

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. Eine Mersenne-Zahl besitzt im Zweisystem die Ziffernentwicklung $11111 \dots 1111$. Das ist auch die Anzahl der Spiele in einem im K.-o.-System ausgetragenen Pokalwettbewerb mit 2^n Mannschaften.

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

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

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

$X = 2^a$ 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 Mersenne-Zahl $M_n = 2^n - 1$ 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 Mersenne-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 des 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 52 Mersenne-Primzahlen gefunden. Die größte ist

$$2^{136279841} - 1.$$

Es ist 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. Für eine Rekordliste siehe Mersenne-Primzahlen.

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 all 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, also eine Mersenne-Primzahl ist. Euler bewies, dass auf diese Weise alle geraden vollkommenen Zahlen erzeugt werden können. Bevor wir 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 von n 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. 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

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

□

Damit können wir den Satz von Euklid-Euler beweisen.

SATZ 13.7. Eine gerade Zahl n ist genau dann vollkommen, wenn $n = 2^{k-1}(2^k - 1)$ ist mit $2^k - 1$ prim.

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

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

gegeben. 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. Es 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 nach Lemma 13.6 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. Die Summe der echten Teiler von $220 = 2 \cdot 2 \cdot 5 \cdot 11$ ist

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$$

und die Summe der echten Teiler von $284 = 2 \cdot 2 \cdot 71$ ist

$$1 + 2 + 4 + 71 + 142 = 220.$$

Zwei verschiedene Zahlen sind genau dann befreundet, wenn

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

ist. Der folgende Satz erlaubt es, einige weitere befreundete Zahlenpaare zu finden, aber keineswegs alle. Man spricht von der *Regel von Thabit*.

SATZ 13.9. *Es 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 $m + n$. Nach Aufgabe ***** sind a und b teilerfremd und somit ist nach Lemma 13.6

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

$$= (2^{k+1} - 1) \cdot 9 \cdot 2^{2k-1}.$$

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

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

□

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

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

Zahlentheoretische Funktionen

DEFINITION 13.10. Eine Funktion

$$\mathbb{N}_+ \longrightarrow \mathbb{C}$$

nennt man *zahlentheoretische Funktion*.

Eine zahlentheoretische Funktion ist also einfach eine komplexwertige Folge. Im zahlentheoretischen Kontext sind die beiden folgenden Definitionen wichtig.

DEFINITION 13.11. Eine zahlentheoretische Funktion

$$f: \mathbb{N}_+ \longrightarrow \mathbb{C}$$

heißt *multiplikativ*, wenn für teilerfremde Zahlen m, n stets

$$f(mn) = f(m)f(n)$$

gilt.

An multiplikativen zahlentheoretischen Funktionen haben wir bisher die eulersche φ -Funktion, die Teileranzahlfunktion (siehe Aufgabe *****) und die Teilersummenfunktion (siehe Lemma 13.6) kennengelernt.

DEFINITION 13.12. Zu zahlentheoretischen Funktionen $f, g: \mathbb{N}_+ \rightarrow \mathbb{C}$ heißt die durch

$$(f * g)(n) := \sum_{d \text{ teilt } n} f(d)g\left(\frac{n}{d}\right)$$

definierte Funktion die *Faltung* von f und g .

Diese Summe kann man auch in der Form

$$\sum_{n=de} f(d)g(e)$$

schreiben. Summiert wird nur über die positiven Teilerpaare, was bei dieser Schreibweise übersehen werden könnte.

LEMMA 13.13. Zu multiplikativen zahlentheoretischen Funktionen $f, g: \mathbb{N}_+ \rightarrow \mathbb{C}$ ist auch die Faltung $f * g$ multiplikativ.

Beweis. Es seien f, g multiplikativ und es seien m, n teilerfremde natürliche Zahlen. Zu einer Faktorzerlegung

$$de = mn$$

gibt es aufgrund der Teilerfremdheit eine eindeutige Aufspaltung $d = ru$ und $e = sv$ mit r, u und s, v teilerfremd und mit $rs = m$ und $uv = n$. Daher ist

$$\begin{aligned} (f * g)(m \cdot n) &= \sum_{d \cdot e = m \cdot n} f(d)g(e) \\ &= \sum_{rs=m, uv=n} f(ru)g(sv) \\ &= \sum_{rs=m, uv=n} f(r)f(u)g(s)g(v) \\ &= \left(\sum_{r \cdot s = m} f(r)g(s) \right) \cdot \left(\sum_{u \cdot v = n} f(u)g(v) \right) \\ &= (f * g)(m) \cdot (f * g)(n), \end{aligned}$$

also ist auch $f * g$ multiplikativ. □

DEFINITION 13.14. Die zahlentheoretische Funktion $\mathbb{N}_+ \rightarrow \mathbb{C}$, die für 1 den Wert 1 und sonst überall den Wert 0 besitzt, wird mit I bezeichnet. Sie heißt die *Faltungseinheit*.

DEFINITION 13.15. Die zahlentheoretische Funktion $\mathbb{N}_+ \rightarrow \mathbb{C}$, die überall den Wert 1 besitzt, wird mit U bezeichnet.

DEFINITION 13.16. Die zahlentheoretische Funktion $\mu: \mathbb{N}_+ \rightarrow \mathbb{C}$, die durch

$$\mu(n) := \begin{cases} 0, & \text{falls in der Primfaktorzerlegung von } n \text{ manche Primfaktoren mehrfach auftreten,} \\ (-1)^k, & \text{falls } n = p_1 \cdots p_k \text{ mit verschiedenen Primfaktoren.} \end{cases}$$

gegeben ist, heißt *Möbius-Funktion*.

LEMMA 13.17. *Für die Faltung von zahlentheoretischen Funktionen gelten die folgenden Aussagen.*

- (1) *Die Faltung ist eine kommutative und assoziative Verknüpfung.*
- (2) *Die Faltungseinheit I ist das neutrale Element der Verknüpfung.*
- (3) *Es ist*

$$U * \mu = I.$$

Beweis. Siehe Aufgabe 13.9.

□

Abbildungsverzeichnis

- Quelle = Marin Mersenne.jpeg , Autor = Benutzer Maksim auf Commons, Lizenz = PD 1
- Erläuterung: Die in diesem Text verwendeten Bilder stammen aus Commons (also von <http://commons.wikimedia.org>) und haben eine Lizenz, die die Verwendung hier erlaubt. Die Bilder werden mit ihren Dateinamen auf Commons angeführt zusammen mit ihrem Autor bzw. Hochlader und der Lizenz. 9
- Lizenzklärung: Diese Seite wurde von Holger Brenner alias Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und unter die Lizenz CC-by-sa 3.0 gestellt. 9