370            ROL RL,X
1380            TXA
1390            BNE LL2
1400            LDA RL
1410            AND MSK
1420            BEQ LM1
1430            EOR RL
1440            STA RL
1450            LDA RL,Y
1460            ADC #1
1470            STA RL,Y
1480 ;
1490 ;DEKREMENTIERUNG VON MM
1500 ;
1510 LM1        SEC
1520            LDA MM
1530            SBC #1
1540            STA MM
1550            LDA MM+1
1560            SBC #0
1570            STA MM+1
1580            BCS LR1
1590 ;
1600 ;SUBTRAKTION VON 2
1610 ;
1620 LS1        LDA SM,Y
1630            SEC
1640            SBC #2
1650            STA SM,Y
1660            BCS LI1
1670            LDX L
1680            BEQ LS3
1690 LS2        DEX
1700            LDA SM,X
1710            SBC #0
1720            STA SM,X
1730            BCS LI1
1740            TXA
1750            BNE LS2
1760 LS3        LDA SM,Y
1770            SBC #0
1780            STA SM,Y
1790 ;
1800 ;DEKREMENTIERUNG VON I
1810 ;
1820 LI1        LDA I
1830            SEC
1840            SBC #1
1850            STA I
1860            LDA I+1
1870            SBC #0
1880            STA I+1
1890            BCS LA4
1900 ;
1910 ;TEST, OB ALLE FELDELEMENTE 0
1920 ;
1930            LDX #$FF
1940 LT1        INX
1950            LDA SM,X
1960            BNE LE1
1970            CPX L
1980            BMI LT1
1990 ;
2000 ;ERGEBNIS
2010 ;
2020            LDA #0
2030            STA M+1
2040            LDA #1
2050            STA M
2060            RTS
2070 LE1        LDA #0
2080            STA M+1
2090            STA M
2100            RTS
```

```
100 REM ANWENDUNG DES RABIN-MILLER TESTS
110 DIM B(3):B(1)=2:B(2)=3:B(3)=5:CLS
120 PRINT :INPUT "TESTZAHL N<10^9 EINGEBEN: ",N:IF N>=10^9 THEN 120
130 FOR I=1 TO 3
140   BAS=B(I):EXEC RMTEST N BAS
150   IF RMT=0 THEN EXIT
160   ? "RABIN-MILLER TEST BEZ. ";BAS;" BESTANDEN!"
170 NEXT I
180 IF I<4 THEN 210
190 IF N=25326001 THEN 210
200 ? "N IST PRIM!":GOTO 120
210 ? "N IST ZUSAMMENGESETZT!":GOTO 120
990 ------------------------------
1000 PROC MULT A B MOD N
1010   PROD=0:AA=A MOD N:BB=B MOD N
1020   WHILE BB>0
1030     IF (BB MOD 2)=0 THEN 1050
1040     PROD=(PROD+AA) MOD N
1050     AA=(AA+AA) MOD N
1060     BB=BB DIV 2
1070   WEND
1080 ENDPROC
1990 ------------------------------
2000 PROC POT X E MOD N
2010   POT=1:XX=X MOD N:EE=E
2020   WHILE EE>0
2030     B=XX:IF (EE MOD 2)=0 THEN 2050
2040     A=POT:EXEC MULT A B MOD N:POT=PROD
2050     A=B:EXEC MULT A B MOD N:XX=PROD
2060     EE=EE DIV 2
2070   WEND
2080 ENDPROC
2990 ------------------------------
3000 PROC RMTEST N BAS
3010   S=0:T=N-1:X=BAS:RMT=0
3020   IF (T MOD 2)=1 THEN 3040
3030   T=T/2:S=S+1:GOTO 3020
3040   E=T:EXEC POT X E MOD N:X=POT
3050   IF X=1 OR X=N-1 THEN RMT=1:GOTO 3120
3060   E=2
3070   WHILE S>1
3080     EXEC POT X E MOD N:X=POT
3090     IF POT=N-1 THEN RMT=1:EXIT
3100     S=S-1
3110   WEND
3120 ENDPROC
```

Das erste Programm hat die Untersuchung von Mersenneschen Zahlen auf Primeigenschaft zum Inhalt, wobei man zwischen einer direkten Teilersuche und dem Lucas-Lehmer-Test wählen kann. Wählt man letzteren, so wird eine 6502-Maschinensprachroutine aufgerufen, um die Sache zu beschleunigen. Tatsächlich braucht z.B., um alle 5 "Mersenneschen Problemfälle", nämlich 61,67,89,107 und 257 damit zu überprüfen nur rund eine Minute. Für die ersten drei der von Robinson gefundenen Mersenneschen Primzahlen, nämlich für die Exponenten 521,607 und 1279 braucht das Programm rund 7 bzw. 11 bzw. 105 Minuten und ist damit etwa um den Faktor 6 langsamer als die SWAC damals. Auch darf der Exponent aus programmtechnischen Gründen nicht größer als 2047 sein (bei der SWAC war die obere Schranke 2303).

Mit dem zweiten Programm schließlich können mit Hilfe von Rabin-Miller-Test alle Zahlen < 1 000 000 000 auf Primalität untersucht werden. Es wird dabei die Tatsache verwendet, daß es nur eine einzige Zahl in diesem Bereich gibt, welche starke Pseudoprimzahl für die Basen 2,3 und 5 ist, nämlich 25 326 001. Dieser Primzahltest dauert maximal eine halbe Minute.

Seit ich die eingangs erzählte Geschichte mit der Faktorisierung gelesen habe (zum erstenmal in [2]) hat mich der Gedanke nicht losgelassen, wieviele Sonntage Cole hätte opfern müssen, hätte er schon damals einen Kleincomputer gehabt, wie er heute in vielen Haushalten (meist zum Spielen) herumsteht. Ich habe daher in das erste Programm auch die Möglichkeit einer direkten Teilersuche eingebaut, falls der vorangegangene Lucas-Lehmer-Test negativ verläuft. Wie ich sehen mußte, kommt für diesen Exponenten auch der Computer ganz schön ins Schwitzen. Selbst in der compilierten Version des Programms braucht er noch ca. 6.5 Stunden, womit die Leistung Coles erst ins rechte Licht gerückt wird. Welche Faszination muß für ihn und seinesgleichen von den Primzahlen ausgegangen sein, um soviel Arbeit und Mühe zu investieren? Könnte man diese auch bei vielen jungen Menschen beobachtbare Motivation nicht auch für den Schulunterricht nützen? Dafür einige Anregungen gegeben zu haben, war das Ziel meiner Ausführungen.

Literatur

[1] Borho W., Ein zweitausend Jahre altes Thema der elementaren Zahlentheorie, aus: Mathematische Miniaturen 1, Lebendige Zahlen, Birkhäuser Verlag, 1981.

[3] Pomerance C., Primzahlen im Schnelltest, Spektrum der Wissenschaft, Februar, 1983

[4] Gillies D.B., Three New Mersenne Primes and a Statistical Theory, Math.Comp.,93-95,18(1964

[5] Pomerance C.,J.L.Selfridge,S.S.Wagstaff,Jr, The Pseudoprimes to 25.10 , Math.Comp.,1003-1026, 35(1980)

[6] Wagstaff S.S.,Jr.,Divisors of Mersenne Numbers, Math. Comp., 385-397,40(1983)

[7] Hellmann M.E., Die Mathematik neuer Verschlüsselungssysteme, Spektrum der Wiss.,93-101,10(1971)

[8] Riesel H., Prime Numbers and Computer Methods for Factorization, Birkhäuser Verlag, 1985.

[9] Happy-Computer-Sonderheft 2, Markt & Technik, 1986