Primzahlen und Parallelrechner

Oder: Was 3 und 5 mit 37.399.999.577 und 37.399.999.579 gemeinsam haben

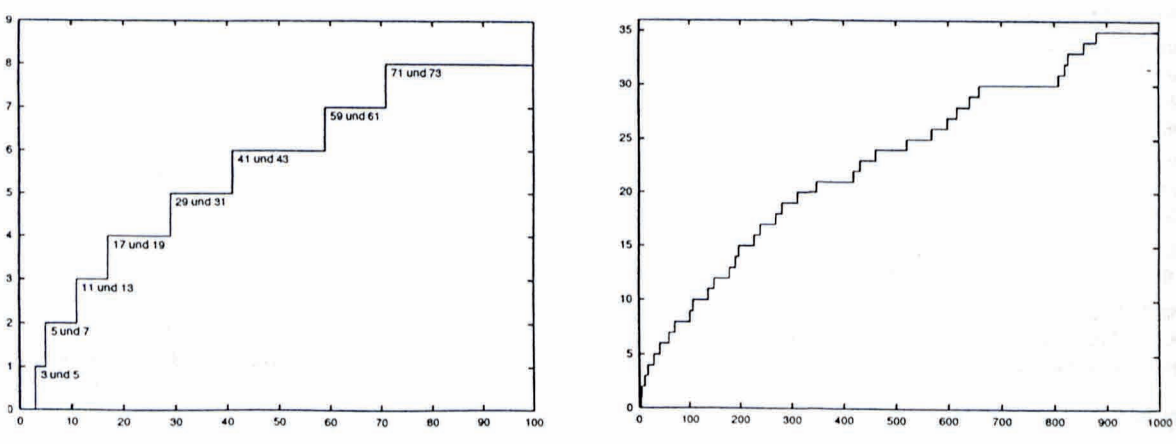
■ Von Martin Kutrib und Jörg Richstein

Noch haben die natürlichen Zahlen lange nicht alle ihre Geheimnisse preisgegeben. Scheinbar leichte Probleme entpuppen sich als sehr harte Nüsse, denen man auch vermehrt mit Hilfe moderner Parallelrechner auf die Schale rückt. Umgekehrt halfen Primzahlen dabei, einen Prozessorfehler aufzudekken, der eine amerikanische Firma knapp eine halbe Milliarde Dollar kostete.

Primzahlen sind die vielleicht geheimnisvollsten Objekte in der Mathematik überhaupt. Ihr Auftreten ist völlig unvorhersagbar, man kann im allgemeinen einer Zahl durch kein einfaches Merkmal ansehen, ob sie prim ist oder nicht.
Primzahlen sind die Bausteine aller natürlichen Zahlen, jede Zahl läßt sich auf eindeutige Weise als Produkt von Primzahlen darstellen. So setzt sich etwa die Zahl 42 aus den Faktoren 2, 3 und 7 zusammen, 524.895.005.199 ergibt sich aus dem Produkt der Primzahlen 3, 127, 5.881 und 234.259, während beispielsweise 524.895.005.197 selbst prim ist und somit keine weiteren Faktoren außer sich selbst (und der Zahl 1) besitzt. Die kleinste (und einzige gerade) Primzahl ist die 2, die größte, heute bekannte Primzahl 2^{859433}-1, eine gigantische Zahl mit 258.716 Stellen, die drei Ausgaben dieser Zeitschrift füllen würde.
Die Mathematiker wissen schon lange, daß die Anzahl der Primzahlen über alle Grenzen wächst. Im scheinbaren Widerspruch dazu tauchen Primzahlen immer seltener auf, je weiter man das Suchintervall in Richtung größerer Zahlen verschiebt. So gibt es zwischen 1 und 1.000 noch 168 Primzahlen, zwischen 10.000 und 11.000 gerade 106 und zwischen 100.000 und 101.000 nur noch 81. Die Paradoxie zwischen ihrem unendlich oftmaligen Auftreten einerseits und ihrer Ausdünnung andererseits erfährt noch eine gewisse Steigerung: Man kann die Länge des Suchintervalls so groß wählen, wie man will, man wird immer ein entsprechendes Intervall dieser Länge finden, das nur aus zerlegbaren Zahlen besteht, also primzahlfrei ist.

Primzahlzwillinge

Es stellt sich die Frage, ob ihre Ausdünnung darauf hindeutet, daß der Abstand zwischen zwei aufeinanderfolgenden Primzahlen allgemein immer größer wird. Oder kommen sie sich vielleicht doch „immer mal wieder" sehr nahe? Die einzigen Primzahlen mit Abstand 1 sind 2 und 3, alle weiteren sind ungerade und daher mindestens durch den Abstand 2 voneinander getrennt. Die Folge dieser Paare mit Abstand 2 beginnt mit 3 und 5, 5 und 7, 11 und 13, 17 und 19, 29 und 31, 41 und 43, ... Man nennt sie aufgrund ihrer Nähe zueinander *Primzahlzwillinge*. Es ist relativ wenig, jedoch einiges Spektakuläres über die Primzahlzwillinge bekannt.
Es scheint zunächst so, daß sehr viele der Primzahlen Teil eines Zwillingspaares sind. Tatsächlich dünnen sie sich jedoch schnell aus. So gibt es unter den 168 Primzahlen unter 1.000 nur noch 69, die Teil eines Zwillingspaares sind. Das größte, bis heute gefundene Paar besteht aus den beiden 4.932stelligen Zahlen $697.053.813 \cdot 2^{16352} \pm 1$ und wurde Anfang dieses Jahres an der Universität Paderborn gefunden. Der Versuch, die Anzahl der Primzahlzwillinge unterhalb einer vorgegebenen Schranke durch eine möglichst einfache Formel voraussagen zu können, hat sich als sehr hartnäkkiges Problem der Zahlentheorie erwiesen. Bereits die Frage, ob es überhaupt unendlich viele Primzahlzwillinge gibt, stellt sich



Primzahlzwillinge scheinen zunächst völlig unregelmäßig aufzutreten. Je größer aber das betrachtete Intervall wird, desto mehr kristallisiert sich ein gleichmäßiges Erscheinen heraus.

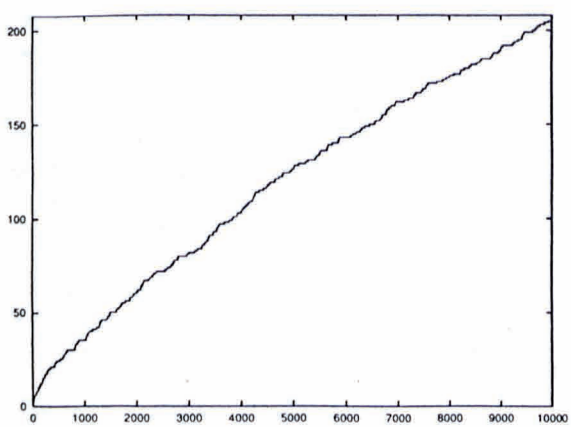
schnell als außerordentlich schwierig heraus.
Der Zahlentheoretiker Edmund Landau (1877 bis 1938) schrieb dazu im Jahre 1927: *„Die Mittel der Zahlentheorie und der Analysis sind bis heute nicht kräftig genug, um diese Frage zu beantworten (Man würde wohl auf ‚ja' wetten)."*
Diese Aussage gilt heute immer noch. Noch immer weiß man nicht, ob es unendlich viele Primzahlzwillingspaare gibt. Bereits seit Mitte des letzten Jahrhunderts wird dies jedoch zumindest vermutet.
Die beiden britischen Mathematiker Godfrey Harold Hardy (1877 bis 1947) und John Edensor Littlewood (1885 bis 1977) vermuteten 1923 eine Näherungsformel für die Anzahl der Primzahlzwillinge unterhalb einer Schranke x, in der mathematischen Notation $\pi_2(x)$, sprich: *pi zwei von x*. Diese Formel, die implizit aussagt, daß es unendlich viele Zwillinge gibt, konnte bis heute nicht bewiesen werden.

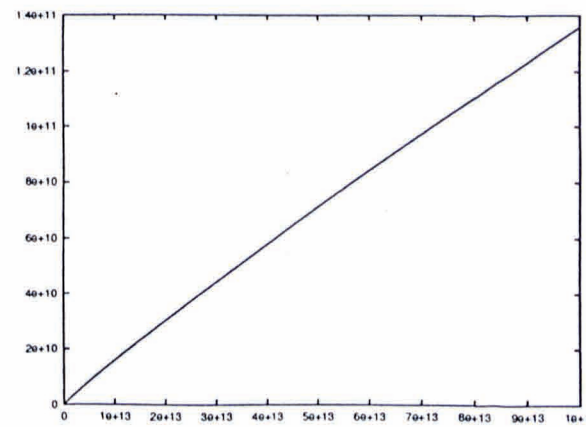
Der Brunsche Primzahlzwillingssatz

Ein höchst interessantes Ergebnis im Zusammenhang mit der Häufigkeit des Auftretens der Zwillingspaare ist im Jahre 1919 von dem norwegischen Mathematiker Viggo Brun erzielt worden: Er untersuchte das Verhalten der Reihe über ihre Kehrwerte, also

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{17}+\frac{1}{19}\right)+\cdots$$

Wenn man sich nicht auf Primzahlzwillinge beschränkt, sondern die Kehrwerte sämtlicher Primzahlen addiert, wächst die Reihe trotz immer kleiner werdender Summanden ins Unendliche, wie der berühmte Mathematiker Leonhard Euler (1707 bis 1783) zeigte. Was geschieht aber nun, wenn man nur Zwillinge in die Summe aufnimmt? Hat man genug Primzahlen herausgenommen, so daß die Reihe konvergiert, also einem Grenzwert entgegenstrebt? Falls es nur endlich viele Primzahlzwillinge gäbe, so würde die Reihe auf eine endliche Summe schrumpfen und wäre auch konvergent. Was geschieht im Falle der Unbeschränktheit von $\pi_2(x)$? Bruns berühmter Primzahlzwillingssatz gibt Antwort darauf: Selbst in diesem Falle bleibt die Reihe über ihre Kehrwerte beschränkt. Man hat also tatsächlich die Schranke hin zur Konvergenz überwunden. Der Grenzwert der Summe wird als *Brunsche Konstante* bezeichnet. Ihre exakte Größe ist bis heute nicht bekannt (Brun wies die Existenz nach, ohne dabei explizit einen Wert anzugeben). Unter Annahme der Richtigkeit der Hardy/Littlewoodschen Vermutung kann man aus den Ergebnissen von Zählungen einen Wert für die Brunsche Konstante extrapolieren, der etwa bei 1,90216 liegt.





Martin Kutrib hat Informatik und Raumflugtechnik an der Technischen Universität Braunschweig studiert. Seit 1989 ist er in der AG Informatik am Mathematischen Institut tätig, wo er 1993 promoviert wurde. Zwischenzeitlich war er ein Jahr an der Universität-GH Siegen beschäftigt. Sein besonderes wissenschaftliches Interesse gilt neben der Theorie der Polyautomaten der Komplexitätstheorie und der Parallelität in Algorithmen und Programmiersprachen.

Zählungen von Primzahlzwillingen

Man begann bereits relativ früh damit, Zählungen von Primzahlzwillingen durchzuführen, um Vermutungen über sie zu bekräftigen oder neue Erkenntnisse gewinnen zu können. Die erste größere, bekannte Zählung wurde von dem Briten J. W. L. Glaisher im Jahre 1878 durchgeführt und umfaßte das Intervall von 1 bis 100.000 (sowie fünf weitere, ebenso lange Intervalle beginnend bei 1.000.000, 2.000.000, 6.000.000, 7.000.000 und 8.000.000). Im Verlauf der letzten Jahrhunderte waren bereits des öfteren Tabellen mit Primzahlen erstellt worden, aus denen man natürlich recht einfach die Anzahl der Zwillinge hätte herausfinden können. So weist Leonhard Euler in seinem Werk „Vollständige Anleitung zur niedern und höheren Algebra" in einer Fußnote auf die Existenz einer Tabelle aus dem Jahre 1746 hin, die sämtliche Primzahlen bis 100.000 enthält. Dabei befaßte man sich jedoch nicht explizit mit Primzahlzwillingen, so daß Glaishers Arbeit wohl als Beginn umfangreicher Zählungen anzusehen ist.

Im Jahre 1923 wurde von Frau G. A. Streatfeild für Hardy und Littlewood eine Zählung aller Primzahlzwillinge bis 1.000.000 vorgenommen, die der Überprüfung der Hardy/Littlewoodschen Vermutung diente. Der Vergleich von vorhergesagten Werten und der tatsächlichen Anzahl ergab eine beeindruckende Übereinstimmung.

Die Intervallgrenzen dieser sämtlich von Hand und mit durchweg erstaunlicher Präzision (wenn auch zum Teil nicht völlig fehlerfrei) durchgeführten Berechnungen wurden mit der Einführung elektronischer Rechenmaschinen schnell übertroffen. Die bis Anfang letzten Jahres weitreichendste Zählung stammt von dem australischen Mathematiker Richard P. Brent, der die Anzahl aller Primzahlzwillinge und die Summe ihrer Kehrwerte bis 10^{11} ermittelte.

Diesen Wert konnten wir im Januar 1994 um eine Zehnerpotenz steigern. Weitere Arbeiten ergaben bis Mai des letzten Jahres die Resultate bis 10^{13}. Eine nochmalige Verschiebung dieser Grenze erschien zunächst mit den seinerzeit zur Verfügung stehenden Methoden äußerst schwierig.

Zählungen von Primzahlzwillingen hatten bis dahin sicher wenig Einfluß auf unser alltägliches Leben. Mit einer Entdeckung des amerikanischen Mathematikers Thomas Nicely änderte sich dies jedoch zumindest für zahlreiche Computeranwender in aller Welt. Etwa zeitgleich mit uns (und ohne Wissen voneinander) hatte er begonnen, sich mit Primzahlzwillingen zu beschäftigen. Dabei begann er im März 1994 damit, auch einen Computer mit dem sogenannten Pentium-Prozessor der Firma Intel zu verwenden. Irgendwann schlich sich ein Fehler in die Berechnung der Summe der Kehrwerte ein. Er ging der Sache nach und konnte nach etlichen Tests feststellen, daß es nur der Prozessor selbst sein konnte, der den Fehler produzierte. Diese Entdeckung führte schließlich dazu, daß Intel anbot, sämtliche schon ausgelieferten Prozessoren auszutauschen. Nicelys Angaben zufolge kostete diese Austauschaktion insgesamt etwa 470 Millionen Dollar. In Gießen sind inzwischen fünf verschiedene Prozessortypen zum Einsatz gekommen, darunter allerdings kein einziger Pentium. Ein Austausch von Ergebnissen, der seit Anfang des Jahres mit Nicely stattfindet, hat bisher keine weiteren Unstimmigkeiten ergeben.

Ermittlung der Anzahl von Primzahlzwillingen

Ein Verfahren, das auf den Astronom E. D. F. Meissel aus dem Jahre 1870 zurückgeht, ermöglicht es, die Anzahl aller Primzahlen bis zu einer gewissen Schranke exakt zu berechnen, ohne dabei vorher jede einzelne explizit bestimmt haben zu müssen. Im vergangenen Jahr wurde mit einer Weiterentwicklung dieses Algorithmus an der Universität Lyon die Anzahl aller Primzahlen bis 10^{18} berechnet.

Leider ist kein vergleichbares Verfahren zur Ermittlung der Anzahl von Primzahlzwillingen bekannt, so daß man auf andere Methoden zurückgreifen muß. Ein Verfahren zur Bestimmung der Primzahlzwillinge in einem Intervall 1 bis x kann zum Beispiel auf einem Verfahren zur Berechnung aller Primzahlen in diesem Intervall basieren.

Das Sieb des Eratosthenes

Ein solches Verfahren wurde bereits von dem griechischen Philosophen und Leiter der Bibliothek von Alexandria, Eratosthenes von Cyrene (276 bis 195 v. Chr.) entwickelt. Es ist heute unter dem Namen „Sieb des Eratosthenes" bekannt: Man schreibe alle Zahlen von 1 bis x auf und streiche die Zahl 1 durch. Dann durchlaufe man die Liste beginnend mit 2 und streiche alle Vielfachen dieser Zahl. Dies wird jeweils mit der nächsten, noch nicht gestrichenen Zahl wiederholt. Nach Abarbeiten der Liste bleiben die Prim-

JUSTUS-LIEBIG-
UNIVERSITÄT
GIESSEN

Dr. Martin Kutrib

AG Informatik
Mathematisches Institut
Arndtstraße 2
35392 Gießen
Telefon (0641) 702-2540
email Martin.Kutrib@informatik.uni-giessen.de

Überleben mit Primzahlen

Im Osten der USA kennt man das Phänomen der „periodischen Zikade". 17 Jahre ihres Lebens verbringen die Nymphen dieser Zikaden im Boden und saugen Pflanzensaft aus den Wurzeln von Waldbäumen. Dann – innerhalb weniger Wochen – kriechen Millionen reifer Nymphen aus dem Boden, erledigen ihre letzte Häutung, paaren sich, legen ihre Eier und sterben. Bemerkenswert ist, daß nicht nur eine, sondern drei verschiedene Arten von periodischen Zikaden strikt synchronisiert nach diesem Fahrplan schlüpfen. An einem beliebigen Ort tauchen die drei Arten gleichzeitig auf; allerdings sind verschiedene Gegenden der USA außer Takt: die Zikaden um Chicago erscheinen nicht zur selben Zeit wie in Neuengland. Im Süden der USA gibt es ebenfalls periodische Zikaden, sie halten einen 13jährigen Zyklus ein.

Warum gibt es Zikaden mit 13- oder 17-Jahres-Zyklus, aber keine Zikaden mit Zyklen von 12, 14, 15, 16 oder 18 Jahren? 13 und 17 sind Primzahlen, und die meisten Räuber der Zikaden leben nicht länger als zwei bis fünf Jahre. Eine Zikadenart zum Beispiel mit einem 15jährigen Zyklus würde auf eine Räuberart mit einem fünfjährigen Zyklus in jedem dritten Zyklus treffen. Dadurch, daß die Zikaden eine Primzahl als Periodenlänge wählen, minimieren sie die Wahrscheinlichkeit, daß ihr Auftauchen mit einem Zyklus ihrer Räuber zusammenfällt.
Der Harvard-Professor Stephen Jay Gould hat diese Geschichte erzählt. Der „Kampf ums Überleben" wird nicht immer mit Zähnen und Klauen ausgetragen, sondern auch mit so raffinierten Strategien wie dem Sieb des Eratosthenes. utz

zahlen übrig. Erhebliche Zeiteinsparung bei diesem Verfahren wird durch die Tatsache ermöglicht, daß alle zerlegbaren Zahlen immer einen Faktor haben, der kleiner oder gleich ihrer Wurzel ist. Um also herauszufinden,ob 1.677 eine Primzahl ist, braucht man sie nur probehalber durch alle Zahlen bis 40 zu teilen ($\sqrt{1.677} \cong 40{,}95$ ...).
Das Sieb des Eratosthenes ist das Standardbeispiel für Siebverfahren, bei denen aus einer Tabelle von Zahlen nach Kriterien, die sich aus den in der Tabelle verbliebenen Zahlen ergeben, Elemente herausgestrichen werden. Siebverfahren sind heute in vielen Bereichen der analytischen Zahlentheorie vielseitige Werkzeuge. Zur Berechnung von $\pi_2(x)$ kann prinzipiell ein Primzahlsieb herangezogen werden, wobei die Primzahlen p in der Tabelle nachträglich jeweils daraufhin überprüft werden müssen, ob $p + 2$ ebenfalls prim ist.

Parallelität

Um Primzahlzwillinge über die Schranke von 10^{12} hinaus zu berechnen, muß das Verfahren verbessert werden, da es zuviel Zeit und im Hauptspeicher zuviel Speicherplatz verschlingt. Die Tabelle mit mehr als 10^{12} Zahlen müßte im Hauptspeicher gehalten werden, was heute übliche Speichergrößen immer noch bei weitem übersteigt. Zur Veranschaulichung: Wenn jemand diese Summe beim Lotto gewinnen wollte, so müßte er 19.230 Jahre lang Woche für Woche eine Million Mark gewinnen.

Jörg Richstein studierte in Gießen Mathematik und ist seit einem Jahr Mitarbeiter der Arbeitsgruppe Informatik. Sein wissenschaftliches Interesse gilt der „Computational Number Theory", einem Grenzgebiet zwischen Informatik und Mathematik, in dem zunehmend parallele Algorithmen verwendet werden, um Probleme der Zahlentheorie zu bearbeiten.

Die Zeitkomplexität eines Verfahrens läßt Rückschlüsse auf die tatsächliche Rechenzeit zu, sie hat beim Sieb des Eratosthenes die Ordnung $\mathbf{O}(x \cdot \log\log x)$, das heißt, es existieren natürliche Zahlen x_0 und c, so daß sich für alle Zahlen $x \geq x_0$ die exakte Zeitkomplexität $t(x)$ des Problems abschätzen läßt durch $t(x) \leq c \cdot x \cdot \log x$. Man kann diese Zeitkomplexität verbessern, wenn man mehrere Prozessoren parallel am Problem arbeiten läßt. Jonathan Sorenson von der Universität von Wisconsin in Madison und Ian Parberry von der Universität von North Texas in Denton haben an diesem Problem gearbeitet und zwei schnelle parallele Primzahlsiebe vorgeschlagen. Die Zeitkomplexitäten haben die Ordnungen $\mathbf{O}(\log x)$ beziehungsweise $\mathbf{O}(\sqrt{x})$. Diese Geschwindigkeit wird aber durch die Verwendung von $\mathbf{O}(x \log\log x/\log x)$ beziehungsweise $\mathbf{O}(\sqrt{x})$ Prozessoren teuer erkauft. Um das Problem mit Parallelrechnern angehen zu können, haben wir das zu untersuchende Intervall in mehreren Stufen zerlegt. Die Anzahl der Prozessoren beziehungsweise ihrer Ressourcen ist durch Parametrisierung skalierbar, so daß ein Einsatz auf massiv parallelen Rechnern in Frage kommt. Das Verfahren beruht auf dem „Farmer-Worker-Prinzip": Ein Prozessor – der „Farmer" – koordiniert die Aufteilung des Intervalls und vergibt Teilprobleme an die Arbeitsprozesse – die „Worker" –, die ihrerseits Zwischenergebnisse an den Farmer melden. Die Kommunikation zwischen den Prozessoren ist zeitaufwendig: Um sie möglichst gering zu halten, erwies es sich als günstig, wenn jeder Prozessor eine Tabelle mit allen Primzahlen von 1 bis $\sqrt{x}$, deren Vielfache gestrichen werden müssen, im lokalen Hauptspeicher hält (Alle Primzahlen von 1 bis $\sqrt{10^{14}}$ lassen sich in weniger als 700 KB speichern). Wir haben bisher für unsere Berechnungen über den Zeitraum von sechs Monaten bis zu 50 parallele Prozessoren eingesetzt. Kurz vor Drucklegung ist es uns gelungen, den Wert für $\pi_2(10^{14})$ zu erreichen: 135.780.321.665. Die Summe über die Kehrwerte aller Primzahlzwillinge bis 10^{14} ist $B(10^{14}) = 1{,}82024496813$, woraus sich eine verbesserte Abschätzung für die Brunsche Konstante ergibt: 1,902160577. Die Schranke von 10^{14} entspricht immerhin dem 1000fachen der alten Marke von Brent, und es ist – in doppeltem Sinne – kein Ende in Sicht.

x	$\pi_2(x)$	$L_2(x)$	$B(x)$	$B(x) + 4c_2/\log x$
10	2	5	0,876190476191	2,023009011333
10^2	8	14	1,330990365719	1,904399633290
10^3	35	46	1,518032463560	1,900305308607
10^4	205	214	1,616893557432	1,903598191218
10^5	1224	1249	1,672799584828	1,902163291856
10^6	8169	8248	1,710776930804	1,901913353328
10^7	58980	58754	1,738357043917	1,902188263223
10^8	440312	440368	1,758815621068	1,902167937961
10^9	3424506	3425308	1,774735957638	1,902160239321
10^{10}	27412679	27411417	1,787478502719	1,902160356233
10^{11}	224376048	224368865	1,797904310955	1,902160541422
10^{12}	1870585220	1870559867	1,806592419176	1,902160630438
10^{13}	15834664872	15834598305	1,813943760685	1.902160571080
10^{14}	135780321665	135780264895	1,820244968130	1.902160577783

Zählergebnisse: Aufgeführt sind neben der jeweiligen Schranke x die Anzahl der Primzahlzwillinge $\pi_2(x)$ bis zu dieser Schranke. Zum Beispiel gibt es bis x = 10 zwei Primzahlzwillinge: 3 und 5 beziehungsweise 5 und 7, daher ist $\pi_2(10) = 2$. Die Näherungsformel von Hardy und Littlewood $L_2(x)$ sagt in diesem Fall fünf Primzahlzwillinge voraus. Nicht immer liegt ihre Vorhersage über dem tatsächlichen Wert, man vergleiche in der Zeile für $x = 10^7$. Die Summe über die Kehrwerte aller Primzahlen wächst zwar langsam, aber ins Unendliche. Addiert man die Kehrwerte aller Primzahlzwillinge, so konvergiert die entstehende Summe B(x) gegen einen Grenzwert, die Brunsche Konstante. In der letzten Spalte steht eine Abschätzung diese Konstante. Man vermutet, daß sie etwa bei 1,90216 liegt.

Grafik: utz

Eratosthenes von Cyrene konnte Primzahlen sieben, und das funktioniert folgendermaßen: Die Zahlen – in diesem Fall von 1 bis 25 – werden mehrfach gesiebt. Die Eins gilt unter Mathematikern nicht als Primzahl. Im Zweier-Sieb bleiben alle Vielfachen von Zwei hängen. Im Dreier-Sieb bleiben alle Vielfachen von Drei hängen; allerdings sind Zahlen wie 6, 12 und 18 schon vorher ausgesiebt worden. Ein Vierer-Sieb ist nicht notwendig, weil alle Zahlen, die hier hängen bleiben könnten, schon im Zweier-Sieb liegen. Im Fünfer-Sieb bleibt nur noch die 25 hängen. Weitere Siebe sind nicht notwendig, weil eine zerlegbare Zahl immer einen Faktor kleiner oder gleich der Wurzel aus dieser Zahl enthält. Sollen – wie in diesem Fall – die Zahlen bis 25 geprüft werden, muß also nur bis $\sqrt{25} = 5$ gesiebt werden. Als Bodensatz bleiben die Primzahlen liegen, darunter vier Primzahlzwillingspaare.

JUSTUS-LIEBIG-
UNIVERSITÄT
GIESSEN

Jörg Richstein

AG Informatik
Mathematisches Institut
Arndtstraße 2
35392 Gießen
Telefon (0641) 702–2540
email Joerg.Richstein@informatik.uni-giessen.de