Prof. Dr. H. Brenner **Osnabrück SS 2008**

Zahlentheorie

Vorlesung 13

Mersenne-Primzahlen

Marin Mersenne (1588-1648)

DEFINITION 13.1. Eine Primzahl der Form 2^n-1 heißt *Mersennesche Primzahl*.

Generell nennt man die Zahl $M_n = 2^n - 1$ die n-te *Mersenne-Zahl*. Mit dieser Bezeichnung sind die Mersenne-Primzahlen genau diejenigen Mersenne-Zahlen, die Primzahlen sind.

LEMMA 13.2. *Ist $2^n - 1$ eine Primzahl, so ist auch n eine Primzahl.*

Beweis. Sei eine Darstellung $n = ab$ mit natürlichen Zahlen a, b gegeben. Wir setzen in der polynomialen Identität

$$X^k - 1 = (X-1)(X^{k-1} + X^{k-2} + \ldots + X + 1)$$

$X = 2^a$ und $k = b$ ein und erhalten, dass $2^a - 1 | 2^n - 1$. Da $2^n - 1$ als prim vorausgesetzt wurde, folgt $2^a - 1 = 1$ oder $2^a - 1 = 2^n - 1$, also $a = 1$ oder $a = n$. □

BEMERKUNG 13.3. Die Mersennezahl $M_n = 2^n - 1$ hat im Dualsystem eine Entwicklung, die aus genau n Einsen besteht. Die ersten Mersenne-Primzahlen sind

$$2^2 - 1 = 3, 2^3 - 1 = 7, 2^5 - 1 = 31, 2^7 - 1 = 127\,.$$

Die Zahl $2^{11} - 1 = 2047 = 23 \cdot 89$ ist die erste Mersene-Zahl, wo der Exponent zwar prim ist, die aber selbst keine Mersenne-Primzahl ist. Dies wurde 1536

von Hudalrichus Regius (Walter Hermann Ryff) gezeigt. Der nächste Kandidat, nämlich $2^{13} - 1 = 8191$, ist wieder prim. Bis ca. 1950 war bekannt, dass für die Exponenten

$$2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 \text{ und } 127$$

Mersenne-Primzahlen vorliegen, und keine weiteren unterhalb dem Exponenten 258. Von verschiedenen Leuten, unter anderem von Cataldi und Mersenne selbst, wurden falsche Behauptungen aufgestellt. Ab ca. 1950 kamen Computer zum Bestimmen von Mersenne-Primzahlen zum Einsatz, und es wurden bisher insgesamt 44 Mersenne-Primzahlen gefunden. Es ist aber unbekannt, ob es unendlich viele Mersenne-Primzahlen gibt.

Alle größten bekannten Primzahlen sind Mersenne-Zahlen. Das liegt daran, dass es für diese Zahlen einen vergleichsweise einfachen Primzahltest gibt, nämlich den *Lucas-Lehmer-Test*. Mit diesem Test wird etwa alle zwei Jahre eine neue größte Primzahl gefunden.

Mersenne-Zahlen stehen in direktem Verhältnis zu den vollkommenen Zahlen.

Vollkommene Zahlen

Definition 13.4. Eine natürliche Zahl n heißt *vollkommen*, wenn sie mit der Summe aller ihrer von n verschiedenen Teiler übereinstimmt.

Bereits Euklid stellte fest, dass die ersten vier vollkommenen Zahlen sich als

$$2^{k-1}(2^k - 1)$$

darstellen lassen:

- Für $k = 2$: $2^1(2^2 - 1) = 6 = 1 + 2 + 3$
- Für $k = 3$: $2^2(2^3 - 1) = 28 = 1 + 2 + 4 + 7 + 14$
- Für $k = 5$: $2^4(2^5 - 1) = 496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$
- Für $k = 7$: $2^6(2^7 - 1) = 8128 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064$.

Euklid bewies, dass $2^{k-1}(2^k - 1)$ immer dann eine vollkommene Zahl ist, wenn $2^k - 1$ eine Primzahl ist, also eine Mersenne-Primzahl ist. Euler bewies, dass auf diese Weise alle geraden vollkommenen Zahlen erzeugt werden können. Bevor wird diesen Satz von Euklid-Euler beweisen, brauchen wir eine kleine Vorüberlegung.

Definition 13.5. Zu einer natürlichen Zahl n bezeichnet man die Summe aller natürlichen Teiler davon als $\sigma(n)$, also

$$\sigma(n) = \sum_{t|n} t\,.$$

Eine vollkommene Zahl kann man also dadurch charakterisieren, dass $\sigma(n) = 2n$ ist.

LEMMA 13.6. *(zur Teilersumme) Zu zwei natürlichen teilerfremden Zahlen n und m gilt*

$$\sigma(nm) = \sigma(n)\sigma(m)\,.$$

Beweis. Bei zwei teilerfremden Zahlen n und m hat jeder positive Teiler t des Produkts nm die eindeutige Form $t = ab$, wobei a ein Teiler von n und b ein Teiler von m ist. Also gilt

$$\sigma(nm) = \sum_{t|mn} t = \sum_{a|m \text{ und } b|n} ab = (\sum_{a|n} a)(\sum_{b|m} b) = \sigma(n)\sigma(m)\,.$$

□

Damit können wir beweisen.

SATZ 13.7. *(Charakterisierung von geraden vollkommenen Zahlen mit Mersenne-Zahlen) Eine gerade Zahl n ist genau dann vollkommen, wenn $n = 2^{k-1}(2^k - 1)$ ist mit $2^k - 1$ prim.*

Beweis. Sei zunächst $n = 2^{k-1}(2^k - 1)$ mit $2^k - 1$ prim. Dann sind die von n verschiedenen Teiler von n gegeben durch

$$2^i,\ i = 0, \ldots, k-1, \text{ und } (2^k - 1)2^i,\ i = 0, \ldots, k-2\,.$$

Daher ist ihre Summe gleich

$$\sum_{i=0}^{k-1} 2^i + (2^k - 1)\sum_{i=0}^{k-2} 2^i = 2^k - 1 + (2^k - 1)(2^{k-1} - 1) = (2^k - 1)2^{k-1} = n\,,$$

also ist n vollkommen. Sei umgekehrt n vollkommen. Wir setzen (in Anlehnung an das Ziel) an

$$n = 2^{k-1}u$$

mit u ungerade und $k \geq 2$, da ja n gerade ist. Für teilerfremde Zahlen ist die Teilersumme gleich dem Produkt der beiden Teilersummen. Daher ist einerseits

$$\sigma(n) = \sigma(2^{k-1}u) = \sigma(2^{k-1})\sigma(u) = (2^k - 1)\sigma(u)$$

und andererseits wegen der Vollkommenheit

$$\sigma(n) = 2n = 2^k u\,.$$

Insgesamt ergibt sich also $(2^k - 1)\sigma(u) = 2^k u$. Da $2^k - 1$ ungerade ist, gilt

$$\sigma(u) = x2^k \text{ und } u = x(2^k - 1)\,.$$

Die Annahme $x > 1$ führt schnell zum Widerspruch, da es dann zumindest die drei verschiedenen Teiler $1, x, x(2^k - 1)$ von u gibt, was zu

$$\sigma(u) \geq (2^k - 1)x + 1 + x > 2^k x$$

führt. Also ist $x = 1$ und somit $\sigma(u) = 2^k = u + 1$. Die Teilersumme einer Zahl u ist aber gleich $u + 1$ nur dann, wenn eine Primzahl vorliegt. □

Es ist unbekannt, ob es unendlich viele vollkommene Zahlen gibt, da es ja auch unbekannt ist, ob es unendlich viele Mersenne-Primzahlen gibt. Es ist unbekannt, ob es überhaupt auch ungerade vollkommene Zahlen gibt.

Befreundete Zahlen

DEFINITION 13.8. Zwei verschiedene natürliche Zahlen m und n heißen *befreundet*, wenn m gleich der Summe der echten Teiler von n ist und umgekehrt.

Das klassische Beispiel für ein befreundetes Zahlenpaar ist 220 und 284. Zwei verschiedene Zahlen sind befreundet genau dann, wenn

$$\sigma(m) = m + n = \sigma(n)$$

ist. Der folgende Satz erlaubt es, einige weitere befreundete Zahlenpaare zu finden, aber keineswegs alle.

Thabit Ibn Qurra (826 (?)-901)

SATZ 13.9. *(Regel von Thabit) Sei $k \geq 2$ eine natürliche Zahl und seien $a = 3 \cdot 2^{k-1} - 1$, $b = 3 \cdot 2^k - 1$ und $c = 9 \cdot 2^{2k-1} - 1$ allesamt Primzahlen. Dann sind*

$$m = 2^k ab \text{ und } n = 2^k c$$

befreundet.

Beweis. Wir berechnen $\sigma(m)$, $\sigma(n)$ und $m + n$. Es ist

$$\begin{aligned}
\sigma(m) &= \sigma(2^k ab) \\
&= \sigma(2^k)\sigma(a)\sigma(b) \\
&= (2^{k+1} - 1)(3 \cdot 2^{k-1})(3 \cdot 2^k) \\
&= (2^{k+1} - 1) \cdot 9 \cdot 2^{2k-1}\,.
\end{aligned}$$

Weiter ist

$$\begin{aligned}\sigma(n) &= \sigma(2^k c)\\ &= \sigma(2^k)\sigma(c)\\ &= (2^{k+1}-1)(1+c)\\ &= (2^{k+1}-1)\cdot 9\cdot 2^{2k-1}\,.\end{aligned}$$

Schließlich ist

$$\begin{aligned}m+n &= 2^k(ab+c)\\ &= 2^k((3\cdot 2^{k-1}-1)(3\cdot 2^k-1)+9\cdot 2^{2k-1}-1)\\ &= 2^k(9\cdot 2^{2k-1}-3\cdot 2^{k-1}-3\cdot 2^k+9\cdot 2^{2k-1})\\ &= 2^k(9\cdot 2^{2k}-9\cdot 2^{k-1})\\ &= 2^k 2^{k-1}\cdot 9(2^{k+1}-1)\,.\end{aligned}$$

□

k	$a=3\cdot 2^{k-1}-1$	$b=3\cdot 2^k-1$	$c=9\cdot 2^{2k-1}-1$	$m=2^kab$	$n=2^kc$
2	5	11	71	220	284
3	11	23	$287=7\cdot 41$		
4	23	47	1151 (prim)	17296	18416
5	47	95	$4607=17\cdot 271$		
6	$95=5\cdot 19$	191	$18431=7\cdot 2633$		
7	191	383	73727	9363584	9437056

Das Paar 1184 und 1210 ist befreundet, aber nicht erhältlich über die Regel von Thabit.

Abbildungsverzeichnis