Zahlentheorie in der Schule

1. Einleitung

Mathematik wird von vielen, insbesondere auch von Schülern, als trocken und langweilig empfunden. Auch wenn man selbst anderer Meinung ist, so wird man doch zugeben müssen, daß nicht alle Teilgebiete der Mathematik gleichermaßen interessant sind. Für die Beschäftigung mit Finanzmathematik etwa ist wohl die unbestrittene Tatsache ihrer Nützlichkeit die einzige Motivation. Sieht man sich dagegen an, was so große Mathematiker wie Gauß, Euler, Legendre, Langrange, Fermat usw. für persönliche Vorlieben innerhalb der Mathematik gehabt haben, so wird man sofort auf die Zahlentheorie stoßen - nach Gauß "die Königin der Mathematik".

Wenn man also dem Schüler zeigen will, wie interessant Mathematik auch sein kann, ist man mit der Zahlentheorie nicht schlecht beraten. Dem kommt entgegen, daß sich viele ihrer Problemstellungen (wenn auch nicht die verwendeten Methoden zu ihrer Lösung) auch dem sprichwörtlichen "Mann von der Straße" erkären lassen, was wohl auch damit zusammenhängt, daß der Hauptgegenstand ihrer Untersuchungen, nämlich die natürlichen Zahlen, jedem von klein auf wohlvertraut sind.

Eine weitere Besonderheit der Zahlentheorie der Zahlentheorie, welche sich sehr positiv auf den natürlichen Lernprozess auswirkt, ist die Tatsache, daß man Sätze aufgrund von Beispielen oft sehr leicht "sehen" kann, obwohl der eigentliche Beweis nicht selten schwierig ist. Ein berühmtes Beispiel dafür ist der Primzahlsatz, der bereits von Gauß als Fünfzehnjähriger vermutet wurde, jedoch erst mehr als hundert Jahre später bewiesen werden konnte. Mit Hilfe eines Computers und unter geschickter Anleitung seines Lehrers, kann heute jeder begabte Schüler in der Zahlentheorie ähnliche "Entdeckungen" machen.

Auf der anderen Seite muß man natürlich auch sehen, daß versucht wurde den Mathematiklehrplan unserer Schulen nach praktischen Erfordernissen auszurichten, was (insbesondere nach der letzten Revision 1989) zur Folge hatte, daß darin Zahlentheorie ähnlich wie abstrakte Algebra so gut wie nicht mehr vorkommt. (Dies ist umso bedauerlicher, als gerade in den letzten Jahren einige besonders schöne Anwendungen der Zahlentheorie wie z.B. auf dem Gebiet der Kryptographie gefunden werden konnten, die zeigen, daß Zahlen-

theorie weit mehr ist als eine vielleicht interessante aber im Grunde nutzlose Spielerei mit Zahlen.) Trotzdem gibt es für den engagierten Lehrer genug Möglichkeiten Zahlentheorie in kleinen appetitanregenden Happen im gängigen Mathematik- bzw. EDV-Unterricht unterzubringen. Im folgenden sollen dafür einige Anregungen gegeben werden, wobei mit die mit Pfeil → versehenen Schlagworte sich auf den Basislehrstoff beziehen. Soweit in Beispielen DERIVE Verwendung findet, ist damit immer die derzeit aktuelle Version 2.10 gemeint. (Eventuelle Rechenzeitangaben beziehen sich dabei auf einen 386/387 PC mit 20 MHz.)

2. Zahlentheorie für das "Guiness Buch der Rekorde"

Im Frühjahr 1992 ging die Meldung eines neuen Primzahlrekords durch die Weltpresse. So konnte man z.B. in einer österreichischen Tageszeitung unter dem Titel "Bisher größte Primzahl entdeckt" folgende Meldung lesen:

> "Mit Hilfe eines Computers hat US-Mathematiker David Slowinski vom Forschungszentrum Chippewa Falls die bisher größte Primzahl ermittelt. Die gigantische, nur durch eins und sich selbst teilbare Zahl besteht aus 227.832 Stellen und füllt 32 Seiten Endlospapier. Slowinski bewertet seine Entdeckung als sensationell, räumt aber ein, daß sie von geringem praktischen Interesse sei."

Von "geringem praktischen Interesse" schienen auch dem Redakteur dieser Meldung Angaben über die Bauart des neuen Rekordhalters unter den bekannten Primzahlen zu sein, obwohl für Mathematiker gerade dies die interessanteste Information darstellt. Tatsächlich kann man in seriöseren Quellen wie z.B. [1] nachlesen, daß es sich dabei um eine Mersennesche Primzahl, also um eine Zahl der Bauart $2^n - 1$ ($n \in \mathbb{N}$), handelt. Wenn hier jemand meint, dies sei selbstverständlich, so ist ihm entgegenzuhalten, daß gerade der letzte Rekordhalter aus dem Jahre 1989, nämlich $391581 \cdot 2^{216\,193} - 1$ (siehe [2]) nicht vom "Mersenneschen Typ" war, wenngleich dies eine seltene Ausnahme darstellt.

Wie groß ist nun Wert des Exponenten n in obiger Darstellung der neuen Rekordprimzahl? Es ist eine interessante Frage, die man der Klasse etwa im Rahmen einer DERIVE-Übungsstunde stellen könnte, ob die in dem Zeitungsausschnitt enthaltenen Angaben über die Stellenanzahl bereits ausreichen, um n zu berechnen. Zunächst ist klar, daß n selbst eine

Primzahl sein muß, da jeder nichttriviale positive Teiler k von n sofort den nichttrivialen Teiler $2^k - 1$ von $2^n - 1$ induziert (→ Hornersche Formeln). Trotzdem muß die gestellte Aufgabe nicht eindeutig lösbar sein. Man rechnet z.B. mit Hilfe des Factor-Befehls von DERIVE leicht nach, daß $2^{17} - 1 = 131071$ und $2^{19} - 1 = 524287$ beide Mersennesche Primzahlen mit gleicher Stellenanzahl sind. Andererseits sieht man leicht ein, daß im Falle einer Mehrdeutigkeit mit n auch genau eine der Zahlen n - 2 oder n +2 ebenfalls Primzahl sein muß, d.h. n gehört dann notwendigerweise einem Paar von Primzahlzwillingen an.

Wie liegen die Dinge in unserem Beispiel? Obige Angaben führen nacheinander auf die Ungleichungen (→ logarithmisches Rechnen)

$$10^{227831} \leq 2^n - 1 < 10^{227832}$$
$$10^{227831} < 2^n \leq 10^{227832}$$
$$227831/_{10}\log 2 < n \leq 227832/_{10}\log 2$$
$$756838{,}2 < n < 756841{,}5$$

Nach Überprüfung der ungeraden Zahlen im angegebenen Bereich auf Primzahleigenschaft ergibt sich wegen $756841 = 47 \cdot 16103$ schließlich für n die eindeutige Lösung 756839 in Übereinstimmung mit [1].

Wir wollen nun noch die vielleicht nicht ganz so triviale Frage beantworten, wie groß eigentlich die Wahrscheinlichkeit a priori dafür war, daß n nicht einem Paar von Primzahlzwillingen angehört. Man geht dazu aus von der empirischen Tatsache, daß die "Primzahldichte" in der Nähe einer großen Zahl $x \in \mathbb{R}^+$ ungefähr $1/\ln x$ beträgt (ebendiese Beobachtung hatte den jungen Gauß, wie oben erwähnt, auf den Primzahlsatz geführt.) Die Wahrscheinlichkeit für zwei beliebig herausgegriffene natürliche Zahlen r und s, die "nicht zu weit von x entfernt liegen", beide prim zu sein, sollte daher ungefähr $1/(\ln x)^2$ betragen (→ Unabhängigkeit von Ereignissen). Etwas anders liegen die Dinge, wenn wir zusätzlich voraussetzen, daß $s = r+2$. In diesem Fall wird nämich die Wahrscheinlichkeit für r und s beide nicht durch eine vorgegebene Primzahl p teilbar zu sein, für $p = 2$ von 1/4 auf 1/2 erhöht (mit r ist auch s ungerade!), für $p \neq 2$ jedoch von vorher $(1-1/p)^2$ auf nunmehr $1-2/p$ erniedrigt (das betrachtete Ereignis tritt genau dann ein, wenn r bei Division durch p nicht den Rest 0 oder p-2 liefert!). Die ursprüngliche Formel $1/(\ln x)^2$ muß daher mit dem Korrekturfaktor

$$C = 2 \prod_{p>2} \frac{1 - 2/p}{(1 - 1/p)^2} = 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right)$$

versehen werden (die Produktbildung hat dabei über alle ungeraden Primzahlen p zu erfolgen).

Die näherungsweise Berechnung von C ist dabei dabei eine hübsche Übungsaufgabe für DERIVE-Adepten. Ein erster naheliegender Gedanke ist es wohl, dazu eine Funktion

prime(x):= if (next_prime(x-1) = x, 1, 0)

einzuführen, welche genau für Primzahlen den Wert 1 und sonst den Wert 0 zurückliefert. Mit eingestellter 15-stelliger Genauigkeit erhält man nach Eingabe von

2 product(1 - prime(i)/(i-1)^2,i,3,10000)

und Auswertung mit "Approximate" nach etwa 265 Sekunden für C den Wert 1,32033659... (der genaue Wert beträgt 1,3203236316...). Obige Formel enthält allerdings viel "Leerlauf", der sich unter Verwendung der Next_prime und Iterate Funktionen von DERIVE (letzere in Verbindung mit zweielementigen Listen) vermeiden läßt (Übungsaufgabe!).

Wieder auf unser oben gestelltes Problem zurückkommend, sollte daher die Wahrscheinlichkeit, daß sich "in der Nähe" von 756 839 ein Primzahlzwilling befindet ungefähr 1.32/ln(756 839)^2 ≈ 0.0072, also weniger als 1% betragen. Aber auch wenn n einem Paar (r,s) von Primzahlzwillingen angehört, so haben 2^r-1 und 2^s-1 nur in etwa einem Viertel aller Fälle die gleiche Stellenanzahl, sodaß sich die Wahrscheinlichkeit einer Mehrdeutigkeit unserer gestellten Aufgabe noch um diesen Faktor vermindert und damit nur etwa 0,18% beträgt.

Eine Bemerkung noch zu unserer Formel $1{,}32.../(\ln x)^2$ für die Dichte von Primzahlzwillingen in der Nähe einer großen Zahl $x \in \mathbb{R}^+$: Obwohl ihre Herleitung nur auf heuristischen Überlegungen beruht, also von einem strengen Beweis weit entfernt ist, bewährt sie sich in der Praxis bei den bisher überprüften Zahlenbereichen außerordentlich gut. Beispielsweise liegen nach [3] im Intervall $[10^9, 10^9 + 150\,000]$ genau 466 Primzahlzwillinge, während der entsprechende Erwartungswert gemäß obiger Formel ungefähr $150\,000 \cdot 1{,}32/\ln(10^9)^2 \approx 461$ beträgt. Wiederum ist es sehr reizvoll DERIVE zum Auszählen von Primzahlzwillingen in gewissen vorgegebenen Intervallen einzusetzen. Begabten Schülern sollte es nicht schwerfallen mit den gleichen Ingredienzien, wie sie oben für die modifizierte Berechnung von C vorgeschlagen wurden, diesen Vorgang vollautomatisch ablaufen zu lassen. Falls die Zahlen und die Intervallängen groß genug gewählt wurden, wird der Vergleich mit den entsprechenden Erwartungs-

werten mit Sicherheit für Staunen sorgen wegen ihrer großen Übereinstimmung. Diese ist umso erstaunlicher, als man nach strengen mathematischen Kriterien bisher nicht einmal zeigen konnte, daß es unendlich viele Primzahlzwillinge gibt, obwohl (nach den im Alltag geltenden Kriterien) alles dafür spricht. (Übrigens hat vor Jahren eine amerikanische Computerfirma sagar einen Preis von 25 000 $ für einen exakten Beweis geboten - also weit mehr, als man etwa mit einem Beweis des "Großen Fermat" verdienen kann. Leider ist die Einsendefrist inzwischen ergebnislos abgelaufen.)

3. Fraktale auch in der Zahlentheorie ?

Wir wollen nun der naheliegenden Frage nachgehen, warum die derzeitige Rekordprimzahl (und mit ihr fast alle ehemaligen Rekordinhaber) gerade die Form $2^n - 1$ hat. Zahlen dieser Bauart werden allgemein "Mersennesche Zahlen" genannt, i.Z. M_n, nach dem Franziskaner Mönch M. Mersenne, der im Jahre 1644 die tollkühne Behauptung aufgestellt hat, daß M_n für $n \leq 257$ genau für die Werte 2,3,5,7,13,17,19,31,67,127,257 von n eine Primzahl ist. (Man beachte, daß z.B. M_{257} immerhin schon 78 Stellen hat!)

Wie oben schon erwähnt wurde, können höchstens die Zahlen $2^p - 1$, wo p selbst Primzahl ist, prim sein. Für diese aber gibt es - und das ist zugleich die Antwort auf obige Frage - ein überaus einfaches Primalitäts-kriterium, welches 1878 von E.Lucas in einem Spezialfall gefunden und 1930 von D.E.Lehmer auf die heutige Form gebracht wurde, wehalb es auch Lucas–Lehmer Test genannt wird. Man definiert dazu die Folge $s_1, s_2, s_3, \ldots$ rekursiv durch

$$s_1 = 4, \quad s_{i+1} = s_i^2 - 2 \quad (i \in \mathbb{N}).$$

Die zu testende Mersennesche Zahl M_p (p ungerade Primzahl) ist nun genau dann prim, wenn s_{p-1} durch M_p teilbar ist.

Man sieht zunächst sofort, daß die Anzahl $p - 2$ der nötigen Rekursions-schritte nur linear mit der Stellenanzahl von M_p wächst, was bestmöglich ist. Zwar verdoppelt sich etwa die Stellenzahl der s_i bei jedem Schritt, doch nach Erreichen von M_p in s_i enthaltene Vielfache von M_p einfach weggelassen werden (d.h. man rechnet mod M_p), da sie die Frage der Teilbarkeit von s_{p-1} durch M_p nicht beeinflussen. Die Folgenglieder haben daher mit wenig Ausnahmen etwa die Größenordnung von M_p. Nimmt man nun an, daß der Aufwand für das Quadrieren einer Zahl dieser Größe etwa quadratisch mit p wächst (tatsächlich gibt es sogar bessere Methoden, wovon noch die Rede

sein wird), so wächst der Gesamtrechenaufwand nicht stärker als ein Polynom 3. Grades in p, d.h. es handelt sich um einen Polynomialzeit-algorithmus.

Wie einfach der Lucas–Lehmer Test wirklich ist, zeigt auch seine Implementation in DERIVE:

```
lltest(p):= if(iterate(mod(s^2-2,2^p-1),s,4,p-2)=0, [p], [])
```

lltest(p) ergibt die Liste [p], falls M_p prim ist, und sonst die leere Liste, wobei für p natürlich nur ungerade Primzahlen eingegeben werden dürfen. Setzt man zur Abkürzung

```
e1(v):= element(v,1)
e2(v):= element(v,2)
```

so liefert die nachfolgende Funktion (kein Zeilenumbruch in DERIVE!)

```
melist(n):= e1(iterate([append(e1(x),lltest(e2(x))), next_prime(e2(x))],
                                                x, [[2],3], n-1))
```

die Liste der ersten n Primzahlen p (in natürlicher Reihnefolge), für welche M_p prim ist.

Überprüft man etwa mit melist(55) die oben von Mersenne angegebene Liste (257 ist die 55. Primzahl in der natürlichen Reihenfolge!), so erhält man die Liste

```
[2,3,5,7,13,17,19,31,61,89,107,127]
```

nach 92,5 Sekunden als Wert zurück. Mersenne hatte also M_{67} und M_{257} fälschlich als Primzahlen angesehen und dafür M_{61},M_{89} und M_{107} "vergessen".

Obige Liste ist auch deshalb nicht uninteressant, welche sie genau die Exponenten von Mersenne Primzahlen enthält, welche noch im "Vorcomputer-zeitalter" gefunden wurden. Erst nach einer "Pause" von fast 4 Jahrzehnten konnte obige Liste fortgesetzt werden. R.M.Robinson fand im Jahre 1952 mit Hilfe der legendären SWAC gleich 5 neue Mersenne Primzahlen, nämlich für p = 521,607,1279,2203,2281, ein "Rekord", der eben jetzt durch D.Slowinski "eingestellt", aber noch nicht überboten wurde. Über die aufgewendete Rechenzeit zum Testen dieser Exponenten (bei ihm mit n bezeichnet) schreibt er in [4] folgendes: "The estimated running time for the program was $0{,}25n^3 + 125n^2$ microseconds, and the actual time was in fair agreement with this. Thus, roughly speaking, the testing time was a minute for the first and an hour for the last of the five new primes. Each minute of machine time is equivalent to more than a year's work for a person using a desk calculator."

Im Vergleich dazu benötigt DERIVE 16 Sekunden Testzeit für den Exponenten 521 und 561,3 Sekunden für den Exponenten 2281. Mit den nächsten drei Exponenten von Mersenne Primzahlen, nämlich 3217 (gefunden 1957 von H.Riesel), 4253 und 4423 (beide gefunden 1961 von A.Hurwitz) wird immerhin schon der Bereich der mehr als 1000-stelligen Primzahlen betreten. Die entprechenden Testzeiten mit DERIVE sind 1475, 3294 bzw. 3679 Sekunden. Wahrscheinlichlich ließen sich auch von den weiteren derzeit bekannten Exponenten von Mersenne Primzahlen, nämlich p = 9689,9941,11213,19937, 21701,23209,44497,86243,110503,132049,216091,756839 (insgesamt sind es also zur Zeit 32) noch einige weitere testen, doch stoßen wir mit DERIVE doch schön langsam an die Grenzen seiner Möglichkeiten (für den Wert 9689 rechnet es z.B. schon 36842 Sekunden, also mehr als 10 Stunden, und irgendwann werden auch Probleme mit der Speicherkapazität auftreten).

Um also ernsthaft weiterzumachen, müßte man erstens auf einen Großcomputer umsteigen und sich zweitens maßgeschneiderter Programme in einer maschinennahen Sprache (am besten natürlich in der jeweiligen Assemblersprache) bedienen. Aber auch dann noch muß man eine ganze Menge von "Tricks" anwenden, um in allerhöchste Regionen vorzustoßen. Z.B. erweist sich die Reduktion der Folgenglieder mod M_p im Lucas-Lehmer Test, wenn man richtig vorgeht, als überraschend harmlos. Aufgrund der Beziehung

$$A \cdot 2^p + B = A(2^p - 1) + (A + B) \equiv A + B \bmod M_p$$

wird eine in Binärdarstellung vorliegende Zahl $(z_n \ldots z_p z_{p-1} \ldots z_0)$ mit $n \geq p$ in einfachster Weise mod M_p reduziert, indem man die beiden Binärzahlen $(z_n \ldots z_p)$ und $(z_{p-1} \ldots z_0)$, welche aus ihr durch ganz elementare computerinterne Operationen hervorgehen, addiert, d.h.

$$(z_n \ldots z_p z_{p-1} \ldots z_0) \equiv (z_n \ldots z_p) + (z_{p-1} \ldots z_p) \bmod M_p.$$

Für p = 7 z.B. rechnet der Computer so (um dieses Beispiel mit DERIVE nachzuvollziehen, muß vorübergehend mit "Options Radix" die Zahlenbasis für Input und Output auf 2 gestellt werden!):

$s_1 = 100,$

$s_2 = 100^{10} - 10 = 1110,$

$s_3 = 1110^{10} - 10 = 11000010 \equiv 1 + 1000010 = 1000011 \bmod M_7$

$s_4 \equiv 1000011^{10} - 10 = 1000110000111 \equiv 100011 + 111 = 101010 \bmod M_7,$

$s_5 \equiv 101010^{10} - 10 = 11011100010 \equiv 1101 + 1100010 = 1101111 \bmod M_7,$

$s_6 \equiv 1101111^{10} - 10 = 1100000\,0011111 \equiv 1100000 + 11111 = 1111111 \equiv 0 \bmod M_7.$

$M_7 = 127$ ist daher prim.

Nachdem sich also die Reduktion mod M_p der Folgenglieder s_i als vollkommen harmlos herausgestellt hat (weshalb wir sie übrigens in unserer Bilanz für den Rechenaufwand auch nicht eigens erwähnt haben), verbleibt als einziger "harter Brocken" das Quadrieren der s_i. Immerhin müssen etwa für den Exponenten $p = 756\,839$ i. allg. Zahlen mit mehr als 220 000 Stellen quadriert werden. In [1] heißt es dazu: "Slowinski and Gage used an algorithm of Schonhage and Strassen that employs the Fast Fourier Transform (in a clever implementation by Dennis Kuba, also of Cray Research). Checking the $M_{756\,839}$ for primality the first time still required many hours of computer time; rechecking it on a machine with 16 processors required 20 minutes." Selbst wenn der Zeitaufwand von 20 Minuten unter Verwendung eines CRAY-2 Supercomputers noch erträglich aussieht, darf man nicht vergessen, daß vorher i.allg. viele andere Kandidaten erfolglos getestet werden . Daß es in diesem Fall nur 85 waren, veranlaßte Slowinski nach [1] zu dem vielsagenden Kommentar "We were incredibly lucky".

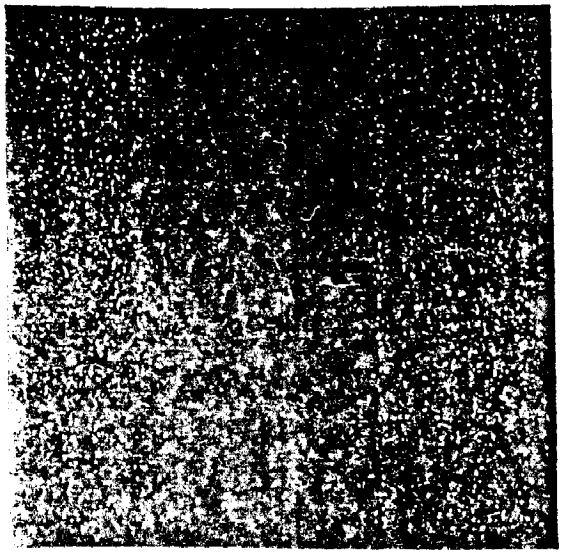
Wir wollen nun nicht auf die technischen Details einer FFT (Fast Fourier Transform) eingehen, sondern hier eine Methode besprechen, die nach [5] von Slowinski im Fall der Mersenne Primzahl $M_{86\,243}$ (gefunden 1982) mit Erfolg angewendet wurde. Um sie zu erklären, gehen wir in einem Gedankenexperiment von einer Rechenmaschine aus, mit der man nur zweistellige Zahlen quadrieren sowie (unbeschränkt) addieren und subtrahieren kann.. Man sieht dann sofort, daß man mit Hilfe der Formel

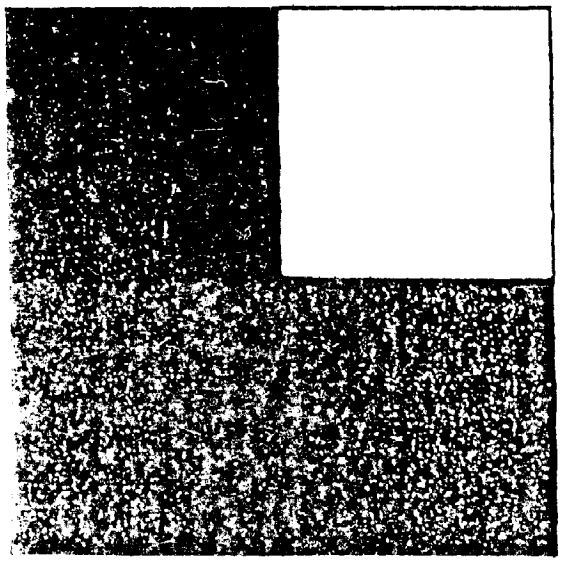
$$(uB+v)^2 = u^2B^2 + (u^2 - (u-v)^2 + v^2)B + v^2,$$

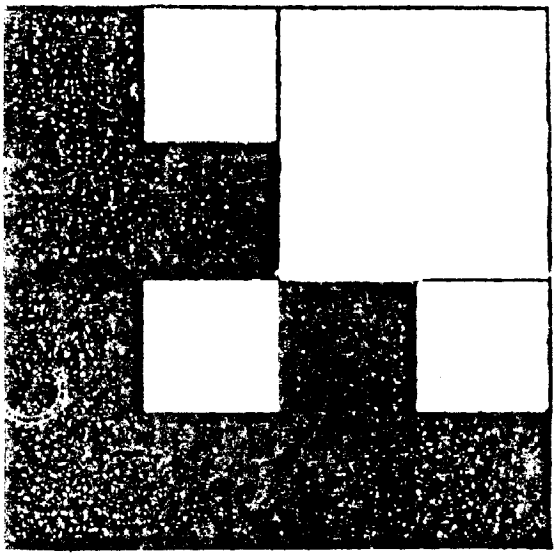
wobei B eine geeignete Potenz von 10 ist, die i.allg. so gewählt wird, daß u und v die gleiche Größenordnung haben, sofort auch bis zu vierstellige Zahlen quadrieren kann, z.B.

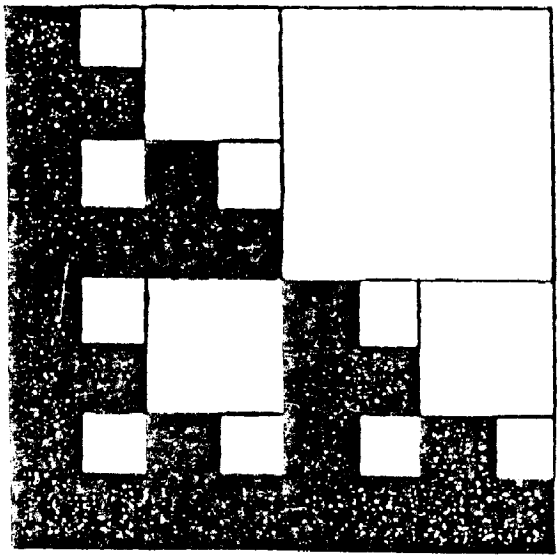
$$\begin{aligned} 4763^2 &= 47^2 \cdot 100^2 + (47^2 - 16^2 + 63^2) \cdot 100 + 63^2 = \\ &= 2209 \cdot 10000 + (2209 - 256 + 3969) \cdot 100 + 3969 = \\ &= 22090000 + 592200 + 3969 = 22686169. \end{aligned}$$

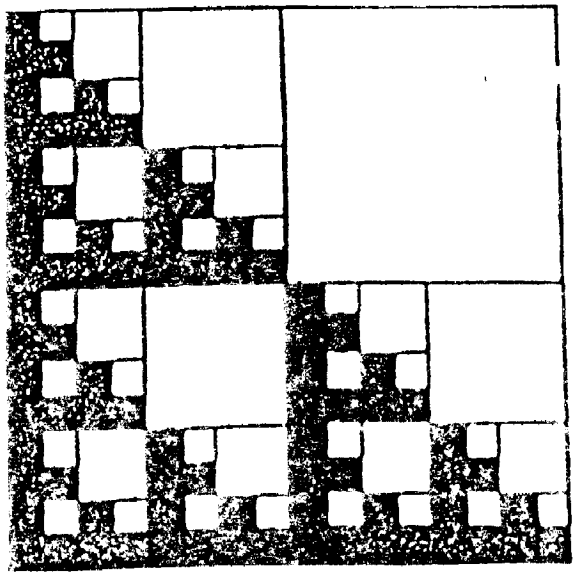
Genausogut kann man damit aber auch z.B. eine 128-stellige quadrieren, indem man die Reduktion gemäß obiger Formel auch auf die kleineren Quadrate (insgesamt also sechsmal) anwendet. Symbolisiert man den Rechenaufwand für das Quadrieren einer n-stelligen Zahl mit einem ausgefüllten Quadrat der Seitenlänge n (in geeignet gewählten Einheiten) und vernachläßigt den Aufwand für die anfallenden Additionen und Subtraktionen, so kann man diese sechs Reduktionen bildlich so darstellen (siehe dazu [6]):

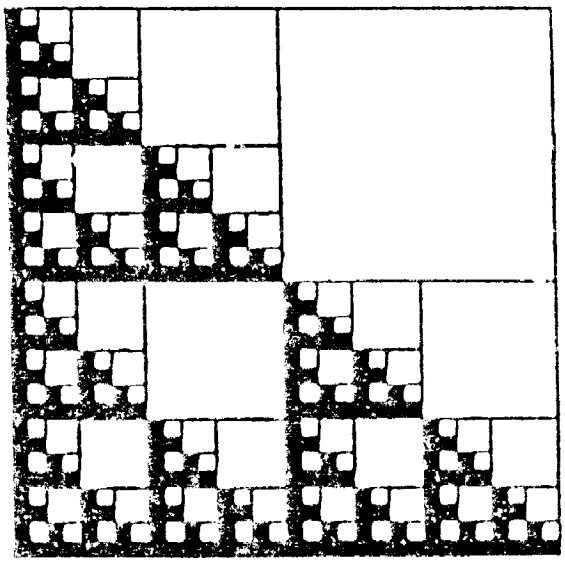












Zumindestens geometrisch können wir die "Ausdünnung" unbegrenzt weit treiben, sodaß wir schließlich im Grenzgebilde ein Fraktal, d.h. eine selbstähnliche Figur vor uns haben (siehe dazu [7]). In unserem Beispiel ist natürlich dann Schluß, wenn wir bei zweiziffrigen Zahlen oder allgemeiner bei Zahlen einer Länge angelangt sind, welche unser Computer mit der eingebauten Arithmetik fehlerfrei quadrieren kann. Setzt man z.B. einen Computer voraus, für den diese binäre Wortlänge 32 beträgt, so rechnet man leicht nach, daß auch zum Testen des Exponenten p = 756 839 höchstens 15 Reduktionen, wie oben beschrieben, notwendig sind.

Wir hatten schon früher angegen, daß der Aufwand zum Quadrieren einer Zahl N, wenn die ganz normale Multiplikation anwendet, quadratisch mit der Stellenanzahl von N wächst, also, wie man kurz sagt, ein $O((\ln N)^2)$ ist. Man kann nun zeigen, daß ein Quadrieren auf die oben angegebene Art eine Verringerung des Rechenaufwands (gemessen z.B. an der Anzahl der Elementaroperationen) auf ein $O((\ln N)^{2^{\log 3}})$ mit sich bringt. ${}_2\log 3 \approx 1.585$ ist dabei aber nichts anderes als die sog. fraktale Dimension (siehe [7] oder auch [8]) unseres oben betrachteten Fraktals! Wir haben hier somit ein weiteres eindrucksvolles Beispiel für das wundervolle Wechselspiel zwischen der Zahlentheorie und anderen mathematischen Teilgebieten vor uns.

4. Das Geburtstagsparadoxon und seine Anwendung in der Zahlentheorie

Gewissermassen ein "Pflichtbeispiel" wegen seines hohen Unterhaltungswerts ist die folgende Aufgabe aus der Wahrscheinlichkeitsrechnung: Wie viele Personen müssen mindestens in einem Raum anwesend sein, damit die Wahrscheinlichkeit, daß zwei darunter sind, welche am gleichen Tag des Jahres Geburtstag haben (Schaltjahre bleiben dabei unberücksichtigt) mehr als 50% beträgt? Das Reizvolle an der Aufgabe ist einerseits die für die meisten überraschende Lösung, zum anderen die Möglichkeit mit den Schülern der Klasse eine Probe aufs Exempel zu machen.

Natürlich wird man unter Zuhilfenahme von DERIVE das Beispiel so zu lösen versuchen, indem man eine Funktion

```
p(m):= product(1-i/365,i,m-1)
```

einführt, welche die Wahrscheinlichkeit angibt, daß von m anwesenden Personen keine zwei am gleichen Tag des Jahres Geburtstag haben. Wir müssen dann nur noch den kleinsten Wert für m bestimmen , sodaß $p(m) < 0.5$ ist. Mit etwas Probieren (oder etwas origineller: graphisch) findet

man für das gesuchte m den erstaunlich kleinen Wert 23 (siehe dazu auch [9]).

Auf diesen Wert hätte man aber auch durch Rechnung kommen können. Um dies zu sehen, wollen wir allgemeiner die Ungleichung

$$\prod_{i=1}^{m-1} (1 - i/n) < 0.5$$

zu lösen versuchen. Ist m klein im Verhältnis zu n, so kann man unter Benutzung von

$$e^{-i/n} = \sum_{k=0}^{\infty} \frac{(-i/n)^k}{k!} \approx 1 - i/n$$

dafür näherungsweise auch schreiben

$$\prod_{i=1}^{m-1} e^{-i/n} = e^{-m(m-1)/(2n)} < 0.5.$$

oder

$$m(m-1)/(2n) < \ln 2.$$

Indem man hierin m(m-1) näherungsweise durch $(m - 1/2)^2$ ersetzt, sieht man, daß für die kleinste Lösung m obiger Ungleichung gilt

$$m \approx 1/2 + \sqrt{2n \ln 2} \approx 1.2 \sqrt{n}.$$

Tatsächlich ist $1.2 \sqrt{365} = 22.9... \approx 23$.

Obige Ausführungen bilden die die Einleitung zu einer der möglichen Antworten auf eine Frage, die wir zum Abschluß wegen ihrer Wichtigkeit noch kurz anreißen wollen, nämlich: Wie kann von einer Zahl, von der man weiß, daß sie zusammengesetzt ist, (möglichst alle) nichttriviale Teiler bestimmen. Diese Problemstellung ist z.B. in Hinblick auf gewisse kryptographische Verfahren von großer Bedeutung und liegt insbesondere dann vor, wenn der Lucas-Lehmer Test eine Mersennesche Zahl als zusammengesetzt ausweist.

Ganz allgemein ist zu sagen, daß Faktorisierungsprobleme weit schwieriger sind, als bloße Untersuchungen auf Primzahleigenschaft. Dies sieht man etwa am Beispiel der zusammengesetzten Zahl M_{67}, für die der Luicas-Lehmer Test nur 0.7 Sekunden benötigt, während man auf die Faktorisierung

$$2^{67} - 1 = 193\,707\,721 \cdot 761\,838\,257\,287$$

mittels des Factor-Befehls bereits 26.5 Sekunden warten muß. Dies ist andererseits erstaunlich schnell, wenn man weiß, daß etwa F.N.Cole nach [10] "die Sonntage von 3 Jahren" für ebendiese Zerlegung aufgewendet hat (siehe dazu auch [11]).

Intern verwendet DERIVE zum Faktorisieren von ganzen Zahlen die

sog. Pollardsche ρ-Methode, welche wir nun kurz skizzieren wollen. Ist dazu N die zu faktorisierende Zahl und p ein (noch unbekannter) Primfaktor von N, so verwendet man eine rekursiv definierte und mod N reduzierte Folge ganzer Zahlen $x_1, x_2, x_3, \ldots$, welche gute Zufallseigenschaften aufweist. Z.B. könnte diese so definiert sein:

$$x_1 = 3,\ x_{i+1} \equiv x_i^2 + 1 \bmod N.$$

Nun weiß man aber, daß diese Folge mod p betrachtet jedenfalls spätestens nach p, i. allg. aber schon nach $C\sqrt{p}$ Schritten (siehe unsere obigen Ausführungen zum Geburtstagsproblem!) periodisch werden muß, nämlich ab der ersten Wiederkehr eines schon dagewesenen Wertes für x_i. Gilt nun $x_{j+l} \equiv x_j \bmod p$ für $j \geq j_0$ (d.h. l ist die Periodenlänge und j_0 bestimmt die Länge der Vorperiode), so gilt für jedes $i = kl \geq j_0$, daß $x_{2i} \equiv x_i \bmod p$. Da also dann p Teiler von $x_{2i} - x_i$ sein muß, muß p auch Teiler von $ggT(x_{2i}-x_i, N)$ sein und im Fall $ggT(x_{2i}-x_i, N) \neq N$ hat man damit einen nichttrivialen Teiler von N gefunden, der entweder p ist, oder p zumindestens als Teiler enthält, was dann auch schon einen Fortschritt darstellt.

Eine Implementierung in DERIVE (die allerdings in Hinblick auf die eingebaute factor-Funktion nur von theoretischen Interesse ist) könnte z.B. so aussehen:

```
e1(v):= element(v,1)
e2(v):= element(v,2)
f(x,n):= mod(x^2+1,n)
g(x,n):= f(f(x,n),n)
h(v,n):= [f(e1(v),n), g(e2(v),n)]
d(v,n):= gcd(f(e1(v),n)-g(e2(v),n),n)
rho(n):= e2(iterate( if(e2(w)=1, [h(e1(w),n), d(e1(w),n)], w) , w, [[3,3],1]))
```

So liefert z.B. rho($2^{53} - 1$) nach 14.2 Sekunden den Primfaktor 6361 von $2^{53} - 1$. Die eingebaute factor-Funktion hätte dafür allerdings nur 1.9 Sekunden benötigt. Ändert man aber z.B. die Definition von f auf

```
f(x,n):=mod(x^53-1,n)
```

so sinkt die Rechenzeit auf 8 Sekunden, also fast die Hälfte, obwohl dieses neue f im Vergleich zum alten viel komplizierter ist. Der Grund dafür ist, daß aufgrund von Sätzen der Zahlentheorie alle Primteiler von $2^p - 1$ die Form $2kp + 1$ mit $k \in \mathbb{N}$ haben müssen. Genau die Teiler dieser Gestalt werden aber durch unser neues f generiert. Überdies ist auch noch bekannt, daß jeder Primteiler von $2^p - 1$ von der Form $8r \pm 1$ sein muß, z.B. ist $6361 = 2 \cdot 53 \cdot 60 + 1 =$

= 8•795 + 1. Trotzdem empfielt es sich i.allg. nicht, die Primteiler von zusammengesetzten Mersenneschen Zahlen durch eine direkte Teilersuche finden zu wollen.

Doch sollte dies alles der Schüler selbst durch "Herumexperimentieren" am Computer herausfinden. "Learning by doing" ist die Devise. Viel zu wenig wird dem Schüler im herkömmlichen Mathematikunterricht Gelegenheit geboten, selbst mathematische Sachverhalte zu "entdecken", obwohl gerade dies zu den bewährtesten Mittel der allgemeinen Motivationssteigerung zählt. Es war meine Absicht zu zeigen, wie sehr sich gerade die Zahlentheorie für solche "Entdeckungsreisen" in der Mathematik anbietet.

Literatur

[1] "The Latest Mersenne Prime", Am. Math. Monthly 99(1992), 960.

[2] Schönwald H.H., "Anfang und Ende der größten z.Zt. bekannten Primzahl", MNU 43/4(1990), 207-208.

[3] Jones,M.F., M.Lal and W.J. Blundon, "Statistics on certain large primes", Math. Comp. 21(1967), 103-107.

[4] Robinson R.M., "Mersenne and Fermat Numbers", Proc.Amer.Math.Soc. 5(1954), 842-846.

[5] Ewing J., "$2^{86243} - 1$ is Prime", The Mathematical Intelligencer 5(1983),60.

[6] Riesel H., "Prime numbers and computer methods for factorization", Birkhäuser Verlag, Boston-Basel-Stuttgart, 1985.

[7] Mandelbrot B.B., "Die fraktale Geometrie der Natur", Birkhäuser Verlag, Basel, 1987.

[8] Reichel H.C., "Fraktale Dimension - über das Titelbild des neuen 5.Klasse-Buches Reichel-Müller-Laub et al.", ÖMG Didaktik Reihe 18 (1990), 124-142.

[9] Stormer W., "Computereinsatz in Stochastikunterricht", ÖMG Didaktik Reihe 19(1991), 189-214.

[10] Bell E.T., "Mathematics Queen and Servant of Science", Tempus Books, 1987.

[11] Wiesenbauer J., "Was sind und was sollen große Primzahlen", ÖMG-Didaktikreihe 14(1986), 212-225.