Paulo Ribenboim

Die Welt der Primzahlen

Geheimnisse und Rekorde

Aus dem Englischen übersetzt von Jörg Richstein.
Auf den neuesten Stand gebracht von Wilfrid Keller.

Mit 29 Tabellen

Springer

5

Welche besonderen Arten von Primzahlen wurden untersucht?

Wir waren bereits verschiedenen Arten besonderer Primzahlen begegnet. Zum Beispiel solchen, die Fermat- oder Mersenne-Zahlen sind (siehe Kapitel 2). Ich werde nun weitere Primzahl-Familien besprechen, darunter die regulären Primzahlen, Sophie-Germain-Primzahlen, Wieferich-Primzahlen, Wilson-Primzahlen, Repunit-Primzahlen sowie Primzahlen in linear rekurrenten Folgen zweiter Ordnung.

Reguläre Primzahlen, Sophie-Germain- und Wieferich-Primzahlen entstammen direkt aus Beweisversuchen von Fermats letztem Satz.

Der interessierte Leser möchte dazu vielleicht mein Buch *13 Lectures on Fermat's Last Theorem* konsultieren, in dem diese Angelegenheiten genauer besprochen werden. Insbesondere befindet sich darin ein umfassendes Literaturverzeichnis mit Hinweisen auf zahlreiche klassische Arbeiten, die im Verzeichnis dieses Buches nicht angegeben sind.

I Reguläre Primzahlen

Reguläre Primzahlen traten erstmals in der Arbeit von Kummer in Verbindung mit Fermats letztem Satz in Erscheinung. In einem Brief an Liouville von 1847 erklärt Kummer, er habe Fermats letzten Satz für alle Primzahlen p bewiesen, die zwei Bedingungen genügen. Tatsächlich hatte er gezeigt, dass wenn p diese Bedingungen erfüllt, es keine ganzen Zahlen x, y, $z \neq 0$ mit $x^p + y^p = z^p$ gibt. Er bemerkte weiter, dass

„es nun reicht herauszufinden, ob dies gemeinsame Eigenschaften aller Primzahlen sind."

Um diese Eigenschaften beschreiben zu können, muss ich einige der von Kummer eingeführten Konzepte erläutern.

Es sei p eine ungerade Primzahl und

$$\zeta = \zeta_p = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$$

eine primitive p-te Einheitswurzel. Man beachte, dass $\zeta^{p-1} + \zeta^{p-2} + \cdots + \zeta + 1 = 0$, da $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + X + 1)$ und $\zeta^p = 1$, $\zeta \neq 1$. Folglich lässt sich ζ^{p-1} durch kleinere Potenzen von ζ ausdrücken. Es sei K die Menge aller Zahlen $a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$ mit rationalen Zahlen $a_0, a_1, \ldots, a_{p-2}$ und A die kleinste Teilmenge von K, die aus denjenigen Zahlen besteht, für die $a_0, a_1, \ldots, a_{p-2}$ ganz sind. Dann ist K ein Körper, den man den p-ten Kreisteilungskörper (oder auch Körper der p-zyklotomischen Zahlen) nennt. A ist ein Ring, der Ganzheitsring der p-zyklotomischen (ganzen) Zahlen. Die Einheiten von A sind diejenigen Zahlen $\alpha \in A$, die die 1 teilen, das heißt, für die $\alpha\beta = 1$ für irgendein $\beta \in A$ erfüllt ist. Ein Element $\alpha \in A$ nennt man ein Primelement, wenn α sich nur dann in der Form $\alpha = \beta\gamma$ mit $\beta, \gamma \in A$ schreiben lässt, wenn β oder γ eine Einheit ist.

Ich werde die Arithmetik der p-zyklotomischen ganzen Zahlen als normal bezeichnen, wenn jede zyklotomische ganze Zahl ein bis auf Einheiten eindeutiges Produkt von Primelementen ist.

Kummer entdeckte bereits 1847, dass die Arithmetik der p-zyklotomischen Zahlen für $p \leq 19$ normal ist. Dies ist jedoch für $p = 23$ nicht der Fall.

Um einen Weg zu finden, mit nichteindeutigen Primfaktorzerlegungen umzugehen, führte Kummer ideale Zahlen ein. Später untersuchte Dedekind bestimmte Mengen zyklotomischer ganzer Zahlen, die er Ideale nannte. Ich werde von einer Definition des Begriffs Ideal absehen und es als dem Leser bekannt voraussetzen. Dedekind-Ideale ermöglichten eine konkrete Beschreibung von Kummers idealen Zahlen. Es bietet sich daher an, Kummers Ergebnisse durch Dedekinds Ideale zu erklären. Ein Primideal P ist ein Ideal, das weder gleich 0 ist, noch mit dem Ring A übereinstimmt und das nur dann ein Produkt $P = IJ$ zweier Ideale sein kann, wenn entweder I oder J gleich P ist. Kummer zeigte, dass für alle Primzahlen $p > 2$ jedes von 0 und A verschiedene Ideal des Ganzheitsrings der p-zyklotomischen Zahlen in eindeutiger Weise ein Produkt von Primidealen ist.

In diesem Zusammenhang erscheint es natürlich, zwei Ideale I und J ungleich dem Nullideal als äquivalent zu betrachten, wenn es zwei von 0 verschiedene zyklotomische ganze Zahlen $\alpha, \beta \in A$ mit der Eigenschaft gibt, dass $A\alpha.I = A\beta.J$. Die Menge der Äquivalenzklassen von Idealen bildet eine kommutative, reguläre Halbgruppe. Kummer zeigte, dass diese Menge endlich ist und damit eine Gruppe bildet, die man nun Idealklassengruppe nennt. Die Anzahl ihrer Elemente heißt Klassenzahl und wird mit $h = h(p)$ bezeichnet. Sie ist eine sehr wichtige arithmetische Invariante.

Das Konzept gebrochener Ideale, Klassen von Idealen und der Endlichkeit der Anzahl der Klassen spielt eine zentrale Rolle in der Theorie algebraischer Zahlkörper. Außer den hier betrachteten Kreisteilungskörpern hatte ich bereits zuvor (Kapitel 3, Abschnitt III, B) den Fall der quadratischen Zahlkörper betrachtet.

Die Klassenzahl $h(p)$ ist genau dann gleich 1, wenn jedes Ideal von A ein Hauptideal ist, das heißt, wenn es die Form $A\alpha$ für ein $\alpha \in A$ hat. Somit gilt $h(p) = 1$ genau dann, wenn die Arithmetik der p-zyklotomischen ganzen Zahlen normal ist. Die Größe von $h(p)$ ist also ein Maß für die Abweichung von der normalen Arithmetik.

Es sei an dieser Stelle gesagt, dass Kummer eine sehr tiefschürfende Theorie entwickelt hat, dabei eine explizite Formel für $h(p)$ fand und in der Lage war, $h(p)$ für kleine p zu berechnen.

Eine der Eigenschaften von p, die Kummer in Verbindung mit Fermats letztem Satz benötigte, war die folgende: p ist kein Teiler der Klassenzahl $h(p)$. Heute nennt man eine Primzahl mit dieser Eigenschaft eine *reguläre Primzahl.*

Die zweite Eigenschaft, die Kummer nannte, bezog sich auf Einheiten. Er zeigte später, dass diese von allen regulären Primzahlen erfüllt ist. Dies ist ein weiteres, schönes Resultat von Kummer, man nennt es heute Kummers Lemma.

In seinem Regularitätskriterium bewies Kummer, dass die Primzahl p genau dann regulär ist, wenn p die Zähler der Bernoulli-Zahlen B_2, B_4, $B_6, \ldots, B_{p-3}$ nicht teilt (die Bernoulli-Zahlen wurden in Kapitel 4, Abschnitt I, A definiert).

Kummer gelang es kurz darauf, alle irregulären Primzahlen unterhalb von 163 zu bestimmen, dies sind 37, 59, 67, 101, 103, 131, 149, 157. Er gab die Hoffnung nicht auf, dass unendlich viele reguläre Primzahlen existieren. Die Klärung dieser Frage stellt ein sehr schwieriges Problem dar, obwohl die Antwort positiv ausfallen sollte, worauf numerische Belege klar hindeuten.

Siegel bewies 1964 unter der Voraussetzung heuristischer Aussagen über die Reste von Bernoulli-Zahlen modulo Primzahlen, dass die Dichte regulärer Primzahlen unter allen Primzahlen $1/\sqrt{e} \cong 61\%$ beträgt.

Auf der anderen Seite war es ein wenig überraschend, als Jensen 1915 bewies, dass es unendlich viele irreguläre Primzahlen gibt. Der Beweis war eigentlich ziemlich einfach, er erforderte einige arithmetische Eigenschaften der Bernoulli-Zahlen.

Es sei $\pi_{\text{reg}}(x)$ die Anzahl der regulären Primzahlen p mit $2 \le p \le x$ und

$$\pi_{\text{ir}}(x) = \pi(x) - \pi_{\text{reg}}(x).$$

Für jede irreguläre Primzahl p nennt man das Paar $(p, 2k)$ ein *irreguläres Paar*, wenn $2 \le 2k \le p-3$ und p den Zähler von B_{2k} teilt. Die Anzahl der irregulären Paare $(p, 2k)$ heißt *Irregularitätsindex* von p und wird mit $\text{ii}(p)$ bezeichnet.

Für $s \ge 1$ sei $\pi_{\text{ii}s}(x)$ die Anzahl der Primzahlen $p \le x$ mit $\text{ii}(p) = s$.

Rekord

Die wichtigsten Berechnungen über reguläre Primzahlen stammen der Reihenfolge nach von Johnson (1975), Wagstaff (1978), Tanner & Wagstaff (1989), Buhler, Crandall & Sompolski (1992), Buhler, Crandall, Ernvall & Metsänkylä (1993) und Buhler, Crandall, Ernvall, Metsänkylä & Shokrollahi (2001). Alle irregulären Primzahlen bis $N = 12 \times 10^6$ wurden zusammen mit ihrem Irregularitätsindex bestimmt. Hier die Ergebnisse (die Primzahl 2 zählt man weder zu den regulären, noch zu den irregulären Primzahlen):

$$\begin{aligned}
\pi(N) &= 788060 \\
\pi_{\text{reg}}(N) &= 477616 \\
\pi_{\text{ir}}(N) &= 310443 \\
\pi_{\text{ii}1}(N) &= 239483 && \text{(die Kleinste ist } 37) \\
\pi_{\text{ii}2}(N) &= 59710 && \text{(die Kleinste ist } 157) \\
\pi_{\text{ii}3}(N) &= 9824 && \text{(die Kleinste ist } 491) \\
\pi_{\text{ii}4}(N) &= 1282 && \text{(die Kleinste ist } 12613) \\
\pi_{\text{ii}5}(N) &= 127 && \text{(die Kleinste ist } 78233) \\
\pi_{\text{ii}6}(N) &= 13 && \text{(die Kleinste ist } 527377) \\
\pi_{\text{ii}7}(N) &= 4 && \text{(die Kleinste ist } 3238481) \\
\pi_{\text{ii}s}(N) &= 0, \text{ für } s \ge 8.
\end{aligned}$$

Der gegenwärtige Stand des Wissens ist: Die größte reguläre Primzahl ist $p = 11999989$. Die längste Sequenz aufeinander folgender regulärer Primzahlen besteht aus 27 Primzahlen und beginnt mit 17881. Die längste Sequenz aufeinander folgender irregulärer Primzahlen besteht aus 14 Primzahlen und beginnt mit 670619.

Die einzigen irregulären, „aufeinander folgenden" Paare $(p, 2k)$, $(p, 2k + 2)$ sind $p = 491$, $2k = 336$ bzw. $p = 587$, $2k = 90$. Es sind keine Drillinge $(p, 2k)$, $(p, 2k + 2)$, $(p, 2k + 4)$ irregulärer Paare bekannt.

Für alle Primzahlen $p \geq 11$ gilt, dass p genau dann eine Wolstenholme-Primzahl ist (siehe Kapitel 2, Abschnitt II, C), wenn p den Zähler der Bernoulli-Zahl B_{p-3} teilt, oder anders ausgedrückt, wenn $(p, p-3)$ ein irreguläres Paar ist.

Man vermutet, ohne es jedoch bisher beweisen zu können, dass es Primzahlen mit beliebig hohem Irregularitätsindex gibt.

Aus der Kombination des Satzes von Kummer, einem Kriterium von Vandiver sowie den oben erwähnten Berechnungen ergibt sich, dass Fermats letzter Satz für jeden primen Exponenten $p < 12 \times 10^6$ richtig ist.

Die Regularität einer Primzahl ist für viele Fragen der Zahlentheorie relevant, wobei seit dem Beweis der allgemeinen Gültigkeit des Fermatschen Satzes die Rolle der regulären Primzahlen in diesem Zusammenhang hauptsächlich von historischem Interesse ist. Die außergewöhnliche mathematische Leistung des kompletten Beweises war das Resultat der Verknüpfung von Arbeiten von G. Frey, K.A. Ribet, J.P. Serre, A. Wiles und R. Taylor.

II Sophie-Germain-Primzahlen

Ich war auf die Sophie-Germain-Primzahlen bereits in Kapitel 2 in Zusammenhang mit einem Kriterium von Euler über Teiler von Mersenne-Zahlen gestoßen.

Zur Erinnerung: p ist dann eine *Sophie-Germain-Primzahl*, wenn auch $2p+1$ prim ist. Es war Sophie Germain, die solche Zahlen zuerst untersuchte und dabei diesen wunderbaren Satz bewies:

Wenn p eine Sophie-Germain-Primzahl ist, dann gibt es keine von 0 verschiedenen ganzen Zahlen x, y, z, die nicht von p geteilt werden und die $x^p + y^p = z^p$ erfüllen.