KAP 1.1
VOLLKOMMENE ZAHLEN UND MERSENNE-ZAHLEN

Auf einem Sonderstempel der US-Post im Staat Illinois aus dem Jahre 1968 ist die bemerkenswerte Meldung zu lesen: 2^{11213}-1 is prim!

Warum hält die amerikanische Post wohl diese Meldung für so wichtig, dass man ihr einen Sonderstempel widmet? Wir werden uns im Folgenden genauer mit Zahlen der Form 2^n-1 beschäftigen.

Wie wir beim Beweis von 1.8f gesehen haben, ist eine Zahl z immer schon dann vollkommen, wenn sie von der Form $z=2^{n-1}(2^n-1)$ ist, wobei der zweite Faktor 2^n-1 prim sein muß. (Also schon wieder diese Zahlen der Form 2^n-1!)

Überprüfen wir das zunächst einmal an einigen kleinen Beispielen:

n	**2^n-1**	**prim**	**z**	**vollkommen**
2	3	ja	6	ja
3	7	ja	28	ja
4	15	nein	120	nein
5	31	ja	496	ja
6	63	nein	2016	nein
7	127	ja	8128	ja
8	255	nein	32640	nein
9	511	nein	130816	nein
10	1023	nein	523776	nein
11	2047	nein	2096128	nein

AUFGABE 1.38 Bestätige die Angaben über die Vollkommenheit der Zahlen. Setze dann die Tabelle bis n=20 fort. (Benutze eventuell ein Programm zu Primfaktorzerlegung.)

Welche Regelmäßigkeit steckt in dieser Tabelle? Da die Zahlen der Form 2^n-1 auch an anderer Stelle eine Rolle spielen, wollen wir uns erst mal diesen zuwenden.

DEFINITION $M_n:=2^n-1$ heißt n-te **Mersenne-Zahl**.
(nach dem französischen Jesuitenpater Marin Mersenne (1588-1648), der die Bedeutung dieser Zahlen als Erster erkannt hat und etliche (auch falsche) Behauptungen über sie aufgestellt hat)

Manche dieser M_n sind prim, andere wiederum nicht. Wie kann man schnell erkennen, für welchen Index n M_n prim ist? Die ersten Beispiele lassen vermuten, daß M_n prim ist, wenn nur n prim ist. Spätestens ab n=11 widerlegt sich diese Behauptung von selbst. Allerdings gilt der

SATZ 1 Ist M_n prim, so ist auch n prim.

Beweis: Wir zeigen die Kontraposition: n nicht prim $\Rightarrow$ M_n nicht prim
Ist nämlich $n=k\cdot l$ $(k,l>1)$, so folgt $M_n=2^{k\cdot l}-1=(2^k)^l-(1^k)^l=(2^k-1)\cdot$Rest nach (F1)

Damit haben wir gleichzeitig ein zweites Ergebnis: M_k teilt $M_{k\cdot l}$ oder in anderen Worten: Jede zweite Mersenne-Zahl ist durch $3=M_2$ teilbar, jede dritte durch $7=M_3$, jede fünfte durch $31=M_5$ usw. Das macht das Faktorisieren von Mersenne-Zahlen wesentlich einfacher: will man z.B. $M_{30}=2^{30}-1=1.073.741.823$ faktorisieren, so weiß man wegen $2\mid 30$ und $3\mid 30$ und $5\mid 30$, daß M_{30} mindestens durch 3, 7 und 31 teilbar ist; tatsächlich gilt: $M_{30}=3^2\cdot 7\cdot 11\cdot 31\cdot 151\cdot 331$.

AUFGABE 1.39 a) Zerlege M_{20}, M_{21} und M_{28} in Primfaktoren.
b) Schreibe ein Programm, daß die Primfaktorzerlegungen aller Mersenne-Zahlen bis n=30 ausgibt.

AUFGABE 1.40 Untersuche die Zahlen $m_n:=2^n+1$ für $n\leq 30$ mit einem geeigneten Programm auf Zerlegbarkeit. Was fällt auf?

AUFGABE 1.41 Beweise: (1) n ungerade $\Rightarrow 3\mid m_n$
(2) m_n prim $\Rightarrow n=2^k$, $k\in N$
(3) $M_n=M_k\cdot m_k$ mit $k=n/2$

AUFGABE 1.42 Benutze c), um M_n für n=32, 34, 36, 38 und 40 zu zerlegen.
Wie viele Stellen hat M_{60}? Gib die Primfaktorzerlegung von M_{60} an.

Schaut man sich die Tabelle der Primfaktorzerlegungen der ersten 30 Mersenne-Zahlen an, so drängt sich die Vermutung auf, daß für $p>2$ gilt: $p\mid M_{p-1}$. Diese Vermutung ist richtig, und wir werden sie später beweisen (kleiner Fermatscher Satz).

Damit haben wir die Frage, welche der M_n prim sind, noch nicht befriedigend beantwortet. Wir werden dies auch nicht können, da dies bis heute eine unbeantwortete Frage der Mathematik ist. Man hat bis heute (1994) genau 30 solcher Mersenne-Primzahlen gefunden - die größte davon hat mehr als 65.000 Ziffern (siehe weiter unten). Die Mersenne-Zahlen eignen sich für Untersuchungen über Zusammensetzbarkeit mit Computern besonders gut . Das liegt unter anderem daran, das sie in der Binärdarstellung aus lauter Einsen bestehen. Mersenne selbst hielt sowohl M_{67} als auch M_{127} für prim und konnte wohl in seinen kühnsten Träumen nicht erahnen, daß es jemals möglich sein würden, dies zu überprüfen. Tatsächlich zeigte 1876 Edouard Lucas (ein Name, der uns noch häufiger begegnen wird), daß M_{67} nicht prim ist, ohne allerdings einen der Primfaktoren angeben zu können, was erst 1903 dem Amerikaner Cole gelang, der in einem der merkwürdigsten Vorträge, der je auf einer wissenschaftlichen Tagung gehalten wurde, auf einer Tafelhälfte zunächst $2^{67}-1$ und danach auf der zweiten Tafelhälfte das Produkt von 193.707.721 und 761.838.257.287 berechnete. Die beiden Ergebnisse stimmten überein. Ohne ein weiteres Wort setzte sich Cole unter dem Applaus der Anwesenden. Ergänzend sei erwähnt, daß die beiden Faktoren prim sind.

Ebenfalls 1876 zeigte Lucas, daß M_{127} tatsächlich prim ist. Diese Zahl - ausgeschrieben 170.141.183.460.469.231.731.687.303.715.884.105.727 - hielt bis 1952 den Weltrekord, als mit den damals noch neuen Computern M_{521} (eine Zahl mit 159 Stellen) als prim nachgewiesen wurde. Über die Verfahren, die Lucas und seine Nachfolger benutzten, werden wir in einem späteren Kapitel noch mehr hören.

Hier sei zunächst nur kurz das von Lucas erdachte und benutzte Verfahren vorgestellt:

> Man bilde nach der Rekursionsvorschrift $x_1=4$ und $x_{n+1}=x_n^2-2$ die sogenannte Lucasfolge: 4, 14, 194, 37634..... M_n ist genau dann prim, wenn M_n Teiler von x_{n-1} ist.

z.B.: $M_3=7 \mid 14$ - $M_4=15$ teilt nicht 194 - $M_5=31 \mid 37634$
Der Nachteil des Verfahrens liegt darin, daß die Testzahlen schnell sehr viel größer als die eigentlich zu untersuchenden Mersenne-Zahlen sind. In den folgenden Jahren wurden deshalb sehr viel effizientere Verfahren entwickelt.

Der amerikanische Mathematiker Lehmer veränderte das Verfahren insofern, als er in der Lucasfolge nur noch die Reste der Folgeglieder bezüglich M_n betrachtete. (Lucas-Lehmer-Test). Wir werden in einem späteren Kapitel darauf zurückkommen.

Kommen wir nun zu den vollkommenen Zahlen. Mit den neu gewonnenen Begriffen können wir nun die im Beweis von 1.8f gewonnen Erkenntnisse so formulieren:

SATZ von EUKLID Ist M_n eine Mersenne-Primzahl, so ist $z=2^{n-1}\cdot M_n$ vollkommen.
Beweis:
$$\sigma(z)=\frac{2^{n-1+1}-1}{2-1}\cdot(M_n+1)=\left(2^n-1\right)\cdot 2^n=2\cdot 2^{n-1}\left(2^n-1\right)=2\cdot 2^{n-1}\cdot M_n$$

Die Umkehrung dieses Satzes bewies Euler, allerdings unter der Voraussetzung, dass z gerade ist. Die Frage, ob es auch ungerade vollkommene Zahlen gibt, ist bis heute ungeklärt.

SATZ von EULER Ist z vollkommen und gerade, dann ist $z=2^{n-1}\cdot M_n$ mit M_n prim.

Beweis: Es sei als z vollkommen und gerade. Dann ist $z=2^{n-1}\cdot b$, wobei b ungerade ist. Es sei $\sigma(b)=B$. Da z vollkommen ist, gilt $\sigma(z)=2z$. Also

$$2z=\sigma(z)=\sigma(2^{n-1}\cdot b)=\sigma(2^{n-1})\cdot\sigma(b)=(2^n-1)B$$

$$\Rightarrow b:B=\frac{z}{2^{n-1}}:\frac{2z}{2^n-1}=\frac{z\cdot\left(2^n-1\right)}{2^{n-1}\cdot 2z}=\frac{2^n-1}{2^n} \quad (*)$$

Die rechte Seite des Bruchs ist vollständig gekürzt. Dann muß b Vielfaches von 2^n-1 sein; es sei z.B. $b=c(2^n-1)$; $c\in\mathbb{N}$;

1. Fall $c>1$: Wegen $b=c(2^n-1)$ hat b mindestens die Teiler 1, 2^n-1, c und b. Es gilt also $\sigma(b)=B\geq b+2^n-1+c+1$ und damit:

$$\frac{B}{b}\geq\frac{b+2^n+c}{b}=\frac{c\left(2^n-1\right)+2^n+c}{c\left(2^n-1\right)}=\frac{2^n(c+1)}{c\left(2^n-1\right)}=\frac{2^n}{2^n-1}\frac{c+1}{c}>\frac{2^n}{2^n-1}$$

Dies ist ein Widerspruch zur Aussage (*). Also muß c=1 sein!

2.Fall c=1: Es ist also $b=2^n-1$. Dann gilt mit (*): $B=2^n=b+1=\sigma(b)$. Die Gleichung $\sigma(x)=x+1$ ist aber nur für primes x erfüllt. Also ist $b=2^n-1=M_n$ prim, was zu beweisen war.

Damit ist zumindest klar, daß es keine geraden vollkommenen Zahlen gibt außer den aus den Mersenne-Primzahlen gebildeten. Mit jeder neuen Mersenne-Primzahl findet man eine neue gerade vollkommenen Zahl und auch nur damit.

Bis heute ist die Frage ungeklärt, ob es ungerade vollkommenen Zahlen gibt. Man weiß jedoch, dass eine solche Zahl, wenn es sie denn gäbe, größer als 10^{100} sein müßte und mindestens 11 verschiedenen Primteiler haben müßte.

Zum Abschluß noch ein Blick in die (mathematische) Vergangenheit. Pater Mersenne veröffentlichte im Jahr 1644 sein Buch *Cogitata Physica-Mathematica*, in dem er die Mersenne-Zahlen mit den Indizes n=2, 3, 5, 7, 13, 17, 19, 31, 67, 127 und 257 zu Primzahlen erklärte. Keiner weiß bis heute, wie er zu seiner Vermutung kam, denn Beweise legte er nicht vor. Allerdings hat er sich ja auch nur bei einigen Zahlenriesen getäuscht, denn M_{67} und M_{257} sind entgegen seiner Vermutung zerlegbar, während er die Primzahlen M_{61}, M_{89} und M_{107} übersah.

Um die vollkommenen Zahlen rankten schon in alten Zeiten Geschichten. Der Lehrer Karls des Großen, der Mönch Alcuin, soll geschrieben haben, daß Gott die Welt in 6 Tagen erschaffen habe und daß der Mond sich in genau 28 Tagen um die Erde drehe, zeige schon die Vollkommenheit dieser Zahlen. Die Griechen kannten sogar schon die beiden nächsten vollkommenen Zahlen 496 und 8128 (im 1.Jahrhundert n. Ch. veröffentlichte der griechische Mathematiker *Nikomachos* sein Werk *Introductio Arithmeticae*, in dem er die ersten vier vollkommenen Zahlen nennt), doch es ist mir nicht bekannt, welchen Mystizismus sie mit ihnen betrieben haben. Nikomachos vermutete übrigens, daß die n-te vollkommenen Zahl genau n Stellen habe. Tatsächlich gibt es aber gar keine vollkommene Zahl mit fünf Stellen (die fünfte vollkommene Zahl ist 33.550.336). Des weiteren stellte Nikomachos die ob des etwas dünnen Zahlenmaterials gewagte - und falsche - Behauptung auf, die vollkommenen Zahlen endeten abwechselnd auf 6 und 8. Hätte er die sechste vollkommene Zahl 8.589.869.056 gekannt, so hätte er sich seine Fehleinschätzung sparen können.

Keith Devlin berichtet in seinem Buch *Sternstunden der modernen Mathematik* (sehr empfehlenswert) von einem englischen Mathematiker, der 1811 über die von Euler 1772 entdeckte 19-stellige vollkommene Zahl $2^{30}(2^{31}-1)$ schrieb: „Sie ist die größte vollkommene Zahl, die je entdeckt wurde, und sie wird es auch bleiben, denn da diese Zahlen zwar sehr merkwürdig sind, jedoch sonst keinen Nutzen haben, ist es unwahrscheinlich, daß je ein andere versuchen wird, eine noch größere vollkommenen Zahl zu finden.“ Wie man sich doch täuschen kann! Eulers Entdeckung war die achte von inzwischen 30 bekannten vollkommenen Zahlen. Allerdings hat sich die Rechenzeit bei den in diesem Zusammenhang auftretenden Problemen durch moderne Computer auch gewaltig verringert. So gibt Devlin an, daß für den Beweis der Zerlegbarkeit von M_{8191} (nicht etwa für die Zerlegung), 1953 ca. 100 Stunden gebraucht wurden, während derselbe Test auf einem CRAY I Computer in den achziger Jahren noch gerade 10 Sekunden benötigt wurden.

AUFGABE 1.43

a) Zeige, daß es zu jeder der ersten sechs vollkommenen Zahlen v_i außer 6 eine Zahl n_i gibt mit $v_i=1^3+2^3+...+n_i^3$. Gib diese Zahlen n_i an.

b) Beweise: Die Summe der Kehrwerte aller Teiler einer vollkommenen Zahlen ist 2.

c) Beweise: Jede vollkommene Zahl v gestattet die Darstellung:

$$v=\frac{1}{2}n(n+1)$$

Hier ist nun die „Hitliste“ der Mersenne-Primzahlen:

n	Länge	Entdeckungsjahr
2	1	?

3	1	?
5	2	?
7	3	?
13	4	1461
17	6	1588
19	6	1603
31	10	1772
61	19	1883
89	27	1911
107	33	1914
127	39	1876
521	157	1952
607	183	1952
1279	386	1952
2203	664	1952
2281	687	1952
3217	969	1957
4253	1281	1961
4423	1332	1961
9689	2917	1963
9941	2993	1963
11213	3376	1963
19937	6002	1971
21701	6533	1978
23209	6987	1979
44497	13395	1979
86243	25962	1983
110503	33265	1983
132049	39761	1983
216091	65050	1983
756839	220000	1992
859433	258716	1994
1.257.787	378632	1996

Letzte Meldung:

WAZ, Jan.97: „Nach neunmonatiger Arbeit an 18 miteinander verbundenen PC´s hat der französische Ingenieur J. Armengaud die bisher längste bekannte Primzahl entdeckt.“

Es handelt sich um $M_{1.398.269}$, nach WAZ der 35. Mersenne Primzahl.

Allerletzte Meldung:

Im Jahr 1997 werden $2^{2.976.221}$ und im Januar 1998 $2^{3.021.377}$ mit 909.526 Stellen als vorerst letzte Mitglieder (Nummer 36 und 37) in den Klub der Mersenne-Primzahlen aufgenommen. Auffällig ist der (prozentual) geringe Abstand der beiden Riesen. Der Nachweis der Primalität der letzteren brauchte etwa eine Woche Rechenzeit auf einem 200 MHZ Pentium (ob mit oder ohne Rechenfehler, ist nicht bekannt). Interessierte können sich auf der Internetseite http://www.utm.edu/research/primes ganz aktuell auf dem Laufenden halten.

01.06.98: $2^{6.972.593}$ mir 2.098.960 Stellen als prim entlarvt.