Werk

Titel: Primzahlen.

Autor: Lang, Serge

Jahr: 1992

PURL: https://resolver.sub.uni-goettingen.de/purl?378850199_0047|log11

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

El. Math., *47*, (1992)

0013-6018/92/020049-13$1.50 + 0.20/0
© 1992 Birkhäuser Verlag, Basel

Primzahlen

Serge Lang,
Yale University,

Serge Lang wurde 1927 in Paris geboren, wo er auch seine ersten Schuljahre absolvierte. Die weitere Ausbildung erhielt er dann allerdings in den Vereinigten Staaten, wo er das California Institute of Technology (Caltech) und die University of Princeton besuchte. Hier erhielt er das Doktorat in Mathematik im Jahre 1951. Nach Aufenthalten am Institute for Advanced Study in Princeton und an der University of Chicago, war er von 1955 bis 1970 Professor an der Columbia University in New York. Gastprofessuren in Princeton und Harvard folgten, und 1972 wurde er Professor an der Yale University. Seine Interessen sind weitgespannt, aber sein Hauptinteresse gehörte immer der Mathematik, besonders der Zahlentheorie. Bis anhin hatte er 34 Bücher und über 70 Forschungsartikel veröffentlicht.

Wer weiss, was eine Primzahl ist? (Verschiedene Zuhörer geben eine Definition.) Hier ist die Definition: Eine *Primzahl* p ist eine ganze Zahl grösser oder gleich 2 mit der

Dieser Beitrag hat eine etwas ungewöhnliche Entstehungsgeschichte. Serge Lang hat im Mai 1991 im Mathematischen Studenten-Kolloquium an der ETH Zürich einen Vortrag mit dem Titel *Primzahlen* gehalten. Im Hinblick auf eine spätere Veröffentlichung gab er uns die Erlaubnis, seinen Vortrag auf Band aufzunehmen, und der vorliegende Artikel entstand aus der Transkription dieser Bandaufnahme. Der Text wurde zwar mehrmals überarbeitet und auch an einigen Stellen ergänzt, aber wir haben die direkte informelle Sprache und auch einige Reaktionen der Zuhörerschaft mit Absicht beibehalten. Wir hoffen, dass auf diese Weise der Enthusiasmus von Serge Lang während seines lebhaften Vortrages auch bei der Lektüre des Textes spürbar wird.

Serge Lang beginnt seinen Vortrag über Primzahlen mit dem einfachen Satz von Euklid. Schrittweise führt er dann seine Zuhörerschaft an weitergehende Probleme heran und gelangt schliesslich zu zahlentheoretischen Fragen, die zwar eine ganz einfache Formulierung zulassen, die aber bis heute unbeantwortet geblieben sind. Natürlich gibt es über diese Fragen Vermutungen, die plausibel sind und mit allen numerischen Experimenten in Einklang stehen; bis jetzt haben sie aber allen Beweisversuchen widerstanden. Die berühmteste und wichtigste darunter ist zweifellos die Riemannsche-Vermutung. Im zweiten Teil seines Vortrages geht Serge Lang auf einige dieser Vermutungen näher ein; er berichtet dabei über ihre Geschichte und auch über neuere Bemühungen zu ihrer Klärung. *ust*

Eigenschaft, dass jeder Teiler von p entweder 1 oder p ist. Nach Konvention nehmen wir $p \geq 2$, die Zahl 1 zählt nicht als Primzahl. Was ist also die Folge der Primzahlen? Sie ist

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots, \text{usw.}$$

Was heisst "usw."? Ist die Folge der Primzahlen unendlich, oder stoppt sie irgendwo? Mit andern Worten: Gibt es unendlich viele Primzahlen oder nur endlich viele? Die Antwort ist seit Euklid bekannt:

Theorem *Es gibt unendlich viele Primzahlen.*

Wissen Sie, wie man das beweist? (Einige Studenten sagen, dass sie keinen Beweis wüssten; ein Student gibt einen Beweis an.) Ja, so werde ich diesen Beweis anschreiben. Es seien 2, 3, $\ldots, P$ die Primzahlen bis zu P. Wir haben zu zeigen, dass es eine weitere Primzahl gibt, die von 2, 3, $\ldots, P$ verschieden ist. Wenn wir dies zeigen können, dann haben wir bewiesen, dass es unendlich viele Primzahlen gibt. Es sei nun

$$N = (2 \cdot 3 \cdot 5 \cdots P) + 1.$$

Falls N eine Primzahl ist, dann ist N grösser als P, und wir haben eine weitere Primzahl gefunden. Was geschieht, wenn N keine Primzahl ist? In diesem Fall ist N teilbar durch eine gewisse Primzahl. In der Tat lässt sich N als Produkt von zwei kleineren positiven ganzen Zahlen schreiben. Falls eine davon eine Primzahl ist, haben wir eine Primzahl q gefunden, die N teilt. Andernfalls können wir diese ganzen Zahlen wiederum in ein Produkt zerlegen. Auf diese Art und Weise kann man weiterfahren, aber, da die Faktoren immer kleiner werden, muss dieses Verfahren nach endlich vielen Schritten abbrechen. Deshalb werden wir an einer bestimmten Stelle einen Primfaktor q von N erhalten. Nun behaupten wir, dass dieser Primfaktor q der Zahl N verschieden ist von den bereits bekannten Primzahlen 2, 3, 5, $\ldots, P$. Weshalb ist dies der Fall? (Einige Zuhörer geben die Antwort.) Ja, wenn man N durch irgendeine der Primzahlen 2, 3, 5, $\ldots, P$ dividiert, dann erhält man den Rest 1, aber q ist eine Primzahl, die N ohne Rest teilt. Damit kann q nicht gleich einer der Primzahlen 2, 3, 5, $\ldots, P$ sein, und wir haben bewiesen, dass es unendlich viele Primzahlen gibt.

Als nächstes betrachten wir ein anderes Problem, das mit Primzahlen zusammenhängt. In der Folge der Primzahlen gibt es Paare wie (3,5), (5,7), (11,13), (17,19), welche aus Primzahlen bestehen, die sich um 2 unterscheiden:

$$5 = 3 + 2; \quad 7 = 5 + 2; \quad 13 = 11 + 2; \quad 19 = 17 + 2\,.$$

Ein Paar von Primzahlen $(p, p+2)$ heisst ein *Primzahlzwilling*. Welches Paar kommt nach (17,19) ? (Einige Studenten geben die Antwort:)

$$(29, 31), \quad (41, 43), \quad (59, 61), \quad (71, 73), \quad \ldots$$

Welche Frage drängt sich hier auf?

Frage: Gibt es unendlich viele Primzahlzwillinge?

Wer sagt "Ja"? (Einige Hände gehen in die Höhe.) Wer sagt "Nein"? (Einige wenige Hände gehen in die Höhe.) (Einige Studenten beginnen einen Beweis zu versuchen.) Ich

habe nicht gefragt, wie man das beweisen kann, ich habe nur gefragt, ob Sie glauben, dass es unendlich viele Primzahlzwillinge gibt oder nicht. Das sind zwei verschiedene Fragen. Im ersten Beispiel mit den Primzahlen habe ich ebenfalls gefragt, ob Sie glauben, dass es unendlich viele gibt. Jedermann glaubte das, aber Sie wussten nicht, wie man das beweisen soll. Also gibt es zwei Fragen. Die eine ist: "Glauben Sie, dass es unendlich viele gibt?" und die andere ist "Können Sie das beweisen?" Im Moment sind wir bei der ersten Frage. Glauben Sie, dass es unendlich viele Primzahlzwillinge gibt oder nicht? Glaubt irgend jemand, dass es nicht unendlich viele gibt, dass nur eine endliche Anzahl davon existiert? (Die Zuhörer schweigen.) Ist es zu gefährlich etwas zu sagen? Dann werde ich Ihnen die Antwort geben. Die Vermutung ist "Ja", aber ein Beweis ist nicht bekannt. Es ist also im Moment nicht bekannt, ob es unendlich viele Primzahlzwillinge gibt oder nicht. Es ist ein ganz berühmtes Problem der Mathematik, eine Antwort auf diese Frage zu finden.

Hier ist eine weitere Frage ähnlicher Art. Sie betrachten ganze Zahlen der Form n^2+1, zum Beispiel

$$2^2+1=5,\ 4^2+1=17,\ 6^2+1=37,\ 8^2+1=65,\ 10^2+1=101\,.$$

Mit Ausnahme von 65 sind diese Zahlen alle Primzahlen. Was für eine Frage drängt sich also auf? (Einige Studenten geben die Antwort.) Ja, die nächste Frage ist:

Frage: Gibt es unendlich viele Primzahlen der Form n^2+1?

Wieviele glauben, dass es unendlich viele davon gibt? (Einige Hände gehen in die Höhe.) Wieviele glauben, dass nur endlich viele davon existieren? (Einige wenige Hände gehen in die Höhe.) Wieviele haben vorsichtigerweise geschwiegen? (Die meisten haben sich in der Tat nicht entscheiden können.) Ich gebe Ihnen hier die Antwort: Die Vermutung ist "Ja", aber es ist kein Beweis dafür bekannt. Dies ist ein weiteres ungelöstes Problem der Mathematik.

Welche Argumente gibt es, die nahelegen, dass es unendlich viele gibt? Ich werde Ihnen solche Argumente nun vorführen, welche darüberhinaus sogar erlauben, eine Vermutung über die Häufigkeit zu formulieren. Wir stellen zu diesem Zweck die folgenden Fragen:

- Wie viele Primzahlen p gibt es mit $p \le x$? Wir nennen diese Anzahl $\pi(x)$.
- Wie viele Primzahlzwillinge $(p, p+2)$ gibt es mit $p+2 \le x$?
- Wie viele Primzahlen p von der Form $p = n^2+1$ gibt es mit $p \le x$?

Wir betrachten zuerst $\pi(x)$. Wir möchten dafür eine Abschätzung erhalten. Eine solche Abschätzung hängt von einer Wahrscheinlichkeit ab. Nach der allgemeinen Philosophie, die auf eine Vermutung von Gauss zurückgeht, ist die Wahrscheinlichkeit dafür, dass die Zahl n eine Primzahl ist, durch $1/\log n$ gegeben. Gauss hatte diese Vermutung 1849 in einem Brief an den Astronomen Encke ausgesprochen, wo er auch feststellte, dass er in den Jahren 1792/93 darauf gestossen sei, also im Alter von 15/16 Jahren. Die Vermutung von Gauss hat sich als grundlegend für die Theorie der Verteilung von Primzahlen herausgestellt. Was bedeutet die Angabe einer solchen Wahrscheinlichkeit? Jede ganze Zahl n ist entweder eine Primzahl oder sie ist keine Primzahl. Also haben wir zu erklären, was wir mit der Aussage meinen, dass die Wahrscheinlichkeit $1/\log n$

sei. Nimmt man die Anzahl der Primzahlen kleiner oder gleich x, also $\pi(x)$, dann sollte $\pi(x)$ einfach die Summe der Wahrscheinlichkeiten

$$\pi(x) \sim \sum_{2 \le n \le x} \frac{1}{\log n}$$

sein. Das ist die Bedeutung der obigen Aussage. Die Formel ist aber auch jetzt noch nicht ganz klar. Eines der Probleme ist zum Beispiel, dass die Beziehung nur näherungsweise gilt; wir haben aus diesem Grund das Zeichen $\sim$ verwendet. Natürlich müssen wir diese Beziehung präziser formulieren. Was wir meinen ist, dass die Gleichung

$$\pi(x) = \sum_{2 \le n \le x} \frac{1}{\log n} + F_1(x)$$

besteht, wo $F_1(x)$ ein Fehlerglied ist, das verglichen mit $\pi(x)$ sehr klein ist. Um die Aussage ganz präzis zu fassen, sollte man auch eine Abschätzung für das Fehlerglied angeben, welche dieses, verglichen mit $\pi(x)$, so klein als möglich macht. Wir werden bald zu einer solchen Abschätzung kommen, aber zuerst möchte ich zeigen, wie man die obige Summe auf eine andere Art und Weise schreiben kann. Die Formel sollte bei Ihnen Erinnerungen wecken, und Sie sollten den Wunsch verspüren, statt der Summe der Terme $1 / \log n$ etwas anderes hinzuschreiben, siehe Figur 1. Die Summe kann interpretiert

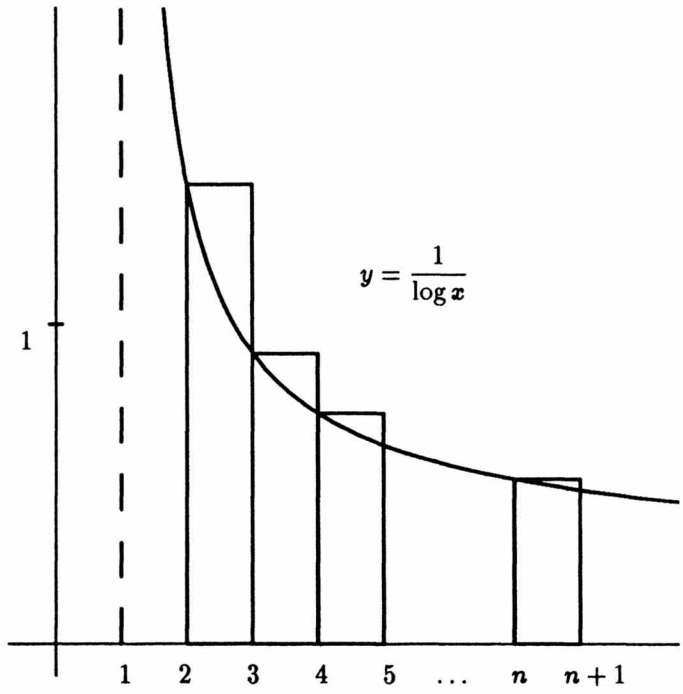

Fig. 1

werden als Riemannsche Summe für das Integral über die Funktion $1/\log x$. Deshalb können wir schreiben

$$\pi(x) = \int_2^x \frac{1}{\log t}\, dt + F_2(x)\,,$$

wo $F_2(x)$ ein neues Fehlerglied ist; die beiden Funktionen $F_1(x), F_2(x)$ sind allerdings nicht sehr verschieden. In der Tat kann man mit etwas Differential- und Integralrechnung auf einfache Weise zeigen, dass die Abschätzung

$$\left| \int_2^x \frac{1}{\log t}\, dt - \sum_{2 \le n \le x} \frac{1}{\log n} \right| \le 3$$

gilt. Damit können wir $\pi(x)$ durch das Integral *oder* die Summe abschätzen. In gewisser Weise ist das Integral einfacher zu handhaben. Mit partieller Integration erhalten wir zum Beispiel sofort

$$\int_2^x \frac{1}{\log t}\, dt = \frac{x}{\log x} + \int_2^x \frac{1}{(\log t)^2}\, dt - \frac{2}{\log 2}\,.$$

Auf der rechten Seite integriert man über eine Funktion, die viel kleiner ist als $1/\log t$, nämlich

$$\frac{1}{\log t} \cdot \frac{1}{\log t}\,.$$

Diese strebt für $t \to \infty$ in der Tat schneller gegen 0 als $1/\log t$. Für $t \to \infty$ können wir deshalb das Verhalten von $\pi(x)$ durch die Formel

$$\pi(x) = \frac{x}{\log x} + \mathrm{o}\left(\frac{x}{\log x}\right)$$

beschreiben, wo wir in der üblichen Weise mit Hilfe des Symbols o ein Fehlerglied $F_3(x)$ bezeichnet haben, für das

$$\lim_{x \to \infty} \frac{F_3(x)}{(x/\log x)} = 0$$

gilt. Nun ist $x/\log x$ keine sehr gute Approximation von $\pi(x)$, weil wir anstelle der guten Summe einfach die gesamte Anzahl der Zahlen von 1 bis x genommen haben und durch die höchste Wahrscheinlichkeit, nämlich $\log x$ geteilt haben. Es ist klar, dass dies keine sehr gute Approximation liefert; denn bei der Division von x durch $\log x$ haben wir eine nur sehr grobe Abschätzung verwendet. Die Summe der Wahrscheinlichkeiten oder das Integral sollten demgegenüber ein besseres Resultat liefern. Trotzdem hat der Ausdruck einen Vorteil: Es ist eine schöne Formel, welche in gewisser, wenn auch grober Weise eine Antwort auf unsere erste Frage gibt. Diese Antwort wurde um 1890 herum gefunden, und sie ist vollständig bewiesen:

Primzahlsatz (Hadamard, de la Vallée Poussin, 1896). *Es gilt für* $x \to \infty$

$$\pi(x) \sim \frac{x}{\log x}.$$

Das Zeichen $\sim$ hat hier eine ganz präzise Bedeutung. Wenn f und g zwei Funktionen der reellen Variablen x sind, schreiben wir "$f(x) \sim g(x)$ für $x \to \infty$", um anzuzeigen, dass

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$

gilt.

Der Primzahlsatz gibt eine erste Approximation für die Anzahl der Primzahlen. Auch heute noch, hundert Jahre nach seiner Entdeckung, ist sein Beweis nicht einfach. In einem Kurs über Funktionentheorie (Residuen, Wegintegrale, etc.) kann man den Beweis in, sagen wir, zwei Stunden geben. Dies ist durchaus vergleichbar mit anderen grossen Sätzen der Funktionentheorie; der Beweis des Riemannschen Abbildungssatzes zum Beispiel benötigt einen ähnlichen Aufwand.

Wir kommen nun zu den andern Fragen über Primzahlen zurück, die wir gestellt haben. Nehmen wir zuerst die Frage über die Primzahlzwillinge. Wir gehen wiederum davon aus, dass für eine ganze Zahl n die Wahrscheinlichkeit, eine Primzahl zu sein, durch $1/\log n$ gegeben ist. Diese Tatsache wollen wir akzeptieren. Können Sie eine Vermutung formulieren, welche die Wahrscheinlichkeit angibt, dass die Zahlen n und $n+2$ Primzahlzwillinge sind? (Ein Student gibt nach einigen Fehlversuchen die korrekte Antwort.) Ja, die Wahrscheinlichkeit sollte

$$\frac{1}{\log n} \cdot \frac{1}{\log(n+2)}$$

betragen. Für grosse n liegt $\log(n+2)$ sehr nahe bei $\log n$. Deshalb können wir anstelle des obigen Produktes das Quadrat

$$\frac{1}{(\log n)^2}$$

schreiben. Wie oben können wir zum entsprechenden Integral übergehen und dieses mit partieller Integration umformen. Bezeichnen wir mit $\pi_Z(x)$ die Anzahl der Primzahlzwillinge unter den Zahlen $2, 3, 4, \ldots, x$, dann lautet die Vermutung also, dass $\pi_Z(x)$ ungefähr durch

$$\frac{x}{(\log x)^2}$$

gegeben wird. Aber wenn ich diesen Ausdruck hinschreibe, so nehme ich implizit an, dass die Wahrscheinlichkeiten unabhängig sind! Sind sie unabhängig? Die Antwort ist "Nein". Wir müssen deshalb vorsichtiger sein, wenn wir diese Formel hinschreiben. Die Antwort ist, dass die Anzahl der Primzahlzwillinge $\pi_Z(x)$ der asymptotischen Formel

$$\pi_Z(x) \sim C_Z \frac{x}{(\log x)^2}$$

oder besser

$$\pi_Z(x) \sim C_Z \int_2^x \frac{1}{(\log t)^2}\, dt$$

genügt, wo C_Z eine positive Konstante ist, welche die wahrscheinlichkeitstheoretischen Abhängigkeiten beschreibt. Das Problem ist dann, diese Konstante C_Z zu berechnen. Wir werden weiter unten eine explizite, allerdings recht komplizierte Formel für diese Konstante angeben und zwar in Form eines unendlichen Produktes. Die Geschichte der Konstanten C_Z ist sehr interessant. Sylvester in 1871 und Brun in 1915 haben einen falschen Ausdruck dafür angegeben, weil sie verschiedene versteckte wahrscheinlichkeitstheoretische Abhängigkeiten zwischen Primzahlen übersehen haben. Hardy und Littlewood haben dies 1923 [HaL 23] festgestellt, und sie haben ihrerseits eine Vermutung für den "richtigen" Wert formuliert. "Richtig" bedeutet in diesem Zusammenhang, dass man eine Tabelle für die Werte von $\pi_Z(x)$ und die Werte von

$$C_Z \frac{x}{(\log x)^2}$$

aufstellen kann, welche die Vermutung von Hardy-Littlewood empirisch verifiziert. Wir haben hier "richtig" also im Sinne der Physik gebraucht. Der Wert, den Hardy und Littlewood für die Konstante C_Z angeben, ist

$$C_Z = 2 \cdot \prod_{p \text{ ungerade}} \left(1 - \frac{1}{(p-1)^2}\right),$$

wo das Produkt über alle ungeraden Primzahlen p zu erstrecken ist.

Wir kommen nun zu der dritten Frage. Was ist die asymptotische Abschätzung für die Anzahl $\pi_Q(x)$ von Primzahlen $p \leq x$ mit $p = k^2 + 1$ für eine gewisse positive ganze Zahl k? Mit der selben heuristischen Technik wie oben haben wir die Wahrscheinlichkeit zu beschreiben, dass n von der Form $n = k^2 + 1$ und eine Primzahl ist. Diese Wahrscheinlichkeit sollte durch

$$\frac{1}{\log n} \cdot \frac{1}{\sqrt{n}}$$

gegeben sein. Wegen $\log \sqrt{x} = \frac{1}{2} \log x$, kommt es bis auf einen konstanten Faktor nicht drauf an, ob wir $\log n$ oder $\log \sqrt{n}$ schreiben. Wir können dann die Summe

$$\sum_{2 \leq n \leq x} \frac{1}{\log n} \cdot \frac{1}{\sqrt{n}}$$

bilden oder das Integral

$$\int_2^x \frac{1}{\sqrt{t} \cdot \log t}\, dt\,.$$

Wiederum behandeln wir das Integral mit partieller Integration und werden damit zu der folgenden Vermutung geführt:

$$\pi_Q(x) \sim C_Q \frac{\sqrt{x}}{\log x}\,.$$

Ähnlich wie oben beschreibt hier die Konstante C_Q die verborgenen wahrscheinlichkeitstheoretischen Abhängigkeiten. Hardy-Littlewood haben auch für diese Konstante C_Q eine Vermutung formuliert; sie lautet

$$C_Q = \prod_{p \text{ ungerade}} \left(1 - \frac{\chi(p)}{p-1}\right) .$$

Dabei ist das Produkt wiederum über alle ungeraden Primzahlen p zu erstrecken, und $\chi(p)$ ist wie folgt definiert: $\chi(p) = 1$ falls -1 ein Quadrat mod p ist, das heisst, wenn $x^2 + 1 \equiv 0 \bmod p$ eine Lösung hat, und $\chi(p) = -1$ falls -1 kein Quadrat mod p ist. (Siehe dazu Lang-Trotter [LaT 76], Part II, insbesondere S. 81, Example 1, wo diese Konstante mit Hilfe eines völlig anderen wahrscheinlichkeitstheoretischen Modells berechnet wurde.)

(Ein Student fragt, wie man auf solche Vermutungen geführt werde.) Ja, lassen Sie mich auf diese Frage eingehen. Wie kommt man auf die Idee, dass es unendlich viele Primzahlzwillinge oder Primzahlen von der Form $k^2 + 1$ gibt? Betrachten Sie das, was wir bis anhin gemacht haben als eine Art Antwort? Ja? So ungefähr? Ja, es ist wenigstens etwas; es suggeriert nicht nur, dass es unendlich viele gibt, sondern es gibt Ihnen auch ein qualitatives Mass für ihre Anzahl an. Man kann dieses wahrscheinlichkeitstheoretische Modell weiterentwickeln und es verfeinern, wie Hardy-Littlewood es getan haben, um die oben angegebenen Werte für die Konstanten zu erhalten und genauere Aussagen über die Anzahl zu gewinnen. Ich möchte Ihnen im Falle von $\pi(x)$ einen Weg skizzieren, der, folgt man ihm in analoger Weise in den anderen Fällen, schliesslich den Ausdruck in Form eines unendlichen Produktes für die Konstanten liefert. Sie nehmen alle Zahlen 1, 2, 3, 4, 5, 6, $\ldots, x$. Wie viele davon sind durch 2 teilbar? Ungefähr $x/2$. Die Anzahl ganzer Zahlen, kleiner oder gleich x, die nicht durch 2 teilbar sind, ist folglich ungefähr

$$\left(1 - \frac{1}{2}\right) x .$$

Die Anzahl ganzer Zahlen, die nicht durch 3 teilbar sind, ist im wesentlichen gegeben durch

$$\left(1 - \frac{1}{3}\right) x .$$

Die Anzahl ganzer Zahlen, die nicht durch 5 teilbar sind, ist ungefähr gleich

$$\left(1 - \frac{1}{5}\right) x .$$

Um die Anzahl $\pi(x)$ von Primzahlen kleiner oder gleich x zu erhalten, müssen wir uns überlegen, wieviele ganze Zahlen nicht durch 2, nicht durch 3, nicht durch 5 usw. teilbar sind. Wieviele wird man erhalten? Die Antwort ist, grob gesprochen,

$$G(x) \cdot x , \quad G(x) = \prod_{2 \le p \le x} \left(1 - \frac{1}{p}\right) ,$$

wo sich das Produkt über alle Primzahlen erstreckt. Dies ist ein Anfang, um den korrekten Wert der Konstanten für $\pi(x)$ zu bestimmen. Allerdings haben wir hier angenommen, dass die Bedingungen der Nichtteilbarkeit unabhängig sind. In Tat und Wahrheit sind sie dies nicht. Eine offensichtliche solche Abhängigkeit ist zum Beispiel die folgende. Wenn eine ganze Zahl n durch eine Primzahl teilbar ist, so ist sie auch teilbar durch eine Primzahl, die kleiner oder gleich $\sqrt{n}$ ist. Das Produkt in der obigen Formel darf also auf Primzahlen p mit $p \leq \sqrt{n}$ eingeschränkt werden. Wegen dieser und vielen anderen nicht so offensichtlichen Abhängigkeiten müssen wir in der obigen Formel den durch $G(x)$ gegebenen Bruchteil mit einer Konstanten multiplizieren, welche diesen Bedingungen Rechnung trägt. Es zeigt sich, dass die Konstante hier durch e^{γ} gegeben ist, wo γ die Euler-Konstante bezeichnet. Es ist ein Resultat von Mertens, dass die asymptotische Beziehung

$$e^{\gamma} \cdot G(x) \sim \frac{1}{\log x}$$

besteht und dass deshalb

$$\pi(x) \sim e^{\gamma} \cdot G(x) \cdot x \sim \frac{x}{\log x}$$

gilt. (Über die Gründe, weshalb hier die Konstante e^{γ} auftritt, können Sie eine Diskussion in der Arbeit von Hardy und Littlewood [HaL 23] finden; siehe auch Hardy and Wright [HaW 60], Chapter 22, 22.20.)

Wir kommen schliesslich zur grundlegenden Frage: Wie gut ist das Fehlerglied? Diese Frage wird uns zur berühmten Riemannschen Vermutung führen. Nehmen Sie an, Sie hätten eine wahrscheinlichkeitstheoretisch zufällige Verteilung. Wenn Sie die Summe nehmen, welche $\pi(x)$ approximiert, oder das Integral

$$\pi(x) = \int_2^x \frac{1}{\log t}\, dt + F(x) = \mathrm{Li}(x) + F(x)$$

wo $\mathrm{Li}(x)$ das Integral

$$\int_2^x \frac{1}{\log t}\, dt$$

bezeichnet und $F(x)$ das entsprechende Fehlerglied ist, was wird dann die Abschätzung für $F(x)$ sein? Die Vermutung im wahrscheinlichkeitstheoretischen Modell ist, dass eine Konstante C existiert mit

$$|F(x)| \leq C \cdot (\sqrt{x} \cdot \log x)\ .$$

Diese Abschätzung besagt, dass der absolute Betrag des Fehlergliedes $F(x)$ verglichen mit dem Hauptterm $x/\log x$ sehr klein ist.[1]) Es ist übrigens einfach zu sehen, dass die Konstante C klein ist, wenn sie überhaupt existiert. In der Arbeit [Sch 76] hat Schoenfeld unter der Voraussetzung, dass C existiert, für $x > 2657$ die Abschätzung

$$|F(x)| = |\pi(x) - \mathrm{Li}(x)| \leq \frac{1}{8\pi}\sqrt{x} \cdot \log x$$

1) Ich danke Hugh Montgomery, der mich auf verschiedene Literaturstellen über diese Konstante hingewiesen hat, insbesondere auf [Sch 76].

bewiesen. Die Werte für $x \leq 2657$ können leicht berechnet werden. Wenn man dies tut, so erhält man auch einen Eindruck davon, wie gut die Approximation von $\pi(x)$ durch $\mathrm{Li}(x)$ ist. Die Vermutung, dass das Fehlerglied durch

$$|F(x)| \leq C(\sqrt{x} \cdot \log x)$$

abgeschätzt werden kann, ist die berühmte *Riemannsche Vermutung*, welche nach der übereinstimmenden Meinung der Mathematiker die grösste bis heute nicht bewiesene Vermutung in der Mathematik ist.

Das Problem der Abschätzung der Anzahl Primzahlen, wurde im Laufe unserer Überlegungen auf die Aufgabe zurückgeführt, dem wahrscheinlichkeitstheoretischen Modell eine präzise Bedeutung zu geben und das Fehlerglied so genau wie möglich abzuschätzen. In wahrscheinlichkeitstheoretischen Begriffen sagt die Riemannsche Vermutung, dass die Folge der Primzahlen sich wie eine zufällige Folge im wahrscheinlichkeitstheoretischen Modell verhält, in welchem die Wahrscheinlichkeit dafür, dass n eine Primzahl ist, durch $1/\log n$ gegeben ist.

Es gibt andere Phänomene in der Zahlentheorie (und anderswo), die auf ähnliche Weise beschrieben werden können. Man konstruiert sich ein wahrscheinlichkeitstheoretisches Modell. Nach dem Gesetz der grossen Zahlen kennt man darin das Fehlerglied für eine zufällige Folge. Die zugehörige Vermutung lautet dann, dass eine gegebene Folge — wie hier die Folge der Primzahlen — sich wie eine zufällige Folge in diesem Modell verhält. (Siehe [LaT 76] für solche wahrscheinlichkeitstheoretische Modelle für verschiedene andere Probleme der Zahlentheorie.)

Wir haben hier die Riemannsche Vermutung formuliert, ohne irgend etwas, ausser die Definition der Primzahl und die Definition des Logarithmus zu benötigen. Manchmal, oder sogar üblicherweise wird sie in komplizierterer Weise mit Hilfe von Begriffen der komplexen Analysis formuliert. Man definiert die sogenannte *Zetafunktion* wie folgt. Für komplexe Zahlen s mit $\mathrm{Re}(s) > 1$ ist sie durch die Formel

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

definiert, wo das Produkt über alle Primzahlen p zu erstrecken ist. Man zeigt dann, dass diese Funktion für alle komplexen Zahlen mit $\mathrm{Re}(s) > 0$ eine meromorphe Fortsetzung besitzt. Die Riemannsche Vermutung ist dann gleichbedeutend mit der Vermutung, dass alle Nullstellen von $\zeta(s)$ mit $0 < \mathrm{Re}(s) < 1$ auf der Geraden $\frac{1}{2} + it$ liegen. Man braucht wiederum ungefähr zwei Stunden (nach einem Kurs in Funktionentheorie), um zu zeigen, dass die beiden hier angegebenen Formulierungen der Riemannschen Vermutung äquivalent sind.

Lassen Sie mich schliessen mit einem Problem, welches sich an unsere Frage anschliesst, ob es unendlich viele Primzahlen von der Form $k^2 + 1$ gibt. Statt $k^2 + 1$ wollen wir allgemeiner ein Polynom $f(t)$ mit ganzzahligen Koeffizienten ansehen. Wir fragen, ob es unendlich viele ganze Zahlen k gibt, mit der Eigenschaft, dass $f(k)$ eine Primzahl

ist. Es ist offensichtlich, dass f einige notwendige Bedingungen erfüllen muss. Erstens, wenn wir schreiben

$$f(t) = a_d t^d + \cdots + a_1 t + a_0 ,$$

mit ganzen Zahlen $a_0, a_1, \ldots, a_d$ und $a_d \neq 0$, dann müssen wir $a_d > 0$ voraussetzen. Zweitens muss das Polynom f irreduzibel sein. Drittens, wenn wir die Werte $f(k)$ für $k \in \mathbf{Z}$ betrachten, so darf es keine Primzahl p geben, die alle diese Werte teilt. Um letzteres zu illustrieren rufen wir in Erinnerung, dass für alle ganzen Zahlen k die Äquivalenz $k^3 \equiv k \bmod 3$ gilt. Die Werte des Polynoms $t^3 - t - 3$ sind folglich alle durch 3 teilbar, obschon dieses Polynom über den rationalen Zahlen irreduzibel ist. Es kann folglich nicht unendlich viele Primzahlen repräsentieren. Die Primzahl 3 lässt sich in diesem Beispiel übrigens durch irgend eine Primzahl ersetzen: ist p eine beliebige Primzahl, so ist das Polynom $t^p - t - p$ irreduzibel über den rationalen Zahlen, aber für jede ganze Zahl k ist $k^p - k - p$ durch p teilbar. Es ist eine Vermutung von Bouniakowsky, dass diese drei Bedingungen auch hinreichend sind: Erfüllt das Polynom f die drei oben genannten Bedingungen, dann gibt es unendlich viele positive ganze Zahlen k mit der Eigenschaft, dass $f(k)$ eine Primzahl ist [Bou 1854]. Für $f(t) = at + b$ mit a und b relativ teilerfremde ganze Zahlen und $a > 0$ besagt die Vermutung, dass es in der durch $at + b$ gegebenen arithmetischen Progression unendlich viele Primzahlen gibt. Wie einige von Ihnen vielleicht wissen, ist dies ein berühmtes Resultat von Dirichlet. Dieser Spezialfall der Vermutung ist also bewiesen.

Schinzel hat die Vermutung von Bouniakowsky später wiederentdeckt und auf den Fall mehrerer Polynome verallgemeinert [SchS 58].[2]) Es seien $f_1, f_2, \ldots, f_r$ Polynome mit ganzzahligen Koeffizienten. Sie sollen die folgenden drei Bedingungen erfüllen:

- der höchste Koeffizient von f_i für $i = 1, 2, \ldots, r$ ist positiv;
- das Polynom f_i für $i = 1, 2, \ldots, r$ ist irreduzibel über den rationalen Zahlen;
- es gibt keine Primzahl, die für alle positiven ganzen Zahlen k das Produkt $f_1(k) \cdot f_2(k) \cdots f_r(k)$ teilt.

Unter diesen Voraussetungen vermutete Schinzel, dass es unendlich viele positive ganze Zahlen k gibt mit der Eigenschaft, dass die Werte $f_i(k)$ für $i = 1, 2, \ldots, r$ Primzahlen sind. Für das Paar von Polynomen $f_1(t) = t$ und $f_2(t) = t + 2$ stimmt diese Vermutung mit der früheren überein, dass es unendlich viele Primzahlzwillinge gibt.

Es gibt auch eine quantitative Formulierung der Vermutung von Bouniakowsky-Schinzel. Es seien $d_1, d_2, \ldots, d_r$ die Grade der Polynome $f_1, f_2, \ldots, f_r$. Der Einfachheit halber schreiben wir in Vektorschreibweise $(f) = (f_1, f_2, \ldots, f_r)$. Wir definieren $\pi_{(f)}(x)$ als die Anzahl der positiven ganzen Zahlen $k \leq x$ mit der Eigenschaft, dass die Werte $f_1(k), f_2(k), \ldots, f_r(k)$ alle Primzahlen sind. (Wir ignorieren dabei die endliche Anzahl der Werte von k, für welche einer (oder mehrere) der Werte $f_i(k)$ negativ ist.) Unter den gleichen Bedingungen, die oben bei der Vermutung von Bouniakowsky-Schinzel genannt worden sind, haben Bateman und Horn [BaH 62] vermutet, dass

$$\pi_{(f)}(x) \sim (d_1 d_2 \cdots d_r)^{-1} \cdot C(f) \cdot \int_2^x \frac{1}{(\log t)^r}\, dt ,$$

2) Man vergleiche dazu die Diskussion in der Einleitung von [HaR 74].

gilt, wo $C(f)$ durch die Formel

$$C(f) = \prod_p \left((1 - \frac{1}{p})^{-r} \cdot (1 - \frac{N_{(f)}(p)}{p}) \right) ,$$

gegeben ist. Hier ist das Produkt über alle Primzahlen p zu erstrecken, und $N_{(f)}(p)$ bezeichnet die Anzahl Lösungen der Kongruenz

$$f_1(k) \cdot f_2(k) \cdots f_r(k) \equiv 0 \bmod p \ .$$

Falls $N_{(f)}(p) = p$ für eine Primzahl p, dann gilt $C(f) = 0$ und

$$\pi_{(f)}(x) \leq d_1 + d_2 + \cdots + d_r$$

für alle x; wir sehen hier von diesem trivialen Fall ab. Bateman und Horn haben ihre Vermutung heuristisch untermauert, insbesondere haben sie Computerberechnungen durchgeführt. Man beachte, dass, für $r = 1$ und $f(t) = f_1(t) = t^2 + 1$ die Vermutung von Bateman-Horn im wesentlichen mit der Vermutung von Hardy-Littlewood übereinstimmt, welche von Primzahlen der Form $k^2 + 1$ handelt.

Der Ausdruck für die Konstante $C(f)$ vor dem logarithmischen Integral ist ein Beispiel eines ganz allgemeinen Phänomens, das bei der Lösung von Gleichungen auftritt. Die Dichte der Lösungen wird ausgedrückt durch lokale Dichten, welche einerseits das Verhalten modulo der Primzahlen beschreiben und andererseits das Verhalten über den reellen Zahlen. In unserem Beispiel beschreibt der Faktor, in welchem die Grade der Polynome auftreten, eine Abschätzung über den reellen Zahlen. Der Faktor, welche die Primzahl p enthält, beschreibt das Verhalten modulo p, insbesondere die Lösungsanzahl modulo p. In [HaL 23] und [LaT 76] sind weitere Beispiele zu finden, bei denen ganz analoge Phänomene auftreten.

Bibliographie

[BaH 62] P. Bateman und R. Horn: A heuristic asymptotic formula concerning the distribution of prime numbers, Math. Comp. 16 (1962) pp. 363–367

[Bou 1854] V.J. Bouniakowsky, Sur les diviseurs numériques invariables des fonctions rationelles entières, Mem. Sc. Math. et Phys. T VI (1854), pp. 307–329

[Br 15] V. Brun: Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare. Archiv for Math. (Christiania) 34 Part 2 (1915) pp. 1–15

[HaR 74] H. Halberstam und H. Richert, *Sieve Methods*. Academic Press, 1974

[HaL 23] G. H. Hardy und J.E. Littlewood: Some problems of "partitio Numerorum"; III: On the expression of a number as a sum of primes. Acta Math. 44 (1923) pp. 1-70

[HaW 80] G.H. Hardy und E.M. Wright: *"An Introduction to the Theory of Numbers"*. Fourth Edition, Oxford University Press, 1980

[LaT 76] S. Lang und H. Trotter: Frobenius distributions in GL_2-extensions. Springer Lecture Notes 504, Springer-Verlag 1976

[SchS 58] A. Schinzel und W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers. Acta Arith. 4 (1958) pp. 185–208

[Sch 76] L. Schoenfeld: Some sharper Tchebychev estimates II. Math. Comp. 30 (1976) pp. 337–360

[Syl 1871] J. Sylvester: On the partition of an even number into two prime numbers. Nature 56 (1896–1897) pp. 196-197 (= Math. Papers 4 pp. 734–737)

Serge Lang
Yale University
New Haven
Connecticut 06520, USA

Unter den vielen Büchern, die Serge Lang veröffentlicht hat, beanspruchen im Zusammenhang mit seinem Artikel die folgenden zwei unmittelbares Interesse. Sie enthalten eine Reihe von Vorträge, die er an ein allgemeines Publikum beziehungsweise an eine Schulklasse richtete.

Serge Lang: *The beauty of doing mathematics. Three public dialogues.* Springer 1985. Deutsche Übersetzung: *Faszination Mathematik. Ein Wissenschaftler stellt sich der Öffentlichkeit.* Vieweg Verlagsgesellschaft 1989

(Besprechung in "Elemente der Mathematik": Vol. 42 (1987) p. 81 (Hj. Stocker)).

Serge Lang: *Math! Encounters with High School Students.* Springer-Verlag, 1985. Deutsche Übersetzung: *Mathe! Begegnung eines Wissenschaftlers mit Schülern.* Vieweg Verlagsgesellschaft 1991.

(Besprechung in "Elemente der Mathematik": Vol. 43 (1988) p. 64 (H. Zeitler)).